This application is officially maintained in electronic form. To View: Click the desired Document Description. To Download and Print: Check the desired document(s) and click Start Download.

Available Documents

Mail Room Date	Document Code	Document Description	Document Category	Page Count
11-21-2019	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
07-17-2018	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
03-08-2018	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
02-20-2018	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
07-03-2017	TRIAL.REQ.D	Request for Trial Denied	PROSECUTION	16
06-02-2017	LET.	Miscellaneous Incoming Letter	PROSECUTION	2
06-02-2017	N417	EFS Acknowledgment Receipt	PROSECUTION	2
02-10-2017	LET.	Miscellaneous Incoming Letter	PROSECUTION	1
02-10-2017	DRW.NONBW	Drawings-other than black and white line drawings	PROSECUTION	3
02-10-2017	N417	EFS Acknowledgment Receipt	PROSECUTION	2
02-10-2017	SCORE	Placeholder sheet indicating presence of supplemental content in SCORE	PROSECUTION	1
01-19-2017	TRIAL.REQ.D	Request for Trial Denied	PROSECUTION	17
01-18-2017	TRAN.LET	Transmittal Letter	PROSECUTION	1
01-18-2017	NPL	Non Patent Literature	PROSECUTION	3
01-18-2017	N417	EFS Acknowledgment Receipt	PROSECUTION	2
12-30-2016	TRAN.LET	Transmittal Letter	PROSECUTION	1
12-30-2016	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	14
12-30-2016	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	31
12-30-2016	N417	EFS Acknowledgment Receipt	PROSECUTION	2
08-30-2016	TRIAL.REQ.D	Request for Trial Denied	PROSECUTION	15
05-27-2016	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
06-11-2015	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
03-25-2015	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
03-12-2015	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
01-27-2015	SOL.NTC.SUIT	Report on the filing or determination of an action regarding a patent	PROSECUTION	1
12-14-2014	NPL	Non Patent Literature	PROSECUTION	23
12-14-2014	NPL	Non Patent Literature	PROSECUTION	84
12-14-2014	NPL	Non Patent Literature	PROSECUTION	34
12-14-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
12-12-2014	LET.	Miscellaneous Incoming Letter	PROSECUTION	2
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	17
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	16
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	16
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	35
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	27
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	17
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	23
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	10
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	16
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	12

12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	13
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	12
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	21
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	10
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	39
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	18
12-12-2014	REF.OTHER	Other Reference-Patent/App/Search documents	PROSECUTION	16
12-12-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
10-22-2014	ISSUE.NTF	Issue Notification	PROSECUTION	1
10-09-2014	NTC.PUB	Notice of Publication	PROSECUTION	1
10-08-2014	APP.FILE.REC	Filing Receipt	PROSECUTION	3
09-19-2014	NOA	Notice of Allowance and Fees Due (PTOL-85)	PROSECUTION	12
09-19-2014	892	List of references cited by examiner	PROSECUTION	1
09-19-2014	IIFW	Issue Information including classification, examiner, name, claim, renumbering, etc.	PROSECUTION	3
09-19-2014	FWCLM	Index of Claims	PROSECUTION	1
09-19-2014	1449	List of References cited by applicant and considered by examiner	PROSECUTION	5
09-19-2014	BIB	Bibliographic Data Sheet	PROSECUTION	1
09-19-2014	SRFW	Search information including classification, databases and other search related notes	PROSECUTION	1
09-19-2014	SRNT	Examiner's search strategy and results	PROSECUTION	22
09-19-2014	IFEE	Issue Fee Payment (PTO-85B)	PROSECUTION	1
09-19-2014	WFEE	Fee Worksheet (SB06)	PROSECUTION	2
09-19-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
08-06-2014	SRNT	Examiner's search strategy and results	PROSECUTION	1
08-06-2014	SRNT	Examiner's search strategy and results	PROSECUTION	1
07-31-2014	ADS	Application Data Sheet	PROSECUTION	7
07-31-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
07-31-2014	DIST.E.FILE	Terminal Disclaimer-Filed (Electronic)	PROSECUTION	2
07-31-2014	WFEE	Fee Worksheet (SB06)	PROSECUTION	2
07-31-2014	DISQ.E.FILE	Terminal Disclaimer-Electronic-Approved	PROSECUTION	1
07-31-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
07-22-2014	CFILE	Request for Corrected Filing Receipt	PROSECUTION	1
07-22-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
07-22-2014	ADS	Application Data Sheet	PROSECUTION	7
07-16-2014	SES.LOSS	Notification of loss of entitlement to small entity status	PROSECUTION	1
07-16-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
07-02-2014	M327	Miscellaneous Communication to Applicant - No Action Count	PROSECUTION	1
06-28-2014	EARLYPUB	Request for Early Publication	PROSECUTION	1
06-28-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
06-27-2014	A.PE	Preliminary Amendment	PROSECUTION	1
06-27-2014	CLM	Claims	PROSECUTION	2
06-27-2014	N417	EFS Acknowledgment Receipt	PROSECUTION	2
06-27-2014	WFEE	Fee Worksheet (SB06)	PROSECUTION	1
08-29-2013	ADS	Application Data Sheet	PROSECUTION	4
08-29-2013	N417	EFS Acknowledgment Receipt	PROSECUTION	2
07-26-2013	A.PE	Preliminary Amendment	PROSECUTION	1
07-26-2013	CLM	Claims	PROSECUTION	4
07-26-2013	NPL	Non Patent Literature	PROSECUTION	21
07-26-2013	NPL	Non Patent Literature	PROSECUTION	15
07-26-2013	IDS	Information Disclosure Statement (IDS) Form (SB08)	PROSECUTION	5
07-26-2013	TRAN.LET	Transmittal Letter	PROSECUTION	1
07-26-2013	N417	EFS Acknowledgment Receipt	PROSECUTION	2
06-12-2013	WFEE	Fee Worksheet (SB06)	PROSECUTION	1

06-12-2013	APP.FILE.REC	Filing Receipt	PROSECUTION	3
06-05-2013	WFEE	Fee Worksheet (SB06)	PROSECUTION	1
05-06-2013	OATH	Oath or Declaration filed	PROSECUTION	4
05-06-2013	TRNA	Transmittal of New Application	PROSECUTION	2
05-06-2013	WFEE	Fee Worksheet (SB06)	PROSECUTION	2
05-06-2013	N417	EFS Acknowledgment Receipt	PROSECUTION	3
05-06-2013	SPEC	Specification	PROSECUTION	25
05-06-2013	CLM	Claims	PROSECUTION	3
05-06-2013	ABST	Abstract	PROSECUTION	1
05-06-2013	DRW	Drawings-only black and white line drawings	PROSECUTION	7
05-06-2013	WFEE	Fee Worksheet (SB06)	PROSECUTION	1

Close Window

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of Illinois on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
17cv7300	10/10/2017	Northern District of Illinois

PLAINTIFF	DEFENDANT
William Grecia	Discover Financial Services, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,887,308 B2	11/11/2014	William Grecia
2	8,533,860 B1	9/10/2013	William Grecia
3	8,402,555 B2	3/19/2013	William Grecia
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Thomas G. Bruton	Anya Ellis	11/21/2018

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

EWS-003994

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Southern District of New York on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:18 Civ. 3696	4/26/2018	for the Southern District of New York

PLAINTIFF	DEFENDANT
WILLIAM GRECIA	JPMORGAN CHASE & CO.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,887,308	11/11/2014	WILLIAM GRECIA
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Southern District of New York on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:15-cv-9210	11/23/2015	for the Southern District of New York

PLAINTIFF	DEFENDANT
William Grecia	Visa Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,887,308	11/11/2014	William Grecia
2	8,533,860	9/10/2013	William Grecia
3	8,402,555	3/19/2013	William Grecia
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Ruby J. Krajick	/s/ P. Canales	11/24/2015

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of Illinois on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
17cv7300	10/10/2017	Northern District of Illinois

PLAINTIFF	DEFENDANT
William Grecia	Discover Financial Services, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,887,308 B2	11/11/2014	William Grecia
2	8,533,860 B1	9/10/2013	William Grecia
3	8,402,555 B2	3/19/2013	William Grecia
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Thomas G. Bruton	Anya Ellis	10/11/2017

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Trials@uspto.gov
Tel: 571-272-7822

Paper 7
Entered: July 3, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INCORPORATED,
Petitioner,

v.

WILLIAM GRECIA,
Patent Owner.

Case IPR2017-00793
Patent 8,887,308

Before JAMESON LEE, MICHAEL W. KIM, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

KIM, *Administrative Patent Judge*.

DECISION
Decision Denying Instituting *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

A. Background

MasterCard International Incorporated ("Petitioner") filed a Petition requesting *inter partes* review of claim 1 of U.S. Patent No. 8,887,308 (Ex. 1001, "the '308 Patent"). Paper 1 ("Pet."). William Grecia ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition shows "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a); *see also* 37 C.F.R. § 42.4(a). Upon consideration of the Petition and Preliminary Response, we are unpersuaded that Petitioner has met its burden of showing a reasonable likelihood that it would prevail in showing that claim 1 is unpatentable.

B. Related Proceedings

Patent Owner has identified the following actions as related to the '308 patent: (1) *Grecia v. DISH Network L.L.C.*, Case No. 4:16-cv-588 (N.D. Cal.) (February 3, 2016); (2) *Grecia v. MasterCard Incorporated,* Case No. 1:15-cv-9059 (S.D.N.Y.) (November 18, 2015); (3) *Grecia v. American Express Company*, Case No. 1:15-cv-9217 (S.D.N.Y.) (November 23, 2015); (4) *Grecia v. Visa Inc.*, Case No. 1:15-cv-9210 (S.D.N.Y.) (February 23, 2015); (5) *Grecia v. McDonald's Corporation,* Case No. 1:16-cv-2560 (N.D. Ill.) (February 24, 2016). Paper 4, 1. The '308 patent also is the subject of IPR2016-00602, IPR2016-01519, and

IPR2017-00797.[1] Paper 4, 1. Related Patent No. 8,402,555 is the subject of IPR2016-00789, IPR2016-00788, and IPR2017-00799.[2] Paper 4, 1–2. Related Patent 8,533,860 is the subject of IPR2016-00422, IPR2016-00600, and IPR2017-00791.[3] Paper 4, 1–2.

C. The '308 Patent

The '308 Patent relates generally to "digital rights management [("DRM")] which employs electronic ID, as part of a web service membership, to manage access rights across a plurality of devices." Ex. 1001, 1:23–27. In addition to encryption, DRM systems use a layer of authentication in which permission is granted for access to the cipher key required to decrypt files for access. *Id.* at 1:42–44. According to the '308 Patent, prior art DRM methods rely on content providers to maintain computer servers to receive and send session authorization keys to client computers with an Internet connection. *Id.* at 2:55–57. "At times, content providers will discontinue servers or even go out of business some years after DRM encrypted content was sold to consumers causing the ability to access files to terminate." *Id.* at 2:60–63. DRM opponents also criticize the inability of current DRM measures to allow unlimited interoperability between different machines. *Id.* at 3:1–3. Accordingly, the '308 Patent discloses that "[a]n object of the present invention is to provide unlimited

---

[1] The Board declined to institute review in IPR2016-00602 and in IPR2016-01519. IPR2017-00797 terminated by settlement.

[2] The Board declined to institute review in IPR2016-00789. IPR2017-00799 terminated by settlement.

[3] IPR2015-00422 terminated by settlement. The Board declined to institute review in IPR2016-00600.

interoperability of digital media between unlimited machines with management of end-user access to the digital media." *Id.* at 3:12–14.

D. Independent Claim 1

Independent claim 1 is the only claim of the '308 Patent, and is reproduced below (some paragraphing added to improve clarity):

> 1. A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:
>
> a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of:
>
> a memory connected to the at least one CPU;
>
> a storage connected to the at least one CPU; and
>
> a database connected to the at least one CPU through the Internet;
>
> wherein the access request further comprises verification data provided by at least one user,
>
> wherein the verification data is recognized by the apparatus as a verification token; then
>
> b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then
>
> c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b)
>
> wherein the API is related to a verified web service,
>
> wherein the verified web service is a part of the database apparatus,
>
> wherein establishing the API communication requires a credential assigned to the apparatus of (a),

wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus to complete the verification process,

wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier; then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of: the received verification data of (a); and the received query data of (e);

wherein the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content,

wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content.

E. Asserted Grounds of Unpatentability

Petitioner challenges independent claim 1 on the following ground.

References	Basis	Challenged Claim
Ameerally[4] and Muller[5]	§ 103(a)	1

Petitioner also relies on the Declaration of Peter Alexander, Ph.D. (Ex. 1007).

II. ANALYSIS

A. Independent Claim 1 as Unpatentable over Ameerally and Muller

Petitioner asserts that independent claim 1 is obvious over Ameerally and Muller. Pet. 13–54 (citing Exs. 1001, 1004, 1005, 1007). Patent Owner disagrees. Prelim. Resp. 21–24 (citing Exs. 1001, 1004, 1005, 1007).

1. Ameerally (Ex. 1004)

Ameerally relates generally to "employing promotional codes with which particular digital media items are associated in a promotional database of a digital media purchase system." Ex. 1004 ¶ 4. Figure 1 of Ameerally depicts a block diagram of a system including digital media purchase system 100, and is set forth below.

[4] U.S. Patent Application Publication No. 2006/0212401, published Sept. 21, 2006 (Ex. 1004; "Ameerally").
[5] U.S. Patent Application Publication No. 2005/0203959, published Sept. 15, 2005 (Ex. 1005; "Muller").

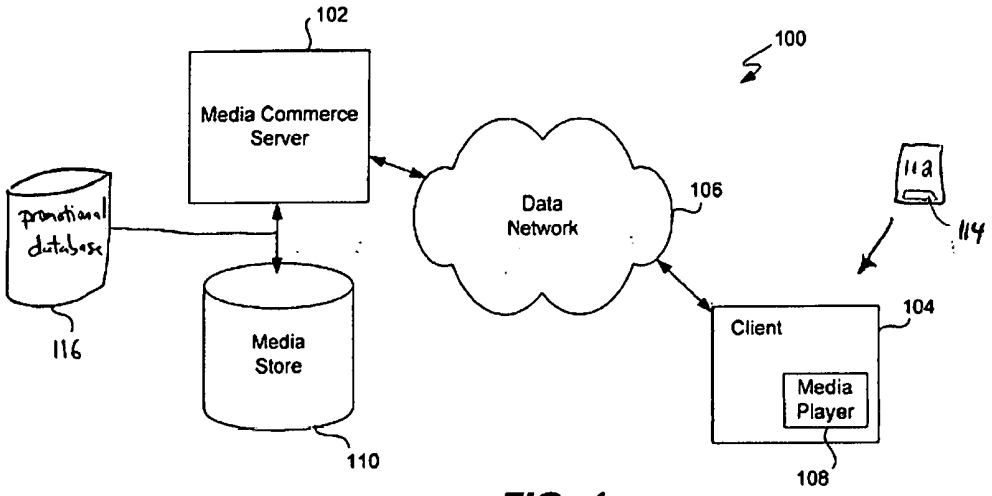


FIG. 1

Figure 1 depicts a system including digital media purchase system 100. Ex. 1004, Fig. 1. As shown above, digital media purchase system 100 includes digital media commerce server 102 and client 104, with each client 104 including digital media player 108. *Id.* ¶ 19. Digital media purchase system 100 also includes promotional database 116. *Id.* ¶ 27. Users of client 104 may receive promotional media 112, which includes unique promotional code 114. *Id.* ¶ 29. Unique promotional code 114 is provided to promotional database 116, and the record for promotional code 114 is accessed to locate a particular digital media content associated with promotional code 114. *Id.* ¶¶ 29, 39. The particular digital media content associated with promotional code 114 is then made accessible to the user of client 104. *Id.* ¶ 42.

2. Muller (Ex. 1005)

Muller relates generally to distribution of digital media items in a client-server environment. Ex. 1005, Abstr. Figure 1A of Muller depicts a block diagram of media purchase system 100, and is set forth below.

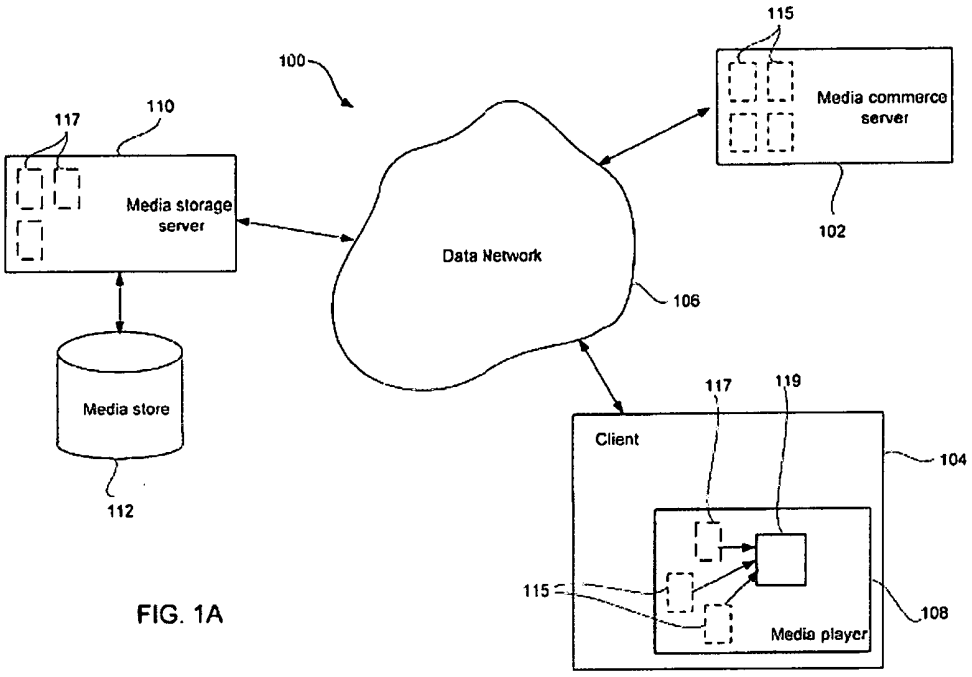


FIG. 1A

Figure 1 depicts a block diagram of media purchase system 100. Ex. 1005, Fig. 1A. As shown above, media purchase system 100 includes media commerce server 102, data network 106, media storage server 110, media store 112, and client 104, which includes media player 108. *Id.* ¶¶ 30, 35. Digital media content files 117 are stored on media store 112 and retrieved via media storage server 110. *Id.* ¶ 35. Digital media item components 115 are stored on media commerce server 102. *Id.* ¶ 30.

In order for media player 108 to acquire purchased digital media content files 117, a media access response is received at media player 108. *Id.* ¶ 35. The media access response is then used by media player 108 to retrieve digital media content files 117 by interacting with media storage server 110 through data network 106, and to digital media item components 115 from media commerce server 102. *Id.* ¶ 36. The particular digital media item is assembled at media player 108 by merging digital media item components 115 and digital media content files 117. *Id.*

3. Analysis

Petitioner asserts that independent claim 1 is obvious over Ameerally and Muller. Pet. 13–54 (citing Exs. 1001, 1004, 1005, 1007). Patent Owner disagrees that Petitioner has met its burden of showing that there is a reasonable likelihood that independent claim 1 would have been obvious over Ameerally and Muller. Prelim. Resp. 21–24 (citing Exs. 1001, 1004, 1005, 1007). We agree with Patent Owner.

Independent claim 1 recites "creating a computer readable authorization object by writing into the data store of (a) . . . ." Petitioner asserts that the following in Muller corresponds to the aforementioned claim limitation:

> Here, the query data response from the media commerce server, i.e., the received "query data requested in (d)" of claim 1, is written into memory to provide a "computer readable authorization object." As described above, the media commerce server response (media access response) that contains a media content URL, a download key, and a security token, and one or more digital media item components 115 that include license keys and user account information (i.e., query data) to the client computer/media player (i.e., apparatus of (a)). Alexander Decl. (Ex. 1007) at ¶¶ 157–160; Ex. 1005, Muller at [0057], [0035].
>
> The claimed "computer readable authorization object" is created when the received media access information and digital media item components 115 are written into the memory of the client computer. Alexander Decl. (Ex. 1007) at ¶ 157. As described in Muller, the digital media item components 115 (i.e., part of the query data) are stored in the memory of the client computer (i.e., the data store of (a)). Ex. 1005, Muller at [0036], [0040].

Pet. 46–48.

Independent claim 1 then recites "wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-

referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content." Petitioner asserts that the following in Muller corresponds to the aforementioned claim limitation:

> As described above, the computer readable authorization object is represented by the stored media access response information, such as a media content URL, a download key, and a security token, as well as user account information, licensing information, DRM data, etc. that are part of the media access response.
>
> Following the receipt of media access information, the client performs a series of "subsequent user access requests to retrieve media content files. Alexander Decl. (Ex. 1007) at ¶ 174. Muller discloses cross referencing when the security token and media storage access pointers are used to reference the storage locations and retrieve individual digital media content items. Id. at ¶ 175; Ex. 1005, Muller at [0035].

Pet. 52–54. As an initial matter, we discern that the use of the word "the" in the latter limitation indicates that both limitations are referring to the same "computer readable authorization object."

In summary, Petitioner asserts, at various points in the Petition, that each of the following items in Muller corresponds to the recited "computer readable authorization object": query data response from the media commerce server; media commerce server response; media access response; media content URL; a download key; a security token; digital media item components 115; license keys; user account information; media access information; media access response information; licensing information; DRM data; media storage access pointers; media information response; various combinations of these items; and various combinations of these items when "written into the memory of the client computer." This listing is

problematic, however, as the Petition, at various points, mentions some of these items as corresponding to the recited "computer readable authorization object," but not others, with no explanation as to why that is the case. Furthermore, the Petition does not explain adequately how some of these items meet all the requirements of the aforementioned claim limitations for a "computer readable authorization object." Because Petitioner treats the mapping of "computer readable authorization object" in such a diverse and varied manner, we are unpersuaded that Petitioner has met its burden of showing that "the petition identifies, in writing and with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim." *See* 35 U.S.C. § 312(a)(3). Insofar as we can discern from the Petition, no single "computer readable authorization object" from the prior art has been identified to account for all the limitations directed to the claimed computer readable authorization object.

Most prominently, on page 48 of the Petition, Petitioner mentions digital media item components 115, and, indeed, only mentions digital media item components 115, as being disclosed in Muller as "stored in the memory of the client computer (i.e., the data store of (a))," which is the language in this portion of the Petition that most closely mirrors the claim limitation of "creating a computer readable authorization object by writing into the data store of (a) . . . ." Pet. 46, 48. Of all the purportedly stored items disclosed on pages 47–48 of the Petition, the Petition only actually cites Muller for storing this one item. Later in the Petition, however, with respect to the recited "wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during

subsequent user access requests to determine one or more of a user access permission for the cloud digital content," Petitioner does not make any mention of digital media item components 115, even though a mention would be expected, given that the claim, again, recites "computer readable authorization object." Pet. 52–54.

Relatedly, in that same later portion of the Petition, Petitioner asserts that the items corresponding to the recited "computer readable authorization object" is "used to reference the storage locations and retrieve individual digital media content items," which is the language in this portion of the Petition that most closely mirrors the claim limitation of "wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content." *Id.* at 54. This appears to be the only mention of "digital media content items," in at least this portion of the Petition, and Muller also does not refer to "digital media content items." *See generally* Pet.; Ex. 1005. Muller does refer to a "digital media item" that is assembled by merging digital media item components 115 and digital media content files 117. Ex. 1004 ¶ 36. When page 54 of the Petition, as informed by the aforementioned portion of Muller, is read in conjunction with page 48 of the Petition, however, the resulting claim mapping is that digital media item components 115 are used to retrieve . . . themselves, which is illogical, and, thus, digital media item components 115 cannot correspond properly to the recited "computer readable authorization object."

Other asserted mappings of items in Muller to "computer readable authorization object" are also problematic. For example, page 54 of the

Petition specifically mentions "media storage access pointers" as performing the functions required by the recited "computer readable authorization object," while page 48, and, indeed, the rest of the Petition, makes no mention of "media storage access pointers" at all.[6] Furthermore, page 54 of the Petition later reads: "One of ordinary skill in the art would understand that retrieval of the digital media components (content files) would require a 'de-referencing' operation, i.e., extracting a pointer from the media information response (such as the XML data structure discussed in Muller (Ex. 1005 at [0027]) and forming a cross referenced URL identifying the data file location. Alexander Decl. (Ex. 1007) at ¶177." Pet. 54. One of the items listed on pages 47 and 53–54 of the Petition as corresponding to the recited "computer readable authorization object" is "media content URL." Petitioner has not explained the difference between "media content URL" and "cross referenced URL." Plausibly, the two could be one and the same. This is relevant, because if "media content URL" is meant to correspond to the "media storage access pointers" mentioned earlier on page 54 of the Petition, Petitioner has not explained adequately how or why a "de-referencing" operation, using the "media content URL," is used to obtain the "cross referenced URL," when, as noted above, the two could plausibly be one and the same.

In a further example, pages 50–51 of the Petition reads: "The 'download key' and 'security token' that are part of the media access

[6] The Alexander Declaration does mention "data pointers to one or more digital media item components 117 located at the media storage server. Ex. 1007 ¶ 158. Such language is not set forth in the Petition, however, and the portion of the Petition that includes "media storage access pointers" does not refer to the aforementioned portion of the Alexander Declaration.

response are interpreted, i.e., recognized, by the client computer as ***necessary*** components to access the digital media content components located at the media storage server 110. Alexander Decl. (Ex. 1007) at ¶ 166; Ex. 1005, Muller at [0051], [0060]." Pet. 50–51 (emphasis added). Yet, pages 47–48 of the Petition do not impart any particular significance to either "download key" or "security token" with respect to the recited "computer readable authorization object," while page 54 imparts some significance to "security token," but not "download key." Even in that regard, however, page 54 of the Petition specifically refers to "security token" and "media storage access pointers" separately, but only asserts that the latter is used for the "cross-referencing action" required of the recited "computer readable authorization object."

In another example, pages 47–48 of the Petition refer to "license keys," while pages 54 of the Petition refers to "license information," with no explanation to account for the differences in language.[7] Furthermore, while Petitioner asserts that the former is included in digital media items components 115, no such mention is made concerning the latter.

Accordingly, in view of Petitioner's confusing and shifting rationales as to what items in Muller correspond to the recited "computer readable authorization object," we conclude that Petitioner does not adequately account for "creating a computer readable authorization object by writing into the data store of (a) . . . ." and "wherein the computer readable

[7] The Alexander Declaration does refer to Muller's disclosure of "licensing information (e.g., license keys)." Ex. 1007 ¶ 159 (citing Ex. 1005 ¶ 35). That only indicates, however, that "licensing information" is broader than "license keys," and does not assist appreciably in determining how either corresponds to the recited "computer readable authorization object."

authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content," as recited in independent claim 1.

To the extent Petitioner actually regards the entirety of Muller's "media access response" as the recited "computer readable authorization object," and believes a limitation with regard to the "computer readable authorization object" is met if at least a part of the identified object satisfies the limitation, that position has not been clearly articulated. Neither Patent Owner nor the Board has been provided with sufficient notice of that position. We decline to make that assumption.

In any event, we disagree with any contention that if the "computer readable authorization object," as identified by Petitioner, includes numerous items, such as the *fifteen* items identified by Petitioner and additional combinations suggested by Petitioner on pages 46–48 and 53–54 of the Petition, then each limitation of the recited "computer readable authorization object" is considered met if any item of the identified object meets the limitation. Petitioner should not expect the Board to search through every possible permutation of arguments and evidence, scattered in disparate parts of the record and not sufficiently linked by Petitioner's presentation, and put together, for Petitioner, the one permutation that may support Petitioner's alleged ground of unpatentability. It is Petitioner who must make out its own case. The Board is not a party in this proceeding and must remain neutral and unbiased.

4. Conclusion

On this record, we are unpersuaded that Petitioner has shown a reasonable likelihood that it will prevail in establishing that independent claim 1 is unpatentable over Ameerally and Muller.

B. Conclusion

For the reasons set forth above, we do not institute an *inter partes* review of independent claim 1 of the '308 patent on any ground.

III. ORDER

For the reasons given, it is:

ORDERED that that no trial or *inter partes* review is instituted for any claim of the '308 patent on any ground in this proceeding.

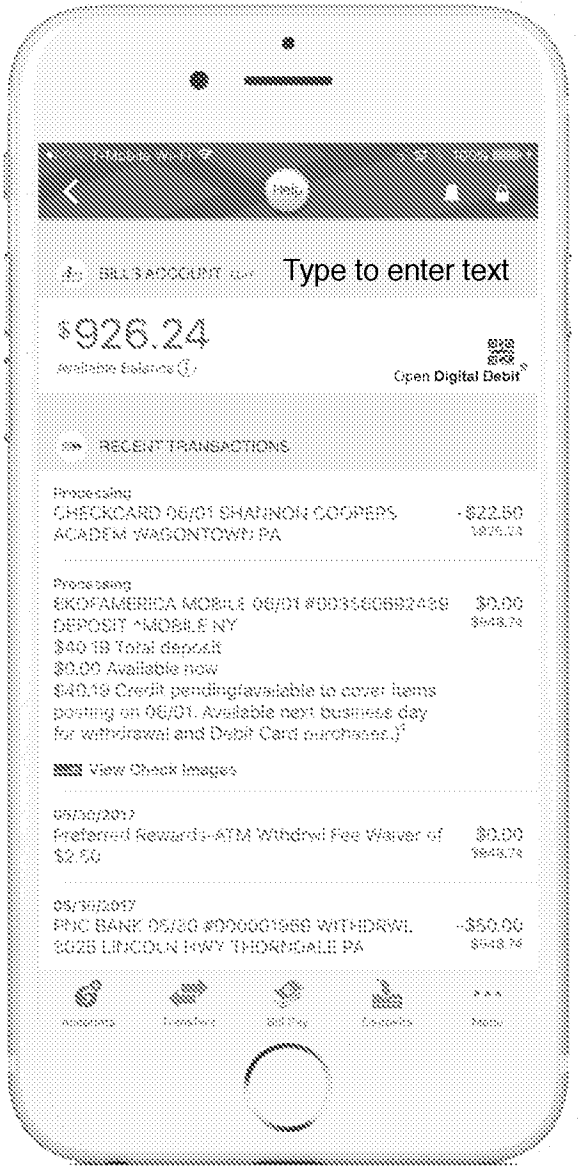
PETITIONER:

Brian Michaelis
Joseph Lanser
Joseph Walker
David A. Klein
SEYFARTH SHAW LLP
bmichaelis@seyfarth.com
jlanser@seyfarth.com
jmwalker@seyfarth.com
daklein@seyfarth.com

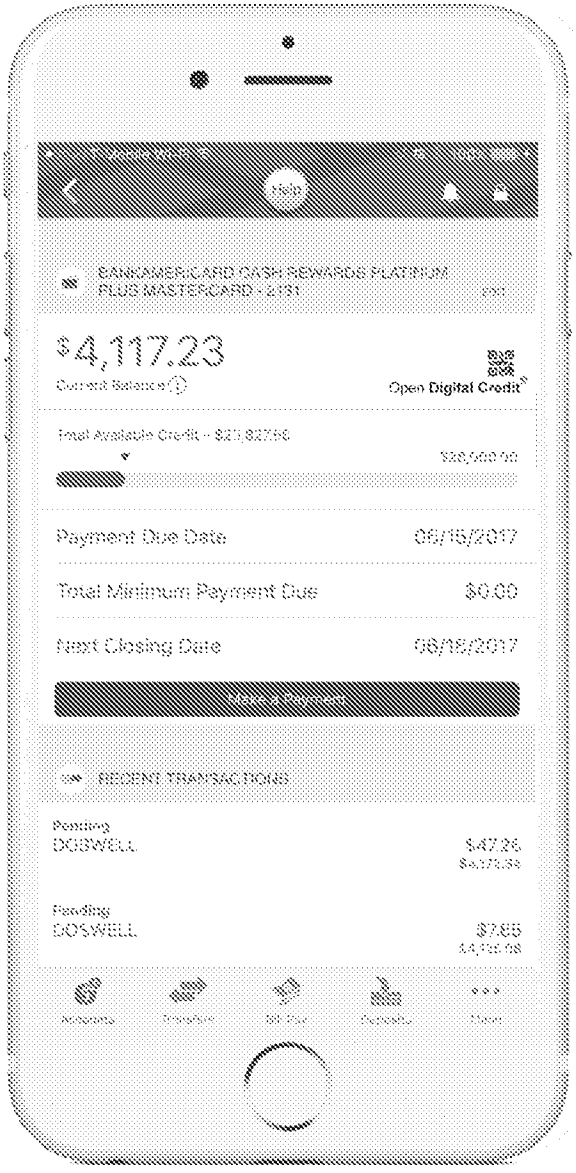
PATENT OWNER:

Isaac Rabicoff
RABICOFF LAW LLC
isaac@rabilaw.com

(Page 1 of 2) Inventor and current owner of this letters patent hereby deposit for historical record —one use case— out of many possible use cases by which the Inventor and current patent owner is making, using, and selling the invention with concurrent venture ownership interests in the product, patent, and trademarks comprising all or a portion of the illustrations hereto. Signed this day June 2, 2017 /william grecia/



(Page 2 of 2) Inventor and current owner of this letters patent hereby deposit for historical record —one use case— out of many possible use cases by which the Inventor and current patent owner is making, using, and selling the invention with concurrent venture ownership interests in the product, patent, and trademarks comprising all or a portion of the illustrations hereto. Signed this day June 2, 2017 /william grecia/



Electronic Acknowledgement Receipt

EFS ID:	29376096
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	02-JUN-2017
Filing Date:	06-MAY-2013
Time Stamp:	08:30:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	DDG_WG_IP_notice.pdf	4978386 029545a6c559d14f1df57c620bae1e2a060b 5699	no	2

Warnings:

Information:	
Total Files Size (in bytes):	4978386

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

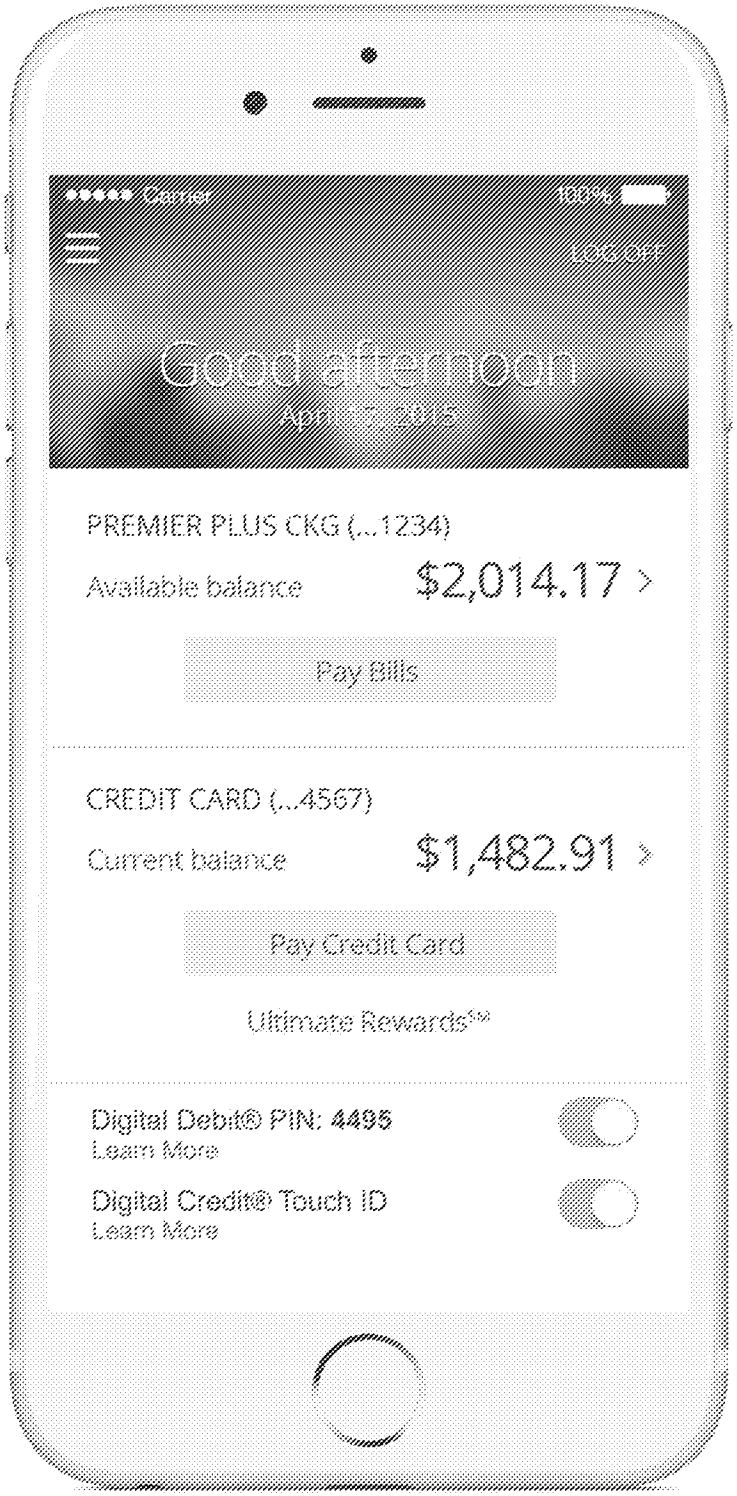
Inventor submits a record of current day practicing products in presentation to entities after December 2016. Claim steps of this patent for which products must perform to operate are:

Independent Claim Steps:

1) Receive a verification token from a user
2) Authenticate the verification token
3) Establish a connection with the API web service of Apple or Google
4) Request an identification reference (Device Token for push notifications)
5) Receive the identification reference (Device Token for push notifications)
6) Write at least one of the verification token or the identification reference into a data store (e.g., metadata) associated with the computer based apparatus.


T-Mobile Wi-Fi
6:15 PM
41%
RICOH
Device Number:
3025553000
Device Pin:
3309
RESET DEVICE PIN

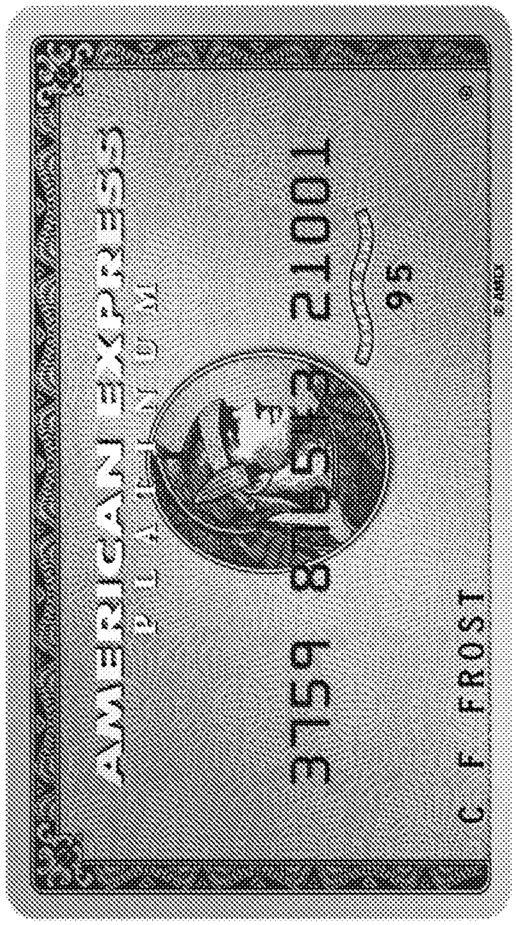
EWS-004019

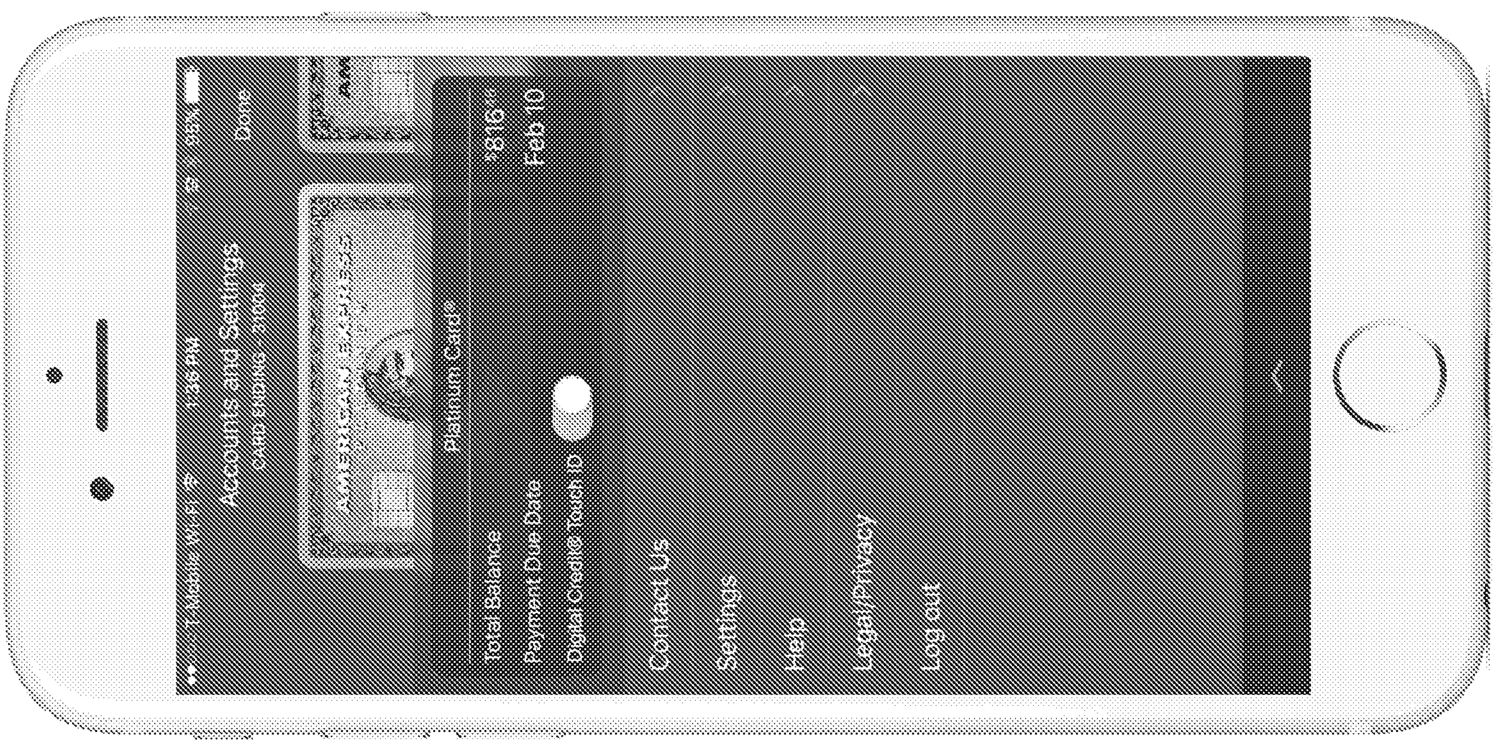

Carrier
100%
LOG OFF
Good afternoon
PREMIER PLUS CKG (...1234)
Available balance
$2,014.17
Pay Bills
CREDIT CARD (...4567)
Current balance
$1,482.91
Pay Credit Card
Ultimate Rewards℠
Digital Debit® PIN: 4495
Learn More
Digital Credit® Touch ID
Learn More


CHASE
5417 1234 5678 1234
DIGITAL DEBIT
00/00
D. BARRETT
mastercard


CHASE
SAPPHIRE
RESERVE
DIGITAL CREDIT
VISA
Infinite
D. BARRETT

EWS-004020


AMERICAN EXPRESS
PLATINUM
C F FROST


Accounts and Settings
Done
Platinum Card®
Total Balance
Payment Due Date
Feb 10
Contact Us
Settings
Help
Legal/Privacy
Log out

Electronic Acknowledgement Receipt

EFS ID:	28318875
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	10-FEB-2017
Filing Date:	06-MAY-2013
Time Stamp:	07:01:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Inventor_practice_disclosure.pdf	5549329 7abc70245aac0658c9d0cb935211685525f44c26	no	4

Warnings:

Information:	
Total Files Size (in bytes):	5549329

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SCORE Placeholder Sheet for IFW Content

Application Number: 13888051 Document Date: 02/10/2017

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://Score.uspto.gov/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Trials@uspto.gov
571-272-7822

Paper 7
Entered: January 19, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DISH NETWORK L.L.C.,
Petitioner,

v.

WILLIAM GRECIA,
Patent Owner.

Case IPR2016-01519
Patent 8,887,308 B2

Before RAMA G. ELLURU, JAMES B. ARPIN, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

DISH Network L.L.C. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claim 1 of U.S. Patent No. 8,887,308 B2 (Ex. 1001, "the '308 patent"). William Grecia ("Patent Owner") filed a Preliminary Response (Paper 5, "Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." For the reasons that follow, we decline to institute an *inter partes* review.

I. BACKGROUND

A. Related Proceedings

The parties identify nine federal district court cases involving the '308 patent. Pet. 2; Paper 4. The parties also identify four related petitions for *inter partes* review. Pet. 2; Paper 4.

B. The '308 Patent

The '308 patent describes a digital rights management system that manages access rights across a plurality of devices via digital media personalization to protect digital media subject to illegal copying. Ex. 1001, 1:20–27, 4:48–49. The system includes a first receipt module, an authentication module, a connection module, a request module, a second receipt module, and a branding module. *See id.* at Fig. 1. The first receipt module receives a branding request from a user (content acquirer). *Id.* at 5:46–48. The branding request is a read and write request of metadata of the digital media and includes a membership verification token corresponding to

the digital media. *Id.* at 5:48–51. The authentication module authenticates the membership verification token. *Id.* at 5:57–58. The connection module establishes communication with a communication console. *Id.* at 5:59–61. The request module requests an electronic identification reference from the communication console. *Id.* at 6:5–7. The second receipt module receives the electronic identification reference. *Id.* at 6:7–9. The branding module brands metadata of the digital media by writing the membership verification token and the electronic identification reference into the metadata. *Id.* at 6:9–12.

Figure 3 of the '308 patent, which illustrates this process, is reproduced below.

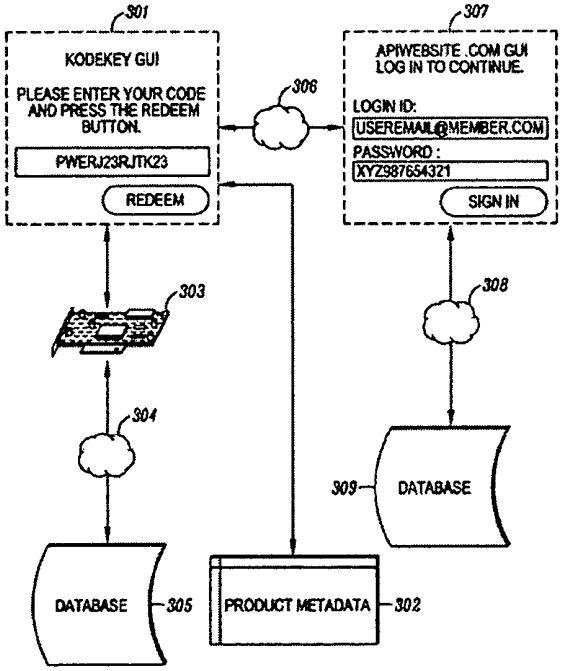


FIG. 3

Figure 3 is a flow chart of a digital media personalization process. *Id.* at 4:24–26. A user (i.e., content acquirer) posts a branding request via Kodekey GUI 301, which prompts the user to enter a token and press the

redeem button. *Id.* at 6:66–7:4. Kodekey GUI 301 is connected to token database 305, which is used to authenticate the token. *Id.* at 7:7–8, 8:20–22. After authentication, the user is redirected to APIwebsite.com GUI 307, which prompts the user to enter a login ID and password to access the digital media from database 309. *Id.* at 7:11–12, 15–18. The APIwebsite.com GUI interfaces to a web service membership (e.g., Facebook), where an electronic identification for the user is collected and sent to Kodekey GUI 301. *Id.* at 7:11–15, 10:41–44. Kodekey GUI 301 also is connected to product metadata 302, which is readable/writable metadata associated with the digital media to be acquired. *Id.* at 7:4–5. Product metadata 302 is branded by writing the token and the user's electronic identification reference into the metadata. *Id.* at 8:28–31, 11:24–27. For a subsequent access request, the user's electronic identification reference is compared against the electronic identification reference in metadata 302. *Id.* at 13:54–56. If there is a match, access rights are granted to the user. *Id.* at 13:56–58.

C. Challenged Claim

Petitioner challenges claim 1 of the '308 patent, which recites:

> 1. A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:
>
> a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of:
>
> a memory connected to the at least one CPU;
>
> a storage connected to the at least one CPU; and

a database connected to the at least one CPU through the Internet; wherein

the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then

b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then

c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b) wherein the API is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier; then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of:

the received verification data of (a); and

the received query data of (e); wherein

the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests

> to determine one or more of a user access permission for the cloud digital content.

Id. at 14:31–15:14.

D. Asserted Grounds of Unpatentability

Petitioner challenges claim 1 of the '308 patent on the following ground: obviousness over Tiu,[1] Fetterman,[2] and the knowledge of a person of ordinary skill in the art ("POSITA") under 35 U.S.C. § 103.[3] Pet. 5, 34–67. In support of its arguments, Petitioner proffers the declaration of Dr. Benjamin Goldberg, Ph.D. (Ex. 1011). *See id.*

E. Claim Construction

We construe claims in an unexpired patent by applying the broadest reasonable interpretation in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard). Under this standard, claim terms

---

[1] Tiu, U.S. Publ'n No. 2008/0222199 A1, published Sept. 11, 2008 (Ex. 1004).
[2] Fetterman, U.S. Publ'n No. US 2008/0313714 A1, published Dec. 18, 2008 (Ex. 1006).
[3] Because grounds in an *inter partes* review must be based on "patents or printed publications" (35 U.S.C. § 311(b); 37 C.F.R. § 42.104(b)(2)), we understand Petitioner's reference to "the knowledge of the Person of Ordinary Skill in the Art ('POSITA')" (Pet. 5) here to refer to a person of skill in the art's understanding of the applied reference or combined references and not to supply missing limitations or as shorthand to incorporate an unspecified disclosure by reference to supply missing limitations (37 C.F.R. § 42.6(a)(3)).

generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). A "claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer," however, and clearly set forth a definition of the claim term in the specification. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002).

Petitioner provides proposed interpretations for various limitations of the claims. Pet. 15–20. Patent Owner responds. Prelim. Resp. 17–23. For purposes of this Decision, we conclude that no term requires express construction to resolve a controversy in this proceeding. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.").

II. DISCUSSION

Petitioner argues that claim 1 of the '308 patent would have been obvious over Tiu, Fetterman, and the knowledge of a POSITA. Pet. 5, 34–67. For the reasons explained below, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing on its asserted ground.

A. Tiu

Tiu describes a system for managing multimedia content appearing on user pages of an online social network (e.g., Friendster). Ex. 1004 ¶ 8. For example, the system lets a Friendster user display a video from a third party

website (e.g., YouTube) on his or her Friendster user page (landing page). *See id.* ¶ 28.

Figure 5 of Tiu, which illustrates how to display such a video on a landing page, is reproduced below.

FIG. 5

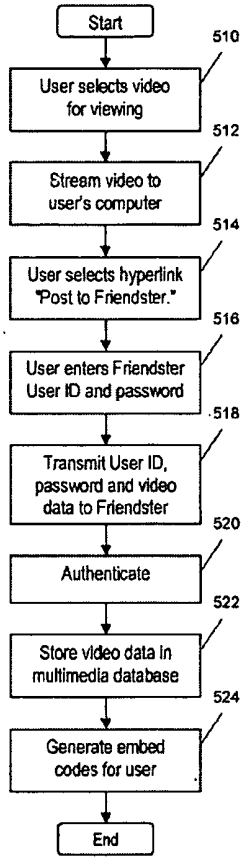


Figure 5 is a flow diagram of the steps for generating a webpage with embed codes for multimedia content (e.g., the video). *Id.* ¶¶ 18, 34. Steps 510–518 are carried out by the server computer of the external video site, while steps 520–524 are carried out by the server computer of the online social network. *Id.* ¶ 34. In step 510, the user navigates to an external video site (e.g., YouTube), where the user selects a video for viewing. *Id.* ¶ 35. In step 512,

the video is streamed to the user's computer where it is displayed. *Id.* In step 514, the user may select the hyperlink "Post to Friendster," which allows the user to feature the video on the user's landing page. *Id.* If the user selects the hyperlink, the user is prompted for his or her Friendster user ID and password in step 516. *Id.* In step 518, the external video site transmits this information along with information about the video to the online social network. *Id.* In step 520, the online social network authenticates the user ID against the password using its user database. *Id.* ¶ 36. After authentication, the information about the video is stored in a multimedia content database of the online social network along with the user ID in step 522. *Id.* Finally, in step 524, embed codes corresponding to the video are generated and inserted into the HTML file corresponding to the user's landing page.

B. Fetterman

Fetterman describes a system for accessing data from a web-based social network via a third-party application. Ex. 1006 ¶ 26. As shown in Figure 1 of Fetterman, which is reproduced below, the system includes third-party application 115, network device 140, and a web-based social network (e.g., Facebook) comprising application program interface 105, cache memory 130, and distributed database 135. *Id.* ¶ 18.

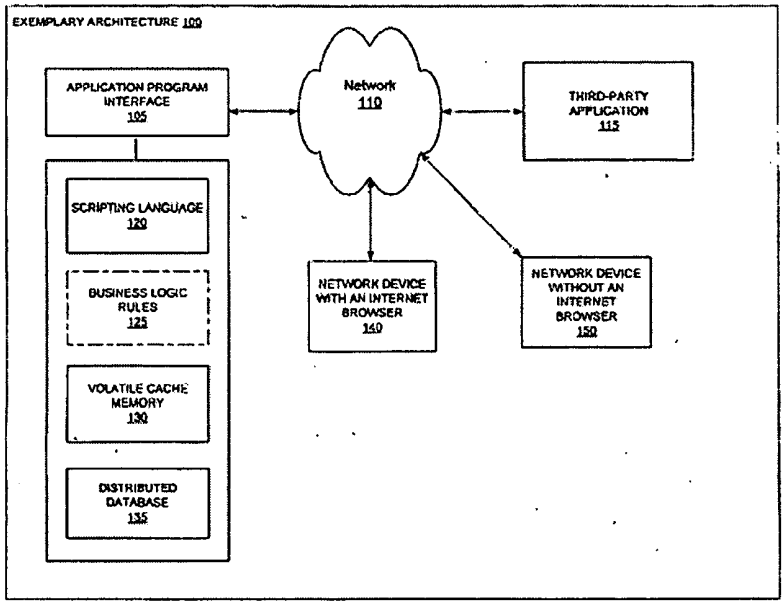


FIG. 1

Figure 1 illustrates an architecture for network authentication. *Id.* ¶ 6.

Third-party application 115 may be a program for generating an electronic birthday card. *Id.* ¶ 19. A user of device 140 may use third-party application 115 to access data from memory 130 or database 135 through application program interface 105. *Id.* ¶¶ 23, 26. To gain such access, the user first logs into the third-party application. *Id.* ¶¶ 27–28. If the user is logging into the third-party application for the first time, the user will be asked to log into the social network (if not already logged in) to accept the terms of service for using the third-party application. *Id.* ¶ 27. After accepting the terms of service, the user will be directed to return to the third-party application, where the user will be able to access data from the social network. *Id.* Alternatively, the user may complete the login process (including logging into the social network and accepting the terms of service) via the third-party application. *Id.* ¶ 28, Figs. 3A–3B.

C. Analysis

Claim 1 recites: (1) "establishing an API communication between the apparatus of (a) and a database apparatus," (2) "establishing the API communication requires a credential assigned to the apparatus of (a)," and (3) "the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action . . . to determine one or more of a user access permission for the cloud digital content." We address these limitations in turn.

1. "establishing an API communication between the apparatus of (a) and a database apparatus"

For this limitation, Petitioner identifies Tiu's computer 270 as the "apparatus of (a)" and Tiu's database 254 of an online social network as a "database apparatus." Pet. 37 (discussing claim limitation (a), which recites "an apparatus"), 47. Petitioner also identifies Fetterman's network device 140 as the "apparatus of (a)" and Fetterman's web-based social network (e.g., Facebook) as a "database apparatus." *See id.* at 48. As Petitioner notes, Tiu's database 254 "is in direct communication with the API communications 290 from the *third-party content site 280*," not computer 270. *Id.* at 47 (emphasis added). On the other hand, according to Petitioner, "Fetterman teaches that the user device . . . itself calls to Facebook's API from the user's browser such that the user device communicates directly with Facebook and its databases using a Facebook API call." *Id.* at 48 (citing Ex. 1006 ¶¶ 23, 28, Fig. 2); *see also id.* at 31 (citing Ex. 1006 ¶¶ 23, 28). Petitioner further argues that "a POSITA would have been motivated to use the simpler login API method provided by the Facebook API described

by Fetterman in place of the more effort-intensive coding process required in Tiu whereby the third party server mediates the API."[4] *Id.* at 48; *see also id.* at 33 ("[T]he POSITA would be freed from having to program the third-party server to act as an API agent between the user's device and social network and, instead, the API could simply be called from the user's device using a few lines of HTML code."). We are unpersuaded by Petitioner's argument.

In support of its argument, Petitioner cites disclosures in Fetterman that describe an API communication between a web-based social network and a *third party application*, not a user device. For example, paragraph 23 of Fetterman teaches that "the *third-party application 115* . . . may access a distributed database and/or a volatile cache memory associated with a social network through an application program interface for the social network." Ex. 1006 ¶ 23 (emphasis added). Similarly, paragraph 28 of Fetterman teaches "logging into the third-party application and the social network from [the same] screen 320," which illustrates a login procedure for the *third-party application*. *Id.* ¶¶ 8, 28, Fig. 3A.

In addition, Petitioner directs us to Figure 2 of Fetterman, asserting that "the Facebook API documentation explains to the programmer of the third-party application that the web page presented to the user of the third-party application should include HTML code to call to Facebook's API such that the user's device itself becomes an 'API client.'" Pet. 31–32. We note

[4] Petitioner proposes an assessment of a person of ordinary skill in the art. Pet. 13–14 (citing Ex. 1011 ¶ 10). Patent Owner does not challenge Petitioner's proposed assessment and does not propose an alternative. To the extent necessary and for purposes of this Decision, we adopt Petitioner's assessment.

Petitioner's later assertion with respect to Figure 2, however, that "'YOUR_API_KEY' represents the API key assigned to the vendor of the third-party application that wants to gain access to Facebook on the user's behalf." *Id.* at 53. That the API key is assigned to the vendor of the third-party application implies an API communication between Facebook and the *vendor of the third-party application*, not the user's device itself.

Given the cited disclosures, Petitioner does not explain persuasively why one of ordinary skill in the art would have considered combining Tiu and Fetterman to arrive at the claimed invention, which includes "an API communication between the apparatus of (a) and a database apparatus." Moreover, we note that logging into Facebook from the Facebook site as described in Figure 2 of Fetterman requires switching from the third-party site to the Facebook site to log into Facebook via Facebook's site, rather than at the third-party site, and then switching back to the third-party site to access data from Facebook. Ex. 1006, Fig. 2 ("for a Facebook API client to use the API, the user of the client application must be logged in to Facebook," "the user will be directed to close their browser window and return to the application"). Such a process seems "more effort-intensive" (*see* Pet. 48) than logging into a social network from the third-party site, where the user can stay to exchange data with the social network, as described in Tiu. Accordingly, we are unpersuaded by Petitioner's proffered reasoning for replacing Tiu's API communication with Fetterman's API communication, namely, to *simplify* the coding process. *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) ("there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

Based on the record before us, we are unpersuaded that the recited "API communication" would have been obvious over Tiu, Fetterman, and the knowledge of a POSITA.

2. "establishing the API communication requires a credential assigned to the apparatus of (a)"

For this limitation, Petitioner argues that Fetterman's API key teaches a "credential assigned to the apparatus of (a)." Pet. 53. According to Petitioner, "Fetterman discloses that when a user is prompted to engage in an API communication with Facebook, it is provisioned an API key that will, in turn, be sent to Facebook as proof that the user is allowed to engage in the API communication." *Id.* Thus, Petitioner concludes, "a POSITA would find it obvious that an API key would be utilized in calls to the social network site Friendster in Tiu, a social network similar to Facebook, which Patent Owner admits required API keys for utilization of its API services." *Id.* at 53–54.

We are unpersuaded by Petitioner's argument. As discussed above, Petitioner identifies Fetterman's network device 140 as the "apparatus of (a)." *Id.* at 48. With respect to Fetterman's API key, Petitioner acknowledges that it "represents the API key assigned to the vendor of the third-party that wants to gain access to Facebook on the user's behalf," not to device 140. *Id.* at 53; *see also* Ex. 1006, Fig. 2 ("api_key" is "[u]niquely assigned to the vendor"); Prelim. Resp. 29 ("Because Fetterman teaches that the API key is assigned to the *vendor* application and [Petitioner] maintains that the apparatus of (a) is the *user* device, Fetterman when combined with

Tiu does *not* disclose a credential assigned to the apparatus of (a)." (emphases added)).

We note Petitioner's assertion that "[t]he '308 Patent itself admits that it was known that APIs used by social network sites, like Facebook, required a credential[] such as an API key, in order to utilize the API," and that "[s]uch credentials were assigned to the apparatus." Pet. 51–52 (citing Ex. 1001, 10:51–11:7 ("Facebook API system . . . called from a connected apparatus (which is usually an Internet powered desktop or browser based application) with an API Key")). Petitioner, however, does not proffer sufficient persuasive reasoning for combining Tiu and Fetterman, in view of the knowledge of a POSITA, in order to obtain an API key assigned to Tiu's computer 270 or Fetterman's device 140. *See Kahn*, 441 F.3d at 988 ("there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

Based on the record before us, we are unpersuaded that the recited "credential assigned to the apparatus of (a)" would have been obvious over Tiu, Fetterman, and the knowledge of a POSITA.

3. *"the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action . . . to determine one or more of a user access permission for the cloud digital content"*

For this limitation, Petitioner argues that,

> [i]n Tiu, the use of the third-party content site username and password located in the EMBED CODE or located in the table of the multimedia content database 257 (in either instance, the claimed 'authorization object') to access content on a third-party website, acts as a cross-reference insofar as the username and password are for accessing the third-party content site (e.g.,

> Flickr) but are called from the user's social network (e.g., Friendster).

Pet. 65; *see also id.* at 66 ("calling on information in the multimedia content database 257 of the social network account for the HTML landing page code in order to pull information for retrieving content from a third-party site constitutes a cross-referencing action").

We are unpersuaded by Petitioner's argument. The claim recites that the *apparatus of (a)* uses a cross-referencing action to determine a user access permission for cloud digital content. As discussed above, Petitioner identifies Tiu's computer 270 as "the apparatus of (a)." *See also* Pet. 65. Petitioner does not explain persuasively that Tiu's computer 270 uses a cross-referencing action to determine a user access permission for cloud digital content. For example, using third-party content site Flickr's username and password for accessing content on the Flickr site implies a cross-referencing action at the Flickr site, not at computer 270. *See id.*; *see also id.* at 43 ("the same username and password will be sent to the third-party site every time someone visits the user's landing page (William's Landing Page), thus triggering a call to the third-party site for William's content"); Ex. 1004 ¶ 30 ("The query that is issued to an external web site for content associated with a user includes the user ID and password of that user as proof that access to the user's account maintained by the external web site is authorized."). Accordingly, based on the record before us, we are unpersuaded that the recited limitation "the apparatus of (a) using a cross-referencing action . . . to determine one or more of a user access permission for the cloud digital content" would have been obvious over Tiu, Fetterman, and the knowledge of a POSITA.

In view of the foregoing, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in showing that claim 1 would have been obvious over Tiu, Fetterman, and the knowledge of a POSITA.

III. CONCLUSION

For the foregoing reasons, Petitioner has not demonstrated a reasonable likelihood that it would prevail with respect to challenged claim 1 of the '308 patent.

IV. ORDER

For the reasons given, it is

ORDERED that the Petition is *denied* and no trial is instituted.

PETITIONER:

Robert R. Laurenzi
Shyamkrishna Palaiyanur
KAYE SCHOLER LLP
robert.laurenzi@kayescholer.com
shyam.palaiyanur@kayescholer.com

PATENT OWNER:

Patrick D. Richards
Clare Frederick
RICHARDS PATENT LAW P.C.
patrick@richardspatentlaw.com
clare@richardspatentlaw.com

Submission of Inventor and current Patent Owner as of 1/18/17 practice of this patent and a file wrapper record of a duly marked product in accordance with 35 U.S.C. § 287(a).

Respectfully submitted
/william grecia/
William Grecia
Inventor and Patent Owner

Electronic Acknowledgement Receipt

EFS ID:	28101236
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	18-JAN-2017
Filing Date:	06-MAY-2013
Time Stamp:	20:21:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Practicing_Status_pto.pdf	1247103 31f2cb000d9d1c55b9ad5bb0bba19ebe447c33c5	no	4

Warnings:

Information:	
Total Files Size (in bytes):	1247103

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Junior patents citing this patent as prior art for inclusion within this file wrapper for educational reference:

U.S. Patents 9,342,832 and 9,519,802

US009519802B2

(12) **United States Patent**
Dutta

(10) **Patent No.: US 9,519,802 B2**
(45) **Date of Patent: Dec. 13, 2016**

(54) **SYSTEMS AND METHODS FOR DOCUMENT AND DATA PROTECTION**

(71) Applicant: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.**, New York, NY (US)

(72) Inventor: **Siddhartha Dutta**, Peoria, AZ (US)

(73) Assignee: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 13 days.

(21) Appl. No.: **14/272,262**

(22) Filed: **May 7, 2014**

(65) **Prior Publication Data**

US 2015/0324592 A1 Nov. 12, 2015

(51) **Int. Cl.**
G06F 21/00 (2013.01)
G06F 21/62 (2013.01)
G06F 21/60 (2013.01)

(52) **U.S. Cl.**
CPC ***G06F 21/6245*** (2013.01); ***G06F 21/602*** (2013.01); *G06F 2221/2107* (2013.01)

(58) **Field of Classification Search**
CPC G06F 21/60; G06F 21/602; G06F 21/6245; G06F 221/2107
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,239,226 B2 7/2007 Berardi et al.
7,627,531 B2 12/2009 Breck et al.
8,402,555 B2 3/2013 Grecia
8,458,487 B1 * 6/2013 Palgon et al. 713/185
8,533,860 B1 9/2013 Grecia
8,887,308 B2 11/2014 Grecia
2007/0113171 A1 * 5/2007 Behrens et al. 715/513
2011/0154467 A1 6/2011 Bomar et al.
2011/0213807 A1 9/2011 Mattsson
2011/0307710 A1 12/2011 McGuire et al.
2012/0173431 A1 7/2012 Ritchie et al.
2012/0278339 A1 11/2012 Wang
2012/0278897 A1 * 11/2012 Ang H04L 61/2596 726/26
2013/0246422 A1 * 9/2013 Bhargava et al. 707/737

OTHER PUBLICATIONS

International Preliminary Report on Patentability dated Oct. 26, 2015 in Application No. PCT/US2015/024877.
Sommers, "Tokenization in Depth—A Detailed Look at Tokenization and its Advantages over Encryption," Shift4 Secure Payment Processing, 2010, Shift4 Corporation, 1-12.
International Search Report and Written Opinion dated Jul. 20, 2015 in Application No. PCT/US2015/024877.

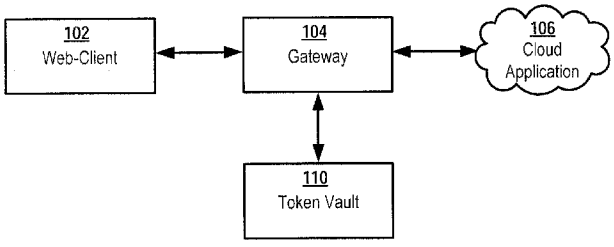
* cited by examiner

Primary Examiner — Kendall Dolly
(74) *Attorney, Agent, or Firm* — Snell & Wilmer L.L.P.

(57) **ABSTRACT**

The present disclosure includes a method comprising encrypting sensitive data, generating a token comprising a data identifier, tokenizing the encrypted sensitive data, and/or storing the encrypted sensitive data in association with the token to a token vault. Tokenizing may comprise mapping the encrypted sensitive data to the token. The method may further comprise storing the token to a cloud application, wherein the cloud application comprises a software application that functions within a cloud computing environment.

14 Claims, 4 Drawing Sheets



100A

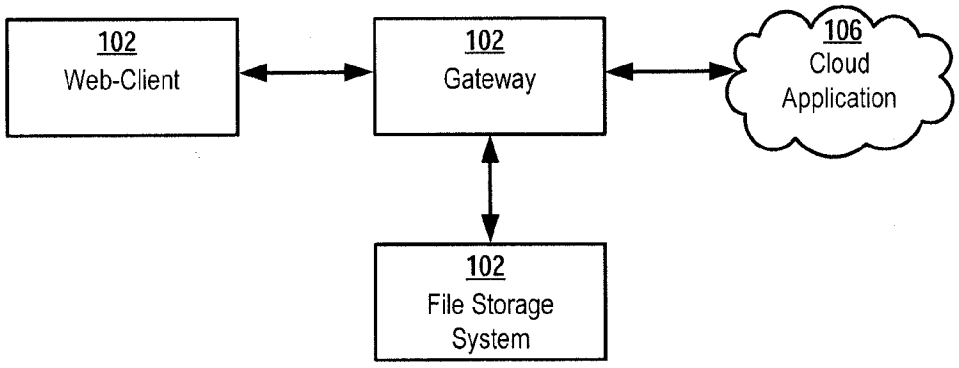

102
Web-Client
102
Gateway
106
Cloud
Application
102
File Storage
System

FIG. 1A

100B

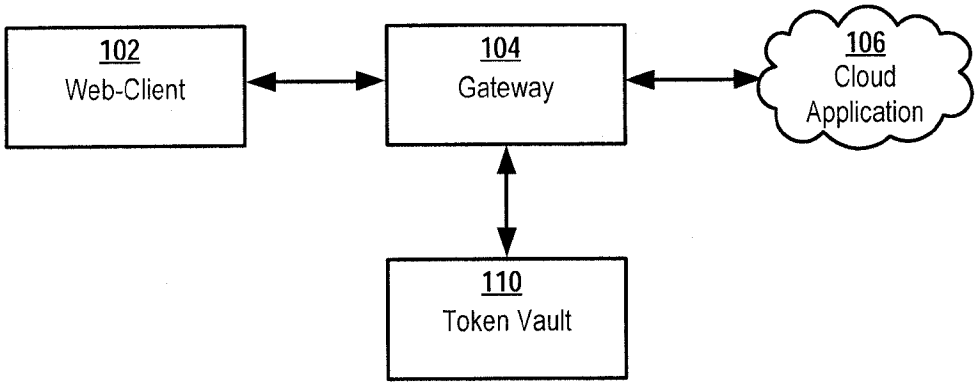

102
Web-Client
104
Gateway
106
Cloud
Application
110
Token Vault

FIG. 1B

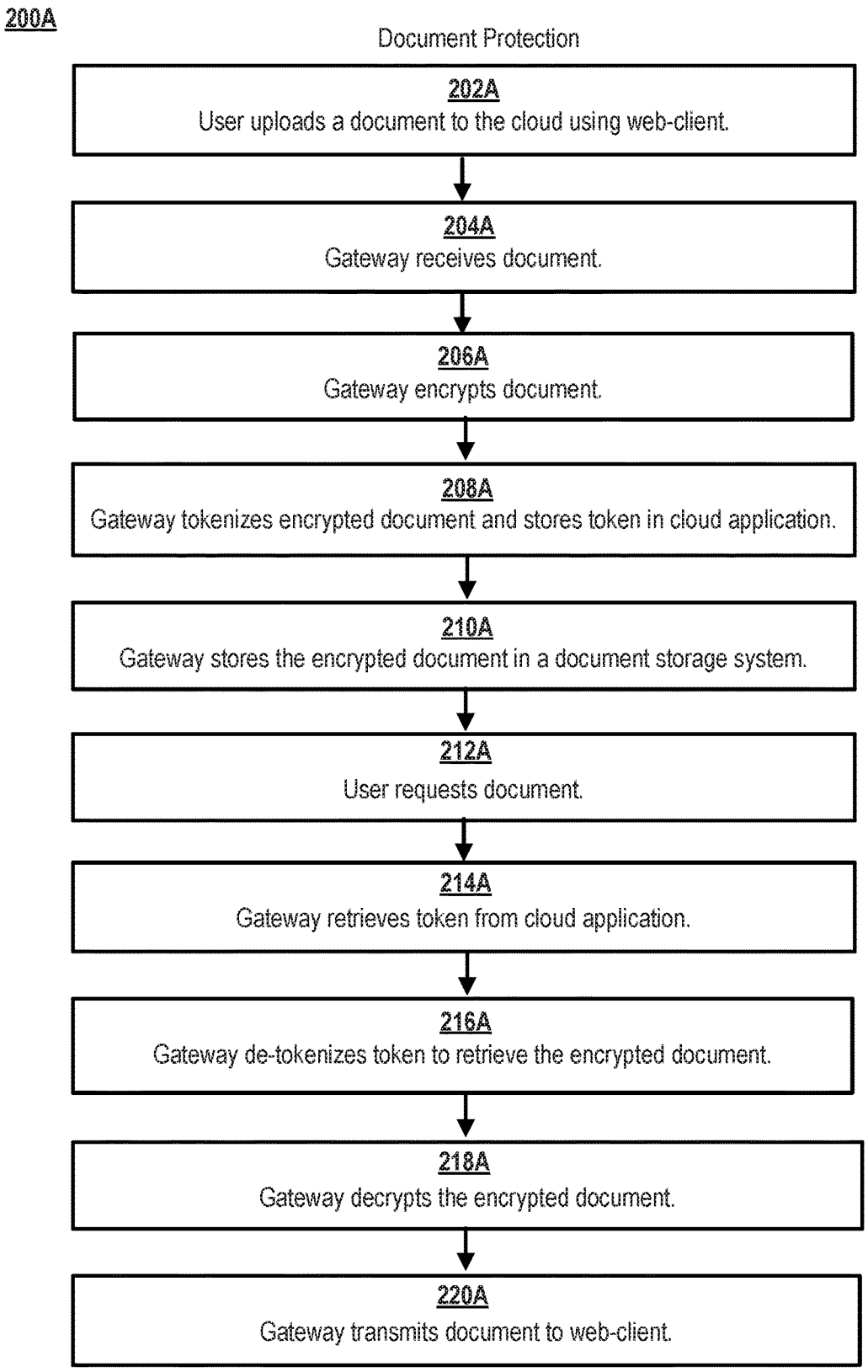

200A
Document Protection
202A
User uploads a document to the cloud using web-client.
204A
Gateway receives document.
206A
Gateway encrypts document.
208A
Gateway tokenizes encrypted document and stores token in cloud application.
210A
Gateway stores the encrypted document in a document storage system.
212A
User requests document.
214A
Gateway retrieves token from cloud application.
216A
Gateway de-tokenizes token to retrieve the encrypted document.
218A
Gateway decrypts the encrypted document.
220A
Gateway transmits document to web-client.

FIG. 2A

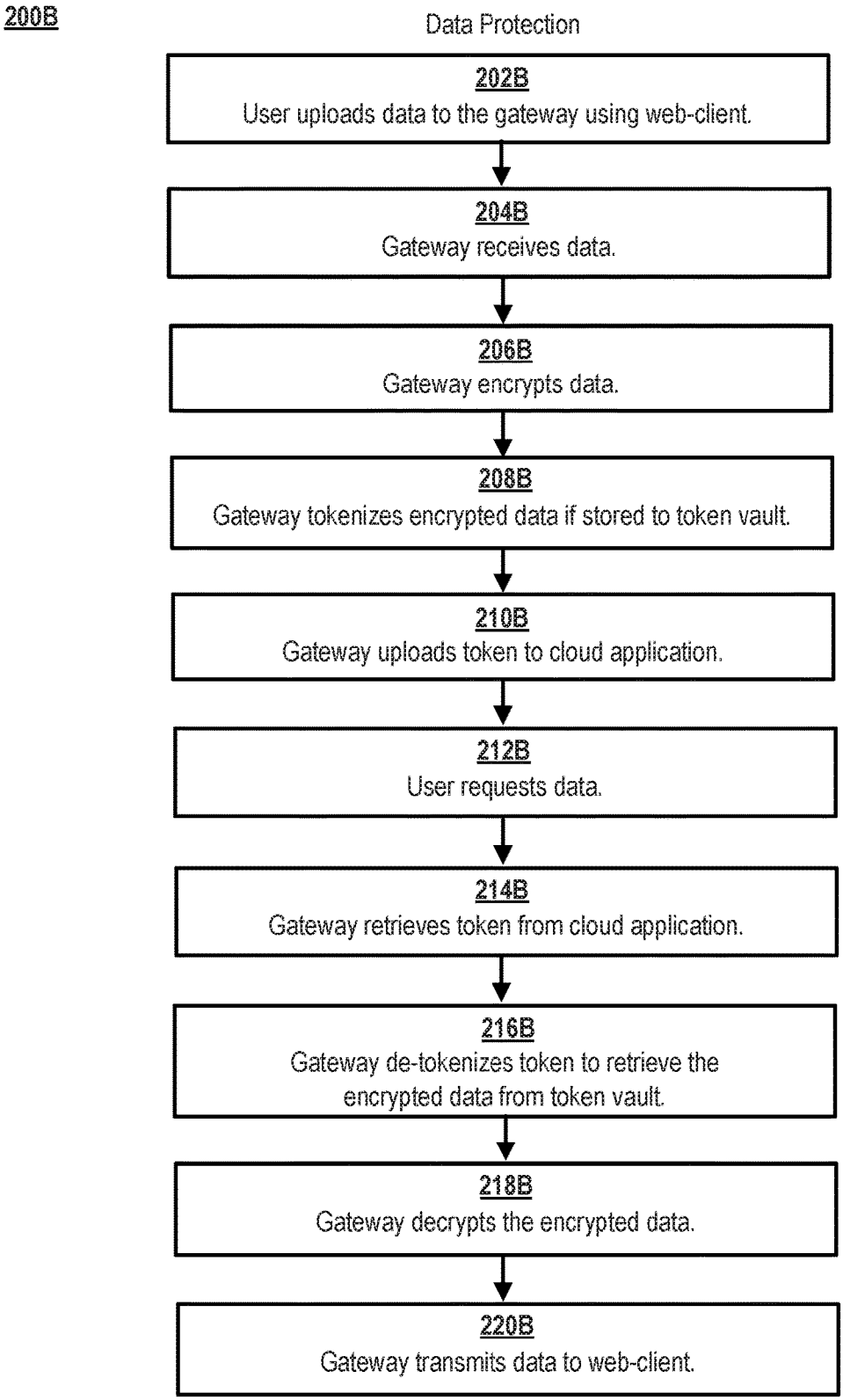

200B
Data Protection
202B
User uploads data to the gateway using web-client.
204B
Gateway receives data.
206B
Gateway encrypts data.
208B
Gateway tokenizes encrypted data if stored to token vault.
210B
Gateway uploads token to cloud application.
212B
User requests data.
214B
Gateway retrieves token from cloud application.
216B
Gateway de-tokenizes token to retrieve the encrypted data from token vault.
218B
Gateway decrypts the encrypted data.
220B
Gateway transmits data to web-client.

FIG. 2B

SYSTEMS AND METHODS FOR DOCUMENT AND DATA PROTECTION

FIELD

The present disclosure generally relates to document and data protection, and more particularly, to systems and methods for the protection of sensitive documents and/or data in conjunction with a cloud computing application, or external hosting services.

BACKGROUND

At present, enterprise documents and data are protected in several ways, each having their respective disadvantages. Briefly, documents and/or data may be encrypted and uploaded to a cloud computing application. Obviously, this method leaves sensitive data and/or documents exposed to unwanted decryption if encryption keys are breached. In addition, encryption may break application/user functions such as Search, Sort, etc. In addition, many cloud providers will not accept documents exceeding a certain file size (e.g., five megabytes). Moreover, company policies may prohibit the exportation of sensitive data to a cloud application, while some markets (e.g., China, Germany, and Switzerland) may have very strict data exportation laws, such that documents and/or data stored in a Europe-based cloud may not be exported, for example, to a United States based location.

To mitigate some of these problems, various enterprises have stored unencrypted documents and/or data to a local data storage system (e.g., a token vault or file system) through the use of a tokenization system. To gain access to this data, and to leverage cloud applications for data and document distribution within the enterprise, the data and/or documents have been tokenized (i.e., associate the documents or data with a random alphanumeric string or file path) and the token stored to the cloud application. Disadvantages exist here as well. For example, a hacker or disgruntled employee may hack into the token vault or file system, and gain access to the unencrypted documents and/or data stored on the enterprise system.

SUMMARY

The present disclosure includes a method comprising of a system or process that entails encrypting sensitive data, generating a token comprising a data identifier, tokenizing the encrypted sensitive data, and/or storing the encrypted sensitive data in association with the token to a token vault. Tokenizing may comprise mapping the encrypted sensitive data to the token. The method may further comprise storing the token to a cloud application, wherein the cloud application comprises a software application that functions within a cloud computing environment. In addition, the token comprises a randomly generated value. Moreover, the system may retrieve the token from a cloud application and/or identify the encrypted sensitive data, based upon a token associated with the encrypted sensitive data. The system may also decrypt the encrypted sensitive data and present it to the user.

The present disclosure further includes a method for encrypting a sensitive document. The method may include encrypting the sensitive document to create an encrypted sensitive document, generating a token comprising a document identifier, tokenizing the encrypted sensitive document, and/or storing the encrypted sensitive document to a local file storage system. Tokenizing may comprise associating the token with the encrypted sensitive document, and a token may comprise a file path. The method may also include storing the token to a cloud application, wherein the cloud application that comprises a software application that functions within a cloud computing environment. The method may, in addition, comprise receiving a request for the sensitive document. The method may include receiving the token from a cloud application and/or identifying the encrypted sensitive document, based upon a token associated with the encrypted sensitive document. The system may also decrypt the encrypted sensitive document and present it to the user.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present disclosure will become more apparent from the detailed description set forth below when taken in conjunction with the drawings. The left-most digit of a reference number identifies the drawing in which the reference number first appears.

FIG. **1**A illustrates, in accordance with various embodiments, a system for protecting a sensitive document;

FIG. **1**B illustrates, in accordance with various embodiments, a system for protecting sensitive data;

FIG. **2**A illustrates, in accordance with various embodiments, a process for protecting a sensitive document; and

FIG. **2**B illustrates, in accordance with various embodiments, a process for protecting sensitive data.

DETAILED DESCRIPTION

The detailed description of exemplary embodiments herein makes reference to the accompanying drawings, which show the exemplary embodiments by way of illustration and their best mode. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the disclosure, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the disclosure. Thus, the detailed description herein is presented for purposes of illustration only and not of limitation. For example, the steps recited in any of the method or process descriptions may be executed in any order and are not limited to the order presented. Moreover, any of the functions or steps may be outsourced to or performed by one or more third parties. Furthermore, any reference to singular includes plural embodiments, and any reference to more than one component may include a singular embodiment.

As used herein, a "document" may comprise any record (e.g., electronic record) that provides, comprises, and/or includes information. A document may, in various embodiments, be referenced and accessed by a file path associated with the document (e.g., C:/mydocuments/patent applications/systems and methods for document and data protection).

As used herein, "data" (or a "data element") may comprise any information whatsoever. Thus, data may not be accessible, as above, via a file path. Rather, data may comprise, for example, a transaction account (credit card) number, expiry date, and the like.

As used herein, a document or data may be "tokenized" by associating an identifier with the document and/or data. For example, a document may be tokenized by associating a file path or "token" with the document. The file path may comprise the directory location of the document within a file storage system. Data may likewise be tokenized by associ-

ating an identifier or "token" with the data. A token may, in various embodiments, comprise a random number, which may be associated with the data.

Referring to FIG. **1**A, a system **100**A for protecting a sensitive document is shown. The system **100**A may comprise a web-client **102**, a gateway **104**, a cloud application **106**, and/or a file storage system **108**.

A web-client **102** may include any device (e.g., personal computing device/mobile communication device) which communicates via any network. A web-client **102** may communicate (e.g., via a network) with a gateway **104**. Web-client **102** may be associated with and/or used by a consumer, a merchant, or both. Web-client may comprise a variety of browsing software or browser applications (e.g., Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, or any other of the myriad software packages available for browsing the internet). Such browser applications may comprise Internet browsing software installed within a computing unit or a system to conduct online transactions and/or communications. These computing units or systems may take the form of a computer or processor, or a set of computers/processors, although other types of computing units or systems may be used, including laptops, notebooks, hand held computers, personal digital assistants, cellular phones, smart phones (e.g., iPhone®, BlackBerry®, Droid®, etc.) set-top boxes, workstations, computer-servers, main frame computers, mini-computers, PC servers, pervasive computers, network sets of computers, personal computers, such as iPads, iMACs, and MacBooks, kiosks, terminals, point of sale (POS) devices and/or terminals, televisions, or any other device capable of receiving data over a network.

As those skilled in the art will appreciate, web-client **102** may include an operating system (e.g., Windows NT, 95/98/2000/CE/Mobile, OS2, UNIX, Linux, Solaris, MacOS, PalmOS, etc.) as well as various conventional support software and drivers typically associated with computers. A web-client may implement security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). A web-client may implement one or more application layer protocols, including, for example, http, https, ftp, and sftp. Transactions originating at a web client may pass through a firewall (not shown; see below) in order to prevent unauthorized access from users of other networks.

A gateway **104** may comprise any hardware and/or software configured to communicate with a cloud application **106**, a web-client **102**, a file storage system **108**, and/or a transaction vault **110**, as described below. For example, a gateway **104** may perform encryption/decryption operations as well as tokenize a document and/or data.

Encryption may be performed by way of any of the techniques now available in the art or which may become available—e.g., Twofish, RSA, El Gamal, Schorr signature, DSA, PGP, PKI, and symmetric and asymmetric cryptosystems.

A cloud application **106** may comprise any software application that functions within a cloud computing environment. Briefly, a cloud computing environment may comprise a network of remote servers hosted on the internet to store, manage, and/or process data. Thus, a cloud computing environment may serve, for example, to replace one or more local servers or personal computers.

A file storage system **108** may comprise any combination of hardware and/or software configured to store documents and/or data. For example, a file storage system **108** may comprise one or more databases, hard disk drives, and the like.

With reference now to FIG. **1**B, a system **100**B for protecting sensitive data is shown. The system may comprise a web-client **102**. Similarly, the system may comprise a gateway **104** as well as one or more cloud applications **106**. The system **100**B may further comprise a token vault **110**.

A token vault **110** may comprise a data storage system, such as one or more databases, that store one or more tokens. As described herein, a document and/or data may be associated with a token—"tokenized." Where data is tokenized, the token associated with the data may be stored securely within the token vault **110**. A mapping table may be stored within the token vault **110** to map data to its corresponding token.

With reference to FIG. **2**A, an example process **200**A for protecting one or more sensitive documents is disclosed. Returning briefly to the definition of document, a document may be referenced and accessed by a file path associated with the document (e.g., C:/mydocuments/patent applications/systems and methods for document and data protection).

Accordingly, to protect the document, a user of a web-client **102** may upload the document to a cloud application **106** residing within a cloud computing environment and/or a gateway **104** (step **202**A). The gateway **104** may receive the document (step **204**A) and/or encrypt the document (step **206**A). In response to encrypting the document, the gateway **104** may tokenize the document by associating the file or directory path of the document with the document. This document token may be stored by the gateway **104** (e.g., via a network) to a cloud application **106** (step **208**A). The gateway **104** may further store the encrypted document to the file storage system **108**.

In response to a request by a user for a particular document (e.g., via the web-client **102**) (step **212**A), the gateway may retrieve the token associated with the document from the cloud application **106** (step **214**A). This may occur, for example, in response to a request from the gateway for the token from the cloud application **106**. In various embodiments, the gateway **104** may "de-tokenize" the token, meaning that the gateway **104** may read and/or store the file or directory path comprising the token. The gateway **104** may further request, retrieve, and/or receive the encrypted document associated with the token from the file storage system **108** (step **216**A). The gateway **104** may, in addition, decrypt the encrypted document (step **218**A), and communicate the decrypted document to the user (step **220**A).

With reference now to FIG. **2**B, a process **200**B for protecting sensitive data is shown. In various embodiments, a user may upload, using a web-client **102**, data to the gateway **104** (step **202**B). The gateway **104** may receive the data (step **204**B). In response to receiving the data, the gateway **104** may encrypt the data and/or store it to the token vault **110** (step **206**B). The gateway may further tokenize the data (step **208**B). For example, the gateway **104** may generate a random number or "token," and associate that token with the encrypted data stored in the token vault **110**. As described herein, the token vault **110** may include a mapping table (or other data structure, such as a database, suitable for storing a mapping between one or more tokens and one or more encrypted data elements). The token may therefore be stored by the gateway **104** with its associated mapping in the mapping table held within the token vault **110**. The gateway **104** may upload one or more tokens associated with one or more data elements to the cloud application **106** (step **210**B).

In various embodiments, the user may request data (e.g., using the web-client **102**) (step **212**B). The gateway **104** may receive this request and retrieve one or more tokens

associated with the requested data from the cloud application **106** (step **214**B). The gateway **104** may de-tokenize the token to retrieve the encrypted data from the token vault **110** (step **216**B). As described herein, the process of de-tokenization may simply comprise locating, within the mapping table, the data stored in association with the token or tokens. The gateway **104** may further decrypt the data retrieved from the token vault **110** (step **218**B). In response to decrypting the data, the gateway **104** may communicate the data to the user's web-client **102** (step **220**B).

Thus, the systems and methods **100**A, **100**B, **200**A, and **200**B may mitigate the data insecurities and problems associated with many conventional systems. For example, although a conventional system may store a token to a cloud application, the system may leave the documents and/or data associated with the token unencrypted and open to theft by a hacker. Moreover, where a conventional system may leave the documents and data unencrypted, the systems and methods **100**A, **100**B, **200**A, and **200**B may encrypt the documents and data, so that even a compromised token (e.g., in the case of data) will lead to unsuccessful data theft. Further still, the systems and methods **100**A, **100**B, **200**A, and **200**B described herein permit the storage of encrypted documents and data across international borders, as described above, as well as the storage of documents and data greater than a particular size accepted by a could provider.

As used herein, the term "network" includes any cloud, cloud computing system or electronic communications system or method which incorporates hardware and/or software components. Communication among the parties may be accomplished through any suitable communication channels, such as, for example, a telephone network, an extranet, an intranet, Internet, point of interaction device (point of sale device, personal digital assistant (e.g., iPhone®, Palm Pilot®, Blackberry®), cellular phone, kiosk, etc.), online communications, satellite communications, off-line communications, wireless communications, transponder communications, local area network (LAN), wide area network (WAN), virtual private network (VPN), networked or linked devices, keyboard, mouse and/or any suitable communication or data input modality. Moreover, although the system is frequently described herein as being implemented with TCP/IP communications protocols, the system may also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI, any tunneling protocol (e.g. IPsec, SSH), or any number of existing or future protocols. If the network is in the nature of a public network, such as the Internet, it may be advantageous to presume the network to be insecure and open to eavesdroppers. Specific information related to the protocols, standards, and application software utilized in connection with the Internet is generally known to those skilled in the art and, as such, need not be detailed herein. See, for example, DILIP NAIK, INTERNET STANDARDS AND PROTOCOLS (1998); JAVA 2 COMPLETE, various authors, (Sybex 1999); DEBORAH RAY AND ERIC RAY, MASTERING HTML 4.0 (1997); and LOSHIN, TCP/IP CLEARLY EXPLAINED (1997) and DAVID GOURLEY AND BRIAN TOTTY, HTTP, THE DEFINITIVE GUIDE (2002), the contents of which are hereby incorporated by reference. The various system components described herein may be independently, separately or collectively coupled to the network via one or more data links including, for example, a connection to an Internet Service Provider (ISP) over a local loop as is typically used in connection with standard modem communication, cable modem, Dish networks, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods, see, e.g., GILBERT HELD , UNDERSTANDING DATA COMMUNICATIONS (1996), which is hereby incorporated by reference. It is noted that the network may be implemented variously. For example, network may be implemented as an interactive television (ITV) network. The systems and methods disclosed herein contemplate the use, sale and/or distribution of any goods, services or information over any network having functionality similar to that described above with reference to network.

The various system components described herein may be independently, separately or collectively coupled to the network via one or more data links including, for example, a connection to an Internet Service Provider (ISP) over a local loop as is typically used in connection with standard modem communication, cable modem, Dish networks, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods, see, e.g., GILBERT HELD, UNDERSTANDING DATA COMMUNICATIONS (1996), which is hereby incorporated by reference. It is noted that the network may be implemented variously. For example, network may be implemented as an interactive television (ITV) network. The systems and methods disclosed herein contemplate the use, sale and/or distribution of any goods, services or information over any network having functionality similar to that described above with reference to network.

Phrases and terms similar to a "transaction account holder," "buyer," "participant", "consumer," and/or "user" may include any person, entity, software and/or hardware that receives items in exchange for consideration (e.g. financial payment). For example, a buyer may purchase, lease, rent, barter or otherwise obtain items from a supplier and pay the supplier using a transaction account.

As used herein, "transmit" may include sending electronic data from one system component to another over a network connection. Additionally, as used herein, "data" may include encompassing information such as commands, queries, files, data for storage, and the like in digital or any other form.

Phrases or terms similar to "transaction account" may include any account that may be used to facilitate a financial transaction. A "transaction account" as used herein refers to an account associated with an open account or a closed account system (as described herein). The transaction account may exist in a physical or non-physical embodiment. For example, a transaction account may be distributed in non-physical embodiments such as an account number, frequent-flyer account, and telephone calling account or the like. Furthermore, a physical embodiment of a transaction account may be distributed as a financial instrument.

In general, transaction accounts may be used for transactions between the user (or "transaction account holder") and merchant through any suitable communication means, such as, for example, a telephone network, intranet, the global, public Internet, a point of interaction device (e.g., a point of sale (POS) device, personal digital assistant (PDA), mobile telephone, kiosk, etc.), online communications, off-line communications, wireless communications, and/or the like.

Phrases and terms similar to an "item" may include any good, service, information, experience, data, discount, rebate, points, virtual currency, content, access, rental, lease, contribution, account, credit, debit, benefit, right, reward, points, coupons, credits, monetary equivalent, anything of value, something of minimal or no value, monetary value, non-monetary value and/or the like. Moreover, the "transactions" or "purchases" discussed herein may be associated with an item. Furthermore, a "reward" may be an item.

An "account", "account code", or "account number", as used herein, may include any device, code, number, letter, symbol, digital certificate, smart chip, digital signal, analog signal, biometric or other identifier/indicia suitably configured to allow the consumer to access, interact with or communicate with the system (e.g., one or more of an authorization/access code, personal identification number (PIN), Internet code, other identification code, and/or the like). The account number may optionally be located on or associated with a rewards card, charge card, credit card, debit card, prepaid card, telephone card, embossed card, smart card, magnetic stripe card, bar code card, transponder, radio frequency card or an associated account. The system may include or interface with any of the foregoing cards or devices, QR codes, Bluetooth, Near Field Communication, or a transponder and RFID reader in RF communication with the transponder (which may include a fob). Typical devices may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation.

As used herein, a system, computing unit or device may include a "pervasive computing device," which may include a traditionally non-computerized device that is embedded with a computing unit. Examples can include watches, Internet enabled kitchen appliances, restaurant tables embedded with RF readers, wallets or purses with imbedded transponders, etc.

The account code may be distributed and stored in any form of plastic, electronic, magnetic, radio frequency, wireless, audio and/or optical device capable of transmitting or downloading data from itself to a second device. A customer account code may be, for example, a sixteen-digit transaction account code, although each transaction account provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's transaction account codes comply with that company's standardized format such that the company using a fifteen-digit format will generally use three-spaced sets of numbers, as represented by the number "0000 000000 00000". The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type, etc. In this example, the last (fifteenth) digit is used as a sum check for the fifteen digit number. The intermediary eight-to-eleven digits are used to uniquely identify the customer. A merchant account code may be, for example, any number or alpha-numeric characters that identify a particular merchant for purposes of card acceptance, account reconciliation, reporting, or the like.

It should be noted that the transfer of information in accordance with the present disclosure, may be completed in a format recognizable by a merchant system or account issuer. In that regard, by way of example, the information may be transmitted from a contactless (e.g., an RFID device) to a contactless (e.g., RFID) reader or from the contactless reader to the merchant system in a variety of formats, e.g., magnetic stripe or multi-track magnetic stripe format.

As used herein, phrases and terms similar to "financial institution," "transaction account issuer" and "payment processor" may include any person, entity, software and/or hardware that offers transaction account services. Although often referred to as a "financial institution," the financial institution may represent any type of bank, lender or other type of account issuing institution, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution.

The terms "payment vehicle," "financial transaction instrument," "transaction instrument," or "transaction account product" may be used interchangeably throughout to refer to a financial instrument. As used herein, an account code may or may not be associated with a physical financial instrument.

In the detailed description herein, references to "one embodiment", "an embodiment", "an example embodiment", "various embodiments", etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described. After reading the description, it will be apparent to one skilled in the relevant art(s) how to implement the disclosure in certain embodiments.

In various embodiments, the methods described herein are implemented using the various particular machines described herein. The methods described herein may be implemented using the particular machines, and those hereinafter developed, in any suitable combination, as would be appreciated immediately by one skilled in the art. Further, as is unambiguous from this disclosure, the methods described herein may result in various transformations of certain articles.

For the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical system.

The various system components discussed herein may include one or more of the following: a host server or other computing systems including a processor for processing digital data; a memory coupled to the processor for storing digital data; an input digitizer coupled to the processor for inputting digital data; an application program stored in the memory and accessible by the processor for directing processing of digital data by the processor; a display device coupled to the processor and memory for displaying information derived from digital data processed by the processor; and a plurality of databases. Various databases used herein may include: client data; merchant data; financial institution data; and/or like data useful in the operation of the system. As those skilled in the art will appreciate, user computer may include an operating system (e.g., Windows NT, 95/98/2000, XP, Vista, OS2, UNIX, Linux, Solaris, MacOS, etc.) as well as various conventional support software and drivers typically associated with computers. A user may include any individual, business, entity, government organization, software and/or hardware that interact with a system.

In an embodiment, various components, modules, and/or engines of the systems described herein may be implemented as micro-applications or micro-apps. Micro-apps are

typically deployed in the context of a mobile operating system, including for example, a Palm mobile operating system, a Windows mobile operating system, an Android Operating System, Apple iOS, a Blackberry operating system and the like. The micro-app may be configured to leverage the resources of the larger operating system and associated hardware via a set of predetermined rules which govern the operations of various operating systems and hardware resources. For example, where a micro-app desires to communicate with a device or network other than the mobile device or mobile operating system, the micro-app may leverage the communication protocol of the operating system and associated device hardware under the predetermined rules of the mobile operating system. Moreover, where the micro-app desires an input from a user, the micro-app may be configured to request a response from the operating system which monitors various hardware components and then communicates a detected input from the hardware to the micro-app.

The system contemplates uses in association with web services, utility computing, pervasive and individualized computing, security and identity solutions, autonomic computing, cloud computing, commodity computing, mobility and wireless solutions, open source, biometrics, grid computing and/or mesh computing.

Any databases discussed herein may include relational, hierarchical, graphical, or object-oriented structure and/or any other database configurations. Common database products that may be used to implement the databases include DB2 by IBM (Armonk, N.Y.), various database products available from Oracle Corporation (Redwood Shores, Calif.), Microsoft Access or Microsoft SQL Server by Microsoft Corporation (Redmond, Wash.), MySQL by MySQL AB (Uppsala, Sweden), or any other suitable database product. Moreover, the databases may be organized in any suitable manner, for example, as data tables or lookup tables. Each record may be a single file, a series of files, a linked series of data fields or any other data structure. Association of certain data may be accomplished through any desired data association technique such as those known or practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, using a key field in the tables to speed searches, sequential searches through all the tables and files, sorting records in the file according to a known order to simplify lookup, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in pre-selected databases or data sectors. Various database tuning steps are contemplated to optimize database performance. For example, frequently used files such as indexes may be placed on separate file systems to reduce In/Out ("I/O") bottlenecks.

More particularly, a "key field" partitions the database according to the high-level class of objects defined by the key field. For example, certain types of data may be designated as a key field in a plurality of related data tables and the data tables may then be linked on the basis of the type of data in the key field. The data corresponding to the key field in each of the linked data tables is preferably the same or of the same type. However, data tables having similar, though not identical, data in the key fields may also be linked by using AGREP, for example. In accordance with one embodiment, any suitable data storage technique may be utilized to store data without a standard format. Data sets may be stored using any suitable technique, including, for example, storing individual files using an ISO/IEC 7816-4 file structure; implementing a domain whereby a dedicated file is selected that exposes one or more elementary files containing one or more data sets; using data sets stored in individual files using a hierarchical filing system; data sets stored as records in a single file (including compression, SQL accessible, hashed via one or more keys, numeric, alphabetical by first tuple, etc.); Binary Large Object (BLOB); stored as ungrouped data elements encoded using ISO/IEC 7816-6 data elements; stored as ungrouped data elements encoded using ISO/IEC Abstract Syntax Notation (ASN.1) as in ISO/IEC 8824 and 8825; and/or other proprietary techniques that may include fractal compression methods, image compression methods, etc.

In one exemplary embodiment, the ability to store a wide variety of information in different formats is facilitated by storing the information as a BLOB. Thus, any binary information can be stored in a storage space associated with a data set. As discussed above, the binary information may be stored on the financial transaction instrument or external to but affiliated with the financial transaction instrument. The BLOB method may store data sets as ungrouped data elements formatted as a block of binary via a fixed memory offset using either fixed storage allocation, circular queue techniques, or best practices with respect to memory management (e.g., paged memory, least recently used, etc.). By using BLOB methods, the ability to store various data sets that have different formats facilitates the storage of data associated with the financial transaction instrument by multiple and unrelated owners of the data sets. For example, a first data set which may be stored may be provided by a first party, a second data set which may be stored may be provided by an unrelated second party, and yet a third data set which may be stored, may be provided by an third party unrelated to the first and second party. Each of these three exemplary data sets may contain different information that is stored using different data storage formats and/or techniques. Further, each data set may contain subsets of data that also may be distinct from other subsets.

As stated above, in various embodiments, the data can be stored without regard to a common format. However, in one exemplary embodiment, the data set (e.g., BLOB) may be annotated in a standard manner when provided for manipulating the data onto the financial transaction instrument. The annotation may comprise a short header, trailer, or other appropriate indicator related to each data set that is configured to convey information useful in managing the various data sets. For example, the annotation may be called a "condition header", "header", "trailer", or "status", herein, and may comprise an indication of the status of the data set or may include an identifier correlated to a specific issuer or owner of the data. In one example, the first three bytes of each data set BLOB may be configured or configurable to indicate the status of that particular data set; e.g., LOADED, INITIALIZED, READY, BLOCKED, REMOVABLE, or DELETED. Subsequent bytes of data may be used to indicate for example, the identity of the issuer, user, transaction/membership account identifier or the like. Each of these condition annotations are further discussed herein.

The data set annotation may also be used for other types of status information as well as various other purposes. For example, the data set annotation may include security information establishing access levels. The access levels may, for example, be configured to permit only certain individuals, levels of employees, companies, or other entities to access data sets, or to permit access to specific data sets based on the transaction, merchant, issuer, user or the like. Further-

more, the security information may restrict/permit only certain actions such as accessing, modifying, and/or deleting data sets. In one example, the data set annotation indicates that only the data set owner or the user are permitted to delete a data set, various identified users may be permitted to access the data set for reading, and others are altogether excluded from accessing the data set. However, other access restriction parameters may also be used allowing various entities to access a data set with various permission levels as appropriate.

The data, including the header or trailer may be received by a stand alone interaction device configured to add, delete, modify, or augment the data in accordance with the header or trailer. As such, in one embodiment, the header or trailer is not stored on the transaction device along with the associated issuer-owned data but instead the appropriate action may be taken by providing to the transaction instrument user at the stand alone device, the appropriate option for the action to be taken. The system may contemplate a data storage arrangement wherein the header or trailer, or header or trailer history, of the data is stored on the transaction instrument in relation to the appropriate data.

One skilled in the art will also appreciate that, for security reasons, any databases, systems, devices, servers or other components of the system may consist of any combination thereof at a single location or at multiple locations, wherein each database or system includes any of various suitable security features, such as firewalls, access codes, encryption, decryption, compression, decompression, and/or the like.

A firewall may comprise any hardware and/or software suitably configured to protect systems, components, and/or enterprise computing resources from users of other networks. Further, a firewall may be configured to limit or restrict access to various systems and components behind the firewall for web clients connecting through a web server. A firewall may reside in varying configurations including Stateful Inspection, Proxy based, access control lists, and Packet Filtering among others. A firewall may be integrated within a web server or any other CMS components or may further reside as a separate entity. A firewall may implement network address translation ("NAT") and/or network address port translation ("NAPT"). A firewall may accommodate various tunneling protocols to facilitate secure communications, such as those used in virtual private networking. A firewall may implement a demilitarized zone ("DMZ") to facilitate communications with a public network such as the Internet. A firewall may be integrated as software within an Internet server, any other application server components or may reside within another computing device or may take the form of a standalone hardware component.

The computers discussed herein may provide a suitable website or other Internet-based graphical user interface which is accessible by users. In one embodiment, the Microsoft Internet Information Server (IIS), Microsoft Transaction Server (MTS), and Microsoft SQL Server, are used in conjunction with the Microsoft operating system, Microsoft NT web server software, a Microsoft SQL Server database system, and a Microsoft Commerce Server. Additionally, components such as Access or Microsoft SQL Server, Oracle, Sybase, Informix MySQL, Interbase, etc., may be used to provide an Active Data Object (ADO) compliant database management system. In one embodiment, the Apache web server is used in conjunction with a Linux operating system, a MySQL database, and the Perl, PHP, and/or Python programming languages.

Any of the communications, inputs, storage, databases or displays discussed herein may be facilitated through a website having web pages. The term "web page" as it is used herein is not meant to limit the type of documents and applications that might be used to interact with the user. For example, a typical website might include, in addition to standard HTML documents, various forms, Java applets, JavaScript, active server pages (ASP), common gateway interface scripts (CGI), extensible markup language (XML), dynamic HTML, cascading style sheets (CSS), AJAX (Asynchronous Javascript And XML), helper applications, plug-ins, and the like. A server may include a web service that receives a request from a web server, the request including a URL (http://yahoo.com/stockquotes/ge) and an IP address (123.56.789.234). The web server retrieves the appropriate web pages and sends the data or applications for the web pages to the IP address. Web services are applications that are capable of interacting with other applications over a communications means, such as the internet. Web services are typically based on standards or protocols such as XML, SOAP, AJAX, WSDL and UDDI. Web services methods are well known in the art, and are covered in many standard texts. See, e.g., ALEX NGHIEM, IT WEB SERVICES: A ROADMAP FOR THE ENTERPRISE (2003), hereby incorporated by reference.

Middleware may include any hardware and/or software suitably configured to facilitate communications and/or process transactions between disparate computing systems. Middleware components are commercially available and known in the art. Middleware may be implemented through commercially available hardware and/or software, through custom hardware and/or software components, or through a combination thereof. Middleware may reside in a variety of configurations and may exist as a standalone system or may be a software component residing on the Internet server. Middleware may be configured to process transactions between the various components of an application server and any number of internal or external systems for any of the purposes disclosed herein. WebSphere MQTM (formerly MQSeries) by IBM, Inc. (Armonk, N.Y.) is an example of a commercially available middleware product. An Enterprise Service Bus ("ESB") application is another example of middleware.

Practitioners will also appreciate that there are a number of methods for displaying data within a browser-based document. Data may be represented as standard text or within a fixed list, scrollable list, drop-down list, editable text field, fixed text field, pop-up window, and the like. Likewise, there are a number of methods available for modifying data in a web page such as, for example, free text entry using a keyboard, selection of menu items, check boxes, option boxes, and the like.

The system and method may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the system may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, lookup tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the system may be implemented with any programming or scripting language such as C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Microsoft Active Server Pages, assembly, PERL, PHP, awk, Python,

Visual Basic, SQL Stored Procedures, PL/SQL, any UNIX shell script, and extensible markup language (XML) with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the system may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the system could be used to detect or prevent security issues with a client-side scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography and network security, see any of the following references: (1) "Applied Cryptography: Protocols, Algorithms, And Source Code In C," by Bruce Schneier, published by John Wiley & Sons (second edition, 1995); (2) "Java Cryptography" by Jonathan Knudson, published by O'Reilly & Associates (1998); (3) "Cryptography & Network Security: Principles & Practice" by William Stallings, published by Prentice Hall; all of which are hereby incorporated by reference.

Each participant is equipped with a computing device in order to interact with the system and facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, cellular telephones, touch-tone telephones and the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are contemplated by the system. The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a mini-computer, a PC server, a network of computers located in the same of different geographic locations, or the like. Moreover, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

The electronic commerce system may be implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

As will be appreciated by one of ordinary skill in the art, the system may be embodied as a customization of an existing system, an add-on product, upgraded software, a stand alone system, a distributed system, a method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, the system may take the form of an entirely software embodiment, an entirely hardware embodiment, or an embodiment combining aspects of both software and hardware. Furthermore, the system may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any suitable computer-readable storage medium may be utilized, including hard disks, CD-ROM, optical storage devices, magnetic storage devices, and/or the like.

The system and method is described herein with reference to screen shots, block diagrams and flowchart illustrations of methods, apparatus (e.g., systems), and computer program products according to various embodiments. It will be understood that each functional block of the block diagrams and the flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions.

These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions that execute on the computer or other programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks. These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

Accordingly, functional blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions, and program instruction means for performing the specified functions. It will also be understood that each functional block of the block diagrams and flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, can be implemented by either special purpose hardware-based computer systems which perform the specified functions or steps, or suitable combinations of special purpose hardware and computer instructions. Further, illustrations of the process flows and the descriptions thereof may make reference to user windows, webpages, websites, web forms, prompts, etc. Practitioners will appreciate that the illustrated steps described herein may comprise in any number of configurations including the use of windows, webpages, web forms, popup windows, prompts and the like. It should be further appreciated that the multiple steps as illustrated and described may be combined into single webpages and/or windows but have been expanded for the sake of simplicity. In other cases, steps illustrated and described as single process steps may be separated into multiple webpages and/or windows but have been combined for simplicity.

Benefits, other advantages, and solutions to problems have been described herein with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any elements that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of the disclosure. The scope of the disclosure is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more." Moreover, where a phrase similar to 'at least one of A, B, and C' or 'at least one of A, B, or C' is used in the claims or specification, it is intended that the phrase be interpreted to mean that A alone may be present in an embodiment, B alone may be present in an embodiment, C alone may be present in an embodiment, or that any combination of the elements A, B and C may be

present in a single embodiment; for example, A and B, A and C, B and C, or A and B and C. Although the inventions have been described as a method in certain embodiments, it is contemplated that it may be embodied as computer program instructions on a tangible computer-readable carrier, such as a magnetic or optical memory or a magnetic or optical disk. All structural, chemical, and functional equivalents to the elements of the above-described exemplary embodiments that are known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present disclosure, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. 112(f) unless the element is expressly recited using the phrase "means for." As used herein, the terms "comprises", "comprising", or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus.

What is claimed is:

1. A method comprising:

intercepting, by a tokenization gateway computer-based system, sensitive data prior to the sensitive data reaching a cloud application in an externally hosted system, wherein the sensitive data is being uploaded to the externally hosted system;

encrypting, by the tokenization gateway computer-based system and in response to the intercepting, the sensitive data to create encrypted sensitive data;

associating, by the tokenization gateway computer-based system, a file path with the encrypted sensitive data;

generating, by the tokenization gateway computer-based system and in response to the encrypting, a token comprising a data identifier;

tokenizing, by the tokenization gateway computer-based system and in response to the generating, the encrypted sensitive data, wherein the tokenizing comprises mapping the encrypted sensitive data to the token;

storing, by the tokenization gateway computer-based system and in response to the tokenizing, the token to the cloud application, wherein the cloud application comprises a software application that functions within the externally hosted system, wherein the externally hosted system includes a cloud computing environment;

storing, by the tokenization gateway computer-based system and in response to the storing the token to the cloud application, the encrypted sensitive data to a token vault internal to the tokenization gateway computer-based system, wherein the token vault comprises a data storage system;

retrieving, by the tokenization gateway computer-based system, the token from the cloud application in response to a request from the computer-based system for the token from the cloud application,

reading, by the tokenization gateway computer-based system, the file path associated with the token; and

in response to the reading the file path associated with the token, receiving and decrypting, by the tokenization gateway computer-based system, the encrypted sensitive data.

2. The method of claim **1**, wherein the token comprises the file path, wherein the file path comprises a directory location of the encrypted sensitive data within the data storage system.

3. The method of claim **2**, wherein the token comprises a randomly generated value, and wherein a mapping table is stored in the token vault, wherein the mapping table maps the encrypted sensitive data to the token.

4. The method of claim **3**, further comprising receiving, by the tokenization gateway computer-based system, a request for the sensitive data.

5. The method of claim **1**, further comprising identifying, based upon the token associated with the encrypted sensitive data, the encrypted sensitive data.

6. A system comprising:

a tangible, non-transitory memory communicating with a tokenization gateway processor,

the tangible, non-transitory memory having instructions stored thereon that, in response to execution by the tokenization gateway processor, cause the tokenization gateway processor to perform operations comprising:

intercepting, by the tokenization gateway processor, sensitive data prior to the sensitive data reaching a cloud application in an externally hosted system,

wherein the sensitive data is being uploaded to the externally hosted system;

encrypting, by the tokenization gateway processor and in response to the intercepting, the sensitive data to create encrypted sensitive data;

associating, by the tokenization gateway processor, a file path with the encrypted sensitive data;

generating, by the tokenization gateway processor and in response to the encrypting, a token comprising a data identifier;

tokenizing, by the tokenization gateway processor and in response to the generating, the encrypted sensitive data, wherein the tokenizing comprises mapping the encrypted sensitive data to the token;

storing, by the tokenization gateway processor and in response to the tokenizing, the token to the cloud application, wherein the cloud application comprises a software application that functions within the externally hosted system, wherein the externally hosted system includes a cloud computing environment;

storing, by the tokenization gateway processor and in response to the storing the token to the cloud application, the encrypted sensitive data to a token vault internal to the tokenization gateway processor, wherein the token vault comprises a data storage system;

retrieving, by the tokenization gateway processor, the token from the cloud application in response to a request from the tokenization gateway processor for the token from the cloud application,

reading, by the tokenization gateway processor, the file path associated with the token; and

in response to the reading the file path associated with the token, receiving and decrypting, by the tokenization gateway processor, the encrypted sensitive data.

7. The system of claim **6**, wherein the token comprises the file path, wherein the file path comprises a directory location of the encrypted sensitive data within the data storage system.

8. The system of claim 7, wherein the token comprises a randomly generated value, and wherein a mapping table is stored in the token vault, wherein the mapping table maps the encrypted sensitive data to the token.

9. The system of claim 8, further comprising receiving, by the tokenization gateway processor, a request for the sensitive data.

10. The system of claim 6, further comprising identifying, based upon the token associated with the encrypted sensitive data, the encrypted sensitive data.

11. An article of manufacture including a non-transitory, tangible computer readable storage medium having instructions stored thereon that, in response to execution by a tokenization gateway computer-based system, cause the computer-based system to perform operations comprising:

intercepting, by the tokenization gateway computer-based system, a sensitive document prior to the sensitive document reaching a cloud application in an externally hosted system,

wherein the sensitive document is being uploaded to the externally hosted system;

encrypting, by the tokenization gateway computer-based system and in response to the intercepting, the sensitive document to create an encrypted sensitive document;

associating, by the tokenization gateway computer-based system, a file path with the encrypted sensitive document;

generating, by the tokenization gateway computer-based system and in response to the encrypting, a token comprising a document identifier;

tokenizing, by the tokenization gateway computer-based system and in response to the generating, the encrypted sensitive document, wherein the tokenizing comprises associating the token with the encrypted sensitive document;

storing, by the tokenization gateway computer-based system and in response to the tokenizing, the token to the cloud application, wherein the cloud application comprises a software application that functions within the externally hosted system, wherein the externally hosted system includes a cloud computing environment;

storing, by the tokenization gateway computer-based system and in response to the storing the token to the cloud application, the encrypted sensitive document to an internal to the tokenization gateway computer-based system, wherein the token vault comprises file storage system;

retrieving, by the computer-based system, the token from the cloud application in response to a request from the computer-based system for the token from the cloud application,

reading, by the tokenization gateway computer-based system, the file path associated with the token; and

in response to the reading the file path associated with the token, receiving and decrypting, by the tokenization gateway computer-based system, the encrypted sensitive document.

12. The article of claim 11, wherein the token comprises the file path, wherein the file path comprises a directory location of the encrypted sensitive document within the document storage system.

13. The article of claim 12, wherein the token comprises a randomly generated value, and wherein a mapping table is stored in the token vault, wherein the mapping table maps the encrypted sensitive document to the token.

14. The article of claim 13, further comprising receiving, by the tokenization gateway computer-based system, a request for the sensitive document.

* * * * *

US009342832B2

(12) **United States Patent**
Basu et al.

(10) **Patent No.: US 9,342,832 B2**
(45) **Date of Patent: May 17, 2016**

(54) **SECURING EXTERNAL SYSTEMS WITH ACCOUNT TOKEN SUBSTITUTION**

(75) Inventors: **Gourab Basu**, Half Moon Bay, CA (US); **Michael Mori**, San Mateo, CA (US); **Ross Sakata**, Foster City, CA (US); **Steve Cracknell**, San Mateo, CA (US); **Millie Yee**, Santa Clara, CA (US); **Mark Carlson**, Half Moon Bay, CA (US); **Patrick Stan**, Pacifica, CA (US); **Surendra Keshan**, Cupertino, CA (US); **Edward Katzin**, San Francisco, CA (US)

(73) Assignee: **Visa International Service Association**, San Francisco, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 494 days.

(21) Appl. No.: **13/208,733**

(22) Filed: **Aug. 12, 2011**

(65) **Prior Publication Data**

US 2012/0041881 A1 Feb. 16, 2012

Related U.S. Application Data

(60) Provisional application No. 61/373,163, filed on Aug. 12, 2010, provisional application No. 61/381,322, filed on Sep. 9, 2010.

(51) **Int. Cl.**

G06Q 20/00	(2012.01)
G06Q 20/38	(2012.01)
G06Q 20/02	(2012.01)
G06Q 20/12	(2012.01)
G06Q 20/32	(2012.01)
G06Q 20/36	(2012.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/385*** (2013.01); ***G06Q 20/02*** (2013.01); ***G06Q 20/12*** (2013.01); ***G06Q 20/322*** (2013.01); ***G06Q 20/3674*** (2013.01); ***G06Q 20/382*** (2013.01); ***G06Q 20/38215*** (2013.01)

(58) **Field of Classification Search**

CPC G06Q 20/385
USPC 705/67, 17, 44, 64, 71, 78
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,903,652	A	5/1999	Mital	
5,903,880	A *	5/1999	Biffar	G06Q 20/06 235/379
6,005,945	A *	12/1999	Whitehouse	380/51

(Continued)

FOREIGN PATENT DOCUMENTS

WO	WO 01/09855 A1	2/2001

OTHER PUBLICATIONS

Ulf Mattsson, "The Difference between Tokenization and Encryption", Nov. 7, 2011.*

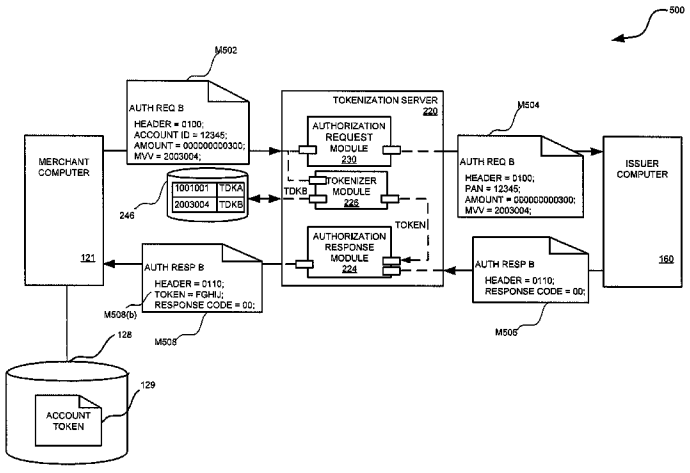
(Continued)

Primary Examiner — Steven Kim
(74) *Attorney, Agent, or Firm* — Kilpatrick Townsend & Stockton LLP

(57) **ABSTRACT**

Systems, apparatuses, and methods for providing an account token to an external entity during the lifecycle of a payment transaction. In some embodiments, an external entity may be a merchant computer requesting authorization of a payment message. In other embodiments, the external entity may be a support computer providing a payment processing network or a merchant support functions.

21 Claims, 12 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,182,894	B1	2/2001	Hackett	
6,236,981	B1 *	5/2001	Hill	705/67
6,327,578	B1 *	12/2001	Linehan	705/65
6,385,596	B1	5/2002	Wiser	
6,745,936	B1 *	6/2004	Movalli	G06Q 20/04 235/379
6,891,953	B1	5/2005	DeMello	
7,032,168	B1 *	4/2006	Gerace	G06Q 30/0277 705/14.73
7,287,692	B1	10/2007	Patel et al.	
7,403,922	B1	7/2008	Lewis et al.	
7,603,382	B2	10/2009	Halt, Jr.	
7,650,314	B1	1/2010	Saunders	
7,664,701	B2	2/2010	Phillips	
7,757,298	B2	7/2010	Shuster	
8,083,137	B2	12/2011	Tannenbaum	
8,170,922	B2 *	5/2012	Cavagnaro	705/26.1
8,381,213	B1 *	2/2013	Naamad et al.	718/100
8,402,555	B2	3/2013	Grecia	
8,533,860	B1	9/2013	Grecia	
8,571,995	B2 *	10/2013	Spies	G06Q 20/20 380/262
8,651,374	B2 *	2/2014	Brabson	G06Q 20/385 235/379
8,751,391	B2	6/2014	Freund	
8,887,308	B2	11/2014	Grecia	
9,065,643	B2 *	6/2015	Hurry	G06Q 20/3829
2001/0032878	A1 *	10/2001	Tsiounis et al.	235/379
2002/0073045	A1 *	6/2002	Rubin	G06Q 20/04 705/65
2003/0191709	A1 *	10/2003	Elston et al.	705/40
2004/0073688	A1 *	4/2004	Sampson	G06F 17/30067 709/229
2004/0107170	A1 *	6/2004	Labrou et al.	705/64
2004/0143552	A1 *	7/2004	Weichert et al.	705/64
2005/0027543	A1 *	2/2005	Labrou et al.	705/1
2005/0187873	A1 *	8/2005	Labrou et al.	705/40
2006/0123465	A1	6/2006	Ziegler	
2006/0167819	A1	7/2006	Bhambri et al.	
2006/0277148	A1 *	12/2006	Thackston	G06Q 20/02 705/41
2007/0022058	A1 *	1/2007	Labrou et al.	705/67
2007/0050635	A1 *	3/2007	Popp	713/185
2007/0125840	A1 *	6/2007	Law et al.	235/379
2007/0192245	A1 *	8/2007	Fisher	G06Q 20/02 705/39
2007/0294539	A1 *	12/2007	Shulman	G06F 17/30436 713/186
2008/0091617	A1	4/2008	Hazel et al.	
2008/0091944	A1 *	4/2008	von Mueller et al.	713/168
2008/0103982	A1	5/2008	Hammad et al.	
2008/0313264	A1	12/2008	Pestoni	
2009/0024908	A1	1/2009	Kottke et al.	
2009/0037388	A1	2/2009	Cooper	
2009/0070583	A1	3/2009	Von Mueller et al.	
2009/0228714	A1 *	9/2009	Fiske et al.	713/186
2009/0248581	A1 *	10/2009	Brown	705/67
2009/0249082	A1 *	10/2009	Mattsson	713/193
2009/0254440	A1 *	10/2009	Pharris	705/17
2009/0288012	A1 *	11/2009	Hertel et al.	715/738
2010/0257612	A1 *	10/2010	McGuire et al.	726/26
2010/0318468	A1 *	12/2010	Carr	G06Q 20/027 705/79
2010/0327054	A1 *	12/2010	Hammad	G06F 21/34 235/375
2011/0106710	A1 *	5/2011	Reed et al.	705/71
2011/0126274	A1 *	5/2011	Sadeckas	G06F 21/335 726/7
2011/0154467	A1 *	6/2011	Bomar et al.	726/9
2011/0161233	A1 *	6/2011	Tieken	705/71
2011/0213807	A1 *	9/2011	Mattsson	707/802
2011/0246369	A1 *	10/2011	de Oliveira et al.	705/64
2012/0136789	A1 *	5/2012	Kendrick	G06Q 20/12 705/44
2012/0317036	A1 *	12/2012	Bower et al.	705/75

OTHER PUBLICATIONS

Petition for Inter Partes Review of U.S. Pat. No. 8,533,860 Challenging Claims 1-30 Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104, filed Feb. 17, 2016, Before the USPTO Patent Trial and Appeal Board, IPR 2016-00600, 65 pages.

* cited by examiner

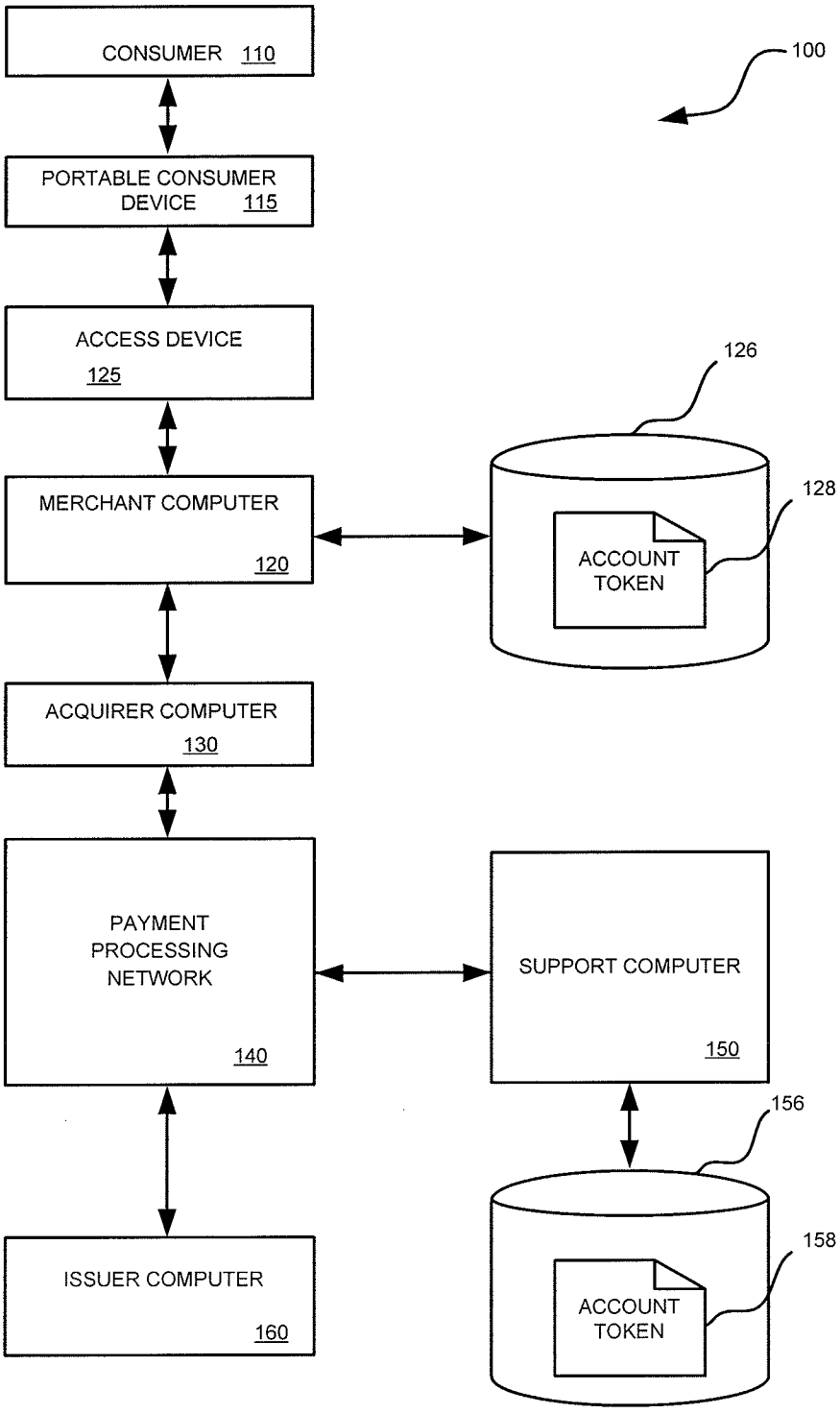

CONSUMER 110
100
PORTABLE CONSUMER DEVICE 115
ACCESS DEVICE 125
126
MERCHANT COMPUTER 120
128
ACCOUNT TOKEN
ACQUIRER COMPUTER 130
PAYMENT PROCESSING NETWORK 140
SUPPORT COMPUTER 150
156
158
ACCOUNT TOKEN
ISSUER COMPUTER 160

FIG. 1

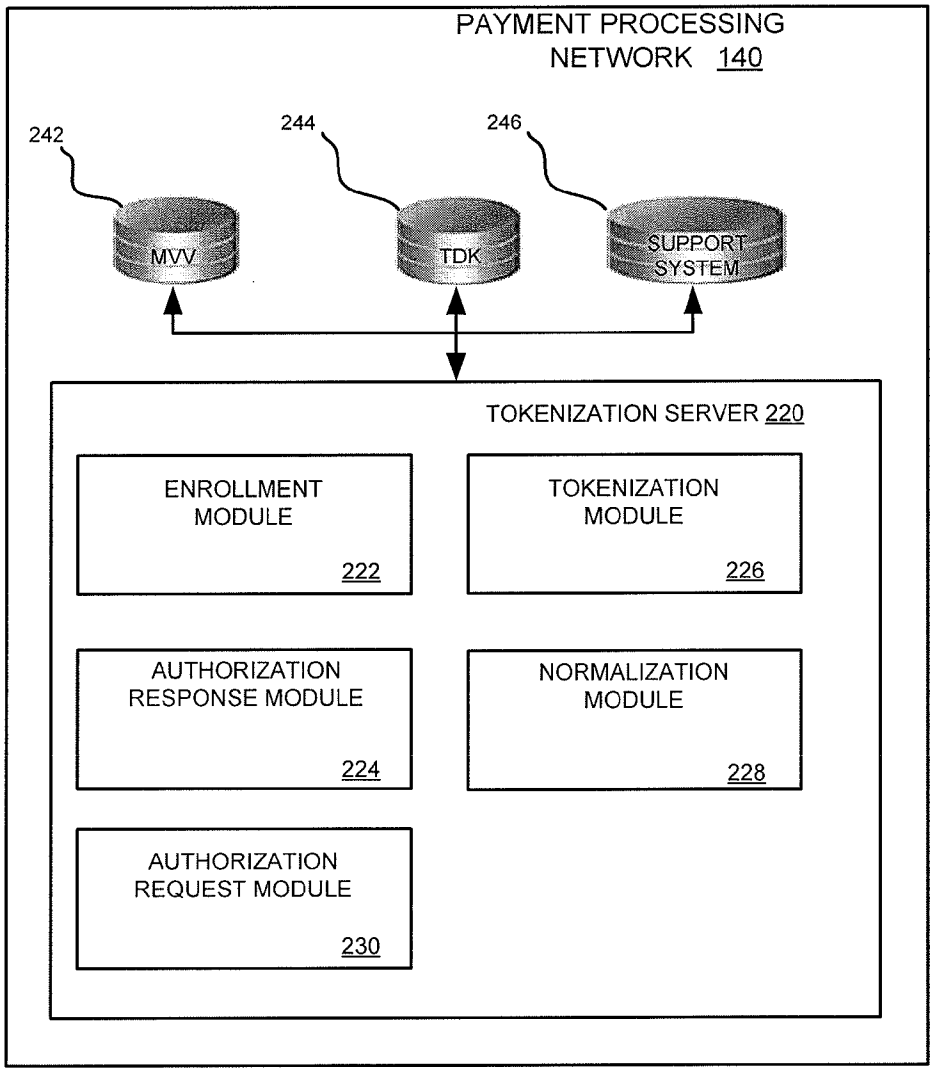

PAYMENT PROCESSING NETWORK 140
242
244
246
MVV
TDK
SUPPORT SYSTEM
TOKENIZATION SERVER 220
ENROLLMENT MODULE 222
TOKENIZATION MODULE 226
AUTHORIZATION RESPONSE MODULE 224
NORMALIZATION MODULE 228
AUTHORIZATION REQUEST MODULE 230

FIG. 2

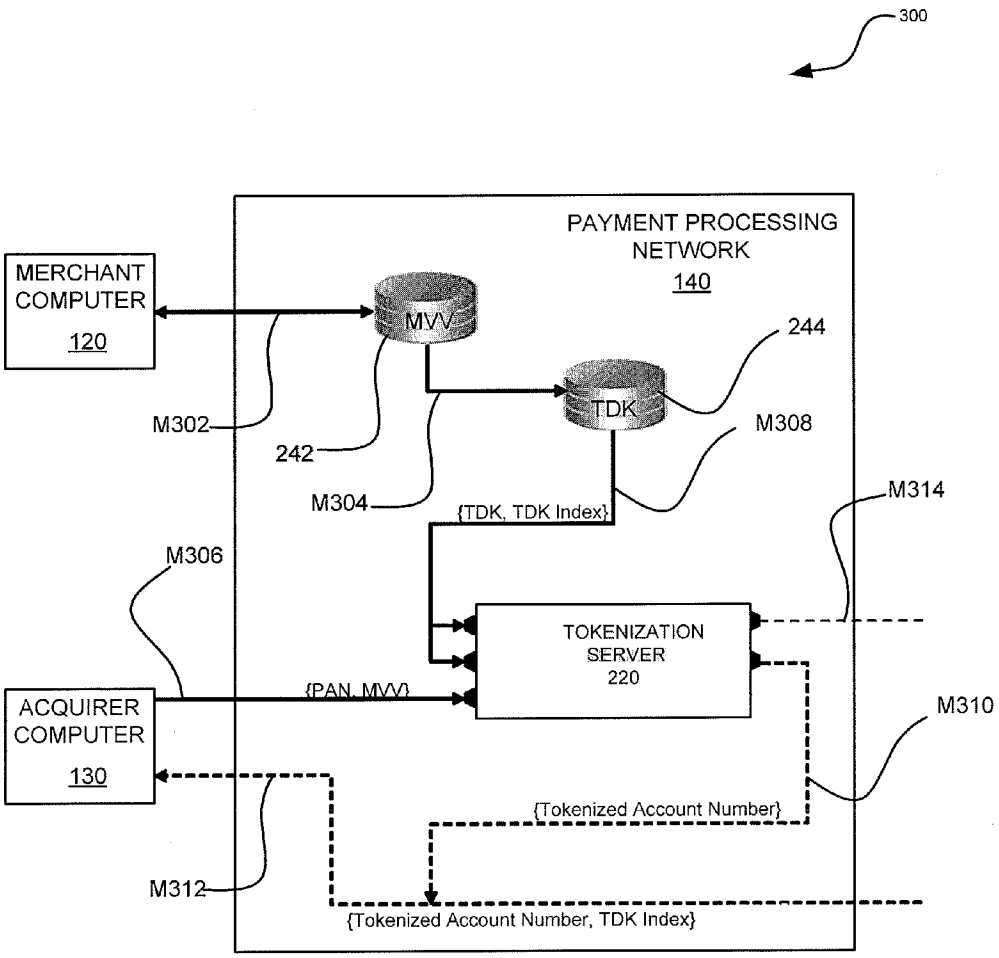

300
PAYMENT PROCESSING NETWORK
140
MERCHANT COMPUTER
120
MVV
TDK
244
M302
242
M304
M308
{TDK, TDK Index}
M314
M306
TOKENIZATION SERVER
220
{PAN, MVV}
ACQUIRER COMPUTER
130
M310
{Tokenized Account Number}
M312
{Tokenized Account Number, TDK Index}

FIG. 3

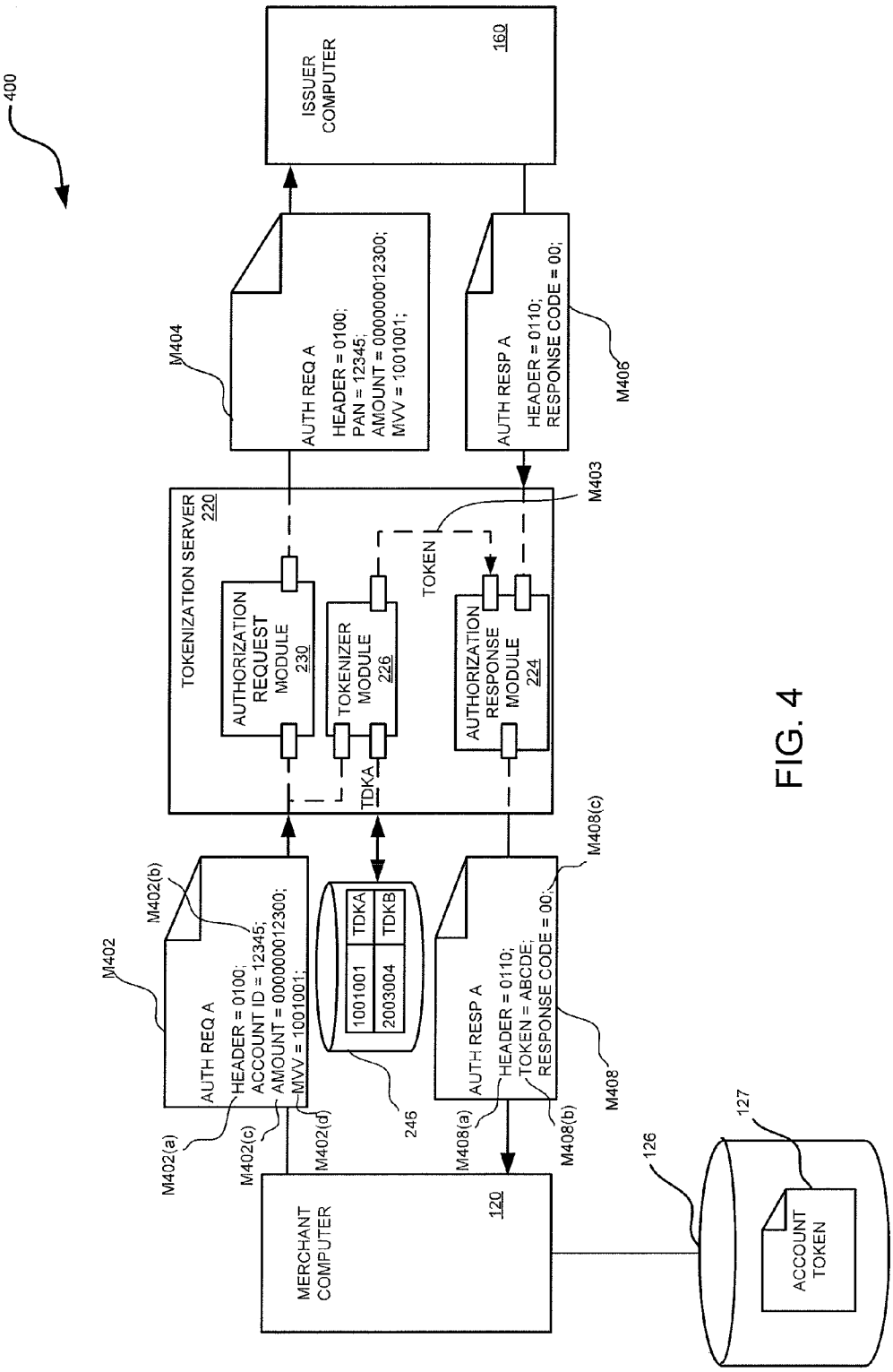

400
ISSUER COMPUTER
160
M404
AUTH REQ A
HEADER = 0100;
PAN = 12345;
AMOUNT = 000000012300;
MVV = 1001001;
AUTH RESP A
HEADER = 0110;
RESPONSE CODE = 00;
M406
M403
TOKEN
TOKENIZATION SERVER
220
AUTHORIZATION REQUEST MODULE
230
TOKENIZER MODULE
226
AUTHORIZATION RESPONSE MODULE
224
TDKA
M402(b)
M402
AUTH REQ A
HEADER = 0100;
ACCOUNT ID = 12345;
AMOUNT = 000000012300;
MVV = 1001001;
TDKA
TDKB
1001001
2003004
245
M408(c)
AUTH RESP A
HEADER = 0110;
TOKEN = ABCDE;
RESPONSE CODE = 00;
M408
M402(a)
M402(c)
M402(d)
M408(a)
M408(b)
MERCHANT COMPUTER
120
126
127
ACCOUNT TOKEN

FIG. 4

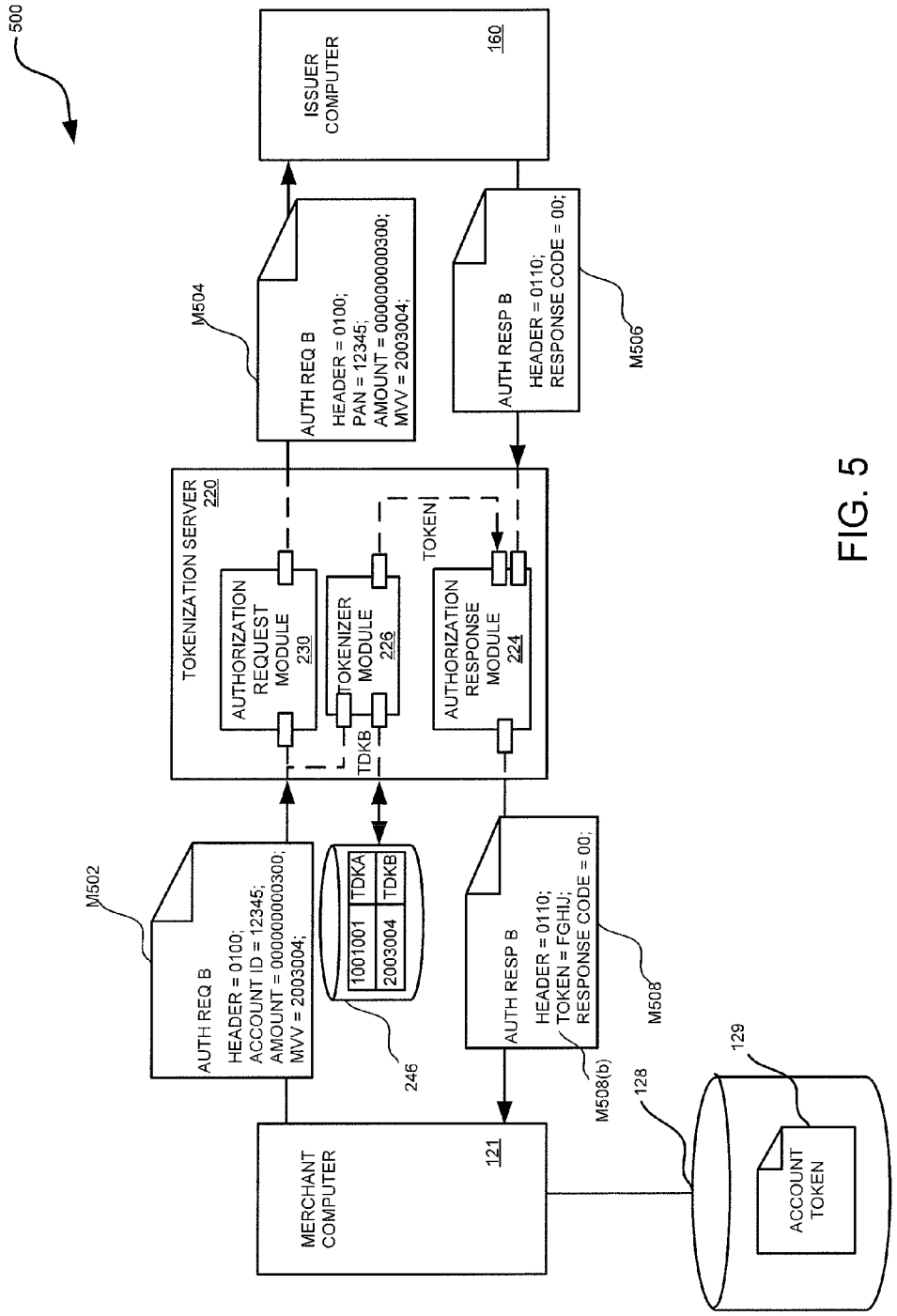

500
ISSUER COMPUTER
160
M504
AUTH REQ B
HEADER = 0100;
PAN = 12345;
AMOUNT = 000000000300;
MVV = 2003004;
AUTH RESP B
HEADER = 0110;
RESPONSE CODE = 00;
M506
TOKENIZATION SERVER
220
AUTHORIZATION REQUEST MODULE
230
TOKENIZER MODULE
226
AUTHORIZATION RESPONSE MODULE
224
TOKEN
TDKB
M502
AUTH REQ B
HEADER = 0100;
ACCOUNT ID = 12345;
AMOUNT = 000000000300;
MVV = 2003004;
1001001
TDKA
2003004
TDKB
246
AUTH RESP B
HEADER = 0110;
TOKEN = FGHIJ;
RESPONSE CODE = 00;
M508
M508(b)
MERCHANT COMPUTER
121
128
129
ACCOUNT TOKEN

FIG. 5

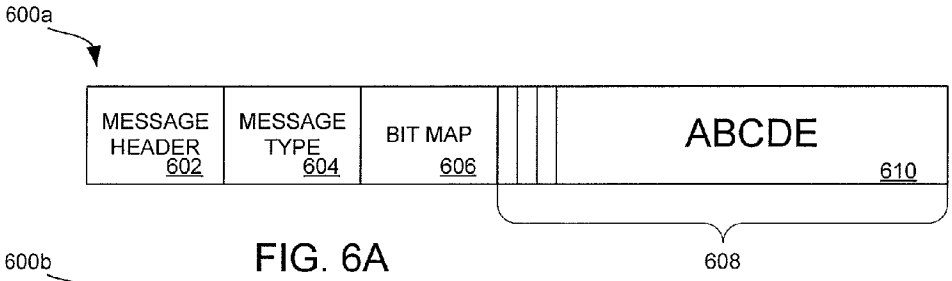


FIG. 6A

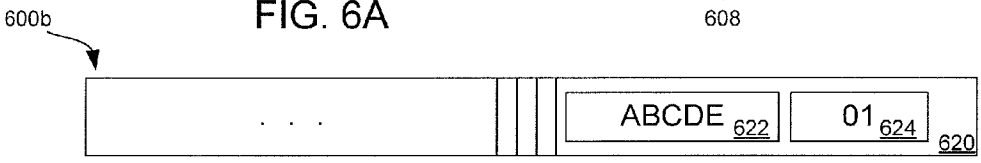


FIG. 6B

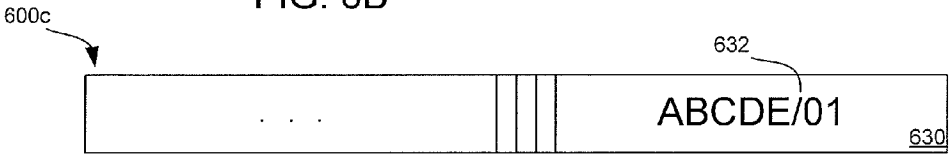


FIG. 6C

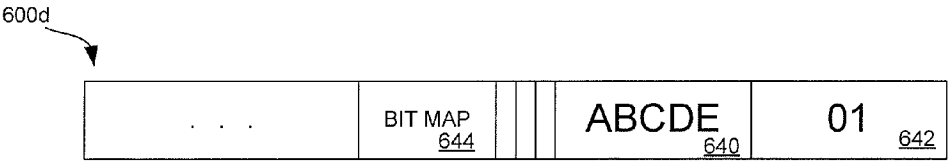


FIG. 6D

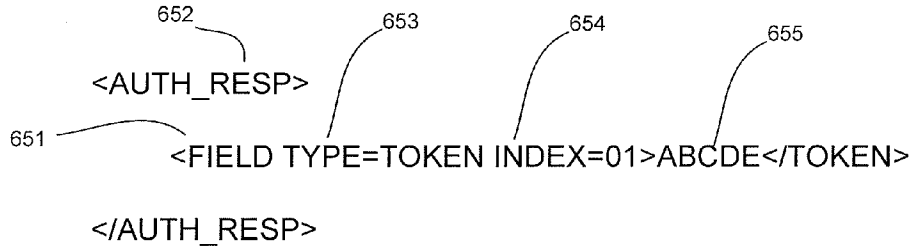


FIG. 6E

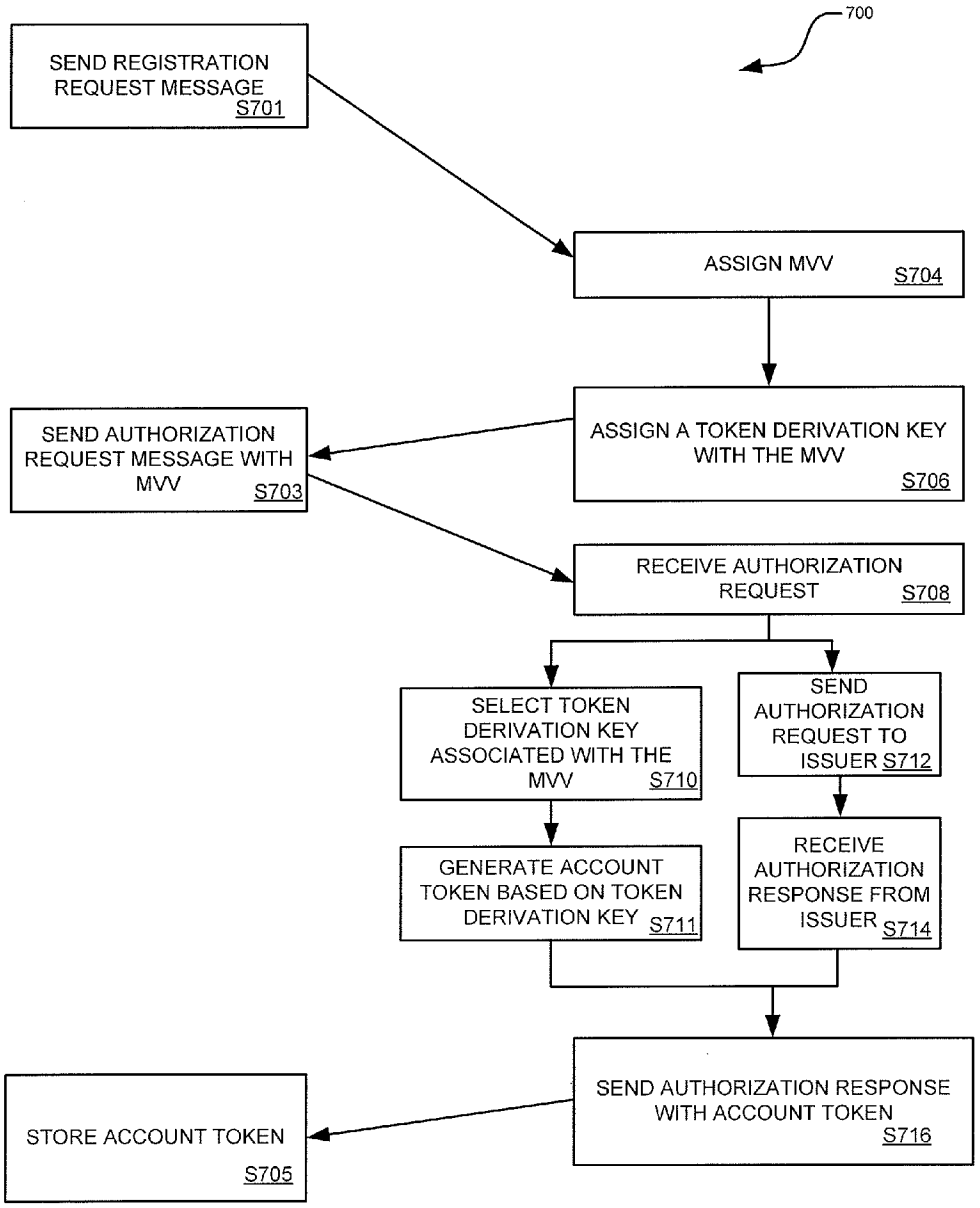

700
SEND REGISTRATION REQUEST MESSAGE S701
ASSIGN MVV S704
ASSIGN A TOKEN DERIVATION KEY WITH THE MVV S706
SEND AUTHORIZATION REQUEST MESSAGE WITH MVV S703
RECEIVE AUTHORIZATION REQUEST S708
SELECT TOKEN DERIVATION KEY ASSOCIATED WITH THE MVV S710
SEND AUTHORIZATION REQUEST TO ISSUER S712
GENERATE ACCOUNT TOKEN BASED ON TOKEN DERIVATION KEY S711
RECEIVE AUTHORIZATION RESPONSE FROM ISSUER S714
SEND AUTHORIZATION RESPONSE WITH ACCOUNT TOKEN S716
STORE ACCOUNT TOKEN S705

FIG. 7

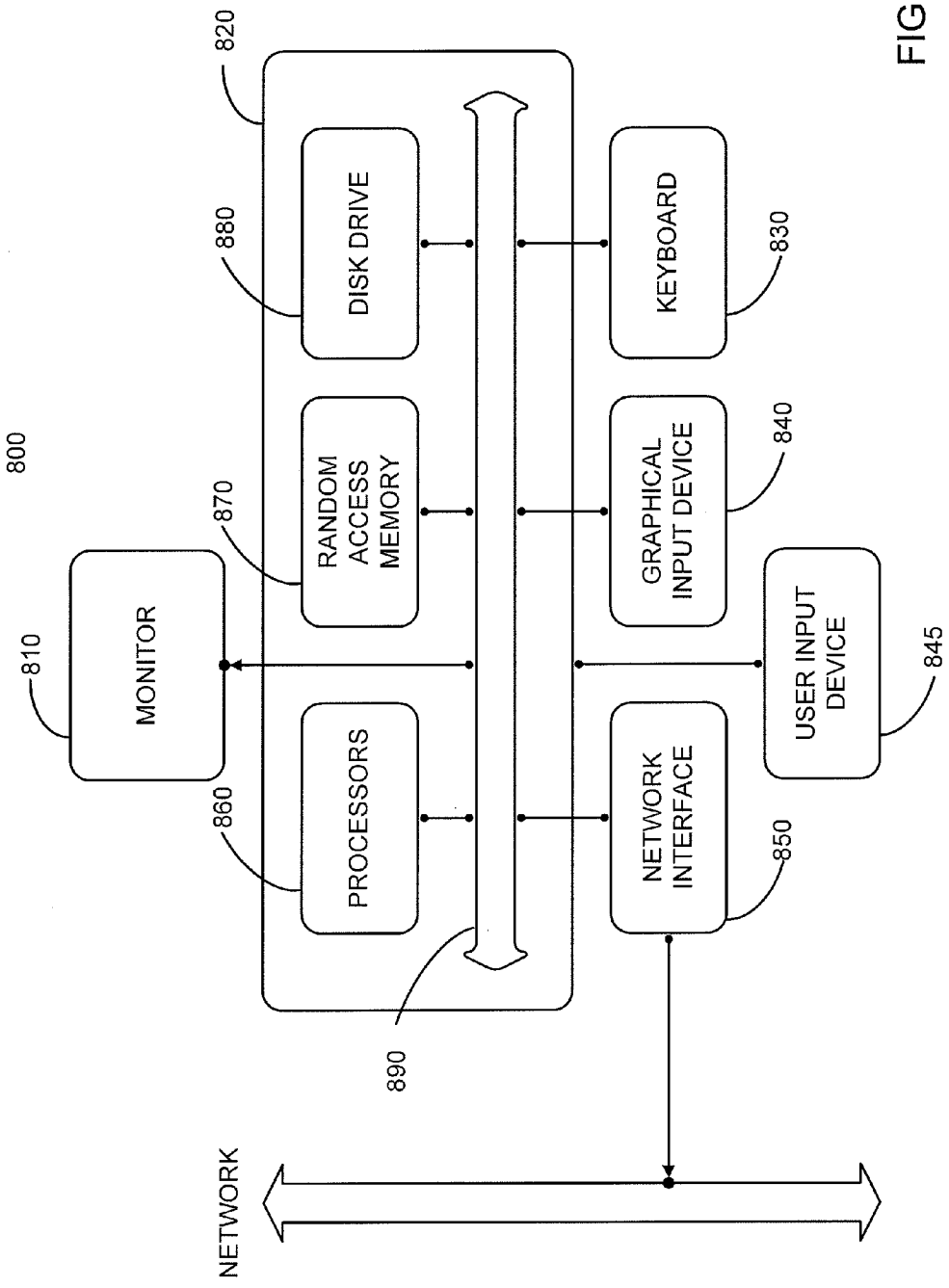

800
820
880
DISK DRIVE
KEYBOARD
830
870
RANDOM ACCESS MEMORY
GRAPHICAL INPUT DEVICE
840
810
MONITOR
USER INPUT DEVICE
845
860
PROCESSORS
NETWORK INTERFACE
850
890
NETWORK

FIG. 8

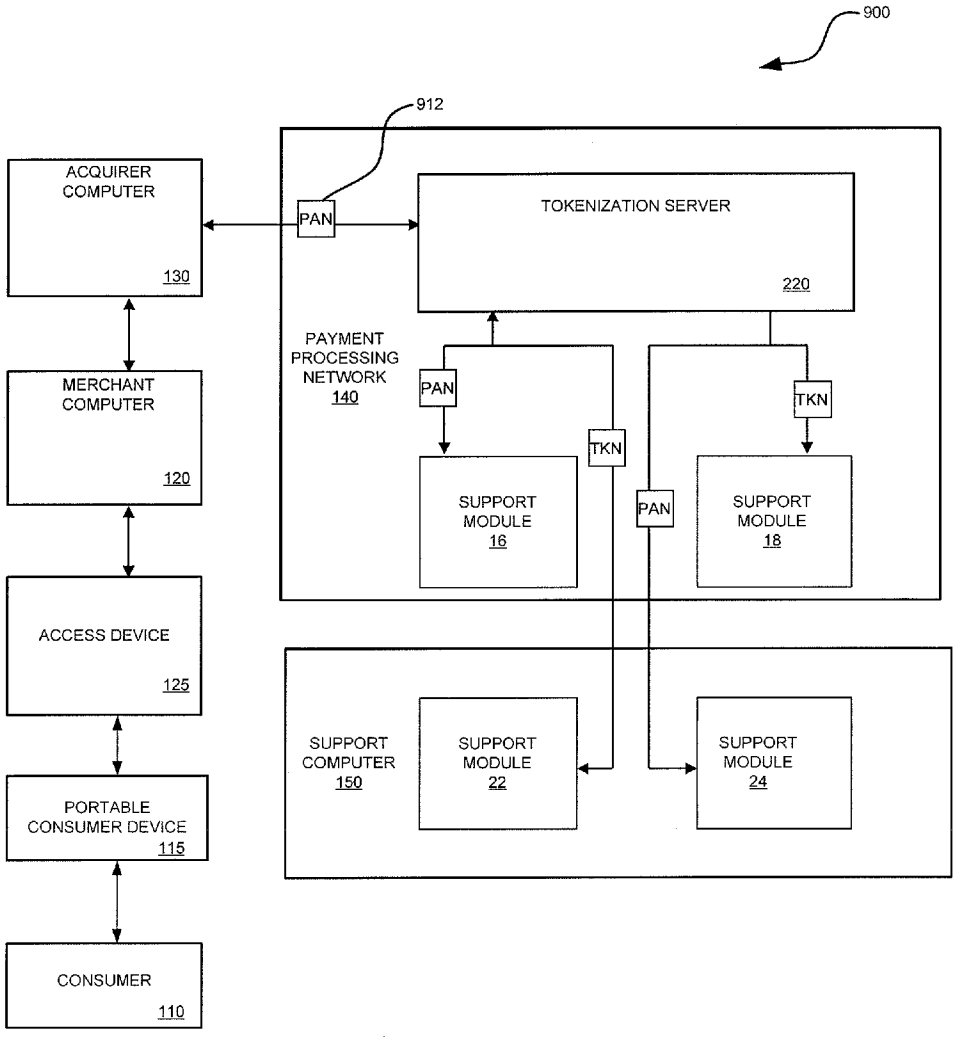

900
912
ACQUIRER COMPUTER
130
MERCHANT COMPUTER
120
ACCESS DEVICE
125
PORTABLE CONSUMER DEVICE
115
CONSUMER
110
PAN
TOKENIZATION SERVER
220
PAYMENT PROCESSING NETWORK
140
PAN
TKN
TKN
PAN
SUPPORT MODULE
16
SUPPORT MODULE
18
SUPPORT COMPUTER
150
SUPPORT MODULE
22
SUPPORT MODULE
24

FIG. 9

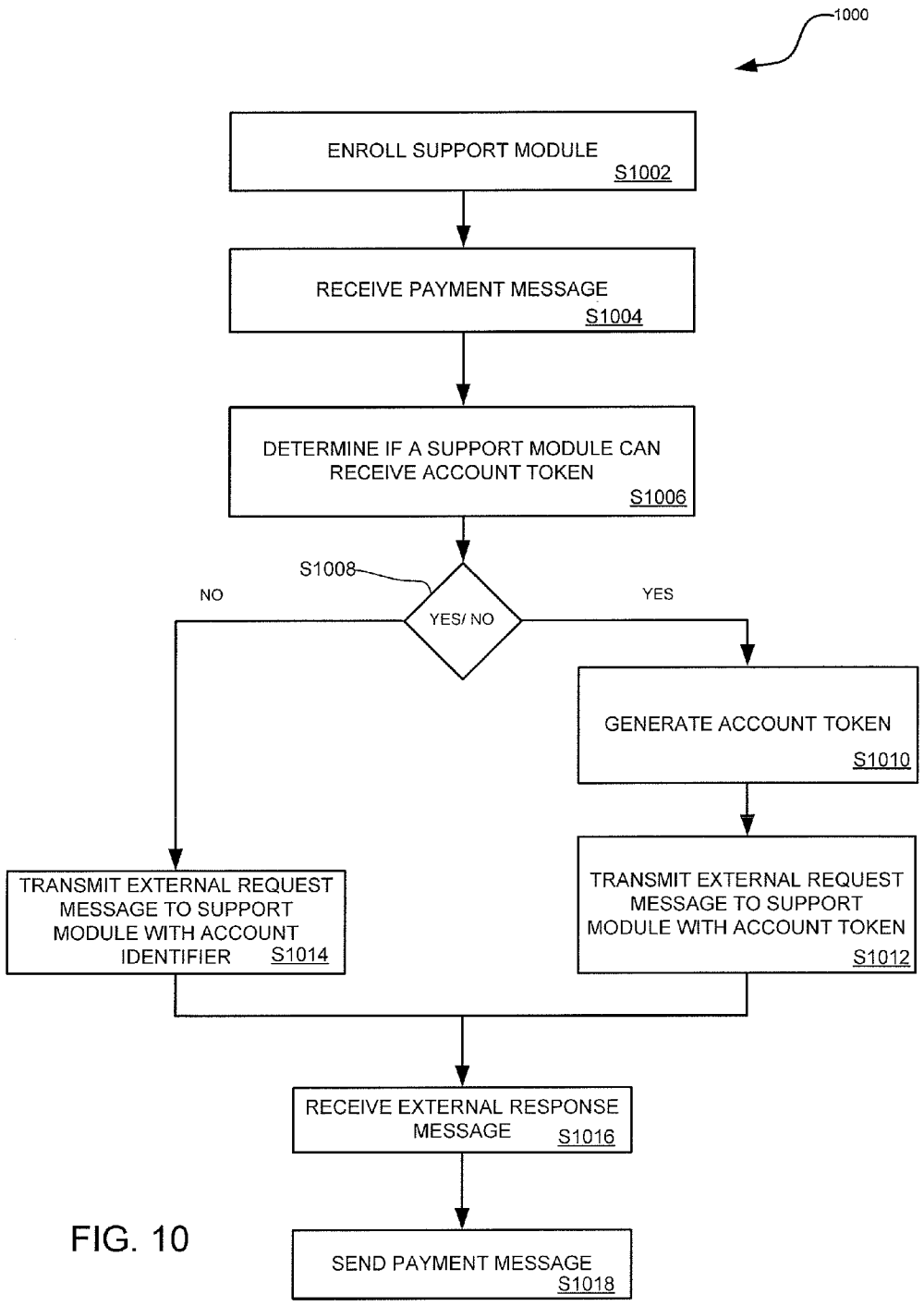

1000
ENROLL SUPPORT MODULE
S1002
RECEIVE PAYMENT MESSAGE
S1004
DETERMINE IF A SUPPORT MODULE CAN RECEIVE ACCOUNT TOKEN
S1006
S1008
YES/ NO
NO
YES
GENERATE ACCOUNT TOKEN
S1010
TRANSMIT EXTERNAL REQUEST MESSAGE TO SUPPORT MODULE WITH ACCOUNT IDENTIFIER
S1014
TRANSMIT EXTERNAL REQUEST MESSAGE TO SUPPORT MODULE WITH ACCOUNT TOKEN
S1012
RECEIVE EXTERNAL RESPONSE MESSAGE
S1016
SEND PAYMENT MESSAGE
S1018

FIG. 10

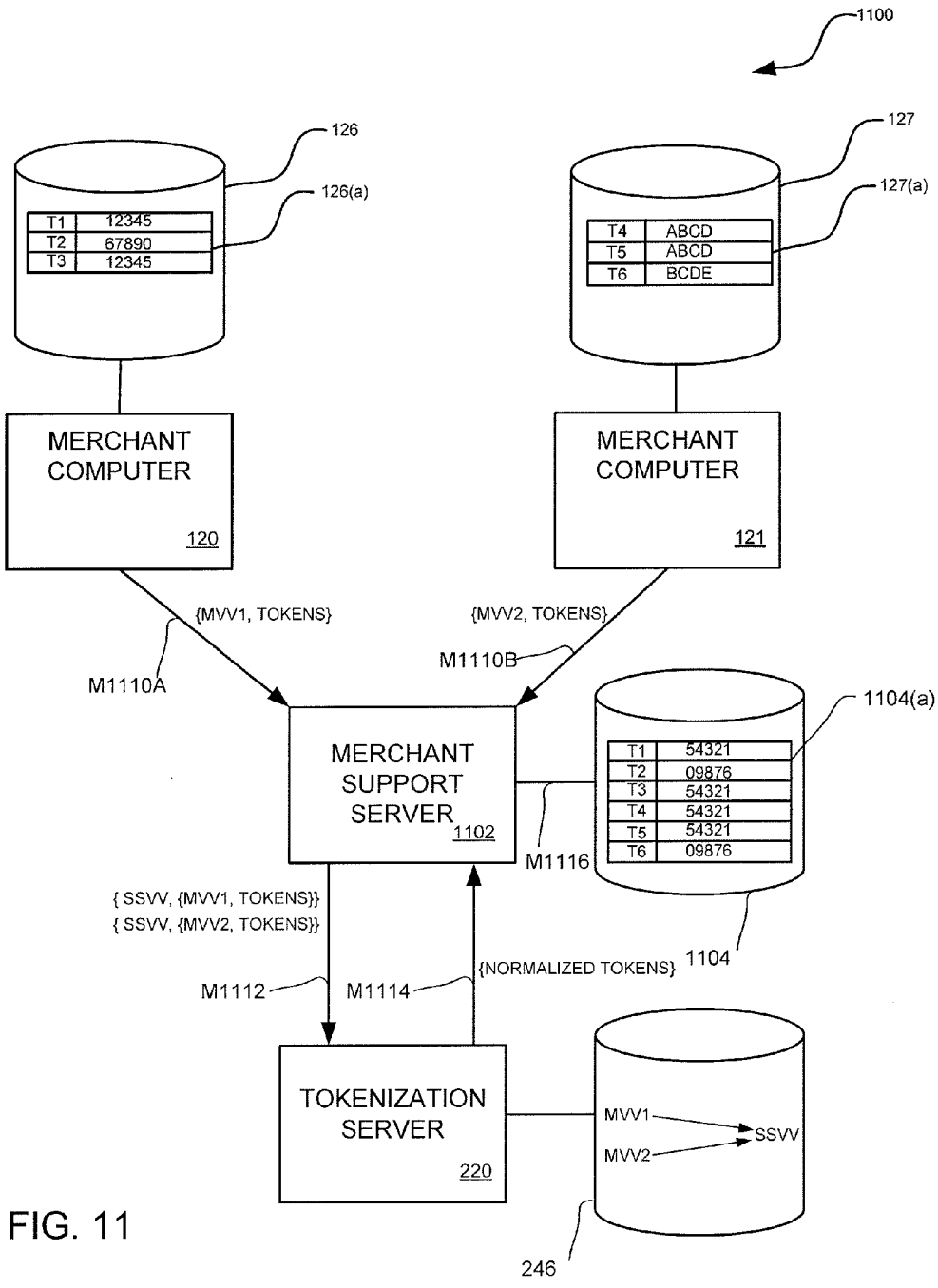

1100
126
126(a)
T1 12345
T2 67890
T3 12345
127
127(a)
T4 ABCD
T5 ABCD
T6 BCDE
MERCHANT COMPUTER 120
MERCHANT COMPUTER 121
{MVV1, TOKENS}
{MVV2, TOKENS}
M1110A
M1110B
MERCHANT SUPPORT SERVER 1102
1104(a)
T1 54321
T2 09876
T3 54321
T4 54321
T5 54321
T6 09876
M1116
1104
{ SSVV, {MVV1, TOKENS}}
{ SSVV, {MVV2, TOKENS}}
{NORMALIZED TOKENS}
M1112
M1114
TOKENIZATION SERVER 220
MVV1
MVV2
SSVV
246

FIG. 11

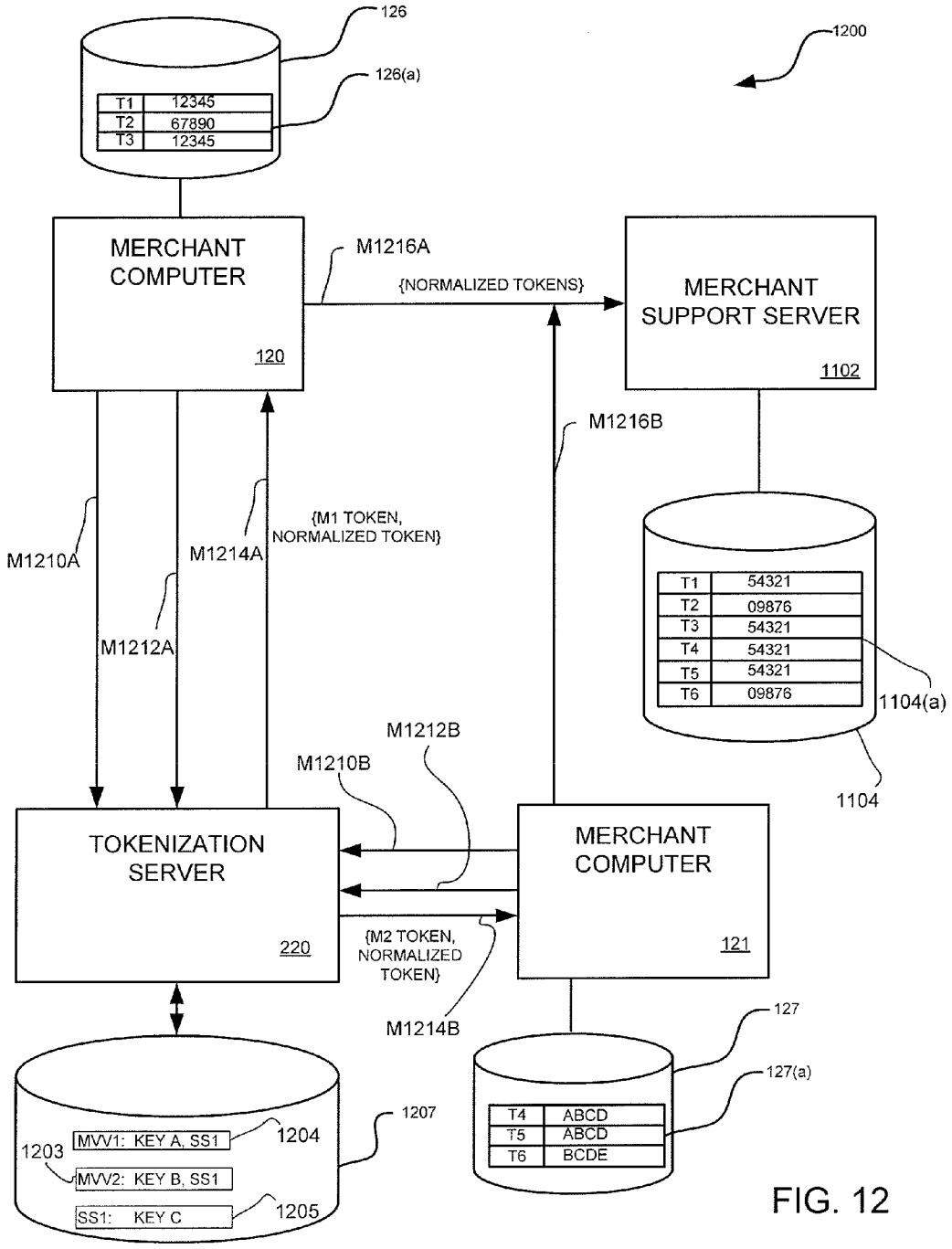

126
126(a)
T1 12345
T2 67890
T3 12345
1200
MERCHANT COMPUTER
120
M1216A
{NORMALIZED TOKENS}
MERCHANT SUPPORT SERVER
1102
M1216B
M1210A
M1214A
{M1 TOKEN, NORMALIZED TOKEN}
M1212A
T1 54321
T2 09876
T3 54321
T4 54321
T5 54321
T6 09876
1104(a)
1104
M1212B
M1210B
TOKENIZATION SERVER
220
MERCHANT COMPUTER
121
{M2 TOKEN, NORMALIZED TOKEN}
M1214B
127
127(a)
T4 ABCD
T5 ABCD
T6 BCDE
1207
1203
MVV1: KEY A, SS1
1204
MVV2: KEY B, SS1
SS1: KEY C
1205

FIG. 12

SECURING EXTERNAL SYSTEMS WITH ACCOUNT TOKEN SUBSTITUTION

CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 61/373,163, filed Aug. 12, 2010, entitled "SECURING SECONDARY SYSTEMS WITH TOKEN PAN SUBSTITUTION," and U.S. Provisional Application No. 61/381,322, filed Sep. 9, 2010, entitled "ACCOUNT NUMBER TOKENIZATION," which are herein incorporated by reference in their entirety for all purposes.

BACKGROUND

As methods and devices for engaging in financial transactions have increased, old problems of protecting sensitive information persist. For example, one common source of fraud occurs when a hacker gains access to a data center and obtains sensitive information such as credit card numbers and other cardholder data. As another example, an employee entrusted to maintain sensitive information can provide a fraudster access to the cardholder data, either by voluntary act, trick, negligence, or accident.

To protect sensitive information from such fraud, a data center may encrypt the data it stores. For example, a merchant may wish to track financial transactions at one or more stores to gain insight on the purchasing tendencies of its customers. In this example, the merchant may store financial information (e.g., credit card numbers) associated with the purchases. However, because such information is sensitive and could be used to conduct fraudulent transactions, the merchant may secure the credit card numbers it collects by encrypting the credit numbers it stores in its data center.

A merchant processor that performs payment gateway services on behalf of a merchant is another example of a data center. For example, the merchant processor (as provided by CYBERSOURCE™, of Mountain View, Calif.), may receive payment information from a merchant computer, process the payment information into the format of an authorization request message, send the authorization request message to the appropriate payment processing network (as may be offered by VISA™), receive an authorization response message, and route the authorization response message back to the merchant computer so that the merchant can provide a good or service to a customer.

Other examples of data centers include acquirers and acquirer processors. An acquirer is typically a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant. Acquirers may facilitate and manage financial transactions on behalf of merchants. An acquirer processor is typically a transaction processing entity that has a business relationship with a particular acquirer. Acquirer processors may provide merchants with transaction clearing, settlement, billing and reporting services.

In addition to the payment services described above, the acquirer or acquirer processor can also provide a variety of financial reports to the merchants registered for its services. For example, once a transaction has completed, the merchant may request information specifically for that transaction by sending a report request message to the acquirer or acquirer processor. The acquirer or acquirer processor may respond to the report request message by sending full payment information related to the specified transaction to the merchant.

To provide full payment information back to the merchant as part of these financial reports, the acquirer or acquirer processor may store the credit card numbers involved in the transactions. Accordingly, the acquirer or acquirer processor can be a form of a data center that stores cardholder information and other sensitive information. For the reasons described above, the acquirer or acquirer processor may protect the cardholder information against potential fraudsters. In one approach, the acquirer or acquirer processor may encrypt the credit card numbers that it receives. Further, to avoid collisions between the credit card numbers, the acquirer or acquirer processor may use an encryption key specific to each merchant when the acquirer or acquirer processor encrypts an account number, for example.

When a data center (e.g., a merchant processor, merchant, acquirer processor, or acquirer) maintains a database of sensitive information, the data center may have to comply with a number regulations. Such regulations attempt to increase controls around cardholder data to reduce credit card fraud via its exposure. For example, the Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. As part of the PCI DSS, a data center that stores and/or processes cardholder information must ensure that the cardholder data is secured. Further, the data center must perform periodic compliance testing.

As described above, a data center may encrypt cardholder information to comply with the PCI DSS. There are many known methods of encryption. Comparatively secure encryption systems are typically expensive and may consume large portions of a computer system's processing bandwidth.

Embodiments of the invention address the above problems, and other problems, individually and collectively.

SUMMARY

Embodiments of the present invention can be directed to systems, apparatuses, and methods for providing account tokens to external systems during the lifecycle of a payment transaction. As is explained below, an account token is a less sensitive form of an account identifier. Such account tokens can be sent to external entities, such as a merchant or a support computer, during the lifecycle of a transaction.

Some embodiments are directed to a method for providing an account token to a merchant computer. The method may involve a tokenization server receiving an authorization request message sent by a merchant computer. The authorization request message may request authorization for payment of a good or service and may include an account identifier and a merchant verification value. A token derivation key is then selected using the merchant verification value. The tokenization server then uses the token derivation key to generate the account token of the account identifier. The account token is inserted in an authorization response message that is then sent to the merchant computer.

Some embodiments are directed to a server that provides an account token to a merchant computer. The server receives an authorization request message sent by a merchant computer. The authorization request message includes an account identifier and a merchant verification value. The server then selects a token derivation key using the merchant verification value. The server then uses the token derivation key to generate the account token of the account identifier. The account token is inserted in an authorization response message that is then sent to the merchant computer.

Some embodiments are directed to a computer readable medium for performing a method of providing an account token to a merchant computer. The method may involve a

tokenization server receiving an authorization request message sent by a merchant computer. The authorization request message includes an account identifier and a merchant verification value. A token derivation key is then selected using the merchant verification value. The tokenization server then uses the token derivation key to generate the account token of the account identifier. The account token is inserted in an authorization response message that is then sent to the merchant computer.

Some embodiments are directed to a method for providing an account token to an external entity. The method may involve receiving a payment message that is associated with an account identifier. Then a tokenization server generates an account token of the account identifier associated with the payment message. An external request message with the account token is then transmitted to an external entity. An example of an external entity is a support computer that provides a risk score for a transaction. An external response message is then received. An example of an external response message is a risk score that corresponds to the payment message. After the external response message is received, the account identifier is then determined from the account token.

Some embodiments are directed to a server that provides an account token to an external entity. The server may receive a payment message that is associated with an account identifier. The server then generates an account token of the account identifier associated with the payment message. An external request message with the account token is then transmitted by the server to an external entity. An example of an external entity is a support computer that provides a risk score for a transaction. An external response message is then received by the server. An example of an external response message is a risk score that corresponds to the payment message. After the external response message is received, the account identifier is then determined from the account token.

Some embodiments are directed to a computer readable medium that includes instructions that, when executed by a processor, performs a method for providing an account token to an external entity. The method may involve receiving a payment message that is associated with an account identifier. Then a tokenization server generates an account token of the account identifier associated with the payment message. An external request message with the account token is then transmitted to an external entity. An example of an external entity is a support computer that provides a risk score for a transaction. An external response message is then received. An example of an external response message is a risk score that corresponds to the payment message. After the external response message is received, the account identifier is then determined from the account token.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a system that uses account tokens, according to example embodiments.

FIG. **2** is a block diagram of the components of a payment processing network, according to example embodiments.

FIG. **3** is a block diagram that shows the messages involved in sending an account token, according to example embodiments.

FIG. **4** is a block diagram that shows the messages involved in sending an account token to a first merchant, according to example embodiments.

FIG. **5** is a block diagram that shows the messages involved in sending an account token to a second merchant, according to example embodiments.

FIGS. **6**A, **6**B, **6**C, **6**D, and **6**E are diagrams that show various formats of an authorization request message, according to example embodiments.

FIG. **7** is a flow diagram that shows a method for generating an account token, according to example embodiments.

FIG. **8** is a block diagram illustrating the primary functional components of a computer or computing system that may be used to implement an element or component used in some embodiments of the present invention.

FIG. **9** is a block diagram showing account tokens sent to a support computer, according to example embodiments.

FIG. **10** is a flow diagram showing steps for sending an account token to a support computer, according to an example embodiment.

FIG. **11** is a block diagram showing a first technique for normalizing account tokens, according to example embodiments.

FIG. **12** is a block diagram showing a second technique for normalizing account tokens, according to example embodiments.

DETAILED DESCRIPTION

Embodiments of the invention relate to methods and systems for mitigating risks associated with transmitting and storing sensitive account identifiers. Particularly, example embodiments of the invention relate to generating an account token at a payment processing network as part of an authorization process involving a merchant computer, an acquirer computer, and/or a support computer.

However, prior to discussing the example embodiments of the invention, a further description of some terms can be provided for a better understanding of embodiments of the invention.

As used herein, an "account identifier" can refer to any information that identifies an account that holds value for a user. An account identifier can be represented as a sequence of characters or symbols. An account identifier is typically provided as part of a transaction, such as a payment transaction, that credits value to the account, debits value to the account, or performs any other suitable action on the account. Credit card numbers, checking and saving account numbers, prepaid account numbers, aliases and/or a passwords, phone numbers, and any other suitable identifier are all examples of account identifiers.

As used herein, an "account token" can refer to the result of transforming an account identifier into a form that is not considered sensitive in the context of the environment in which the account token resides. A "tokenization algorithm" can refer to the sequence of steps used to transform an account identifier into an account token. Still further, a "reverse tokenization algorithm" can refer to the sequence of steps used to transform the account token back to the account identifier. The tokenization algorithm may replace sensitive data, or portions thereof, with a value that is not considered sensitive.

As used herein, a "token derivation key" can refer to any piece of information that is used as a parameter of a tokenization algorithm. The token derivation key can be used to vary the output of a tokenization algorithm. In some embodiments, a token derivation key is symmetric as the same token derivation key is used for both tokenization and reverse tokenization. In other embodiments, a token derivation key is asymmetric as the token derivation key used to tokenize an account identifier is not used in the reverse tokenization algorithm. Instead, a second token derivation key is used in the reverse tokenization.

An "authorization request message" can refer to a message, or sequence of messages, that requests an issuer of the payment card to authorize a transaction. An authorization request message according to an embodiment of the invention may comply with ISO (International Organization for Standardization) 8583, which is a standard for systems that exchange electronic transactions made by cardholders using payment cards. An authorization request message according to other embodiments may comply with other suitable standards.

An "authorization response message" can refer to a message, or sequence of messages, that responds to a merchant's and/or acquirer's request to authorize a transaction. An authorization response message according to an embodiment of the invention may comply with ISO 8583, which, as described above, is a standard for systems that exchange electronic transactions made by cardholders using payment cards. An authorization response message according to other embodiments may comply with other suitable standards.

A "merchant verification value" may refer to any information that identifies a merchant as a participant in a service or program. As an example, a merchant verification value may be assigned to a business, person, or organization that has agreed to accept payment cards when properly presented by the cardholder. A merchant verification value can be any combination of characters and/or symbols. Further, a merchant verification value can be transmitted to a payment processing network as part of an authorization request message.

A "support system verification value" may refer to any information that identifies a support system as a provider of a service or program. As an example, a support system verification value may be assigned to a web service that provides a fraud score for a transaction. As another example, a support system verification value can be assigned to an alert web service that sends a message to a consumer's communication device (e.g., mobile phone) when one or more conditions applied. Such a message can be for a coupon or an alert that a transaction or activity has occurred with regard to a particular account. A support system verification value can be any combination of characters and/or symbols. Further, in some embodiments, a support system verification value can be transmitted to a payment processing network as part of an authorization request message.

A "verification value," as used herein, can refer to a merchant verification value, a support system verification value, or some combination thereof.

Generally, embodiments relate to apparatuses, systems, and methods of securing sensitive data. In particular, some embodiments improve security of a data center that stores, for example, account identifiers by communicating account tokens from a tokenization server to external entities (e.g., merchant computers or a support computers). Further, in some embodiments, the account tokens communicated to the external entity is generated specific for the external entity. For example, when a merchant is enrolled with a tokenization service, the merchant is assigned a merchant verification value and token derivation key. Thereafter, subsequent communications between a merchant computer and a tokenization server may cause the tokenization server to generate an account token specific to the merchant by using the assigned token derivation key.

To illustrate, when a consumer swipes a credit card at a merchant's store to purchase an item, a bank associated with the merchant may send an authorization request message with a particular account identifier and the merchant verification value assigned to the merchant to the payment processing network. In generating an authorization response message, a tokenization server associated with the payment processing network may select the token derivation key assigned to the merchant (as may be determined by matching a merchant verification value included in the authorization request message to a previously assigned token derivation key) and then generate an account token of the account identifier using the token derivation key. The account token is then inserted in the authorization response message, which is then sent back to the merchant via the bank.

A similar technique can be used to communicate account tokens to support systems, as is further described below.

By communicating an account token to the merchant, example embodiments can provide comparatively secure communication and comparatively secure storage for sensitive information, such as the cardholder data (e.g., credit card number) and other financial information. For example, if a fraudster hacks into the merchant's systems, the account tokens of the account identifiers stored by the merchant will not be useful to the fraudster because the account tokens can not be used alone to conduct financial transactions. That is, the fraudster will be unable to use the account tokens to perform financial transactions.

In some embodiments, a merchant and/or support system does not have access to the reverse token derivation keys needed to transform the account tokens to the corresponding account identifiers. Instead, a tokenization server stores the reverse token derivation keys. Therefore, the risk of compromised cardholder data is further limited in that a fraudster may have to breach the merchant and/or support system to obtain the account tokens and may also have to breach the tokenization server to obtain the reverse token derivation keys. Furthermore, even if the account tokens are compromised for a particular merchant and/or support system (e.g., if the fraudster obtains both the account tokens and reverse token derivation keys), the account tokens for other merchants and/or support systems may remain inaccessible to the fraudster.

Still further, because an account token is received in the authorization response message in addition to or in lieu of the actual account identifier, the apparatuses, methods, and systems described herein also reduce merchant post-processing efforts needed to support encryption or hashing of the account numbers after the authorization response message is received.

As a further advantage, the merchant can use the tokenized account identifier to conduct customer analytics in lieu of the original card identifier. Once the card account numbers are removed from the merchant's systems (often during or after the daily batch sales draft clearing process), the merchant can retain the tokenized account identifier for future analytics and customer tracking, while simultaneously complying with security standards (such as Payment Card Industry Data Security Standard (PCI DSS)) and reducing risk of damaging data breaches. For example, in order to maximize sales, merchants often have the need to perform customer activity tracking and segmentation/spend analyses using sales history. However, using the account identifier to identify customers requires long-term storage of cardholder account identifiers, potentially leading to increased data breach risk and security standards non-compliance. Embodiments of the invention provide a method to tokenize the account identifier so that it can be used in lieu of the actual account identifier to perform merchant customer analytics.

In another example, embodiments of the invention may facilitate customer analytics that allow merchants to measure velocity of purchases (e.g., if five transactions occur within a relatively short time period over a disperse geographic area). Based on an application observing the account tokens, the merchant may deny selected transactions if the merchant

detects a suspicious velocity pattern, even if the transaction is authorized by the payment processing network.

In another example, embodiments of the invention may facilitate customer analytics that allow merchants to measure the velocity of purchases to provide various customer loyalty services. For example, based on an application observing the account tokens, the merchant may provide a benefit to repeat customers (e.g., if a customer purchases the same product on five occasions, the merchant can provide the customer with an additional product at no cost).

I. Exemplary Payment System

Example embodiments are typically implemented in the context of a payment transaction. Therefore, prior to further discussing the use of a tokenization server configured to provide account tokens, a brief description of standard consumer purchases will be presented.

An exemplary system **100** for embodiments of the invention can be seen in FIG. **1**. For simplicity of discussion, only one of each component is shown. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than all of the components shown in FIG. **1**. Also, the components in FIG. **1** may communicate via any suitable communication medium (including the internet), using any suitable communication protocol.

FIG. **1** shows a system **100** that can be used in an embodiment of the invention. The system **100** includes a merchant computer **120** and an acquirer computer **130** communicatively coupled to the merchant computer **120**. In a typical payment transaction, a consumer **110** may purchase goods or services at a merchant associated with the merchant computer **120** using a portable consumer device **115**. The acquirer computer **130** can communicate with an issuer computer **160** via a payment processing network **140**.

The consumer **110** may be an individual, or an organization such as a business that is capable of purchasing goods or services.

The portable consumer device **115** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). The portable consumer device **115** can include a processor, and memory, input devices, and output devices, operatively coupled to the processor. Specific examples of portable consumer devices include cellular or wireless phones, personal digital assistants (PDAs), pagers, portable computers, smart cards, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a pre-paid or stored value card).

The payment processing network **140** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization request messages and in some instances also performs clearing services, and a Base II system which performs clearing services in instances when it is not performed by the VIP system.

The payment processing network **140** may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **140** may use any suitable wired or wireless network, including the Internet.

The merchant computer **120** may also have, or may receive communications from, an access device **125** that can interact with the portable consumer device **115**. The access devices **125** according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers, automated teller machines (ATMs), virtual cash registers, kiosks, security systems, access systems, and the like.

If the access device **125** is a point of sale terminal, any suitable point of sale terminal may be used including card or phone readers. The card or phone readers may include any suitable contact or contactless mode of operation. For example, exemplary readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer devices **115**.

In a typical purchase transaction, the consumer **110** purchases a good or service at the merchant associated with the merchant computer **120** using the portable consumer device **115** such as a credit card or mobile phone. The consumer's portable consumer device **115** can interact with an access device **125** such as a POS (point of sale) terminal communicatively coupled to the merchant computer **120**. For example, the consumer **110** may swipe the credit card through a POS terminal or, in another embodiment, may take a wireless phone and may pass it near a contactless reader in a POS terminal.

An authorization request message may then forwarded by the merchant computer **120** to the acquirer computer **130**. After receiving the authorization request message, the authorization request message may then be sent to the payment processing network **140**. The payment processing network **140** may then forward the authorization request message to the issuer computer **160** associated with the portable consumer device **115**.

As shown in FIG. **1**, the payment processing network **140** can be communicatively coupled to a support computer **150**. The support computer **150** can perform functions that support or supplement the authorization process. Fraud scoring system, alert systems, reporting systems, etc are examples of support computers, according to various embodiments.

After the issuer computer **160** receives the authorization request message, the issuer computer **160** may send an authorization response message back to the payment processing network **140** to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing system **140** may then forward the authorization response message back to the acquirer computer **130**. The acquirer computer **130** may then send the response message back to the merchant computer **120**.

After the merchant computer **120** receives the authorization response message, the access device **125** communicatively connected to the merchant computer **120** may then provide the authorization response message for the consumer **110**. The authorization response message may be displayed by the POS terminal, or may be printed out on a receipt.

During the lifecycle of a transaction, the payment processing network **140** may generate account tokens of the account identifiers sent in the authorization request message. In some embodiments, an account token **128** can be generated and sent to the merchant computer **120** and/or the acquirer computer **130**. The merchant computer **120** and/or acquirer computer **130** can store the account token **128** in account token

database **126**. In other embodiments, an account token **158** can be generated and sent to a support computer **150**. The support computer **150** can store the account token **158** in account token database **156**.

At the end of the day, a normal clearing and settlement process can be conducted by the payment processing network **140**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position. During the clearing process, the acquirer computer **130** can send the account token **128** to the payment processing network **140**. The payment processing network **140** may then use the reverse token derivation key for the particular merchant to retrieve the corresponding account identifier. The payment processing network **140** can send the account identifier to the issuer computer **160** to perform clearing and settlement. In some embodiments, clearing and settlement can occur simultaneously.

Once clearing and settlement are performed, the merchant computer **120** may remove the account identifiers stored in their systems. In other embodiments of the invention, as described herein, the merchant computer **120** can receive account tokens in lieu of account identifiers, thus eliminating the need to remove account identifiers stored in the merchant's systems. As an advantage of embodiments of the invention, the merchant computer **120** may retain the account tokens, thereby allowing customer analytics, as described above.

II. Tokenization Server

FIG. **2** is a block diagram that shows components of the payment processing network **140**, according to embodiments of the invention. As shown, the payment processing network **140** includes a tokenization server **220**. The tokenization server **220** may be embodied by one or more computational apparatuses, which can perform the methods and process described herein. Typically, the tokenization server **220** is a computer or cluster of computers that behave as a single computer. For example, the tokenization server **220** can be a mainframe computer, a personal computer, a microprocessor, or some combination thereof. In another example, the tokenization server **220** may include one or more database servers and one or more Web servers. The tokenization server **220** may service the requests of one or more client computers.

The tokenization server **220** may include an enrollment module **222**, an authorization response module **224**, a tokenization module **226**, a normalization module **228**, and an authorization request module **230**.

The enrollment module **222** may receive requests for enrolling external entities, such as merchants and support systems, in the tokenization service provided by the payment processing network **140**. In some embodiments, the enrollment module **222** may assign an identifier to an external entity that is successfully enrolled in the tokenization service. For example, a merchant may be assigned a merchant verification value which is sent in subsequent authorization request messages sent to the payment processing network. The merchant verification values assigned to merchants can be stored in MVV database **242**. Alternatively, a support system may be assigned a support system verification value that uniquely identifies the support system. The support system verification values assigned to support systems can be stored in support system database **246**.

The authorization response module **224** performs a number of functions related to inserting account tokens into messages communicated between the payment processing network **140** and merchants, issuers, and acquirers. For example, according to one embodiment, the payment processing network **140** receives an authorization response messages from an issuer, processes the received authorization response message, and sends the processed authorization response message to the appropriate merchant and/or acquirer. Inserting an account token into the authorization response message by the authorization response module **224** is an example of one type of processing the payment processing network **140** performs. The authorization response module **224** can receive account tokens from the tokenization module **226**.

The tokenization module **226** may generate the account tokens that are used in the embodiments described herein. In one embodiment, the tokenization module **226** generates account tokens based on an merchant verification value received in an authorization request message. For example, the tokenization module **226** may use the merchant verification value as an index into a token derivation key database (as is discussed below) to obtain a token derivation key assigned to the merchant. Once the token derivation key is obtained, the tokenization module **226** can then generate the account token by applying the account identifier to an encryption or hash function, with the merchant's token derivation key as a parameter. This and other techniques are described in greater detail below.

The normalization module **228** may provide facilities that allow the payment processing network **140** to transform an account token from a first account token form to a second account token form. Such may be an advantage for comparing the account tokens received by two or more merchants. This is because the account tokens generated by the tokenization module **226** are merchant specific. As explained below, the normalization module **228** may provide a scheme for generating an account token common to one or more merchants to provide for comprehensive analytics and services, as may be provided by merchant support systems.

The authorization request module **230** may perform a number of functions related to receiving and forwarding authorization request messages. As part of receiving an authorization request message, the authorization request module **230** may forward the authorization request message to the issuer computer **160** or to the support computer **150**. Alternatively, the payment processing network **140** can forward the authorization request message to the issuer computer **160** or to the support computer **150** without using the authorization request module **230**.

Further, the tokenization server **220** may have access to one or more databases of information. As shown in FIG. **2**, the tokenization server **220** may have access to a MVV database **242**, a TDK database **244**, and a support system database **246**. The MVV database **242** can store merchant verification values that are assigned to merchants that enroll in the tokenization services. As discussed above, a merchant verification value is one example of a merchant identifier and other suitable identifiers can also be used in other embodiments of the invention.

The TDK database **244** may store the token derivation keys that are assigned to merchants enrolled in the tokenization services. As described above, a token derivation key can be in any number of suitable forms using, for example, symmetrical or asymmetrical key algorithms. Further, as described above, in some embodiments, the tokenization server **220** can update the token derivation key assigned to a merchant at various points in time. For example, the tokenization server **220** may update a merchant's token derivation key if a fraudster compromises the account token data stored at a merchant. To provide such dynamic updates, the TDK database **244** can associate a token derivation key index with the assigned token derivation key.

The support system database **246** may store information regarding the support systems communicatively coupled to the payment processing network. For example, each support system may be assigned a unique support system verification value at the time that the support system is deployed or, in some embodiments, the support system may perform an enrollment process. Additionally, the support system database **246** may store information on whether the support system is capable of receiving account tokens rather than the account identifiers. In this way, the process of connecting support systems to the payment processing network can be achieved dynamically. Such dynamic connections can be implemented according to various system architectures, such as a directory service, event based systems, or any other scalable architecture.

III. Provisioning Account Tokens to External Parties

As described above, some embodiments of the present invention relate to a tokenization server that generates account tokens of account identifiers for merchants. Other embodiments of the present invention relate to a tokenization server that generates account tokens of account identifiers for support systems of a payment processing network. Further, there are still other embodiments where the tokenization server provides facilities for providing account tokens to a support system of one or more merchants. These various embodiments are described separately below. In particular, Section IV describes various embodiments for generating and sending account tokens to merchants, Section V describes various embodiments for generating and sending account tokens to support systems of the payment processing network, and Section VI describes various embodiments for generating and sending account tokens to merchant support systems.

IV. Provisioning Account Tokens to Merchants

FIG. **3** is a block diagram that illustrates a simplified system **300** that provides account tokens to merchants. In particular, the system includes a first facility for registering a merchant and a second facility for sending an account token in an authorization response message that was generated in response to an authorization request message. The operation of the system **300** is described with reference to FIG. **7**, which shows a flow diagram for a method **700** of sending an account token to a merchant.

A. Merchant Registration

In some embodiments, the merchant computer **120** may transmit a registration request message M**302** to the tokenization server **220**. This is shown as step S**701** of FIG. **7**. The registration request message may include registration information, such as a merchant name, merchant category type, merchant location, contact information, account information, and any other suitable information. The registration information may be transmitted via offline communication channels (e.g., via a telephone) or online communication channels (via software interfaces communicating over the network, for example).

Responsive to receiving the registration request message M**302**, the payment processing network **140** may assign the merchant a merchant verification value (MVV), if a MVV is not already assigned. With respect to FIG. **7**, this is shown as step S**704**. The MVV may be used by the payment processing network **140** to identify the merchant and information corresponding to the merchant. The MVV can be generated and maintained by the payment processing network **140** in MVV database **242** to identify the merchant. The payment processing network **140** may communicate the assigned MVV to the merchant.

In addition to assigning the MVV, the payment processing network **140** may generate a token derivation key (TDK) corresponding to the merchant and/or the MVV (message M**304**). With regard to FIG. **7**, this is shown as step S**706**. As described above, and further explained below, the TDK may be a piece of information used by the tokenization module **226** to generate an account token. The payment processing network **140** may assign a unique TDK for each merchant registered in the tokenization service. In an example embodiment, the payment processing network **140** may store and maintains the TDK in database **244**.

By assigning the TDK to the MVV, the payment processing network **140** provides an additional layer of security to the tokenization algorithm. To illustrate, in the event that a fraudster is able obtain the TDK assigned to merchant **120**, the account token databases maintained by other merchants will be secure. Such is the case because the TDK of one merchant can not be used to reverse tokenize the account tokens generated for other merchants.

In addition to generating the TDK, some example embodiments may generate a TDK index associated with the TDK. The TDK index may allow identification of a particular TDK for those embodiments that may generate multiple or subsequent TDKs for a given MVV. The TDK index and supporting multiple TDKs per merchant are described further below.

A merchant may only need to register once, and after completion of the registration process, subsequent communications with the merchant and or the acquirer of the merchant may include the account token rather than the less secure account identifier, as will be further described below.

B. Authorization

Once a merchant is registered in the tokenization service, a payment processing network may transmit an account token in communications exchanged with the merchant and/or acquirer. One situation that the payment processing network may transmit the account token to the merchant and/or acquirer is in the authorization process, for example, when a consumer's credit card is swiped at a POS terminal located at the merchant site. When the consumer's credit card is swiped, the acquirer computer **130** may transmit an authorization request message M**306** to the payment processing network **140**. This is shown as step S**703** of FIG. **7**. The authorization request message may be in the form of a typical authorization request message, wherein the authorization request message may include the account identifier and the MVV assigned to the merchant (e.g., as may be stored in fields 2 and 62.20 of an ISO 8583 message, respectively).

Once the authorization request message is received by the payment processing network **140** (step S**708** of FIG. **7**), the payment processing network **140** may use the MVV stored in the authorization request message M**306** to retrieve information related to the merchant. As an example, upon receipt of the authorization request message M**306**, the payment processing network **140** may utilize the MVV included in the authorization request message to determine if the merchant participates in the tokenization service. If so, the payment processing network **140** can retrieve the TDK associated with the MVV (step S**710** of FIG. **7**) and send the card account identifier and the TDK to a tokenization module **226**. This is shown as message M**308**. The tokenization module **226** may use the TDK to generate an account token based on the token derivation key (step S**711** of FIG. **7**). The tokenization module **226** may ensure that the account token is unique for each account identifier, and may guarantee that the same account identifier will generate the same account token when the same

TDK is used. The tokenizing function may also prevent, absent the TDK, recovery of the account identifier from the account token.

In example embodiments, the TDK assigned to merchant computer **120** is securely housed in the payment processing network **140**, and is not communicated or otherwise known to external parties. However, if the TDK is somehow compromised for a specific merchant (e.g., the merchant associated with merchant computer **120**), the payment processing network **140** may generate a new TDK for the specific merchant and link the generated TDK with a TDK index. In an example embodiment of the invention, the first generated TDK may be linked with a beginning index (e.g., zero or one) and each successive TDK index generated by the payment processing network may be incremented by a determinable number, such as one. Thus, the TDK index linked to the merchant's original TDK may have the value of zero, the second TDK may be linked with a TDK index with a value of one, the third TDK may be linked with a TDK index with a value of two, and so on.

In other embodiments of the invention, the TDK index is a hidden index. Examples of hidden indexes are numbers produced by a random number function or indexes that are otherwise hidden. For example, the payment processing network **140** may apply such incremental indices described above to a hash function or decryption algorithm. An advantage of using a hidden index is that it provides an additional level of separation to the tokenization scheme. This is because hidden indices hide the relationship between prior and later indices. To illustrate, in an incrementing scheme without hidden indices, a fraudster may observe that two frequently occurring account tokens may represent the same underlying account identifier if the ending of occurrences of one of the account tokens coincides with the beginning of occurrences of the other and if the TDK indices for the two account tokens are one off from each other.

The payment processing network **140** may log the TDK index for every transaction. In this way, for each transaction, the payment processing network **140** may determine the token derivation key used to generate the account token regardless of subsequent token derivation key changes. As shown in FIG. **3**, a TDK index may be sent to the tokenization module **226** (see message M**308**).

Message M**314** is an authorization request message that is sent to an issuer computer **160**. With reference to FIG. **7**, this is shown as step S**712**. In the typical case, an issuer computer **160** performs its functions by using an account identifier and, as a result, may not have a use for an account token. In such cases, the tokenization server **220** can send message M**314** independent of when the token derivation key is selected and the account token is generated. Accordingly, the steps of generating an account token can operate in parallel with the steps of sending an authorization request message M**314** to issuer computer **160** and receiving authorization response message from the issuer. This is shown in FIG. **7** as steps S**710** and S**711** are performed as part of a separate path than steps S**712** and S**714**.

When an authorization response message is received from the issuer computer **160** (step S**714**), the tokenization server **220** may embed the account token and the optional token derivation key index in the authorization response message M**310**. This embedding is shown as message M**310**.

If authorized, the payment processing network **140** may return the account token and the TDK index (if utilized by the payment processing network **140**) to the acquirer computer **130** and/or merchant computer **120** in specified fields of the authorization response message M**312**. This is shown in FIG. **7** as steps S**716**. As described above, the payment processing network **140** may also log the account token and the TDK index for the corresponding transaction.

After the acquirer computer **130** receives the authorization response message M**312**, the acquirer computer **130** may then send the authorization response message M**312** to the merchant computer **120** to be stored in token database **126**. This is shown in FIG. **7** as step S**705**.

The payment processing network optionally provides the ability for the merchant computer **120** to use the account tokens to request the account identifiers to be sent back to the merchant computer **120**. Via a mechanism (e.g., batch, online, remote web interfaces, etc.) the merchant computer **120** can submit the MVV, TDK index, and associated account token(s). The payment processing network **140** can then recover the original card account identifiers for secure transmission back to the merchant if the payment processing network **140** logged the transaction information.

An additional advantage of the embodiments is that it allows a comparatively efficient method and system to provide merchants and/merchant acquirers account tokens. In particular, once a merchant is registered, embodiments do not require separate or additional requests for tokenization. Instead, the payment processing network automatically provides an account token as part of the authorization process. Further, because the payment processing network utilizes the MVV and account identifier stored in the authentication request message (e.g., as stored in field 2 and field 62.20, respectively), embodiments may result in little, if any, changes to how authentication request messages are presently generated.

C. Multiple Merchants

As described above, the tokenization process communicates account tokens between the merchants and the payment processing network **140** as part of an authorization request and response. FIGS. **4-5** are block diagrams that show an exemplary embodiment that receives an authorization request message, generates an account token in response to receiving the authorization request message, and then inserts the generated account token in an authorization response message that is sent back to the merchant. In particular, FIGS. **4-5** highlight, among other things, how embodiments of the present invention can generate, for a single account identifier, account tokens that vary across different merchants but are consistent for the same merchant.

In particular, FIG. **4** shows merchant computer **120** sending an authorization request message M**402** to the payment processing network **140**. Authorization request message M**402** can be an authorization request message sent in response to consumer **110** swiping a credit card at the merchant's access device **125**. Alternatively, message M**402** can be an authorization request message received by the tokenization server **220** when consumer **110** makes an Internet purchase from the merchant's web site. In any case, the authorization request message M**402** can include transaction data, such as information derived from the card (e.g., the account identifier M**402**(*b*)), the terminal (e.g., the merchant verification value M**402**(*d*)), the transaction (e.g., the amount M**402** (*c*)), together with other data which may be generated dynamically or added by intervening systems (e.g., the header M**402**(*a*)). Although FIG. **4** shows the merchant computer **120** sending authorization request message M**402** to the tokenization server **220**, such messages can be sent through an acquirer computer **130**, as is described above.

In some embodiments, authorization request message M**402** can be in the form of an ISO (International Organization for Standardization) 8583 message. In other embodi-

ments, authorization request message M**402** can take the form of a web based call to a web service offered by the tokenization server **220**. For example, the authorization request message M**402** can be in the form of an XML message.

Once the tokenization server **220** receives the authorization request message M**402**, the authorization request module **230** can validate the authorization request message M**402** and then can route the authorization request message M**402** to the issuer computer **160** in the form of authorization request message M**404**. FIG. **4** shows that much of the information found in authorization request message M**402** is also included in authorization request message M**404**. Although not shown, authorization request message M**404** can include additional information, according to some embodiments. For example, some embodiments can include routing information that describe the payments systems that have received the authorization request message.

In addition to verifying the authorization request message M**402** and routing authorization request message M**404** to issuer computer **160**, the tokenization server **220** can also generate an account token for the account identifier associated with the authorization request message M**402**. The steps for generating the account token for the account identifier associated with the authorization request message M**402** can begin before the tokenization server **220** receives an authorization response message M**406**. FIG. **4** shows that authorization request message M**402**, or some portion thereof, is received by the tokenization module **226**. Once the tokenization module **226** receives authorization request message M**402**, the tokenization module **226** can search for the token derivation key associated with the merchant using the MVV of the authorization request message. For example, FIG. **4** shows that the value of the MVV of authorization request message M**402** is '1001001'. The tokenization module **226** then can search the TDK database **246** for a token derivation key associated with '1001001'. According to FIG. **4**, the TDK associated with '1001001' is 'TDKA'. Accordingly, the tokenization module **226** can access the TDK database **246** to retrieve the appropriate token derivation key associated with merchant computer **120**.

After the tokenization module **226** retrieves the token derivation key associated with the MVV, the tokenization module **226** can generate the account token for the account identifier of the authorization request message M**402**. As described above, the tokenization module **226** can use a variety of methods for generating account tokens. In one embodiment, the tokenization module **226** applies a symmetric encryption algorithm to the account identifier. The token derivation key associated with the MVV can be used as the key for the symmetric encryption algorithm.

The generated account token is then sent to and received by the authorization response module. This is shown as message M**403**.

Upon receiving the authorization request message M**404**, the issuer computer **160** can analyze the authorization request message M**404** and make a determination on whether the transaction should be authorized or not. If the issuer **160** verifies that the transaction can proceed, the issuer **160** can send an authorization response message to the payment processing network **140**. This is shown as authorization response message M**406**.

FIG. **4** shows that the account token M**403** and the authorization response message M**406** are received by the authorization response module **224**. In some embodiments, because the tokenization module **226** and the authorization request module **230** operate independently, the authorization response module **224** can receive the account token M**403** and the authorization response message M**406** in any order. When both the account token M**403** and the authorization response message M**406** are received, the authorization response module **224** can then send the authorization response message M**408** to the merchant **120**.

Authorization response message M**408** can be in any form. In some embodiments, authorization response message M**408** generally takes the form of an ISO 8583 message with account token embedded in the fields. The authorization response message M**408** may include a header M**408**(*a*) that indicates that the message is an authorization response message and a response code M**408**(*c*) to indicate whether the authorization request is authorized or denied. As described above, these are fields generally provided by the authorization response message M**406** sent by the issuer computer **160**. It should be noted that the indication that the message is an authorization request message or an authorization response message need not be included in headers **402**(*a*) and **408**(*a*), respectively. For example, as described below with respect to FIGS. **6**A-E, the messages may include a message type field **604** that specifies the message class and category of function. Returning to FIG. **4**, the authorization response module **224** can embed the account token in field M**408**(*b*) of the authorization response message M**408** that is sent to the merchant computer **120**. In some embodiments, as described below, the authorization response module **224** can also embed a token derivation key index in the authorization response message M**408** that is sent to the merchant **120** computer.

As is described in greater detail below, with reference to FIGS. **6**A-E, the format of an authorization response message storing an account token can vary according embodiments of the present invention.

After the authorization response module **224** sends the authorization response message M**408**, the authorization response message M**408** can be received by the merchant computer **120**. Although not shown in FIG. **4**, the merchant computer **120** can receive the authorization response message M**408** via the acquirer computer **130**. The merchant computer **120** can then store the account token **128**, as well as other transaction data, in analytics database **126**. The analytics database **126** does not include any indication of the account identifier used in the transaction, according to example embodiments.

If at some later point in time, the consumer **110** makes another purchase at merchant **120** with the portable consumer device **115**, the tokenization server **220** may generate an account token with the same value as the sent in authorization response message M**408**. That is, the merchant **120** may receive another account token with the value ABCDE.

However, if at some later point in time, the consumer **110** makes another purchase with the portable consumer device **115** at a different merchant, the tokenization server **220** may generate an account token with a different value. For example, FIG. **5** shows another payment transaction processed by the tokenization server **220**. As shown in FIG. **5**, authorization response messages M**502**, M**504** involve transactions using the same account identifier used in FIG. **4**. In particular, account '12345' is used to make a purchase at a merchant. However, the payment transaction involves a different merchant than the one used in FIG. **4**. This is shown in the merchant verification value of the authorization requests M**502**, M**504**, where the merchant verification value involved in the transaction is '2003004'.

In comparison to the payment transaction processed in FIG. **4**, the tokenization module **226** may receive the merchant verification value of '2003004' contained in the authorization request message M**402**. Using the merchant verifica-

tion value, the tokenization module **226** can retrieve token derivation key B from the TDK database **126**. The tokenization module **226** may then use the token derivation key B to generate the account token for the account identifier stored in the authorization request message M**502**. The tokenization module **226** can then send the generated account token to the authorization response module **224** to generate an authorization response message M**508** that is sent to merchant **121**. It is to be noted that the token **508**(*b*) may differ from the token generated for merchant computer **120**. In turn the merchant **121** can store the account token **129** in analytics database **127**. Later, the merchant **121** can use the account token **129** to perform analytics or supplementary processing.

D. Authorization Response Message Formats

As described above, an authorization response message can include an account token that is generated based on an account identifier and a merchant verification value. As is further described above, the account token can be embedded in the authorization response message in any number of ways. For example, FIGS. **6**A-E are diagrams that show different ways an account token can be embedded in the authorization response message. In particular, FIG. **6**A is a diagram showing an authorization response message **600***a* that stores an account token in a field of the authorization response message. As shown in FIG. **6**A, the authorization response message **600***a* can include a message header filed **602**, a message type field **604**, a bit map field **606**, and a number of data fields **608**.

The message header field **602** can contain basic message identifiers and routing information along with message processing control codes and flags.

The message type field **604** can specify the message class and the category of function. For example, a message type field **604** value of '0110' can indicate an authorization response message.

The bit map field **606** can specify which data fields are in an authorization response message. For example, a first bit in the bit map field **606** may indicate if a first type of data field is present in the data fields **608**, a second bit in the bit map field **606** may indicate if a second type of data field is present in the data fields **608**, and a nth bit in the bit map field **606** may indicate if a nth type of data field is present in the data fields **608**. A bit map field can be of any size. In example embodiments, a bit map field is a 64-bit field.

The data fields **608** can include any number fields used to process a message. For example, some fields may indicate a response code (e.g., whether a payment request is authorized or rejected). In particular, the data fields **608** can include an account token field **610**. The account token field **610** can store the account token corresponding to an account identifier sent via a corresponding authorization request message. It is to be noted that when an account token field is present in the authorization response message, an appropriate bit in the bit map field **606** can be set.

Alternatively, an authorization response message can include a token derivation key index associated with the token derivation key used to generate the account token. As described above, providing a token derivation key index to the merchant computer allows the merchant computer to request the tokenization server **220** to return back the account identifier associated with the account token. FIGS. **6**B, **6**C, and **6**D are diagrams showing authorization response messages **600***b*, **600***c*, **600***d* that store a token derivation key index. For example, as shown in FIG. **6**B, an account token and a token derivation key index can be stored in single data field **620** as sub-fields **622**, **624** of authorization response message **600***b*. According to some embodiments, sub-fields **622**, **624** can be of predetermined length. Alternatively, as shown in FIG. **6**C, the account token and token derivation key index can be stored in a single data field **630** of authorization response message **600***c* but may include a separation symbol **632** to indicate where within data field **630** the account token ends and the index begins (or vice versa). Although the separation symbol **632** is shown to be a '/', it is to be appreciated that any other suitable symbol can be used. Using a separation symbol allows for variable length account tokens and token derivation indexes. Still further, in other embodiments, as shown in FIG. **6**D, the account token and token derivation key index can be stored in separate data fields **640**, **642** of the authorization response message **600***d*. Accordingly, the bit map field **644** of the authorization response message **600***d* may include a first indication that the account token field **640** is present and a second indication that the token derivation key index data field **642** is present.

FIGS. **6**A-D describe authorization response message formats that rely on structured placement of the account token and/or index. However, other embodiments can use techniques that provide greater flexibility for the location and content of the data fields stored in the authorization response message. For example, FIG. **6**E shows a simplified diagram illustrating a markup representation of the authorization response message. Instead of relying on a bit map, such as may be present in FIGS. **6**A-D, the authorization response message can be sent in a form that uses tags to identify data and attributes to describe characteristics of the data. For example, the authorization response message can include a message tag **652** to identify that the message is an authorization response message. Further, the message tag **652** can include a number of sub-tags to represent the various fields of the authorization response message. As shown, field tag **651** includes a type attribute **653** and a index attribute **654**. The type attribute **653** indentifies that the type of field is a token field. The optional index attribute **654** identifies the index associated with the account token. The tag content **655** indicates the value of the account token, 'ABCDE'. Although not shown in FIG. **6**E, the field tag **651** can optionally include an end tag.

FIG. **6**E is just an example of one format for a markup representation of the authorization response message. Other embodiments can use alternative markup representations.

V. Account Identifier Substitution for Support Systems

Section IV describes techniques for communicating account tokens to a merchant computer. Such account tokens can be sent to the merchant computer during the authorization of a payment request, for example, in an authorization response message sent from the tokenization server to the merchant computer via an acquirer computer. In addition to communicating account tokens to a merchant, a tokenization server may also communicate with a number of support systems. Such support systems, as described above, may perform primary and auxiliary functions involved with authorizing, settling, and clearing transactions. The support systems may reside within a payment processing network or as an external partner that is in operative communication with the payment processing network. This section now describes methods, systems, and apparatuses for communicating an account token to these support systems.

A. System for Providing Account Tokens to a Support System

FIG. **9** is a block diagram that shows messages exchanged within a system **900** that communicates account tokens to a number of support systems. In certain embodiments, a payment processing network **140** may be in operative communication with one or more acquirer computers **130** via the Internet or some other communication medium.

In embodiments of the invention, the payment processing network **140** may be in further operative communication with a support computer **150**. The support computer **150** may perform supporting functions for the payment processing network **140** via support modules **22** and **24**. An example of a supporting function is scoring a transaction for fraud.

As an illustration of the interaction between the payment processing network **140** and the support computer **150**, a payment transaction is initiated by the acquirer computer **130** when a consumer **110** conducts a transaction with a merchant associated with merchant computer **120** via the access device **125**. As described above, the acquirer computer **130**, for example, may be operated by a banking institution that oversees an account associated with the merchant. The acquirer computer **130** may transmit an authorization request message to the payment processing network **140** and the authorization request message may be received by the tokenization server **220**. In turn, the tokenization server **220** may transmit at least some portion of the authorization request message to other systems. For example, the tokenization server **220** may transmit the account identifier to supporting module **16**. Further, the account identifier may be communicated to the support module **24** of the support computer **150**.

Although the payment processing network **140** may need the account identifier for any number of reasons, such as moving money, checking status, and reporting, some of the support computers may not. For example, a support computer may only use the account identifier as an identifier or unique index. Exacerbating security risks associated with the use of account identifiers, these support computers may store the account identifier in various databases, problem logs, dump logs, core dumps, and other similar memory storages and data structures. Thus not only is the account identifier potentially exposed to fraudsters when the account identifier is transmitted between different systems but there is also a risk that a fraudster may obtain the account identifiers by hacking into these support computer, even long after the transaction has been conducted. Accordingly, the payment processing network **140** may improve security of an account identifier by communicating account tokens rather than account identifier, where possible.

As shown in FIG. **9**, the acquirer computer **130** may communicate the account identifier to the payment processing network **140**. In particular, the tokenization server **220** may receive a primary account number **912**. If the tokenization server **220** determines that the primary account number is new to the tokenization server **220**, the tokenization server **220** may generate an account token of the account identifier. Otherwise, the tokenization server **220** can use the account token previously generated for the account identifier. The account token can be used to identify an account, account identifier, and/or a transaction. The account token may include card characteristics or, in some example embodiments, the card characteristics may be data distinguishable from the account token. The tokenization server **220** may then store the generated account token and, if present, the associated card characteristics. In some embodiments, the characteristics are updated as a change is noticed or periodically refreshed.

Once the tokenization server **220** generates or identifies the account token associated with the primary account number **912**, the tokenization server **220** may communicate the account token to the support modules that do not require the account identifier (e.g., primary account number **912**).

As part of the process of determining whether a support system requires an account identifier, the tokenization server **220** may query support system database **246** (see FIG. **2**) to determine whether the account identifier is required for a specified support system. In such an embodiment, the tokenization server **220** may lookup the support system according to a support system verification value assigned to the support module when the support module is enrolled with the tokenization server **220**. For example, support system database **246** may indicate that the support module **16** requires an account identifier while the support module **18** does not require an account identifier or can accept an account token in lieu of a account identifier. Accordingly, after making the determination, the tokenization server **220** will transmit the account identifier to support module **16** and an account token to support module **18**. A similar process can be used for the support modules **22**, **24** residing on the support computer **150**.

Alternatively, whether or not a support module requires an account identifier or can instead accept an account token may be determined by manual configuration (e.g., input received by an administrator of the payment processing network **140**) or via an application programming interface (API) of the support computer **150** that may allow the tokenization server **220** to interrogate the various support modules **22**, **24** as to their requirements as it relates to receiving an account identifier or an account token.

Embodiments of the invention provide numerous advantages in the development of secure data centers. In particular, embodiments of the invention enable the development of comparatively more secure transactions that transmit an account identifier. Embodiments of the invention can provide such results because they utilize an account token rather than sensitive data, such as the account identifier. Specifically, embodiments of the invention generate account token data that is associated with a account identifier and then communicate the account token data rather than the account identifier to the various support systems. Use of the account token data reduces the risks of communicating the account identifier to various support systems as well as storing sensitive data within such systems.

B. Method for Providing Account Tokens to a Support System

FIG. **10** is a flow diagram showing a method **1000** of providing an account token to a support system. The steps performed by the method **1000** can be performed by the tokenization server **220** or by any other suitable module of the payment processing network **140**. In alternative embodiments, one or more steps described herein can be performed by any other suitable computer system, such the issuer computer **160**, for example.

The method **1000** may begin by enrolling a support module with the tokenization server **220**. This is shown as step S**1002**. A support module may be running within the payment processing network **140** (e.g., support modules **16**, **18**) or within a support computer **150** that operates external and independent of the payment processing network **140** (e.g., support modules **22**, **24**). Enrolling a support module can involve, in some embodiments, communicatively connecting the support module to the tokenization server. For example, the support computer may offer the support module as a web service. In such cases, the tokenization server **220** (or the payment processing network **140** in general) and the support computer **150** may communicate using an APIs defined by each entity. Alternatively, the support modules may be deployed by the system administrator of the payment processing network **140**. In such cases, the support module may be deployed wholly within the payment processing network **140**, external to the payment processing network **140**, or some combination thereof. The enrollment process, whether offered as a web service or as a deployed system, may indicate whether the support module is to receive an account identifier or an

account token in later communications. Such information may be stored in the support system database **246** (see FIG. **2**) or may be accessible via an interface provided by the support module.

Once enrolled, the tokenization server **220** may receive a payment message. This is shown as step S**1004**. As used herein, a "payment message" can refer to either an authorization request message or an authorization response message, which are described above.

After receiving the payment message, the tokenization server **220** may determine if a support module can receive an account token. This is shown as step S**1006**. The tokenization server **220** can determine if the support module can receive an account token using the information received when the support module was enrolled with the tokenization server **220**. For example, the tokenization server **220** may access support system database **246** to determine whether a specific support module can receive an account token.

Step S**1008** is a decision point on whether the support module can receive an account token, as is determined in step S**1006**. If yes, step S**1010** is then performed. Otherwise, step S**1014** is performed.

Step S**1010** involves generating an account token from the account identifier included in the payment message (see step S**1004**). The tokenization server **220** may generate an account token for the account identifier using any of the methods or techniques described above. For example, the tokenization server **220** may encrypt the account identifier using any suitable encryption method. In some embodiments, a single token derivation key is used for tokenizing account identifiers for all support modules. In other embodiments, each support module, or a group of support modules, is assigned a specific token derivation key that is used to generate the account token. As described above, assigning different token derivation keys to different support modules can add an additional level of security among the different support modules.

After the account token is generated, the tokenization server **220** can then transmit an external request message to the support module, wherein the external request message includes the account token. This is shown as step S**1012**. As used herein, an "external request message" can refer to a message that is sent to the support module that causes the support module to provide its supporting function. In some embodiments, the external request message is sent according to an API provided by the support module. For example, the support module can provide a SOAP (Simple Object Access Protocol) procedure that can be used to receive and transmit information from and to the tokenization server **220**. The SOAP procedure may then provide an implementation of a web service provided by the support module. XML can be used to define the message formats for the messages sent between the support module and the tokenization server **220**. Again, examples of such procedures may relate to scoring a transaction for fraud, generating alerts to a customer or merchant, reporting, etc.

As described above, if the support module can not receive an account token based on decision step S**1008**, step S**1014** is then performed. According to step S**1014**, the tokenization server **220** transmits an external request message to the support module with the account identifier. Such an external request message can be sent according the techniques described above, as it relates to step S**1012**.

After the external request message is sent to the support module, the tokenization server **220** can receive an external response message from the support module. This is shown as step S**1016**. As used herein, an "external response message" can refer to a message that is sent back to the tokenization server **220** from the support module in response to processing the external request message. In some embodiments, the external response message is a response message sent according to a SOAP procedure call. XML can be used to define the message format of the external response message. The external response message can include an indication of the web service initiated by the external request message. For example, the external response message can include a field that indicates whether the support function completed successfully or can include specific information, such as the fraud score of a transaction.

After receiving the external response message, the tokenization server **220** can send a payment message. This is shown as step S**1018**. As described above, a payment message can be an authorization request message. For example, the tokenization server **220** may have sent the external request message to a fraud scoring system in step S**1012**. In response to receiving the fraud score in the external response message in step S**1016**, the tokenization server **220** can forward an authorization request message with the fraud score to the issuer computer **160**. The issuer computer **160** can then process the authorization request message and use the fraud score to determine whether the transaction is authorized.

Alternatively, also described above, a payment message can be an authorization response message. For example, the tokenization server **220** may have sent the external request message to a reporting system that can generate reports of transaction histories based on a number of categories. Because the reporting system is not used by the issuer computer **160** as it relates to determining whether a transaction is authorized, the tokenization server **220** can send the external request message after the tokenization server **220** receives the authorization response (e.g., in step S**1004**). Accordingly, the payment message involved in step S**1018** is an authorization response message that may be sent back to the acquirer computer.

Whether the payment message is an authorization request message or an authorization response message, the payment message may include external system data. As used herein, "external system data" can refer to any information obtained from the support module that is to be communicated to an external entity, such as a merchant computer or an issuer computer. For example, external system data can refer to an offer or reward that a consumer obtains after a predetermined number of purchases at a store. As another example, external system data can refer to a risk score that is sent to an issuer so that the issuer can determine whether to authorize the payment request.

Step S**1018** can also include determining the account identifier from the account token stored in the external system data. This step may allow the tokenization server **220** to route the payment message to the appropriate merchant computer, for example.

It is to be noted that the timing of when the various steps of the method **1000** are performed may vary according to example embodiments. For example, in some embodiments the authorization process operates independent of the function performed by the support module. In such cases, steps S**1016** and S**1018** can be performed in any order. Such may be the case where the support module merely logs transactions, for example.

VI. Provisioning Account Tokens for Merchant Support Systems

FIGS. **3**, **4**, **5**, **6**A-E, and **7** describe various embodiments that, in response to an authorization request message, send a merchant specific account token to a merchant in an authorization response message. In comparison, FIGS. **9** and **10**

describe embodiments that, in response to an authorization request message, send account tokens to a support system of the payment processing network.

Although not yet discussed, a merchant may wish to communicate its merchant specific account tokens to a support system. To illustrate, a merchant computer can use a third-party to provide risk analysis services. Accordingly, when a merchant receives an authorization response message with an account token from a payment processing network, the merchant can then send the authorization response message, or portions thereof, to the third-party service provider for further processing. Communicating the account token to the third-party service provider is comparatively secure because the account token can not be used to conduct a transaction. When the third-party service provider receives the account token, it can, for example, compare the account token against a database that stores high risk account tokens and report a risk score back to the merchant.

In order to provide improved risk analysis, it may be desirable for the third-party service provider to compare account tokens it receives from one merchant against account tokens it receives from another merchant. However, as described above, the account tokens that the payment processing network sends to the merchants are specific to that merchant. That is, for a given account identifier, the account token generated for one merchant is going to be different than the account token generated for another merchant. As a result, the third-party service provider will be unable to determine if a first account token from a first merchant and a second account token from a second merchant are associated with the same underlying account identifier. This example illustrates the difficulty of analyzing account tokens across different merchants.

FIGS. **11** and **12** illustrate various approaches that address these and other limitations for third-party support for processing account tokens across multiple merchants.

To begin, FIG. **11** is a block diagram that shows a system **1100** that includes merchants **120**, **121**, a merchant support server **1102**, and the tokenization server **220**. As shown, merchants **120**, **121** may each store account token data in their respective account token databases, **126**, **127**. Such account tokens can be obtained using the techniques described above. As a result, the account token databases **126**, **127** may each store merchant specific account token sets **126**(*a*), **127**(*a*). For simplicity of illustration, account token databases **126**, **127**, as shown in FIG. **11**, can store account tokens for each transaction. However, in other embodiments, additional information can be stored, such as a token derivation key index, and other transaction data, such as time of day, date, location, MVV, merchant category, etc.

FIG. **11** shows that account token database **126** may store account tokens for transactions T**1**-T**3** wherein the three transactions involve only two unique account tokens: '12345', which is involved in two transactions; and '67890', which is involved in one transaction. In comparison, account token database **127** may also store account tokens for transactions T**4**-T**6**, wherein the three transactions also involve only two unique account tokens: 'ABCD', which is involved in two transactions; and 'BCDE', which is involved in one transaction. Thus, based on a comparison of merchant specific account tokens **126**(*a*), **127**(*a*), it would appear that transactions T**1**-T**6** involve four account tokens (i.e., '12345', '6789', 'ABCD', and 'BCDE'), wherein two of the account tokens are each involved in two transactions (i.e., '12345' and 'ABCD'), and the remaining two account tokens are each involved in one transaction (i.e., '6789' and 'BCDE').

To enable the merchant support server **1102** to analyze the merchant specific account tokens **126**(*a*), the merchants **120** may send message M**1110**A to the merchant support server **1102**. Message M**1110**A can include the merchant verification value associated with merchant computer **120**, one or more of the merchant specific account tokens **126**(*a*), and any other transaction data. Message M**1110**A can be sent to the merchant support server **1102** in response to receiving an authorization response message from the payment processing network **140**. Such may be the case when the merchant support server **1102** is involved in the authorization process. Alternatively, the merchant computer **120** may send message M**1110**A as part of a batch processes that runs periodically or at set times.

Similarly, merchant **121** can send message M**1110**B to the merchant support server **1102** to communicate its merchant specific account tokens **127**(*a*) to the merchant support server **1102**.

When the merchant support server **1102** receives messages M**1110**A and/or M**1110**B, the merchant support server **1102** may send a normalization request message M**1112** to the tokenization server **220**. FIG. **11** shows that the normalization request message M**1112** can include multiple verification values. For example, the normalization request message M**1112** can include a verification value associated with the merchant support server **1102** (e.g., SSVV). The tokenization server **220** can use the verification value associated with the merchant support system **1102** to identify the requester of the normalization request. Further, FIG. **11** shows that the normalization request message M**1112** can include a merchant verification value associated with a merchant (e.g., MVV**1** or MVV**2**) and merchant specific account tokens.

Once the tokenization server **220** receives the normalization request message M**1112**, the tokenization server **220** can authorize the request to normalize the account token. In one embodiment, prior to sending message M**1110**A, merchant **120** can register the merchant support server **1102** as a trusted support system. In this case, the tokenization server **220** can store this relationship in the support system database **246**. Accordingly, in one embodiment, the tokenization server **220** can search the support system database **246** using the merchant verification value assigned to the merchant to determine whether the merchant previously registered the merchant support server **1102** as a trusted support system. Alternatively, in another embodiment, the tokenization server **220** can search the support system database **246** using the verification value of the merchant support server **1102** to determine whether the merchant previously registered the merchant support server as a trusted support system.

After the tokenization server **220** determines that the merchant support server **1102** is authorized to normalize the account token data, the tokenization server **220** can reverse tokenize the merchant specific account tokens to obtain the account identifier. In an example embodiment, the normalization module **228** (see FIG. **2**) can normalize the account tokens. For example, with regard to merchant **120**, the normalization module **228** can use the merchant verification value of the merchant **120** (e.g., MVV**1**) to search the TDK database **244** to find the token derivation key associated with merchant **120**. Once the appropriate token derivation key is located, the normalization module **228** can then reverse tokenize the account token using the token derivation key assigned to merchant **120**. This process is appropriate for those embodiments that use symmetric derivation keys. For embodiments that use asymmetric derivation keys, the TDK database **244** may store a token reverse key, which is similarly associated with the merchant verification value. Accordingly,

rather than reverse tokenizing the account token with the token derivation key, the normalization module **228** can reverse tokenize the account token into the account identifier with the token reverse key. Whether a token derivation key is symmetric or asymmetric, a token derivation key index may also be required to reverse tokenize the account token.

The above described approach can be used with respect to any other merchant, such as merchant **121**, and the other merchant's account tokens.

Once the normalization module **228** transforms the account tokens back to the underlying account identifiers, the normalization module **228** then searches the TDK database **244** for the token derivation key assigned to the merchant support system **1102**. With the token derivation key assigned to the merchant support system **1102**, the normalization module **228** can then generate new account tokens of the account identifiers. This new set of account tokens can be referred to as normalized account tokens.

After the normalization module **228** generates the normalized account tokens, the tokenization server **220** then sends the normalized account tokens to the merchant support server **1102**. This is shown as message M**1114**, as a normalization response message. The merchant support server **1102** can store the normalized account tokens in the normalized account token database **1104**. As shown in FIG. **11**, the normalized account token database **1104** stores normalized account tokens **1104**(*a*) that correspond to the six transactions in the merchant account token databases **126**, **127**. However, rather than linking the six transaction with the merchant specific account token (e.g., **126**(*a*) and **127**(*a*)), the transactions are linked to the normalized account tokens **1104**(*a*).

As FIG. **11** shows, the normalized account tokens **1104**(*a*) provides additional insight into the six transactions conducted by merchants **120**, **121**. For example, as described above, a comparison of merchant specific account tokens **126**(*a*), **127**(*a*) does not indicate that transactions **1** and **4** were conducted with the same account identifier because the respective account tokens differ (e.g., '12345' and 'ABCD', respectively). However, based on the normalized account tokens **1104**(*a*), it is clear that transaction **1** and transaction **4** were conducted with the same account identifier because both transactions involve the same normalized account token, (i.e., '54321'). Further, after normalization, the normalized account tokens **1104**(*a*) stored in the normalized account token database **1104** indicate that the six transactions are actually conducted with only two different account identifiers.

The normalization approach described above provides a number of additional advantages. For example, because systems external to the payment processing network store account tokens rather than account identifiers, these systems do not have to provide costly safety systems to ensure they comply with various security standards. In particular, the merchant support server **1102** can be completely shielded from receiving or even communicating account identifiers.

The approach described with respect to FIG. **11** may be well suited for situations that involve batch processing. For example, the merchant support system **1102** may provide a rewards program across merchants. As such, its support function may be run nightly, weekly, monthly, etc. However, because the technique described in context with FIG. **11** involves additional messages communicated between a merchant support system **1102** and the tokenization server **220**, such an approach may not be appropriate if the merchant needs a real time response, such as a fraud alert.

FIG. **12** is a block diagram that shows an alternative approach for normalizing merchant specific account tokens to allow a merchant support server **1102** to compare account tokens across multiple merchants. Compared to system **1100**, the system **1200** shown in FIG. **12** may be better suited for real time analysis offered by the merchant support server **1102**.

In some embodiments, before the tokenization server **220** can provide a normalized account token for account identifiers involved in transactions with merchant **120**, merchant **120** may enroll the merchant support server **1102** as a support system of merchant **120**. This is shown as message M**1210**A. Message M**1210**A can include the merchant verification value of the merchant **120** and a support system verification value for the merchant support server **1102**. For example, merchant **120** may be assigned the merchant verification value 'MVV**1**' and the third party support system **1102** can be assigned the support system verification value 'SSVV'. When a merchant enrolls a merchant support server as a service system of the merchant, the tokenization server **220** creates an association between the verification value of the merchant and the verification value of the merchant support server **1102**. As shown in FIG. **12**, record **1204** of normalization database **1207** may link various information used to tokenize account identifiers for merchant computer **120**. For example, the merchant verification value (e.g., 'MVV**1**') assigned to the merchant computer **120** can be linked to token derivation key (e.g., 'Key A') assigned to merchant **120**. Further, after enrolling the merchant support server **1102** as a support system of the merchant **120**, the record **1204** may include a support system verification value (e.g., 'SSVV') assigned to the merchant support server **1102**.

The record **1205** may include various information used to transform the account identifiers into a normalized account token. For example, the support system verification value (e.g., SSVV) can be linked to a token derivation key (e.g., Key C) that is used to tokenize account identifiers in a format specific to the merchant support server **1102**. Records **1204**, **1205** can be indexed by any suitable field, such as merchant or support system verification value.

Although FIG. **12** shows database **1207** storing the associations between the merchant verification values, support system verification values, and token derivation keys, it is to be appreciated that any combination of the databases **242**, **244**, and **246** (see FIG. **2**) can be used to store such information.

Merchant **121** can enroll the merchant support server **1102** as a support system in a similar manner.

Once the merchant support server **1102** is enrolled as a support system for the merchants, merchant **120** can send an authorization request message to the tokenization server **220** in the typical fashion, as may occur when a consumer swipes their credit card at a POS terminal. This is shown as message M**1212**A. The authorization request message can include information shown in FIG. **4**. For example, the authorization request message may include the merchant verification value assigned to merchant **120** and an account identifier. Upon receiving the authorization request message M**1212**A, the tokenization server **220** can process the transaction as described above. That is, the authorization request M**1212**A can be received by the authorization request module **230**. The authorization request module **230** can then forward the authorization request message to the issuer computer **160** of the portable consumer device **115**. In parallel, while the authorization request message is received by the authorization processing module **230**, the tokenization module **226** can receive the account identifier and merchant verification value stored in the authorization request message. Using the merchant verification value, the tokenization module **226** may identify

the token derivation key assigned to the merchant and then generates an account token using the token derivation key.

Additionally, the tokenization module **220** can use the merchant verification value to determine that the merchant support server **1102** is enrolled as a support system for the merchant **120**. For example, the normalization module **228** can use the merchant verification value sent in the authorization request message to search database **1207** for a record associated with the merchant. For example, record **1204** can be indexed by the merchant verification value, in which case the normalization module would match record **1204** with the merchant verification value 'MVV**1**' sent in the authorization request message. The normalization module **228** can then search record **1204** for an indication that the merchant has enrolled merchant support server **1102** as a support system. FIG. **12** shows that record **1204** includes the support system verification value assigned to the merchant support server **1102** (i.e., SSVV). As described above, this indicates that the merchant **120** has enrolled the merchant support server **1102** as a support system.

After determining that the merchant support server **1102** is a support system for merchant computer **120**, the tokenization module **226** can generate an additional account token using the token derivation key assigned to the merchant support server. This can be done by passing the support system verification value assigned to the merchant support server **1102** and the account identifier sent in the authorization request message to the tokenization module **226**. When the tokenization module **226** receives the account identifier and the support system verification value 'SSVV', it can search normalization database **1207** for the token derivation key assigned to the merchant support server **1102**. For example, the tokenization module **226** can obtain the token derivation key assigned to the support system by matching record **1205** with the support system verification value stored in record **1204** (i.e., 'SSVV'), for example. After the tokenization module **226** locates the record associated with the merchant support server **1102**, the tokenization module **226** can generate a second account token of the account identifier sent in the authorization request message using the token derivation key assigned to the merchant support server **1104**.

After the tokenization module **226** generates the account token based on the token derivation key assigned to the merchant **120** and the account token based on the token derivation key assigned to the merchant support server, the tokenization server **220** can send the account tokens to the merchant **120**. This is shown as message M**1214**A. For example, as explained above, the account token based on the merchant's **120** token derivation key can be inserted in an authorization response message. Further, the account token based on the token derivation key assigned to the merchant support server **1104** can similarly be inserted in the authorization response message.

When the merchant **120** receives the authorization response message M**1214**A, the merchant can then store the account token based on the token derivation key assigned to the merchant in token database **126**. FIG. **12** shows that account token database **126** stores the account tokens for transactions T**1**-T**3**. In addition to storing the account token based on the token derivation key assigned to the merchant **120**, the merchant **120** can also send the account token based on the token derivation key assigned to the merchant support server **1104** to the merchant support server for further processing. For example, the merchant support server **1104** can be configured to assign a risk score to a transaction. In this way, message **1216**A can be part of an authorization process used by the merchant **120**.

The techniques described above can be used by the merchant **121**. For example, merchant **121** can: register the merchant support server **1104** as a support system (M**1210**B); send an authorization request message (M**1212**B), receive an authorization response message that includes an account token based on the token derivation key assigned to merchant **121** and a key based on the token derivation key assigned to the merchant support server (M**1214**B), store the account token based on the token derivation key assigned to the merchant **121** (as shown by the merchant specific account tokens **127**(*a*) stored in account token database **127**), and send the account token based on the token derivation key assigned to the merchant support server **1104** (M**1216**B).

Further, the technique of generating account tokens in response to authorization request messages and sending the account tokens in authorization response messages can be repeated for one or more transactions. For example, as FIG. **12** shows, as was shown in FIG. **11**, merchant **120** may store merchant specific account tokens **126**(*a*) corresponding to three transactions, while merchant **121** may store merchant specific account tokens corresponding to three additional transactions. Similar to FIG. **11**, collectively, the merchant specific account tokens **126**(*a*), **126**(*b*) provide relatively little information regarding the combined transactions. However, as shown in the merchant support server **1104**, the normalized account tokens **1104**(*a*) stored normalized database **1104** illustrate that transaction **1** and transaction **4** actually involve the same underlying account identifier.

However, unlike the embodiments described with reference to FIG. **11**, embodiments according to FIG. **12** provide an improved technique for providing normalized account tokens if the normalization tokens are to be analyzed in real-time. Such is the case because the normalized account tokens are generated by the tokenization server when the tokenization server receives an authorization request message. As such, the normalized account tokens can be generated in parallel to the processing of the merchant specific account token and in parallel to the issuer processing the authorization request message.

VII. Exemplary Computer Apparatuses

FIG. **8** shows a block diagram of an exemplary computer apparatus that can be used in some embodiments of the invention (e.g., in any of the components shown in the prior Figures).

Any of the elements in figures described herein can use any suitable number of subsystems to facilitate the functions described herein. System **800** in FIG. **8** is representative of a computer system capable of embodying various aspects of the present invention. The computer system can be present in any of the elements in figures described herein, including payment processing network **140**, for example. Similarly, the various participants, entities and elements in FIG. **1** may operate one or more computer apparatuses to facilitate the functions described herein. It will be readily apparent to one of ordinary skill in the art that many other hardware and software configurations are suitable for use with the present invention.

For example, the computer may be a desktop, portable, rack-mounted or tablet configuration. Additionally, the computer may be a series of networked computers. Further, the use of other micro processors are contemplated, such as Xeon™, Pentium™ or Core™ microprocessors; Turion™ 64, Opteron™ or Athlon™ microprocessors from Advanced Micro Devices, Inc; and the like. Further, other types of operating systems are contemplated, such as Windows®, WindowsXP®, WindowsNT®, or the like from Microsoft Corporation, Solaris from Sun Microsystems, LINUX,

UNIX, and the like. In still other embodiments, the techniques described above may be implemented upon a chip or an auxiliary processing board. Various embodiments may be based upon systems provided by daVinci, Pandora, Silicon Color, or other vendors.

In one embodiment, computer system **800** typically includes a monitor **810**, computer **820**, a keyboard **830**, a user input device **845**, network interface **850**, and the like. In various embodiments, monitor **810** may be embodied as a CRT display, an LCD display, a plasma display, a direct-projection or rear-projection DLP, a microdisplay, or the like. In various embodiments, display **810** may be used to display user interfaces and rendered images.

In various embodiments, user input device **845** is typically embodied as a computer mouse, a trackball, a track pad, a joystick, wireless remote, drawing tablet, voice command system, and the like. User input device **845** typically allows a user to select objects, icons, text and the like that appear on the display **810** via a command such as a click of a button or the like. An additional specialized user input device **845**, such a magnetic stripe, RFID transceiver or smart card reader may also be provided in various embodiments. In other embodiments, user input device **845** include additional computer system displays (e.g. multiple monitors). Further user input device **845** may be implemented as one or more graphical user interfaces on such a display.

Embodiments of network interface **850** typically include an Ethernet card, a modem (telephone, satellite, cable, ISDN), (asynchronous) digital subscriber line (DSL) unit, FireWire interface, USB interface, and the like. For example, network interface **850** may be coupled to a computer network, to a FireWire bus, or the like. In other embodiments, network interface **850** may be physically integrated on the motherboard of computer, may be a software program, such as soft DSL, or the like.

RAM **870** and disk drive **880** are examples of computer-readable tangible media configured to store data such user, account and transaction level data, calculated aggregated data, super keys, sub keys and other executable computer code, human readable code, or the like. Other types of tangible media include magnetic storage media such as floppy disks, networked hard disks, or removable hard disks; optical storage media such as CD-ROMS, DVDs, holographic memories, or bar codes; semiconductor media such as flash memories, read-only-memories (ROMS); battery-backed volatile memories; networked storage devices, and the like.

In the present embodiment, computer system **800** may also include software that enables communications over a network such as the HTTP, TCP/IP, RTP/RTSP protocols, and the like. In alternative embodiments of the present invention, other communications software and transfer protocols may also be used, for example IPX, UDP or the like.

In various embodiments, computer **820** typically includes familiar computer components such as a processor **860**, and memory storage devices, such as a random access memory (RAM) **870**, disk drive **880**, and system bus **890** interconnecting the above components.

In some embodiments, computer **820** includes one or more Xeon™ microprocessors from Intel Corporation. Further, in the present embodiment, computer **820** may include a UNIX-based operating system.

It should be understood that embodiments of the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software

Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a non-transitory computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such non-transitory computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

The above descriptions are illustrative and are not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention. For example, any of the above described analytics may be combined with any other suitable analytics in any suitable manner in methods or systems according to embodiments of the invention. Thus, although specific features are separately described in this application, they may be combined in certain embodiments of the invention.

A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

What is claimed is:

1. A method comprising:

receiving, by a tokenization server, a registration request message from a merchant computer;

assigning, by the tokenization server, a merchant verification value and a token derivation key to a merchant associated with the merchant computer;

storing, by the tokenization server, the token derivation key and the merchant verification value in a database;

receiving, by the tokenization server, an authorization request message for a transaction that includes an account identifier and the merchant verification value, wherein the authorization request message is sent by the merchant computer;

sending, by the tokenization server, the authorization request message to an issuer computer for authorization of the transaction;

receiving, by the tokenization server from the issuer computer, an authorization response message indicating whether the transaction has been authorized by the issuer computer;

retrieving, by the tokenization server, the token derivation key using the merchant verification value included in the authorization request message from the database;

generating, by the tokenization server, an account token using the token derivation key by encrypting the account identifier using the token derivation key;

inserting, by the tokenization server, the account token in the authorization response message received from the issuer computer; and

sending, by the tokenization server, the authorization response message including the account token to the

merchant computer, wherein the token derivation key is available only to the tokenization server.

2. The method of claim **1** wherein a reverse tokenization key usable to generate the account identifier from the account token is stored on the tokenization server.

3. The method of claim **1**, further comprising:

assigning a token derivation key index to the token derivation key; and

inserting the token derivation key index in the authorization response message before the authorization response message is sent to the merchant computer.

4. The method of claim **3**, further comprising:

assigning a different token derivation key to the merchant associated with the merchant computer; and

assigning a different derivation key index to the different token derivation key.

5. The method of claim **3** wherein the token derivation key index is an incremental index.

6. The method of claim **3** wherein the token derivation key index is a hidden index.

7. The method of claim **1**, further comprising:

generating, by the tokenization server, a reverse tokenization key using the merchant verification value;

receiving an account identifier request from the merchant computer, wherein the account identifier request includes the account token;

determining, by the tokenization server, the account identifier using the reverse tokenization key and the account token; and

sending the account identifier to the merchant computer.

8. The method of claim **1** wherein the account token is generated by applying the account identifier to an encryption or hash function using the token derivation key as a parameter.

9. The method of claim **1** wherein the token derivation key is a key for a symmetric encryption algorithm, and wherein generating the account token further comprises applying the symmetric encryption algorithm to the account identifier.

10. The method of claim **1** wherein the authorization response message includes a bitmap field, and wherein a bit in the bitmap field is set by the tokenization server upon inserting the account token in the authorization response message.

11. The method of claim **1** wherein the authorization response message includes a field tag that identifies a field in the authorization response message containing the account token.

12. The method of claim **1**, further comprising:

receiving, from a merchant support system server, a normalization request message, wherein the normalization request message includes the merchant verification value and the account token, and wherein the merchant support system server is associated with a merchant support system;

generating, by the tokenization server, the account identifier from the account token;

selecting a token derivation key assigned to the merchant support system;

generating, by the tokenization server, a normalized account token using the token derivation key assigned to the merchant support system; and

sending the normalized account token to the merchant support system server.

13. The method of claim **12** wherein the normalization request message further includes a support system verification value that is used to select the token derivation key assigned to the merchant support system.

14. The method of claim **12** wherein the merchant support system is associated with a fraud scoring service that provides a fraud score for the transaction.

15. The method of claim **12** wherein the merchant support system is associated with an alert service that transmits an alert to a mobile device of an account holder.

16. A server computer comprising:

a processor and

a non-transitory computer-readable storage medium coupled to the processor, the computer readable storage medium comprising code that, when executed by the processor, causes the processor to perform a method comprising:

receiving a registration request message from a merchant computer;

assigning a merchant verification value and a token derivation key to a merchant associated with the merchant computer;

storing the token derivation key and the merchant verification value in a database;

receiving an authorization request message for a transaction that includes an account identifier and the merchant verification value, wherein the authorization request message is sent by the merchant computer;

sending the authorization request message to an issuer computer for authorization of the transaction;

receiving, from the issuer computer, an authorization response message indicating whether the transaction has been authorized by the issuer computer;

retrieving the token derivation key using the merchant verification value included in the authorization request message from the database;

generating an account token using the token derivation key by encrypting the account identifier using the token derivation key;

inserting the account token in the authorization response message received from the issuer computer; and

sending the authorization response message including the account token to the merchant computer, wherein the token derivation key is available only to the server computer.

17. The server computer of claim **16** wherein a reverse tokenization key usable to generate the account identifier from the account token is stored on the server computer.

18. The server computer of claim **16**, wherein the method further comprises:

assigning a token derivation key index to the token derivation key; and

inserting the token derivation key index in the authorization response message before the authorization response message is sent to the merchant computer.

19. The server computer of claim **18**, wherein the method further comprises:

assigning a different token derivation key to the merchant associated with the merchant computer; and

assigning a different derivation key index to the different token derivation key.

20. The method of claim **19**, further comprising:

determining that the token derivation key has been compromised prior to assigning the different token derivation key to the merchant.

21. A non-transitory computer readable medium storing computer instructions when executed by a processor of a server causes the processor to perform a method comprising:

receiving a registration request message from a merchant computer;

assigning a merchant verification value and a token derivation key to a merchant associated with the merchant computer;

storing the token derivation key and the merchant verification value in a database;

receiving an authorization request message for a transaction that includes an account identifier and the merchant verification value, wherein the authorization request message is sent by the merchant computer;

sending the authorization request message to an issuer computer for authorization of the transaction;

receiving, from the issuer computer, an authorization response message indicating whether the transaction has been authorized by the issuer computer;

retrieving the token derivation key using the merchant verification value included in the authorization request message from the database;

generating an account token using the token derivation key by encrypting the account identifier using the token derivation key;

inserting the account token in the authorization response message received from the issuer computer; and

sending the authorization response message including the account token to the merchant computer, wherein the token derivation key is available only to the server.

* * * * *

Electronic Acknowledgement Receipt

EFS ID:	27935477
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	30-DEC-2016
Filing Date:	06-MAY-2013
Time Stamp:	04:18:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	juniorart.pdf	17846 0b4b771fdc9c8d1f9675a5c91070fa3bbbd20ae9	no	1

Warnings:

Information:					
2	Miscellaneous Incoming Letter	pat9519802.pdf	1192752 ce119b8b9f895736facf1b88e746c53f3332d831	no	14
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	pat9342832.pdf	2341122 b03e53d2e9bb8c1a15a33f4135a880d8ef807f77	no	31
Warnings:					
Information:					
			Total Files Size (in bytes):	3551720	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Trials@uspto.gov
571-272-7822

Paper 11
Entered: August 30, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS INC.,
Petitioner,

v.

WILLIAM GRECIA,
Patent Owner.

Case IPR2016-00602
Patent 8,887,308 B2

Before GLENN J. PERRY, RAMA G. ELLURU, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges*.

WORMMEESTER, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Unified Patents Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claim 1 of U.S. Patent No. 8,887,308 B2 (Ex. 1003, "the '308 patent"). William Grecia ("Patent Owner") filed a Preliminary Response (Paper 7, "Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." For the reasons that follow, we have decided not to institute an *inter partes* review.

I. BACKGROUND

A. The '308 Patent

The '308 patent is titled "Digital Cloud Access (PDMAS Part III)." Ex. 1003, at [54]. The '308 patent describes a digital rights management system that manages access rights across a plurality of devices via digital media personalization to protect digital media subject to illegal copying. *Id.* at 1:20–27; 4:48–49.

The system includes a first receipt module, an authentication module, a connection module, a request module, a second receipt module, and a branding module. *See id.* at Fig. 1. The first receipt module receives a branding request from a user's (content acquirer's) device. *Id.* at 5:46–48. The branding request is a read and write request of metadata of the digital media and includes a membership verification token corresponding to the digital media. *Id.* at 5:48–51. The authentication module authenticates the membership verification token. *Id.* at 5:57–58. The connection module establishes communication with the user's device. *Id.* at 5:59–61. The

request module requests an electronic identification reference from the user's device. *Id.* at 6:5–7. The second receipt module receives the electronic identification reference. *Id.* at 6:7–9. The branding module brands metadata of the digital media by writing the membership verification token and the electronic identification into the metadata. *Id.* at 6:9–12.

Figure 3, which is reproduced below, illustrates this process.

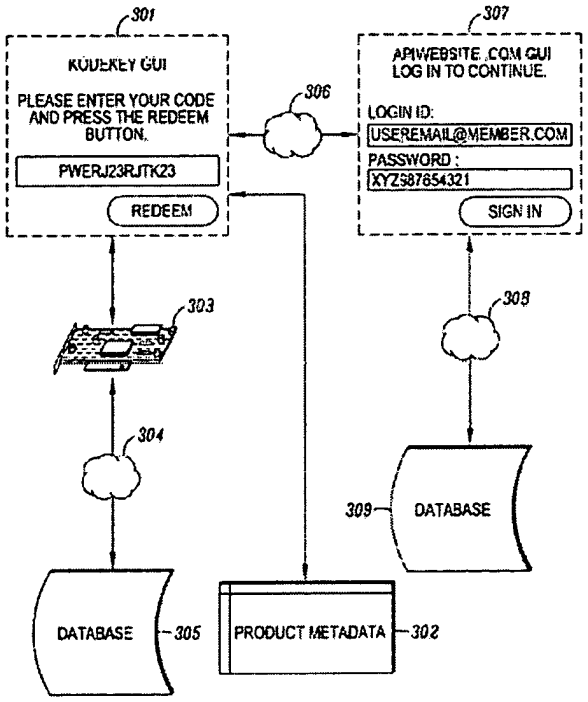


FIG. 3

In particular, Figure 3 is a flow chart of the process of digital media personalization. *Id.* at 1:21–26. A user posts a branding request via Kodekey GUI 301, which prompts the user to enter a token and press the redeem button. *Id.* at 6:66–7:4. Product metadata 302 is associated with the digital media to be acquired. *Id.* at 7:4–5. The Kodekey GUI is connected to token database 305. *Id.* at 7:7:–8. The user is then redirected to APIwebsite.com GUI 307, which prompts the user to enter a login id and password to access the digital media from database 309. *Id.* at 7:11–12, 15–

18. The APIwebsite.com GUI interfaces to a web service membership, where the user's electronic identification is collected and sent back to the Kodekey GUI. *Id.* at 7:11–15. The database containing the digital media is connected to the web service membership. *Id.* at 7:18–20.

B. Challenged Claim

Petitioner challenges claim 1 of the '308 patent, which recites:

> 1. A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:
>
> a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of:
>
> a memory connected to the at least one CPU;
>
> a storage connected to the at least one CPU; and
>
> a database connected to the at least one CPU through the Internet; wherein
>
> the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then
>
> b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then
>
> c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b) wherein the APJ is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database

apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier; then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of:

the received verification data of (a); and

the received query data of (e); wherein

the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing act ion during subsequent user access requests to determine one or more of a user access permission for the cloud digital content.

C. Asserted Grounds of Unpatentability

Petitioner challenges claim 1 of the '308 patent on the following grounds.[1] Pet. 3, 19–52.

[1] In summarizing its asserted grounds on page 3 of the Petition, Petitioner requests cancellation of claim 1 as unpatentable under 35 U.S.C § 103, but states on page 19 of the Petition that the asserted references "anticipate and/or render obvious the claimed subject matter." Given the substance of Petitioner's arguments, we address claim 1 under 35 U.S.C. §§ 102 and 103.

Reference(s)	Basis
DeMello[2]	§ 102
DeMello, Wieder,[3] and "the admitted prior art"	§ 103
Pestoni[4]	§ 102
Pestoni, Wieder, and "the admitted prior art"	§ 103

In support of its arguments, Petitioner proffers the declaration of Ravi S. Cherukuri (Ex. 1009). *See id.*

D. Claim Construction

We construe claims in an unexpired patent by applying the broadest reasonable interpretation in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs. LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard). Under this standard, claim terms are generally given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). A "claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer," however, and clearly set forth a definition of the claim term in the specification. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002).

Petitioner provides proposed interpretations for various limitations of the claims. Pet. 12–19. Patent Owner responds. Prelim. Resp. 20–24. For purposes of this Decision, we conclude that no term requires interpretation at

[2] DeMello, U.S. Patent No. 6,891,953 B1, issued May 10, 2005 (Ex. 1006).
[3] Wieder, U.S. Patent No. 8,001,612 B1, issued Aug. 16, 2011 (Ex. 1008).
[4] Pestoni, U.S. Publ'n No. 2008/0313264 A1, published Dec. 18, 2008 (Ex. 1007).

this time to resolve a controversy in this proceeding. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.").

II. DISCUSSION

A. Anticipation by DeMello

Petitioner argues that DeMello anticipates claim 1 of the '308 patent. *See* Pet. 19–39. For the reasons explained below, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing on its asserted ground.

1. DeMello

DeMello describes a digital rights management system that distributes and protects rights in content, such as electronic books (eBooks). Ex. 1006, at [57], 4:43–45. As shown in Figure 4, which is reproduced below, the system includes a retail site, a fulfillment site, and an activation site.

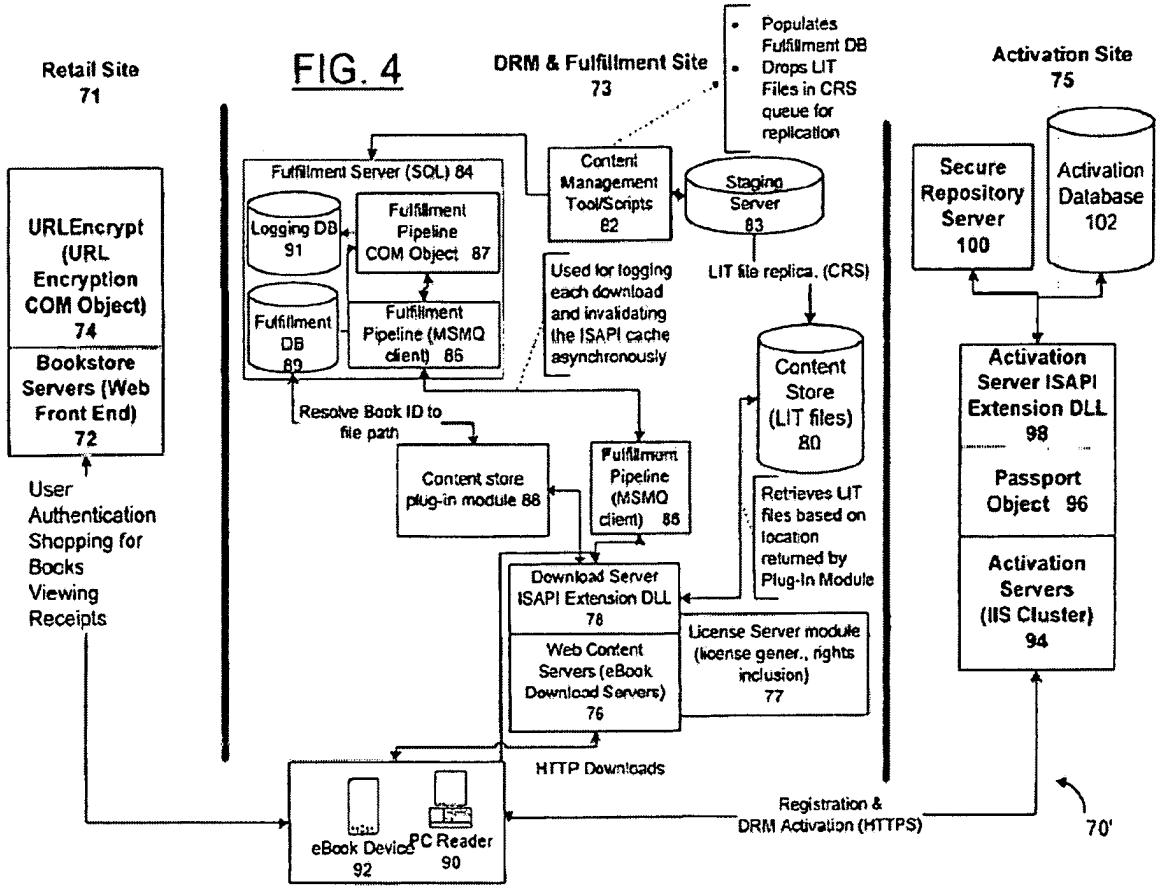


Figure 4 is a block diagram of one embodiment of DeMello's digital rights management system. *Id.* at 4:19–21. The retail site sells eBooks to consumers, the fulfillment site provides the sold eBooks to the consumers, and the activation site enables consumer reading devices to use eBooks with enhanced levels of copy protection (e.g., eBooks requiring licenses). *Id.* at [57], 6:10–16, 21:36–37.

In order to access an eBook, a consumer begins by choosing a title from the retail site and paying for the title. *Id.* at 26:1–4. The retail site then issues a receipt page with a link for downloading the title. *Id.* at 26:4–7. When the consumer clicks on the link, a download server at the fulfillment site adds the consumer's name to the title metadata. *Id.* at 26:15–23, Fig. 4. The title is then downloaded to the consumer's device, and the eBook is

opened to its cover page with the rightful owner's name appearing under the author's name. *Id.* at 26:35–36, 27:45–46.

2. Analysis

Claim 1 recites a "credential assigned to the apparatus of (a)." For this limitation, Petitioner identifies DeMello's reader (user device) as an "apparatus of (a)." Pet. 30. Petitioner further argues that "the claimed 'credential' is shown by the PASSPORT credentials of *DeMello*." *Id.* at 31.

Patent Owner counters that "DeMello's credential [is] assigned to a user—not an apparatus." Prelim. Resp. 2. We agree with Patent Owner.

Claim 1 requires the "credential" to be assigned to the *apparatus of (a)*. As Patent Owner points out, the specification of the '308 patent describes such credential as "an API Key, an Application Secret Key and could also include an Application ID," which "[is] usually embedded in the source code of the apparatus, or stored on a remote Internet server." *Id.* at 28–29 (citing Ex. 100[3], 10:51–56); Ex. 1003, 10:51–66. The apparatus, such as an Internet-powered desktop or a browser-based application, uses the API Key to establish a data exchange session with the API. Ex. 1003, 10:51–58.

By contrast, the "credential in DeMello is assigned to the user, not the device." Prelim. Resp. 28. As Petitioner explains, "[i]n *DeMello*, the reader prompts a *user* to provide login credentials (e.g., PASSPORT™ credentials) to connect to the PASSPORT server via the API of the PASSPORT server to authenticate the *user* at the PASSPORT server." Pet. 31 (emphases added); *see also* Ex. 1006, 23:6–10. Further, Mr. Cherukuri characterizes the PASSPORT credentials as "*user's* credentials." *See* Ex. 1009 ¶ 72 (cited at

Pet. 32) (emphasis added). Neither Petitioner nor Mr. Cherukuri explains persuasively how the *user* PASSPORT credentials in DeMello are assigned to the *reader* (apparatus of (a)). Based on the record presented, we are not persuaded that DeMello discloses the recited credential.

In view of the foregoing, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in showing that DeMello anticipates claim 1.

B. Obviousness over DeMello, Wieder, and the Admitted Prior Art

Petitioner argues that claim 1 of the '308 patent would have been obvious over DeMello, Wieder, and "the admitted prior art." *See* Pet. 19–39. Petitioner does not cite Wieder or the admitted prior art as teaching the elements found to be lacking in the above discussion with respect to DeMello. Accordingly, on this record, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing on its assertion that claim 1 would have been obvious over DeMello, Wieder, and the admitted prior art.

C. Anticipation by Pestoni

Petitioner argues that Pestoni anticipates claim 1 of the '308 patent. *See* Pet. 19, 39–52. For the reasons explained below, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing on its asserted ground.

1. Pestoni

Pestoni describes a system with domain management for digital media. Ex. 1007, at [57]. As shown in Figure 1, which is reproduced below, the system includes a domain administrator, a content provider, and a license server.

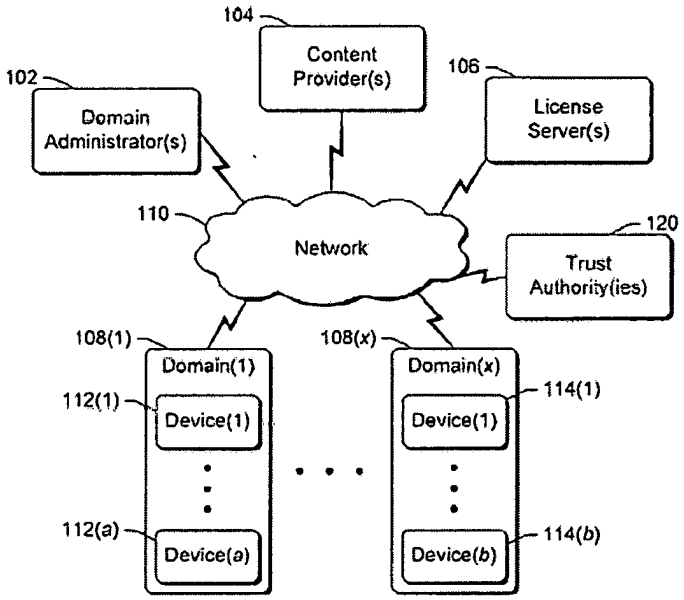


Fig. 1

Figure 1 illustrates one embodiment of a system that employs domain management for digital media. *Id.* ¶ 6. Media playback device 112 or 114 may obtain content from content provider 104 by submitting a content request to the content provider. *Id.* ¶ 67. In order to access and play back the content, the device must have a domain membership license from domain administrator 102 and a content license from license server 106. *Id.* ¶ 17.

To obtain a domain membership license, the device submits a join-domain request to the domain administrator. *Id.* ¶ 38. The request includes

parameters to identify the device, such as a device certificate, user credentials, and a device description. *Id.* ¶ 39. If the domain administrator approves the request, the device becomes a member of the domain and receives a domain membership license. *Id.* ¶¶ 38, 44.

To obtain a content license, the device submits a content license request to the license server. *Id.* ¶¶ 69, 72. The request includes parameters, such as a key ID, a domain ID, and a domain certificate, to identify both the content for which the license is being requested and the domain of which the device is a member. *Id.* ¶ 72. In response to the request, the license server validates the domain certificate, and, if successful, approves the request. *Id.* ¶¶ 75, 79. Once the request is approved, the license server generates a content license, binds the license to the domain identified in the request, and provides the device with the license. *Id.* ¶¶ 79–80, 82, 84.

2. Analysis

Claim 1 recites "requesting the query data, from the apparatus of (a), . . . wherein the query data request is a request for the at least one verified web service [account] identifier." For this limitation, Petitioner identifies Pestoni's content license request as "query data," Pestoni's domain ID as a "verified web service account identifier," and the content playback module of Pestoni's device as an "apparatus of (a)." Pet. 40, 48. Petitioner further argues that "[b]ecause the content license includes the domain ID, the content license generator 260 must necessarily request and receive the domain ID before generating the content license." *Id.* at 48–49. We note that the device (apparatus of (a)) in Pestoni sends to the license server a content license request (query data), which includes various parameters such

as a domain ID (web service account identifier). Ex. 1007 ¶ 72. The content license generator is a part of the license server. *Id.* at Fig. 2.

We are unpersuaded by Petitioner's argument, which relies on an inherency theory. *See* Pet. 49. "If the prior art reference does not expressly set forth a particular element of the claim, that reference still may anticipate if that element is 'inherent' in its disclosure." *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.'" *Id.* (citation omitted). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing *may* result from a given set of circumstances is not sufficient." *Continental Can Co. USA, Inc. v. Monsanto Co.*, 948 F.2d 1264, 1269 (Fed. Cir. 1991).

Here, the content license generator in Pestoni may *receive* the domain ID from the device (apparatus (a)). As Patent Owner points out, however, "Pestoni does not *request* information from the apparatus of (a)." Prelim. Resp. 30 (emphasis added). Nor does Petitioner proffer persuasive evidence showing that the content license generator "necessarily" requests the domain ID from the device. Indeed, Pestoni describes the content license request (query data) from the device as "optionally" including the domain ID (web service account identifier). Ex. 1007 ¶ 94. Given that the content license request may include the domain ID, we are not persuaded that the content license generator *necessarily requests* the domain ID from the device.

Based on the record presented, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in showing that Pestoni anticipates claim 1.

D. Obviousness over Pestoni, Wieder, and the Admitted Prior Art

Petitioner argues that claim 1 of the '308 patent would have been obvious over Pestoni, Wieder, and "the admitted prior art." *See* Pet. 19, 39–52. For the reasons explained below, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing on its asserted ground.

As discussed above, claim 1 recites "requesting the query data, from the apparatus of (a), . . . wherein the query data request is a request for the at least one verified web service [account] identifier." As an alternative to its anticipation argument, Petitioner argues that "it would be obvious to one of skill in the art to implement *Pestoni* with a request and corresponding reception." *Id.* at 49. Petitioner relies on testimony from Mr. Cherukuri's declaration to support this argument. *See id.* (citing Ex. 1009 ¶¶ 97–102).

We are unpersuaded by Petitioner's obviousness argument. As part of its analysis, Petitioner must provide "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). Neither Petitioner nor Mr. Cherukuri proffers any reason, however, for combining Pestoni and any other patent or printed publication to arrive at the claimed invention.

Based on the record presented, we are not persuaded that Petitioner has provided adequately articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *See Kahn*, 441

F.3d at 988. Accordingly, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in showing that claim 1 would have been obvious over Pestoni, Wieder, and the admitted prior art.

III. CONCLUSION

For the foregoing reasons, we are not persuaded that Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to the challenged claim of the '308 patent.

IV. ORDER

For the reasons given, it is

ORDERED that the Petition is *denied* as to the challenged claim, and no trial is instituted.

PETITIONER:

Paul C. Haughey
phaughey@kilpatricktownsend.com

Scott E. Kolassa
skolassa@kilpatricktownsend.com

Jonathan Stroud
jonathan@unifiedpatents.com

Kevin Jakel
kevin@unifiedpatents.com

PATENT OWNER:

Patrick D. Richards
patrick@richardspatentlaw.com

Clare Frederick
clare@richardspatentlaw.com

TO: **Mail Stop 8** **Director of the U.S. Patent & Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of CA on the following:
(X) Patents or ( ) Trademarks

DOCKET NO:
16-cv-00588-YGR

DATE FILED:
February 4, 2016

UNITED STATES DISCTRICT COURT
Ronald Dellums Federal Building
1301 Clay Street
Oakland, CA 94612

PLAINTIFF:
William Grecia

DEFENDANT:
Dish Network L.L.C.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1. 8,887,308		*******SEE ATTACHED COMPLAINT*******
2.		
3.		
4.		
5.		

In the above-entitled case, the following patent(s) have been included.

DATE INCLUDED INCLUDED BY:
( ) Amendment ( ) Answer ( ) Cross Bill ( ) Other Pleading

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1.		
2.		
3.		
4.		
5.		

In the above-entitled case, the following decision has been rendered or judgment issued:

DECISION/JUDGEMENT:

Susan Y. Soong
Susan Y. Soong, Clerk

Clara Pierce
(by) Deputy Clerk, Clara Pierce

Copy 1 – Upon initiation of action, mail this copy to Commissioner
Copy 2 – Upon filing document adding patent(s) mail this copy to Commissioner
Copy 3 – Upon termination of action, mail this copy to the Commissioner
Copy 4 – Case file copy

AO 120 (Rev. 2/99)

TO: **Mail Stop 8**
Director of the U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of CA on the following x Patents or ☐ Trademarks:

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
C 14-05650 JSC	12/30/14	450 Golden Gate Ave., 16th Fl. San Francisco, CA 94102

PLAINTIFF	DEFENDANT
WILLIAM GRECIA	AMAZON.COM INC

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	see complaint		
2	8,887,308		
3			
4			
5			

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Richard W. Wieking	Alfred Amistoso	December 31, 2014

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy

AO 120 (Rev. 2/99)

TO: **Mail Stop 8** **Director of the U.S. Patent & Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern California on the following X Patents or ☐ Trademarks:

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
CV 15-00975 MEJ	3/2/2015	450 Golden Gate Avenue, 16th Floor, San Francisco, CA 94102

PLAINTIFF	DEFENDANT
WILLIAM GRECIA	SAMSUNG TELECOMMUNICATIONS

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,887,308		
2		
3		See Attached.
4		
5		

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Richard W. Wieking	Hilary Jackson	March 4, 2015

Copy 1—Upon initiation of action, mail this copy to Commissioner **Copy 3—Upon termination of action, mail this copy to Commissioner**
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner **Copy 4—Case file copy**

AO 120 (Rev. 2/99)

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been ☐

filed in the U.S. District Court Northern District of California on the following x Patents or ☐ Trademarks:

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
CV 14-04990 WHO	11/12/14	450 Golden Gate Avenue, 16th Floor San Francisco, CA 94102

PLAINTIFF	DEFENDANT
GRECIA	APPLE INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 see complaint		
2 8,887,308		
3		
4		
5		

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Richard W. Wieking	Alfred Amistoso	November 13, 2014

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy

AO 120 (Rev. 2/99)

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Northern District of California on the following X Patents or ☐ Trademarks:

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
CV 14-05649 NC	12/30/2014	for the Northern District of California
PLAINTIFF		DEFENDANT
WILLIAM GRECIA		SONY NETWORK ENTERTAINMENT

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,887,308		
2			
3			
4			
5			

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
Richard W. Wieking	Sandy Morris	December 30, 2014

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy

Electronic Acknowledgement Receipt

EFS ID:	20955085
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	14-DEC-2014
Filing Date:	06-MAY-2013
Time Stamp:	13:03:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	Tokenization_Guidelines_Info_Supplement.pdf	558908 86cbc3b01bcc3b552f6c95bf23b6dbafd06d33a7	no	23

Warnings:	
Information:	

2	Miscellaneous Incoming Letter	EMVCo_Payment_Tokenisation_Spec.pdf	934916 d39a89fce7acb829856e50593e8277d16a4f0d07	no	84
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	EMV_Tokenization.pdf	1148454 4129ddd9e1065ae8ac35ee4b9f3671b4b6341906	no	34
Warnings:					
Information:					
			Total Files Size (in bytes):	2642278	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

DIGITAL WALLET AND TOKENIZATION STATE OF THE ART

All patent applications included in this brief are junior art to U.S. Patent #8,887,308

Key mobile wallet and tokenization patent applications presented in this disclosure:

1) eBay's PayPal digital wallet -pending
2) Google's Google Wallet -pending
3) First Data Corp tokenization (a partner of Google Wallet in 2012) -pending
4) MasterCard tokenization –pending
5) Intuit mobile wallet –pending
6) Apple's Apple Pay -pending

Document Number	Publication Date	Patentee
2011/0320345	12/29/2011	Taveau Sebastien et al.
2012/0166333	06/28/2012	von Behren Rob et al.
2012/0173431	07/05/2012	Ritchie Ben et al.
2012/0239529	09/20/2012	Low Gak Wee et al.
2012/0290376	11/15/2012	Dryer Trevor D. et al.
2012/0296741	11/22/2012	DYKES Robert
2013/0254115	09/26/2013	Pasa Mehmet et al.
2013/0297504	11/07/2013	Nwokolo Obinna et al.
2013/0299596	11/14/2013	CHOI Bong-Sik et al.
2013/0332293	12/12/2013	Ran Alexander S.
2013/0346222	12/26/2013	Ran Alexander S.
2014/0019367	01/16/2014	KHAN Ahmer A. et al.
2014/0089186	03/27/2014	Dunn Eric C. W. et al.
2014/0099886	04/10/2014	Monroe Joshua G.
2014/0214664	07/31/2014	KIM Kyungdong et al.
2014/0279566	09/18/2014	Verma Sanjeev et al.

(19) **United States**

(12) **Patent Application Publication**

Taveau et al.

(10) **Pub. No.: US 2011/0320345 A1**

(43) **Pub. Date: Dec. 29, 2011**

(54) **SMART WALLET**

(75) Inventors: **Sebastien Taveau**, Redwood City, CA (US); **Nadav Naaman**, Tel-Aviv (IL)

(73) Assignee: **eBay, Inc.**, San Jose, CA (US)

(21) Appl. No.: **13/165,180**

(22) Filed: **Jun. 21, 2011**

Related U.S. Application Data

(60) Provisional application No. 61/359,667, filed on Jun. 29, 2010.

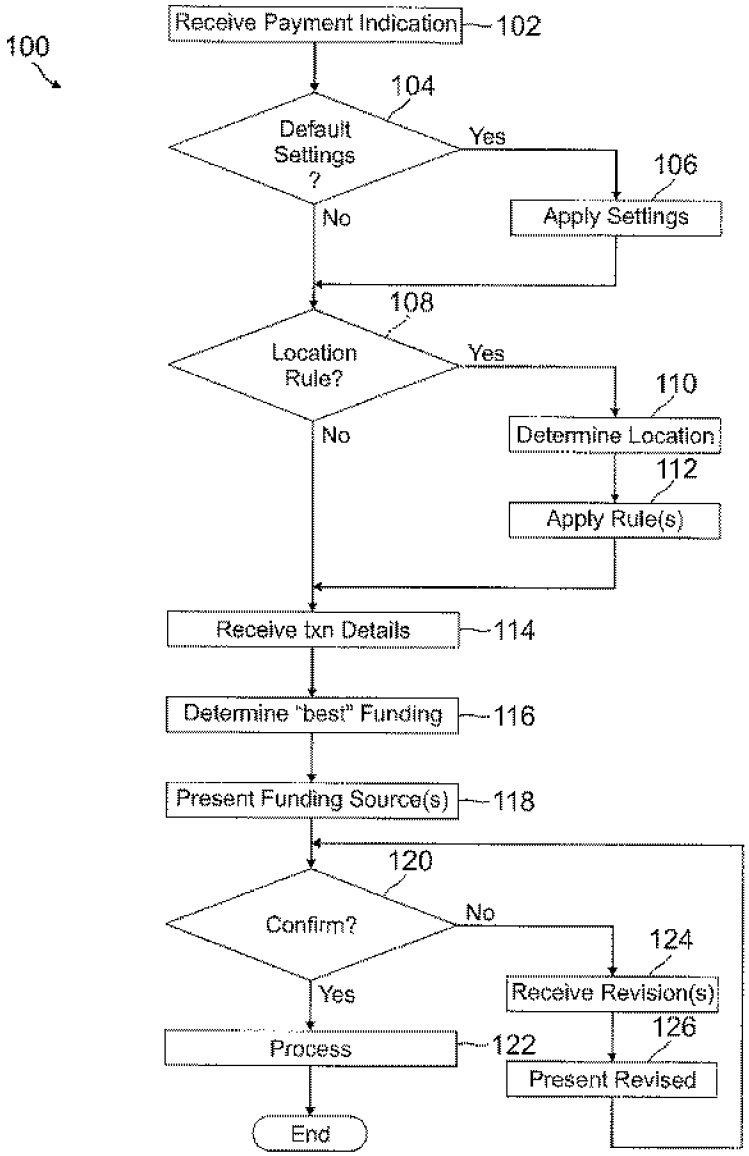
Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)
G06Q 30/00 (2006.01)

(52) **U.S. Cl.** **705/39**

(57) **ABSTRACT**

A user's smart phone is used for payments and holding information, similar to what is contained in a physical wallet. Depending on transaction details, user preferences, and location, one or more "best" funding instruments for the transaction are selected for the user, who may then revise if desired. Access to different functions or information within the phone may vary and require different authentication/security levels depending on type of use (e.g., payment or non-payment) and details of use (e.g., high payment amount vs. low payment amount, use of sensitive information vs. non-sensitive information).



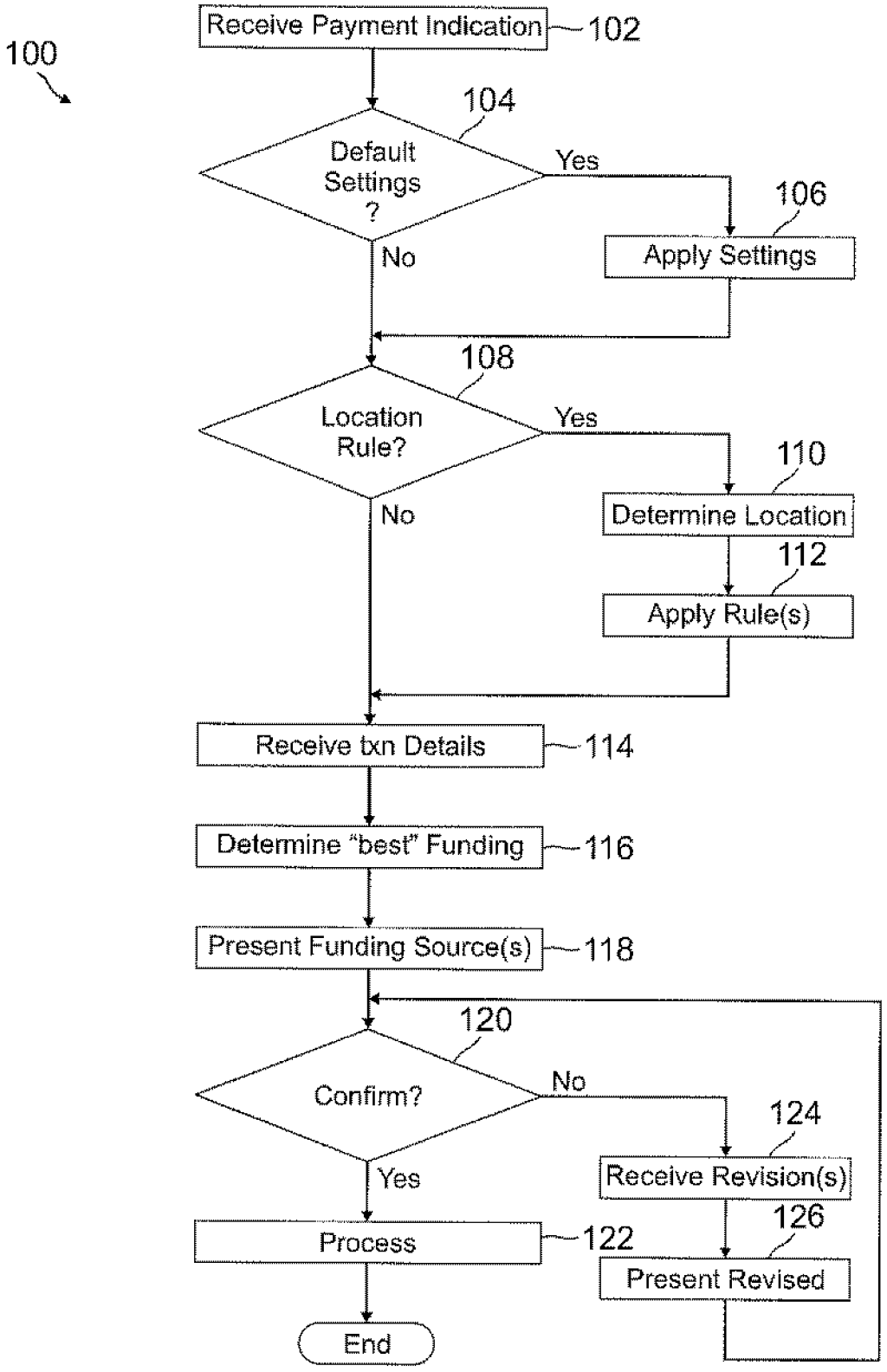

100
Receive Payment Indication
102
104
Default Settings ?
Yes
106
Apply Settings
No
108
Location Rule?
Yes
110
Determine Location
No
112
Apply Rule(s)
Receive txn Details
114
Determine "best" Funding
116
Present Funding Source(s)
118
120
Confirm?
No
124
Receive Revision(s)
Yes
126
Process
122
Present Revised
End

FIG. 1

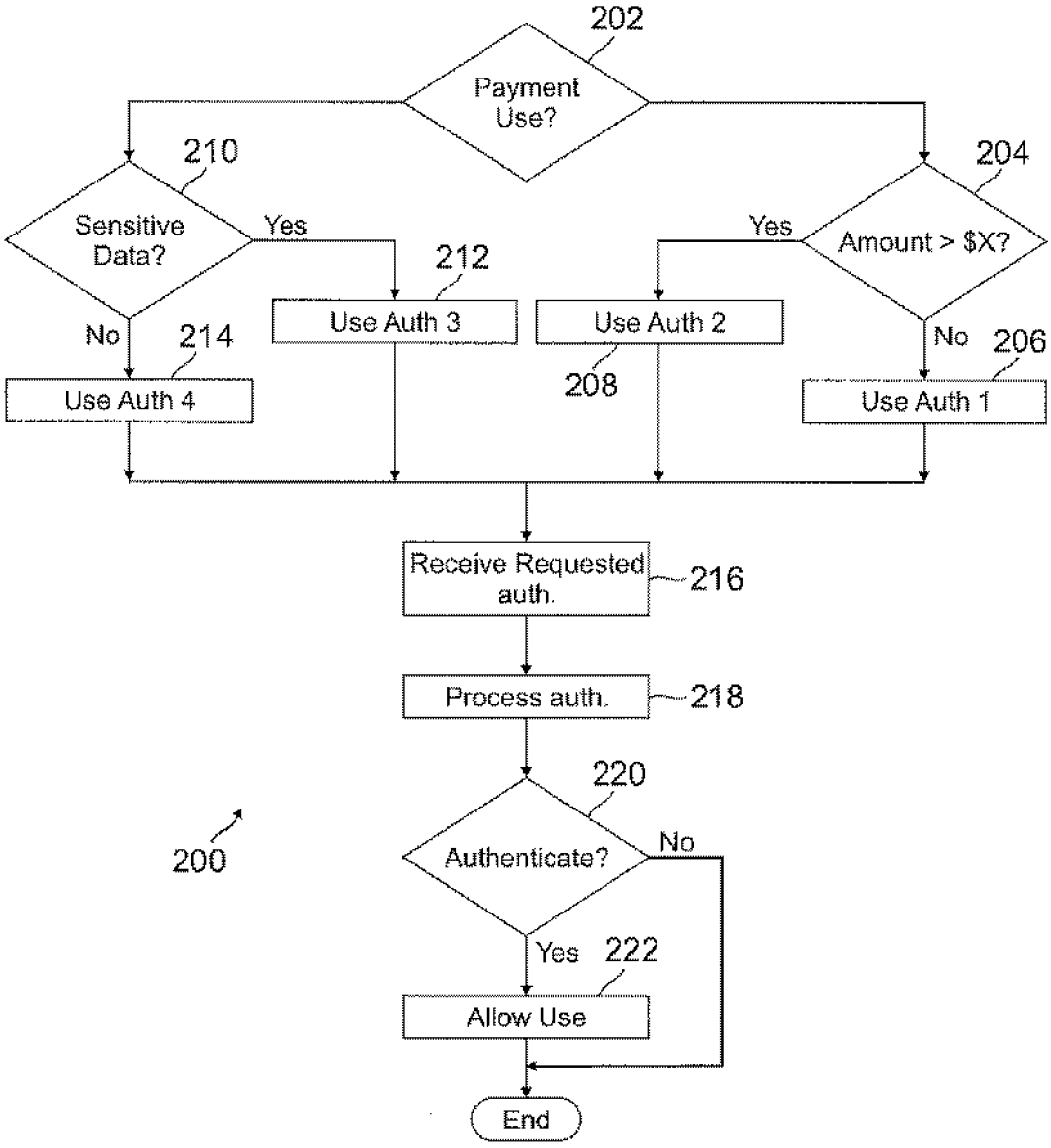

202
Payment Use?
210
Sensitive Data?
Yes
212
Use Auth 3
No
214
Use Auth 4
204
Amount > $X?
Yes
Use Auth 2
208
No
206
Use Auth 1
Receive Requested auth.
216
Process auth.
218
220
Authenticate?
No
Yes
222
Allow Use
End
200

FIG. 2

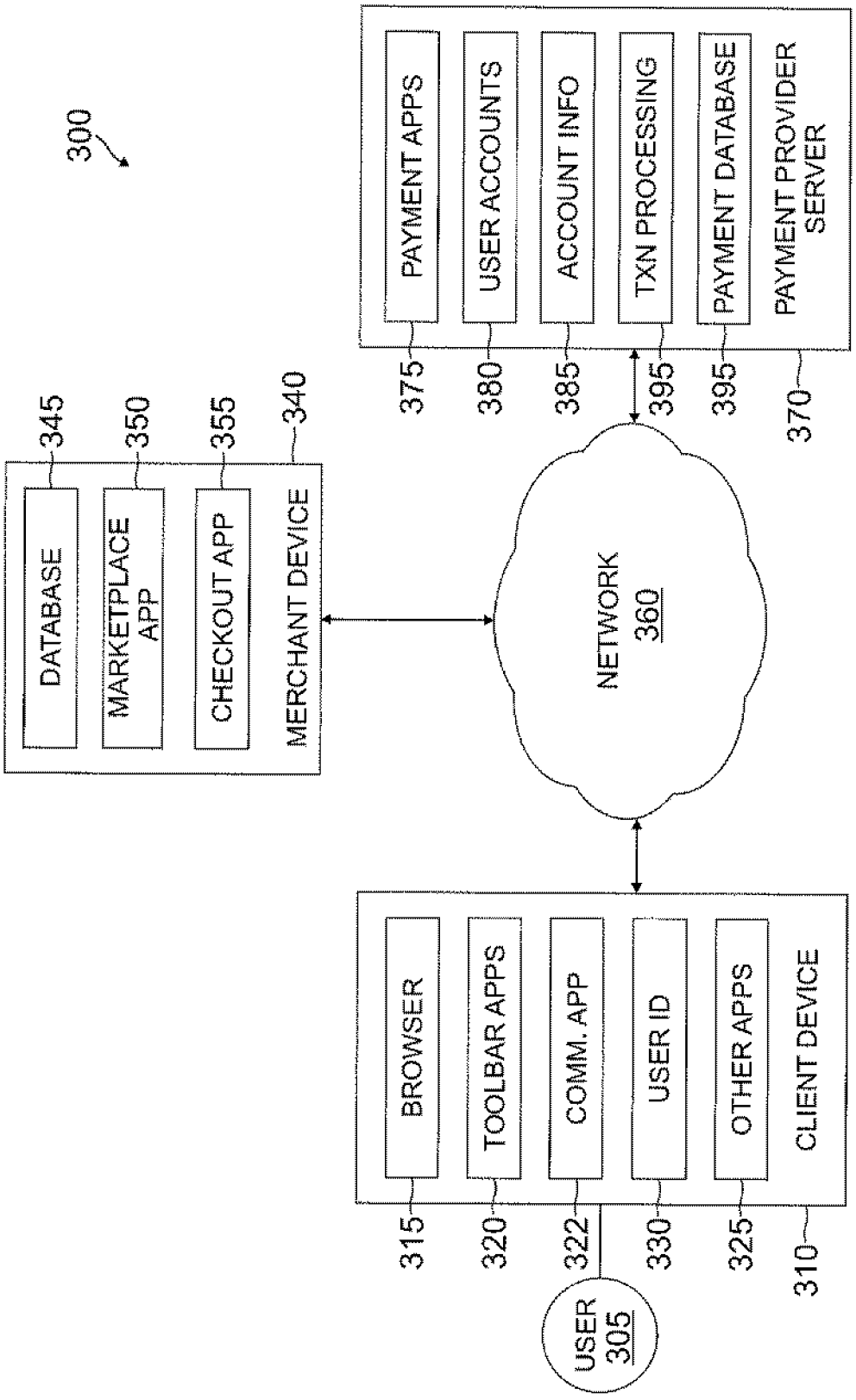

300
PAYMENT APPS
USER ACCOUNTS
ACCOUNT INFO
TXN PROCESSING
PAYMENT DATABASE
PAYMENT PROVIDER SERVER
375
380
385
395
395
370
DATABASE
MARKETPLACE APP
CHECKOUT APP
MERCHANT DEVICE
345
350
355
340
NETWORK 360
BROWSER
TOOLBAR APPS
COMM. APP
USER ID
OTHER APPS
CLIENT DEVICE
315
320
322
330
325
310
USER 305

FIG. 3

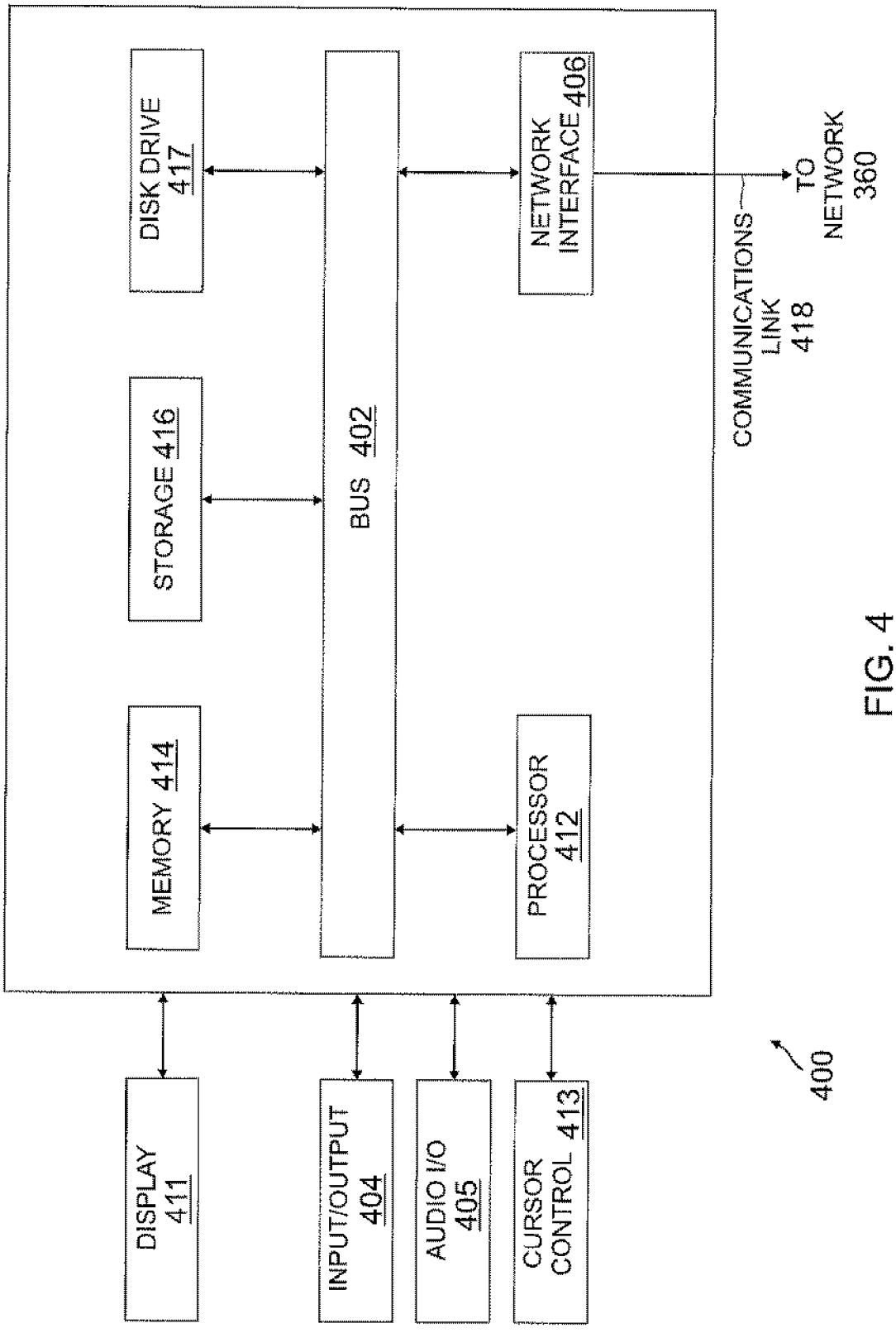

DISK DRIVE 417
STORAGE 416
MEMORY 414
BUS 402
NETWORK INTERFACE 406
PROCESSOR 412
COMMUNICATIONS LINK 418
TO NETWORK 360
DISPLAY 411
INPUT/OUTPUT 404
AUDIO I/O 405
CURSOR CONTROL 413
400

FIG. 4

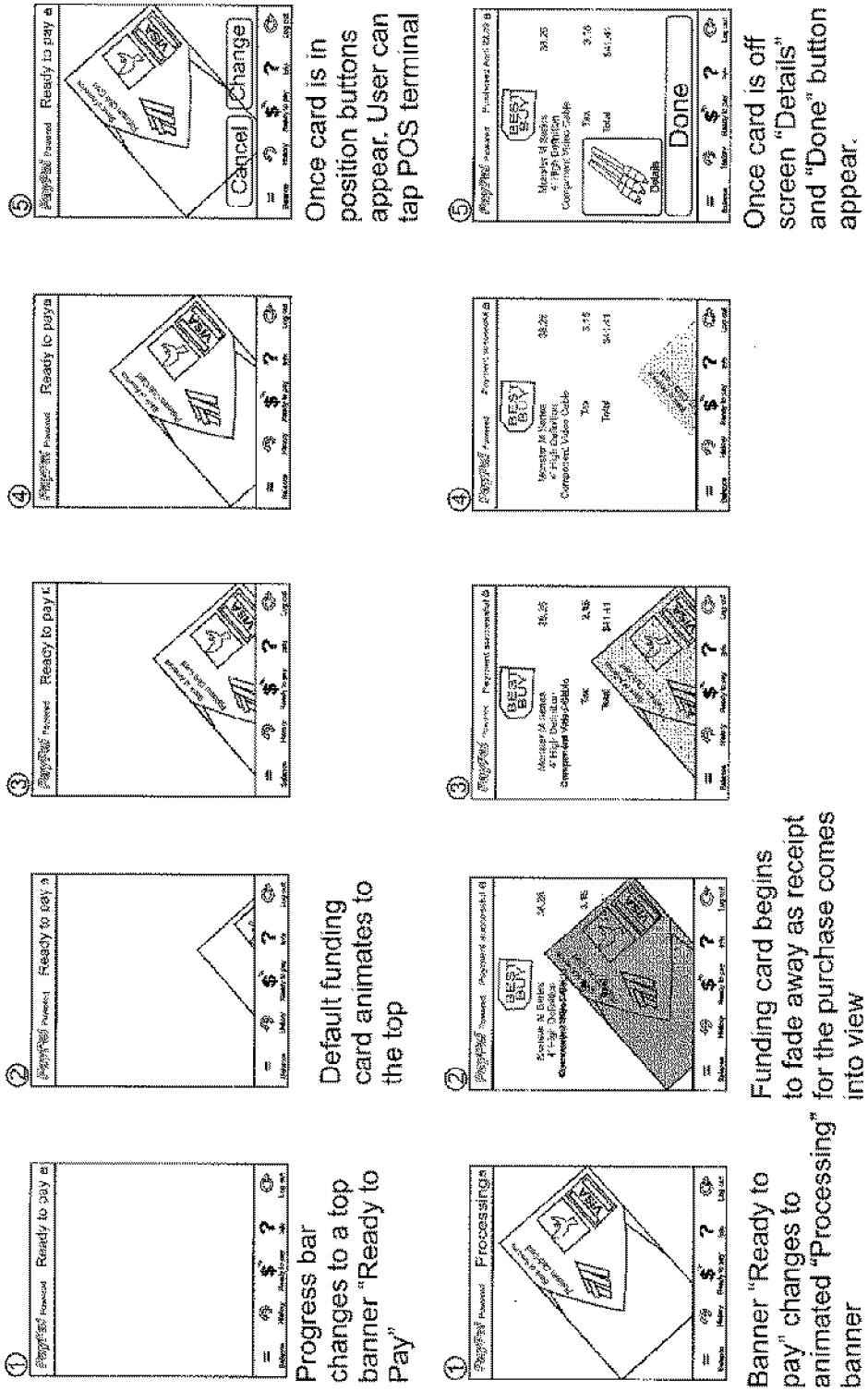

Progress bar changes to a top banner "Ready to Pay"
Default funding card animates to the top
Once card is in position buttons appear. User can tap POS terminal
Banner "Ready to pay" changes to animated "Processing"
Funding card begins to fade away as receipt for the purchase comes into view
Once card is off screen "Details" and "Done" button appear.
Cancel
Change
Done

FIG. 5A

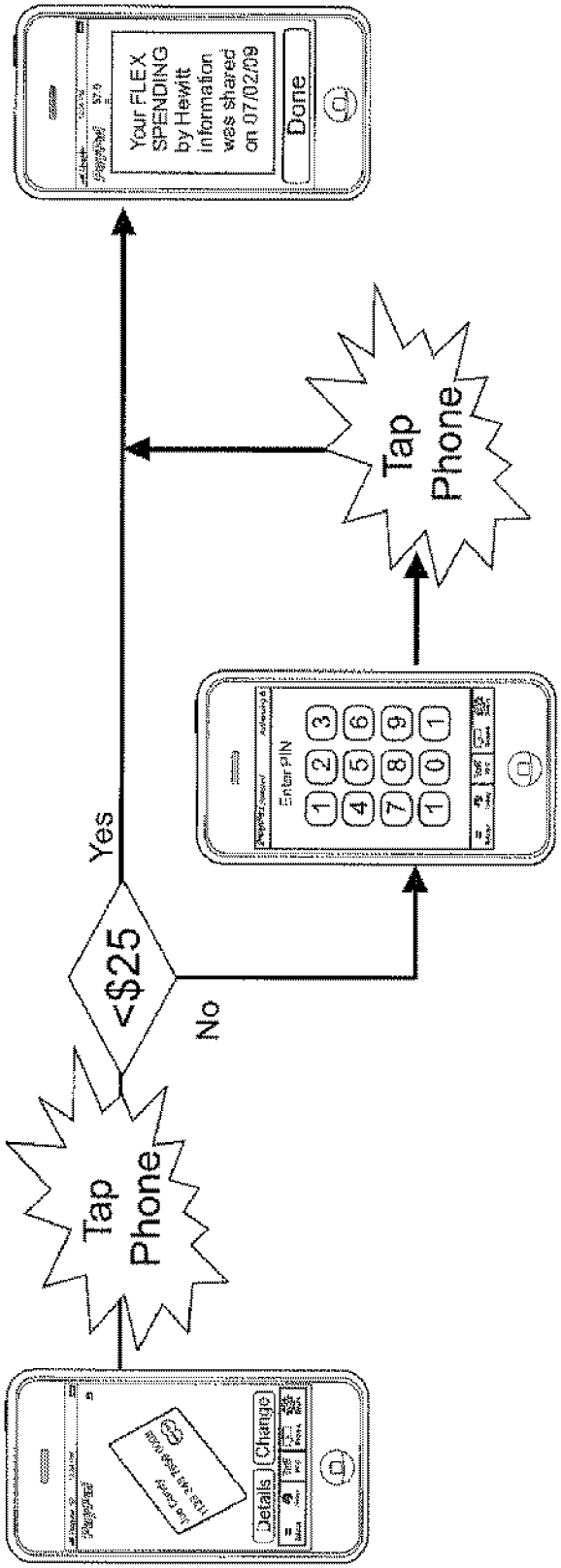

Your FLEX SPENDING by Hewitt information was shared on 07/02/09
Done
Tap Phone
Enter PIN
Yes
<$25
No
Tap Phone
Details
Change

FIG. 5B

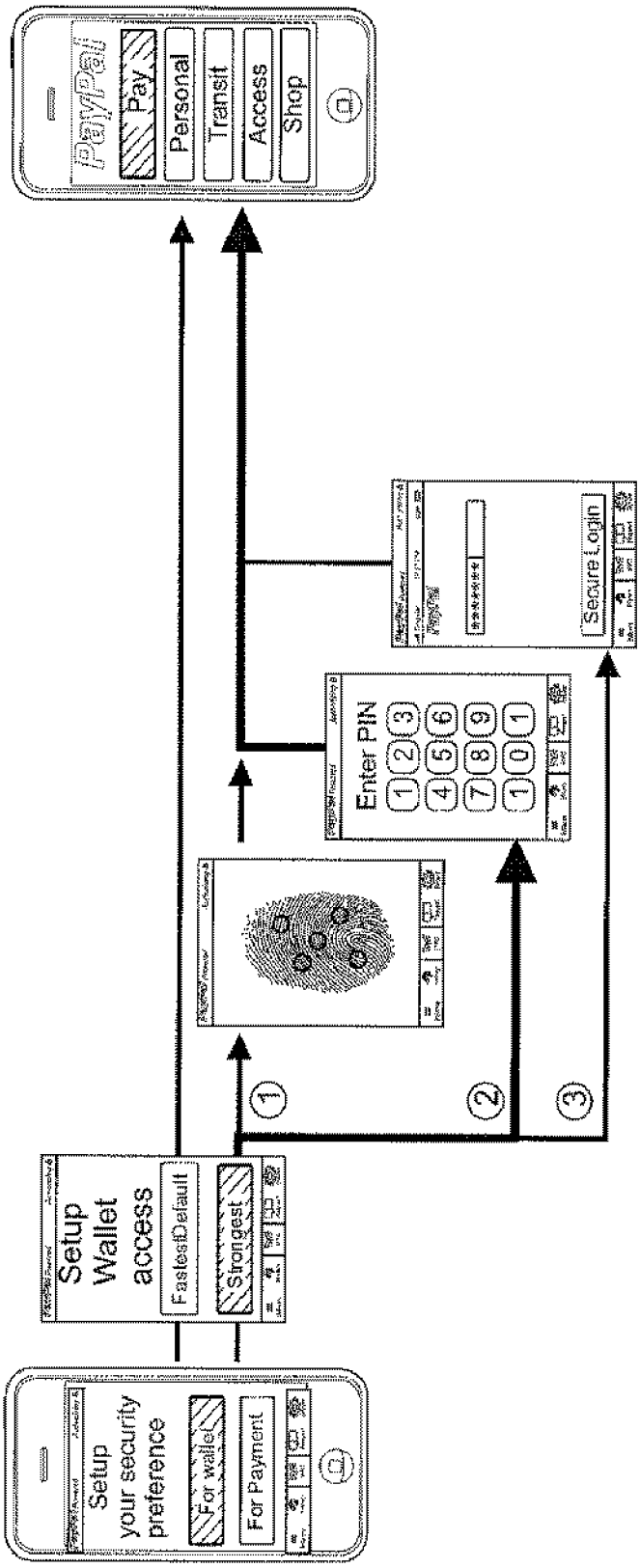

Setup your security preference
For wallet
For Payment
Setup Wallet access
FastestDefault
Strongest
Enter PIN
Secure Login
PayPal
Pay
Personal
Transit
Access
Shop
1
2
3

FIG. 5C

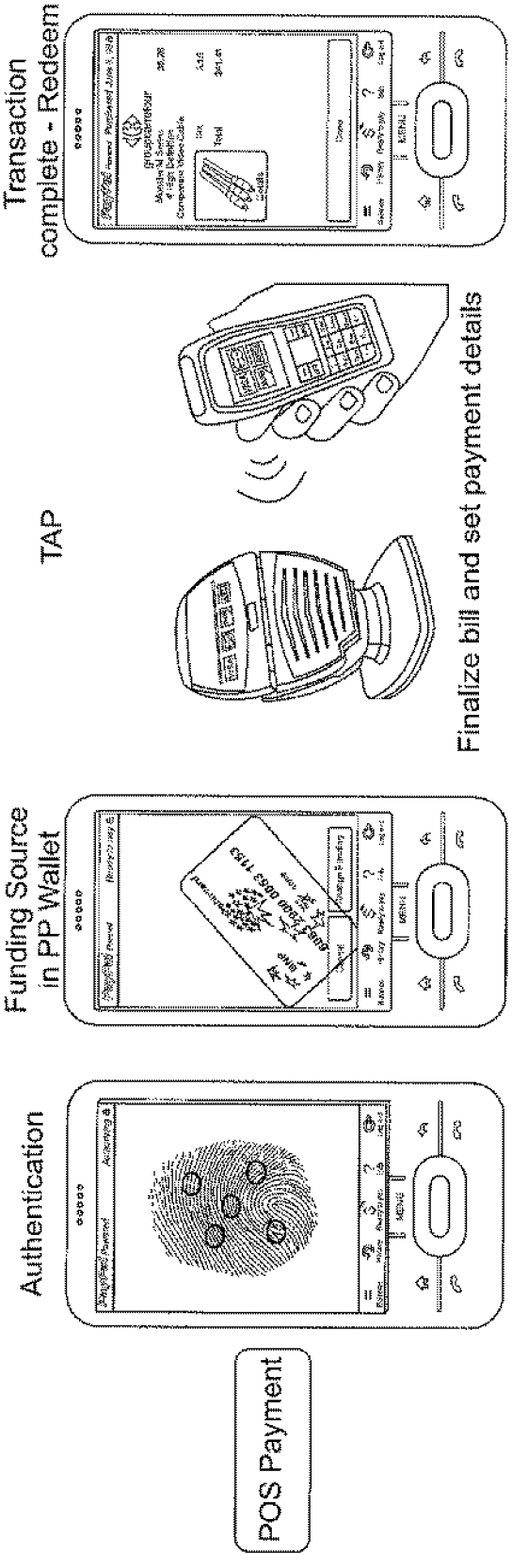

POS Payment
Authentication
Funding Source in PP Wallet
TAP
Finalize bill and set payment details
Transaction complete - Redeem

FIG. 5D

SMART WALLET

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application Ser. No. 61/359,667, filed Jun. 29, 2010, which is incorporated by reference in its entirety.

BACKGROUND

[0002] 1. Field of the Invention

[0003] The present invention generally relates to making payments using mobile devices, and more particularly, to using the mobile device to intelligently make payments.

[0004] 2. Related Art

[0005] Electronic payments are becoming a preferred method of payment because they offer advantages to the user not present with traditional physical payments. With a physical payment, the user is required to carry the funding instrument and present the funding instrument when ready to make a payment. Examples of physical funding instruments include cash, checks, credit cards, debit cards, coupons, gift certificates, gift cards, and the like. These can take up space in a user pocket, purse, or wallet. To reduce space, the consumer may not carry all funding instruments all the time, resulting in the possibility that a desired funding instrument is not available when the consumer is ready to use it at a point of sale (POS). Such physical funding instruments may also be lost or stolen. Thus, physical "wallets" can be cumbersome, inconvenient, and prone to loss.

[0006] To remedy this, mobile devices have been and are being used to make payments through payment providers, such as PayPal, Inc. of San Jose, Calif. Such payment providers typically allow a consumer to make a payment through the user's mobile device, such as through the use of barcodes, communication between the payment provider and the merchant, and other methods. After authentication and/or authorization, the payment is made through a user account with the payment provider, where the account is funded through a funding source, such as the user's bank or credit card. The funding source is typically a single default source selected by the user.

[0007] While this may allow the consumer to forego carrying credit cards, bank cards, and cash, the user must still decide whether to use the payment provider service, another payment service on the mobile device, or a physical funding instrument. This can be disadvantageous, which also applies to physical wallets, because the user must decide which of the many possible funding instruments to use for a particular purchase. This may result in the user choosing a payment instrument that is not the "best" choice for the transaction.

[0008] Therefore, a need exits for a payment solution that overcomes the disadvantages described above with conventional payment methods.

SUMMARY

[0009] According to one embodiment, a consumer has an account with a payment provider, such as PayPal, Inc. The account includes at least one funding source, and preferably several. When the user is ready to make a purchase or payment, such as at a point of sale, the payment provider selects what funding source (e.g., Visa, AMEX, credit cards associated with different rewards programs, PayPal, bank account, coupons, gift cards, etc.) to use based on the transaction information, including the amount, type of purchase, merchant, location, etc. The selection can be based on user selected preferences, payment history of user, goals, preferred or incentivized payment sources of the merchant, or any combination of logic. For example, there may be discounts or other rewards at a certain store if a specific card is used, the user may want to primarily use a card to get sufficient reward points for a goal, the user may want to limit certain cards to a maximum monthly or transaction amount, an AMEX Hilton card may be selected for use at a Hilton hotel, etc.

[0010] This greatly reduces the time and effort for the user to decide which card or other funding instrument to use. This also helps the user make use of coupons, etc., as part of the funding.

[0011] The payment provider may also provide payment directly from a funding source to the merchant so that the recipient need not have an account with the payment provider. This may also apply when the user does not have a payment provider account.

[0012] According to another embodiment, different authentication or security levels are applied to different uses of the user device. For example, payments may require one type of authentication, while non-payments (such as information transfers or displays) may require another type of authentication. Within payments or non-payments, there may be additional different security levels. For example, higher security may be required for higher payment amounts and use or display of more sensitive information, such as social security number, credit card number, and the like.

[0013] These and other features and advantages of the present invention will be more readily apparent from the detailed description of the embodiments set forth below taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE FIGURES

[0014] FIG. **1** is a flowchart showing a process a payment provider performs to process a payment from a user's smart wallet, according to one embodiment;

[0015] FIG. **2** is a flowchart showing a process for using a user mobile device as a digital wallet with different authentication levels according to one embodiment;

[0016] FIG. **3** is block diagram of a networked system suitable for implementing the process described herein according to an embodiment; and

[0017] FIG. **4** is a block diagram of a computer system suitable for implementing one or more components in FIG. **3** according to one embodiment.

[0018] Embodiments of the present disclosure and their advantages are best understood by referring to the detailed description that follows. It should be appreciated that like reference numerals are used to identify like elements illustrated in one or more of the figures, wherein showings therein are for purposes of illustrating embodiments of the present disclosure and not for purposes of limiting the same.

DETAILED DESCRIPTION

[0019] According to various embodiments, a smart digital wallet in a user's mobile device provides the user with, recommendations or decisions on what funding instruments to use based on transaction information, user preferences, user history, and/or funding instrument information. The smart wallet may also be customized with different levels of secu-

rity for making a payment, based in part on user preferences, transaction amount, location, and other factors. Thus, the user's mobile device can be used as a smart wallet to replace physical funding instruments, while providing numerous advantages not available with a physical wallet.

[0020] FIG. **1** is a flowchart showing a process **100** a payment provider performs to process a payment from a user's smart wallet, according to one embodiment. At step **102**, the payment provider receives an indication that the user is ready to make a payment for items. Items, as used herein, may include physical goods, digital goods, services, donations, and anything that the user is making a payment for, to, or regarding. In this embodiment, the user is at a physical location or point of sale (POS) for the payment, such as at a store. In other embodiments, the user may be shopping online and making the payment through a computing device, such as a PC.

[0021] The indication may be received in any number of ways. One example is the user accessing a payment app a user mobile device at the POS, which makes a call to the payment provider through the mobile device. The use may enter credentials to access the user's account and enable payment through the mobile device. Another example is the merchant communicating a purchase transaction to the payment provider at the POS through a merchant device. These can be when the user begins a checkout process, during a checkout process, or after all items have been scanned and totaled. In one embodiment, the minimum information communicated at step **102** is a desire for the user to make a payment and user identity/account information. The latter allows the payment provider to access the user's account and data associated with the account.

[0022] Once the user's account is accessed, the payment provider determines, at step **104**, if there are any default settings to the user's account for payments. Default settings may be determined by the user, such as user defined preferences, by the payment provider, such as based on payment history, or a combination of the two. Default settings include information about the use of funding instruments associated with the user account. For example, the user may have an American Express Hilton Reward credit card, a Citibank debit card or bank account, a Visa Southwest Airlines Reward credit card, and a Visa gift card as some of the funding sources for the user account. The AMEX card may be the main funding source, followed by the Visa gift card, and others in a particular order. So, with a purchase, the AMEX card would be the preferred funding instrument. However, there may be situations where the AMEX card cannot be used, such as at merchants/sites/locations where AMEX is not accepted, the AMEX card is rejected (such as expired, limit reached, fraud suspected, etc.). If the AMEX is unavailable for use, the Visa gift card would be the next choice. However, the Visa gift card may be unavailable because its value has been depleted. The next funding instrument would then be tried.

[0023] The default settings may be changed as needed. For example, the AMEX card may be the first choice because the user wants to accumulate Hilton points for an upcoming vacation stay. However, once enough points are accumulated or no longer needed, the user may replace the AMEX card with the Visa card so that the user can accumulate points quicker for free flights. Such changes may be made by the user through the user's account page with the payment provider.

[0024] If there are default settings, those settings are applied at step **106**. The system also determines, at step **108**, whether there are any location-based restrictions or rules for any of the user's funding instruments. For example, a certain gift card or coupon may only be used within the United States. Another coupon may only be used in California. The Visa gift card may be used anywhere, but may have a bonus if used in Arkansas. The bonus may be a 10% credit on the gift card. The Arkansas use may be Visa wanting more spending in Arkansas to help the Arkansas economy in wake of its recent earthquake.

[0025] If there is at least one location-based rule, a location of the user (or POS) is determined at step **110**. This may be through a location service or function associated with the user's mobile device. Thus, when the user is ready to make a payment, the user's location will be known through the user's mobile device. Typically, the location is at the POS. The user location may also be determined in other ways. One example is the merchant communicating the identity of the user to the payment provider, which informs the payment provider that the user is with the merchant, where the merchant location is known by the payment provider. The payment provider applies the one or more location-based rules at step **112**. This may include changing the priority of the user defined preferences accordingly.

[0026] The system receives, at step **114**, transaction details, which can be through the merchant or the user. Transaction details may include information about the items scanned or to be purchased, such as description, type, quantity, and price, merchant information, such as name, account number, main address, local store address, phone number, the transaction date, and the like, and amount of the transaction, including taxes and any discounts/coupons/rewards applied or to be applied.

[0027] Using this and any other applicable information, the "best" one or more funding instruments are determined, at step **116**, for the user to use in the present transaction. The determination may include processing all or a portion of the information available and received about the user, the merchant, the location, and the transaction. For example, a particular merchant may only accept certain funding instruments (such as Visa and MasterCard only for credit cards), not accept certain funding instruments (such as no American Express or coupons), and/or provide a reward or other incentive for using a particular funding instrument (such as a store branded credit card).

[0028] In another example, a particular coupon or gift card may be applicable to one or more purchases in the transaction. Such coupons or gift cards may then be selected for use. Certain coupons, gift cards, and the like may have upcoming expiration dates. Based on the date of the transaction and the expiration dates of applicable funding instruments, appropriate funding instruments may be selected to be used for this transaction. For example, funding instruments about to expire may be prioritized over later-expiring funding instruments.

[0029] Once funding instruments are selected for the current transaction, the user may be presented with the selection (s), at step **118**, on the user's mobile device. The user may see where each funding instrument is to be applied and how, along with amount applied if appropriate. For example, a certain purchase or item may only allow a certain dollar amount to from a gift card, voucher, or coupon to be applied to the purchase.

[0030] Next, the payment provider makes a determination, at step **120**, whether the user has confirmed the selected funding instruments. This determination may include receiving an electronic signal from the user device of a confirmation resulting from the user tapping or otherwise selecting a "confirm" or similar link/button on the device. If a confirmation is received, the transaction may be processed, at step **122**, with the selected funding instruments. Processing may be through the payment provider, where the payment provider receives payment details through the user device or the merchant, determines whether one or more payments can be approved, debiting user account(s) and crediting merchant account(s) immediately or at a later time, and sending a notification to the user and/or the merchant that the payment for the transaction has been approved or denied. Processing may also be directly through the user. For example, the user may simply present a physical credit card, where processing is through conventional credit card processing with the merchant.

[0031] If the user does not confirm the selected funding sources, the user may decide to revise the selection, such as adding one or more different funding sources, deleting one or more funding sources, or applying a funding source differently (e.g., using a lesser amount of a gift card). For example, even though the payment provider selected the AMEX card based on the user's previously set preference (the user had wanted to accumulate hotel points), the user may no longer need the points. This may be due to the user obtaining a sufficient amount of points, the hotel stay changed, or other reasons. The user also may not have changed user preferences yet. As a result, the user may replace the AMEX card with the Visa card.

[0032] In one embodiment, the user can revise selected funding instruments through the user device. For example, the user may select a funding for revision. The selected funding source may be deleted or otherwise revised accordingly, such as through user actions through the user device. A new funding source may be added, such as by selecting from a list of available funding sources. The list can be in any form and accessed through any number of ways, including a drop down menu or a new window on a browser or app.

[0033] After one or more revisions to the selected funding sources are made by the user, the revisions are communicated to and received by the payment provider at step **124**. Once received, the payment provider may transmit the user-revised payment instrument selections to the user at step **126**. The user may view the revised payment selections, such as on the user device, and confirm or revise again as needed using the steps described above. When the user confirms the payment instruments, the payment can be processed at step **122**.

[0034] Note that the various steps and decisions above may be performed in different sequences and select ones may be omitted, as well as additional steps and decisions added.

[0035] Thus, the user is able to use the "best" funding instruments to pay for a transaction using selections from the payment provider based on user set preferences, location, transaction details, merchant, date, and other factors. Payment can be made through the user's mobile device, thereby eliminated the need for the user to carry physical funding instruments like cash, credit cards, debit cards, checks, coupons, and gift cards.

[0036] FIG. **2** is a flowchart showing a process **200** for using a user mobile device as a digital wallet with different authentication levels according to one embodiment. A typical physical wallet may contain non-payment cards, such as medical insurance cards, frequent flyer numbers, hotel loyalty numbers, social security card, auto club card, and the like, in addition to funding instruments like those discussed above. A mobile device, such as smart phone or tablet, may be able to store such personal information of the user, such that the mobile device can become more like a physical wallet in that it can then contain both payment instruments and user information.

[0037] To use the mobile device for payment, the user typically is required to enter a password or PIN and a user/device identifier, such as a user name, email address, or phone number, unless the user/device identifier is automatically communicated to the payment provider through the mobile device. This can be time-consuming and cumbersome, especially with the small physical and virtual keypads associated with mobile devices. However, such authentication is needed to protect the funding instruments and prevent unauthorized users to make payments from the user's account.

[0038] There may be other data or functions in the phone that do not require the authentication levels of payments. For example, a frequent flyer number or transmitting of a frequent flyer number may not require the level of security as sending a payment. Other information, such as the user's social security number, may require additional security. Even payments may allow different levels of security. For example, a payment transaction of less than $20 may not require as much security as a payment transaction of greater than $200. Thus, FIG. **2** illustrates an example of how a mobile device or user of the mobile device may be authenticated for different information or transactions using the mobile device.

[0039] At step **202**, a determination is made whether the mobile device, for the current use, is to be used for payment. Payment transactions typically will require stronger authentication. The determination may include receiving an indication from the user through the mobile device, such as selecting a payment app, or from a recipient, such as a seller, through a recipient device identifying the user or payer. If the mobile device will be used for a payment transaction, a determination is made, at step **204**, whether the amount of the payment transaction will be greater than a certain amount, X. This amount can be set by the user or the payment provider. Higher amounts typically will require stronger authentication. The amount can include use of funds from the user's account with the payment provider, use of coupons, gift cards, vouchers, etc., and/or use of other funding sources such as credit cards.

[0040] If the anticipated payment amount is less than or equal to X, the payment provider may require the user to authenticate using a first authentication level, Auth**1**, at step **206**. Auth**1** may simply require the user to unlock the mobile device or access a payment app. If the anticipated payment amount is greater than X, the user may be required, at step **208**, to authenticate through a second authentication level, Auth**2**, which is stronger than Auth**1**. An example of Auth**2** may include entry of a user PIN, biometric information, a password, or other data, in addition to what was required at step **206**.

[0041] If, as determined, at step **202**, the current transaction is not for payment, a determination may be made, at step **210**, whether the transaction involves "sensitive" or "confidential" information. Examples of sensitive information may include the user's social security number, a bank account number, a password, credit card numbers including security codes, debit card numbers, etc. Examples of non-sensitive information

stored in the mobile device may include account numbers for airline loyalty programs, hotel loyalty programs, merchant loyalty programs, and the like, medical insurance policy number, dental insurance policy number, AAA membership number, etc. The user may determine which information is sensitive and which is not, such as by designating specific data or types of data.

[0042] At step **212**, the user is required to authenticate at a third authentication level, Auth**3**, when the transaction involves exposure or transmission of sensitive information. Auth**3**, in one embodiment, is a stronger authentication than Auth**1**, but weaker than Auth**2**. In another embodiment, Auth**3** is the same as Auth**2**. Anth**3** may include requiring the user to enter an identifier, such as an email address, phone number, or user name.

[0043] If the information is not sensitive, the user may be requested to authenticate using a fourth authentication level, Auth**4**, at step **214**. Auth**4** may be the same as Anth**1**. In another embodiment, Auth**4** is weaker than Auth**1**, Auth**2**, and Auth**3**. For example, Auth**4** may include the user simply being able to use the mobile device, and thus effectively not requiring any authentication, just possession of the device.

[0044] Note that the above authentication levels are just examples and not limiting. For example, additional authentication levels may be employed. This may be due to more than two levels of authentication for a payment, with the different levels based on a plurality of transaction amount thresholds. Information may also be divided into more than two categories of just sensitive and non-sensitive. Furthermore, determinations, in addition to or in place of, whether the transaction is for a payment and whether the transaction involves sensitive information stored in the mobile device may be included.

[0045] After the specific authentication level is requested/required, the requested information is received, at step **216**, from the user, such as through the user mobile device. The information may be received by the user entering the requested information, such as through a keypad, keyboard, touch pad, touch screen, or other data input. Once received the information is processed by the payment provider, at step **218**. Processing may include determining if the received information is what was requested and whether the received information was what was expected. This can be through accessing the user's account and checking authentication information of the user.

[0046] A determination is then made, at step **220**, whether the user can be authenticated. This determination may include typical authentication procedures for the payment provider, including any fraud analysis, account restrictions, transaction limits, etc.

[0047] If the user is authenticated, the transaction moves forward at step **222**. The transaction can proceed with a payment process, a communication, display or access of data/information, or other use of the mobile device. However, if the user authentication fails, the transaction may not be allowed to proceed until the user is authenticated. Thus, the payment provider may allow the user one or more additional attempts to authenticate, using the same authentication requests or something different. For example, the user may be asked a security question.

[0048] Accordingly, the payment provider (and/or the user) may set different levels of security to be linked on the access to the wallet or some part of the wallet. As an example, the user may not care about protecting coupons or some loyalty components (e.g., frequent flyer card or movie theater reward card), but will care about protecting credit cards or payment instruments. The basic default security settings of the wallet may be speed of transaction over higher security (resulting in more friction or interaction from the user). However, the "smarter" the wallet will be, the better security with little user interaction can be provided by the payment provider.

[0049] For an example, a user could decide that for any transaction, the user does not want to be asked anything. As long as the smart wallet is triggered properly, the transaction will go through. Some users, being more cautious, may want to see any transaction and will ask to be prompted for information of transactions going through the smart wallet. Other users, wanting more security, could decide to be prompted for an actual validation of the transaction by entering a PIN, a password or a fingerprint/biometric component. The level of security could be linked also to the amount of the transaction, as mentioned above. For example, under $20, no action required, between $20 and $50, get a prompt to inform the user, above $50, enter a PIN. These levels could be flexible and decided by the user but again, with a validation/association to the risk profile managed by the payment provider.

[0050] Thus, using the above, a user may have multiple security choices when setting up the user's mobile device and using the mobile device for different transactions or uses. This can provide a more frictionless user experience by not requiring the user to enter passwords/PINs or biometric information for all uses of the phone. Multiple security choices can also protect the user from fraudulent uses of the mobile device by requiring heightened or stronger authentication for higher payments or access to extremely sensitive information.

[0051] There may be several components to such a digital wallet described above, including a user profile, a risk profile, and stored value. A user may create a user profile for the smart wallet. Typically, the more information the user provides, the "smarter" the wallet. The payment provider can use this information to make a more informed decision on funding instruments for each transaction. Examples of what the user may enter into the profile include spending preferences, spending limits, goals, preferred funding instruments, etc. The user profile may be revised by the user, such as by revising profile information. The profile may also be revised by the payment provider, such as based on user transactions. For example, if the user continues to revise funding instruments suggested or presented by the payment provider, the payment provider may revise the user profile accordingly to reflect the user preferences.

[0052] Another component, the user's risk profile, may be based in part on parameters or information from the payment provider. For example, a long time user of the payment provider service with a verified address and payment instruments (e.g., a bank account linked and verified to the user's payment provider account) will have a better risk profile than a user who just registered and has not linked/verified any bank account to his account. Other elements that may be used to build a user risk profile include the make/model of the user's mobile device (e.g., if it is registered with the payment provider (phone number but also hardware/software configurations, browser, etc.)). While the main risk profile may be stored in the cloud, a subset version could be stored on the mobile device with a specific set of parameters, especially for "offline" transactions using a stored value.

[0053] Stored value is an amount of cash the user maintains as a balance with the payment provider for payments. The

payment provider may create an "extrapolation" of this balance on the mobile device of the user. This stored value may be linked to the risk profile of the user. For example, if a user with an excellent risk profile has a $500 balance on his payment provider account, then the payment provider may grant the user access to a stored value of $400 or even $500. A new user to the payment provider with an unverified account may have a $500 account balance with the payment provider, but would be allowed to have a stored value emergency access of only $5 or $50 or whatever amount would be deemed to be an acceptable risk for the payment provider for that user.

[0054] In one embodiment, the payment provider maintains a dynamic stored value management system that will rely on the capacity to enforce a verification of stored value spending against the balance remaining in the cloud. With data based on the mobile device, the payment provider could feed back in real time the stored value spending history against the account balance on a constant basis. However, for some mobile devices with limited functions or for a mobile device going on low battery mode, the payment provider may not be able to feed back this history and will have to grant a level of access in an offline/off the cloud mode. In one example, a user is trying to catch the last subway and the user's mobile device is NFC-enabled, but the battery is almost depleted. However, a contactless reader from the subway company is set to power up the NFC chip on the user device and provide enough energy boost in a short period of time to retrieve a ticket and/or payment to grant access through the gate. At that point, the payment provider may not have the option to provide feedback for any verification to the cloud, but the "smart wallet" will be able to provide the needed funds offline (and register it in the transaction history log for future synchronization). By doing so, the payment provider is taking the risk but also making sure the user experience is on par with the user expectations or online payment transactions.

[0055] The payment provider may manage offline transactions from an offline transaction history log applied against the stored value balance. However, based on the risk profile, the payment provider may associate parameters to this function of the smart wallet, such as number of transaction, transaction amount, time offline, etc. and force back a connection to the cloud to update the smart wallet and the stored value balance.

[0056] In order to manage the user and risk profiles, as well as matching data to trigger some functions of the smart wallet (e.g., user location, user preference from that specific handset, transaction log history, etc.), a back-end module may be in charge of the "smart" or intelligence in the smart wallet. This could be managed by components that are part of the payment provider system. By doing so and creating this "intermediate" buffer, the payment provider can deliver a faster service towards the mobile device and manage the stored value better against the risk profile but also provide a needed protection/isolation of the main user account residing in the payment provider core system.

[0057] From a technical point of view, the wallet may be an application residing on the mobile device and linked to the payment provider wallet in the cloud. Some components of the wallet (e.g., user interfacing) could be normal applications such as Java applet, widget or native type. However security functions (anti-phishing, anti-spoofing mechanisms, etc.) may need to be disassociated from the basic function and be launched from a "trusted" element/component on the mobile device. This could be a hardware and/or a software component. Examples of such components include TrustZone from ARM, Embedded Secure Element, MicroSD Card or SIM card. In one embodiment, the smart wallet or account remains in the cloud at all times and the mechanism to protect it are never exposed to the user or mobile device. For this reason, the user and risk profiles are managed differently.

[0058] The following provides one example of a smart wallet use case. A Costco customer has an American Express Costco branded card. He also goes on a regular basis to a Costco store located near his home. By monitoring the payment history of this user in that store/merchant, the payment provider will know that the user pays 90% of the time with this Amex card. The 10% remaining are payments made with a debit card. Both instruments are registered with the user's payment provider account.

[0059] By using the smart wallet (and assuming the store or merchant is known by the payment provider or the payment provider has created a business addresses register), the user may then have his default payment instrument proposed to him as follows: 1) Payment instrument #**1** (preferred): American Express Costco card; 2) Payment Instrument #**2** (secondary): Debit card; 3) Payment Instrument #**3** (Stored value): Payment Provider Balance extension in physical world. The user may edit or revise as desired.

[0060] This selection will be triggered by the user profile, his specific location (leverage from the GPS position) and (if enabled) a store "wireless" signal sent to the mobile device of the user and "read" by the smart wallet (e.g., through an NFC tag, Bluetooth (existing pairing) or other). By doing triangulation of data, the smart wallet may be able to enhance the choice of payment instruments.

[0061] When the user arrives at the cash register, he connects to the payment provider, such as through an NFC channel, a remote/online session, etc. Transaction information, such as amount, store, merchant, type of purchase, etc., is communicated to the payment provider, as well as the location of the user and/or POS and any other information needed by the payment provider. The payment provider accesses the user's account and preferences and decides which funding instrument or combination of funding instruments to use automatically.

[0062] FIG. **3** is a block diagram of a networked system **300** configured to handle a transaction using a smart wallet, such as described above, in accordance with an embodiment of the invention. System **300** includes a user device **310**, a merchant server **340**, and a payment provider server **370** in communication over a network **360**. Payment provider server **370** may be maintained by a payment provider, such as PayPal, Inc. of San Jose, Calif. A user **305**, such as a sender or consumer, utilizes user device **310** to perform a transaction using payment provider server **370**. Note that transaction, as used herein, refers to any suitable action performed using the user device, including payments, transfer of information, display of information, etc.

[0063] User device **310**, merchant server **340**, and payment provider server **370** may each include one or more processors, memories, and other appropriate components for executing instructions such as program code and/or data stored on one or more computer readable mediums to implement the various applications, data, and steps described herein. For example, such instructions may be stored in one or more computer readable media such as memories or data storage devices internal and/or external to various components of system **300**, and/or accessible over network **360**.

[0064] Network **360** may be implemented as a single network or a combination of multiple networks. For example, in various embodiments, network **360** may include the Internet or one or more intranets, landline networks, wireless networks, and/or other appropriate types of networks.

[0065] User device **310** may be implemented using any appropriate hardware and software configured for wired and/or wireless communication over network **360**. For example, in one embodiment, the user device may be implemented as a personal computer (PC), a smart phone, personal digital assistant (PDA), laptop computer, and/or other types of computing devices capable of transmitting and/or receiving data, such as an iPad™ from Apple™.

[0066] User device **310** may include one or more browser applications **315** which may be used, for example, to provide a convenient interface to permit user **305** to browse information available over network **360**. For example, in one embodiment, browser application **315** may be implemented as a web browser configured to view information available over the Internet, including accessing a loyalty site. User device **310** may also include one or more toolbar applications **320** which may be used, for example, to provide client-side processing for performing desired tasks in response to operations selected by user **305**. In one embodiment, toolbar application **320** may display a user interface in connection with browser application **315** as further described herein.

[0067] User device **310** may further include other applications **325** as may be desired in particular embodiments to provide desired features to user device **310**. For example, other applications **325** may include security applications for implementing client-side security features, programmatic client applications for interfacing with appropriate application programming interfaces (APIs) over network **360**, or other types of applications. Applications **325** may also include email, texting, voice and IM applications that allow user **305** to send and receive emails, calls, and texts through network **360**, as well as applications that enable the user to communicate, transfer information, make payments, and otherwise utilize a smart wallet through the payment provider as discussed above. User device **310** includes one or more user identifiers **330** which may be implemented, for example, as operating system registry entries, cookies associated with browser application **315**, identifiers associated with hardware of user device **310**, or other appropriate identifiers, such as used for payment/user/device authentication. In one embodiment, user identifier **330** may be used by a payment service provider to associate user **305** with a particular account maintained by the payment provider as further described herein. A communications application **322**, with associated interfaces, enables user device **310** to communicate within system **300**.

[0068] Merchant server **340** may be maintained, for example, by a merchant or seller offering various products and/or services in exchange for payment to be received over network **360**. Merchant server **340** may be used for POS or online purchases and transactions. Generally, merchant server **340** may be maintained by anyone or any entity that receives money, which includes charities as well as retailers and restaurants. Merchant server **340** includes a database **345** identifying available products and/or services (e.g., collectively referred to as items) which may be made available for viewing and purchase by user **305**. Accordingly, merchant server **340** also includes a marketplace application **350** which may be configured to serve information over network **360** to browser **315** of user device **310**. In one embodiment, user **305** may interact with marketplace application **350** through browser applications over network **360** in order to view various products, food items, or services identified in database **345**.

[0069] Merchant server **340** also includes a checkout application **355** which may be configured to facilitate the purchase by user **305** of goods or services identified by marketplace application **350**. Checkout application **355** may be configured to accept payment information from or on behalf of user **305** through payment service provider server **370** over network **360**, such as using selected funding instruments from the smart wallet. For example, checkout application **355** may receive and process a payment confirmation from payment service provider server **370**, as well as transmit transaction information to the payment provider and receive information from the payment provider (e.g., a transaction ID).

[0070] Payment provider server **370** may be maintained, for example, by an online payment service provider which may provide payment between user **305** and the operator of merchant server **340**. In this regard, payment provider server **370** includes one or more payment applications **375** which may be configured to interact with user device **310** and/or merchant server **340** over network **360** to facilitate the purchase of goods or services, communicate/display information, and send payments by user **305** of user device **310** and as discussed above.

[0071] Payment provider server **370** also maintains a plurality of user accounts **380**, each of which may include account information **385** associated with individual users. For example, account information **385** may include private financial information of users of devices such as account numbers, passwords, device identifiers, user names, phone numbers, credit card information, bank information, or other financial information which may be used to facilitate online transactions by user **305**. Advantageously, payment application **375** may be configured to interact with merchant server **340** on behalf of user **305** during a transaction with checkout application **355** to track and manage purchases made by users and which funding sources are used, as well as points for a user.

[0072] A transaction processing application **390**, which may be part of payment application **375** or separate, may be configured to receive information from a user device and/or merchant server **340** for processing and storage in a payment database **395**. Transaction processing application **390** may include one or more applications to process information from user **305** for processing an order and payment using various selected funding instruments as described herein. As such, transaction processing application **390** may store details of an order associated with a phrase from individual users. Payment application **375** may be further configured to determine the existence of and to manage accounts for user **305**, as well as create new accounts if necessary, such as the set up, management, and use of a smart wallet for the user/mobile device.

[0073] FIG. **4** is a block diagram of a computer system **400** suitable for implementing one or more embodiments of the present disclosure. In various implementations, the user device may comprise a personal computing device (e.g., smart phone, a computing tablet, a personal computer, laptop, PDA, Bluetooth device, key FOB, badge, etc.) capable of communicating with the network. The merchant and/or payment provider may utilize a network computing device (e.g., a network server) capable of communicating with the network. It should be appreciated that each of the devices utilized

by users, merchants, and payment providers may be implemented as computer system **400** in a manner as follows.

[0074] Computer system **400** includes a bus **402** or other communication mechanism for communicating information data, signals, and information between various components of computer system **400**. Components include an input/output (I/O) component **404** that processes a user action, such as selecting keys from a keypad/keyboard, selecting one or more buttons or links, etc., and sends a corresponding signal to bus **402**. I/O component **404** may also include an output component, such as a display **411** and a cursor control **413** (such as a keyboard, keypad, monse, etc.). An optional audio input/output component **405** may also be included to allow a user to use voice for inputting information by converting audio signals. Audio I/O component **405** may allow the user to hear audio. A transceiver or network interface **406** transmits and receives signals between computer system **400** and other devices, such as another user device, a merchant server, or a payment provider server via network **360**. In one embodiment, the transmission is wireless, although other transmission mediums and methods may also be suitable. A processor **412**, which can be a micro-controller, digital signal processor (DSP), or other processing component, processes these various signals, such as for display on computer system **400** or transmission to other devices via a communication link **418**. Processor **412** may also control transmission of information, such as cookies or IP addresses, to other devices.

[0075] Components of computer system **400** also include a system memory component **414** (e.g., RAM), a static storage component **416** (e.g., ROM), and/or a disk drive **417**. Computer system **400** performs specific operations by processor **412** and other components by executing one or more sequences of instructions contained in system memory component **414**. Logic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to processor **412** for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. In various implementations, non-volatile media includes optical or magnetic disks, volatile media includes dynamic memory, such as system memory component **414**, and transmission media includes coaxial cables, copper wire, and fiber optics, including wires that comprise bus **402**. In one embodiment, the logic is encoded in non-transitory computer readable medium. In one example, transmission media may take the form of aconstic or light waves, such as those generated during radio wave, optical, and infrared data communications.

[0076] Some common forms of computer readable media includes, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, PROM, EPROM, FLASH-EPROM, any other memory chip or cartridge, or any other medium from which a computer is adapted to read.

[0077] In various embodiments of the present disclosure, execution of instruction sequences to practice the present disclosure may be performed by computer system **400**. In varions other embodiments of the present disclosure, a plurality of computer systems **400** coupled by communication link **418** to the network (e.g., such as a LAN, WLAN, PTSN, and/or various other wired or wireless networks, including telecommunications, mobile, and cellular phone networks) may perform instruction sequences to practice the present disclosure in coordination with one another.

[0078] Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa.

[0079] Software, in accordance with the present disclosure, such as program code and/or data, may be stored on one or more computer readable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

[0080] The foregoing disclosure is not intended to limit the present disclosure to the precise forms or particular fields of use disclosed. As such, it is contemplated that various alternate embodiments and/or modifications to the present disclosure, whether explicitly described or implied herein, are possible in light of the disclosure. Having thus described embodiments of the present disclosure, persons of ordinary skill in the art will recognize that changes may be made in form and detail without departing from the scope of the present disclosure. Thus, the present disclosure is limited only by the claims.

What is claimed is:

1. A method for performing a payment transaction using a user device, comprising:

receiving an indication of a desire by a user to make a payment;

accessing, by a processor a payment provider, an account of the user with the payment provider;

determining, by the processor, which one or more of a plurality of funding instruments associated with the account to use for the payment based on at least one of user preferences, transaction information, and location of the user; and

processing the payment using the one or more funding instruments.

2. The method of claim **1**, further comprising receiving the user preferences from the user, wherein the determining is based in part on the user preferences.

3. The method of claim **1**, wherein the plurality of funding instruments comprises one or more of credit cards, debit cards, gift cards, and coupons.

4. The method of claim **1**, wherein the determining comprises selecting at least two funding instruments for the payment.

5. The method of claim **1**, wherein the transaction information comprises information about a merchant and an amount.

6. The method of claim **1**, wherein the determining is based, in part, on the location of a user.

7. The method of claim 1, wherein the determining is based, in part, on a purchase history of a user.

8. The method of claim 1, further comprising receiving different security settings, from the user, for different uses of the user device.

9. The method of claim 8, wherein a higher security setting is required for a higher payment amount.

10. The method of claim 8, wherein a higher security setting is required for use of a higher sensitive information.

11. The method of claim 10, wherein the higher sensitive information comprises at least one of a social security number, a credit card number, a bank account number, and a gift card number.

12. The method of claim 1, further comprising receiving a revised one or more funding instruments from the user and processing the payment nsing the revised one or more funding instruments.

13. A non-transitory machine-readable medium comprising a plurality of machine-readable instructions which when executed by one or more processors of a server are adapted to cause the server to perform a method comprising:

receiving an indication of a desire by a user to make a payment;

accessing an acconnt of the user with a payment provider;

determining which one or more of a plurality of funding instruments associated with the account to use for the payment based on at least one of user preferences, transaction information, and location of the user; and

processing the payment using the one or more funding instruments.

14. The non-transitory machine-readable medium of claim 13, wherein the plurality of funding instruments comprises one or more of credit cards, debit cards, gift cards, and coupons.

15. The non-transitory machine-readable medium of claim 13, wherein the determining comprises selecting at least two funding instruments for the payment.

16. The non-transitory machine-readable medium of claim 13, wherein the transaction information comprises information about a merchant and an amonnt.

17. The non-transitory machine-readable medium of claim 13, wherein the determining is based, in part, on a purchase history of a user.

18. The non-transitory machine-readable medium of claim 13, wherein the method further comprises receiving different security settings, from the user, for different uses of the user device.

19. The non-transitory machine-readable medium of claim 18, wherein a higher security setting is required for a higher payment amount.

20. The non-transitory machine-readable medium of claim 18, wherein a higher security setting is required for use of a higher sensitive information.

21. The non-transitory machine-readable medium of claim 20, wherein the higher sensitive information comprises at least one of a social security number, a credit card number, a bank account number, and a gift card number.

22. The non-transitory machine-readable medium of claim 13, wherein the method further comprises receiving a revised one or more funding instruments from the user and processing the payment using the revised one or more funding instruments.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

von Behren et al.

(10) **Pub. No.: US 2012/0166333 A1**

(43) **Pub. Date: Jun. 28, 2012**

(54) **DIGITAL WALLET**

(75) Inventors: **Rob von Behren**, Berkeley, CA (US); **Jonathan Wall**, San Francisco, CA (US)

(73) Assignee: **GOOGLE Inc.**, Mountain View, CA (US)

(21) Appl. No.: **13/412,957**

(22) Filed: **Mar. 6, 2012**

Related U.S. Application Data

(63) Continuation of application No. 13/277,182, filed on Oct. 19, 2011.

(60) Provisional application No. 61/424,611, filed on Dec. 17, 2010.

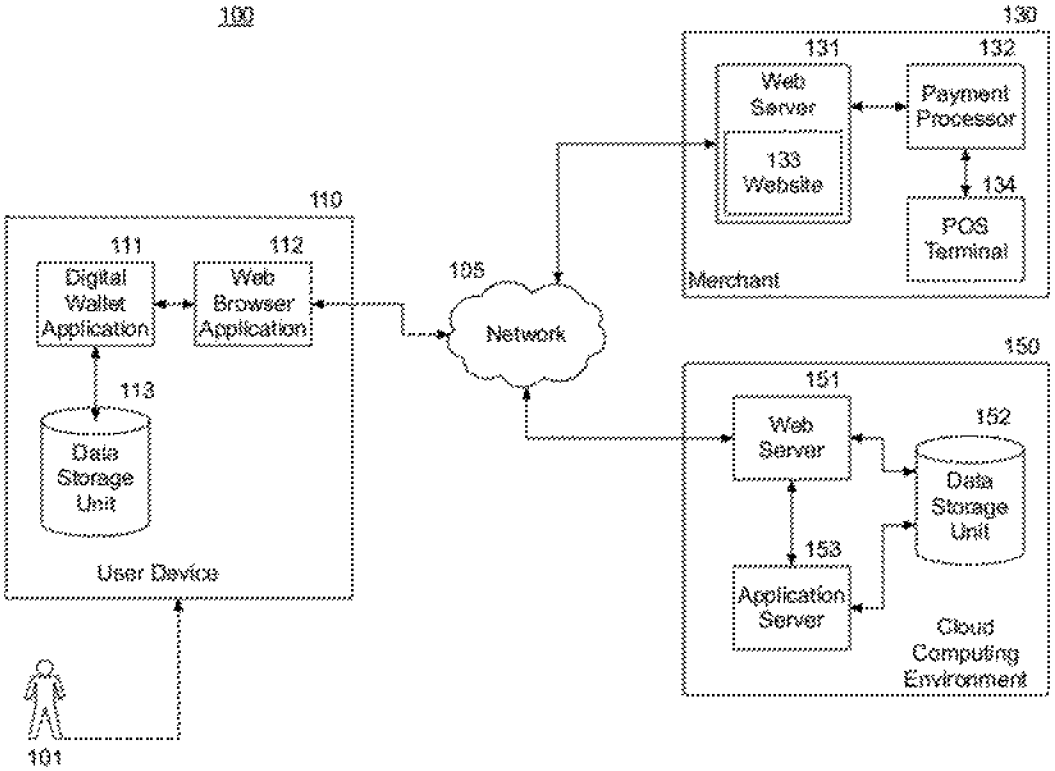
Publication Classification

(51) **Int. Cl.**
G06Q 20/36 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.** **705/41**

(57) **ABSTRACT**

A digital wallet that facilitates fast, convenient, and secure commerce using a mobile electronic device (or non-mobile electronic device) and stores information associated with transactions, such as purchase confirmations and receipts. The digital wallet can store information for use in transactions, including information associated with one or more financial accounts, user information, and shipping information. To complete an online purchase, the digital wallet can interact with a merchant's website to obtain information regarding the purchase. The digital wallet provides a user interface for the user to review and confirm the purchase information. The user interface also allows the user to select from multiple payment options, customize shipping information, or provide information requested by the merchant. The digital wallet can transmit user confirmation to the merchant's website and receive a receipt for the purchase. The digital wallet can store the receipt and synchronize the receipt with a remote storage location.



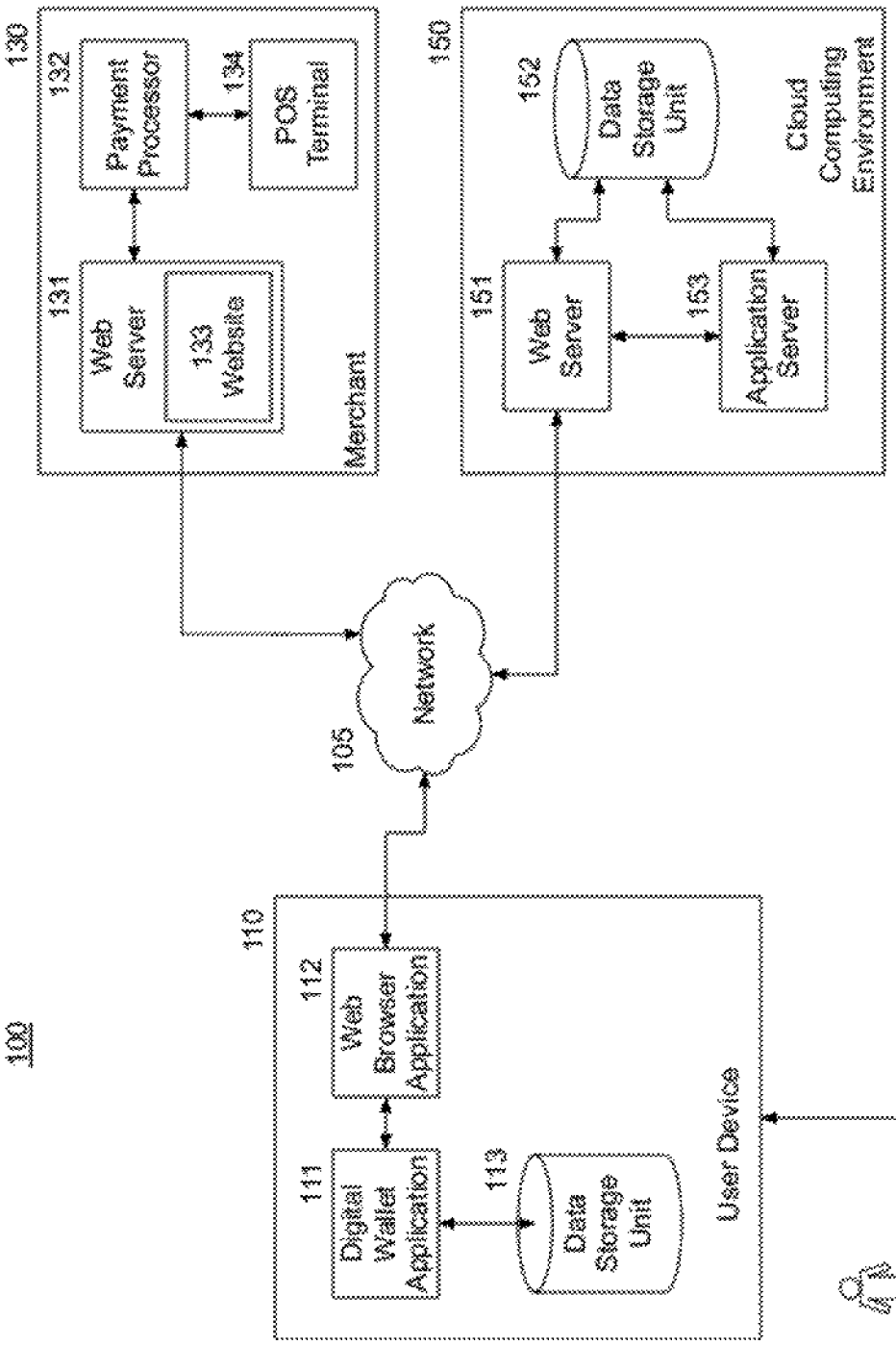

100
130
Merchant
132
Payment Processor
134
POS Terminal
131
Web Server
133
Website
150
Cloud Computing Environment
152
Data Storage Unit
151
Web Server
153
Application Server
105
Network
110
User Device
112
Web Browser Application
111
Digital Wallet Application
113
Data Storage Unit
101

Fig. 1

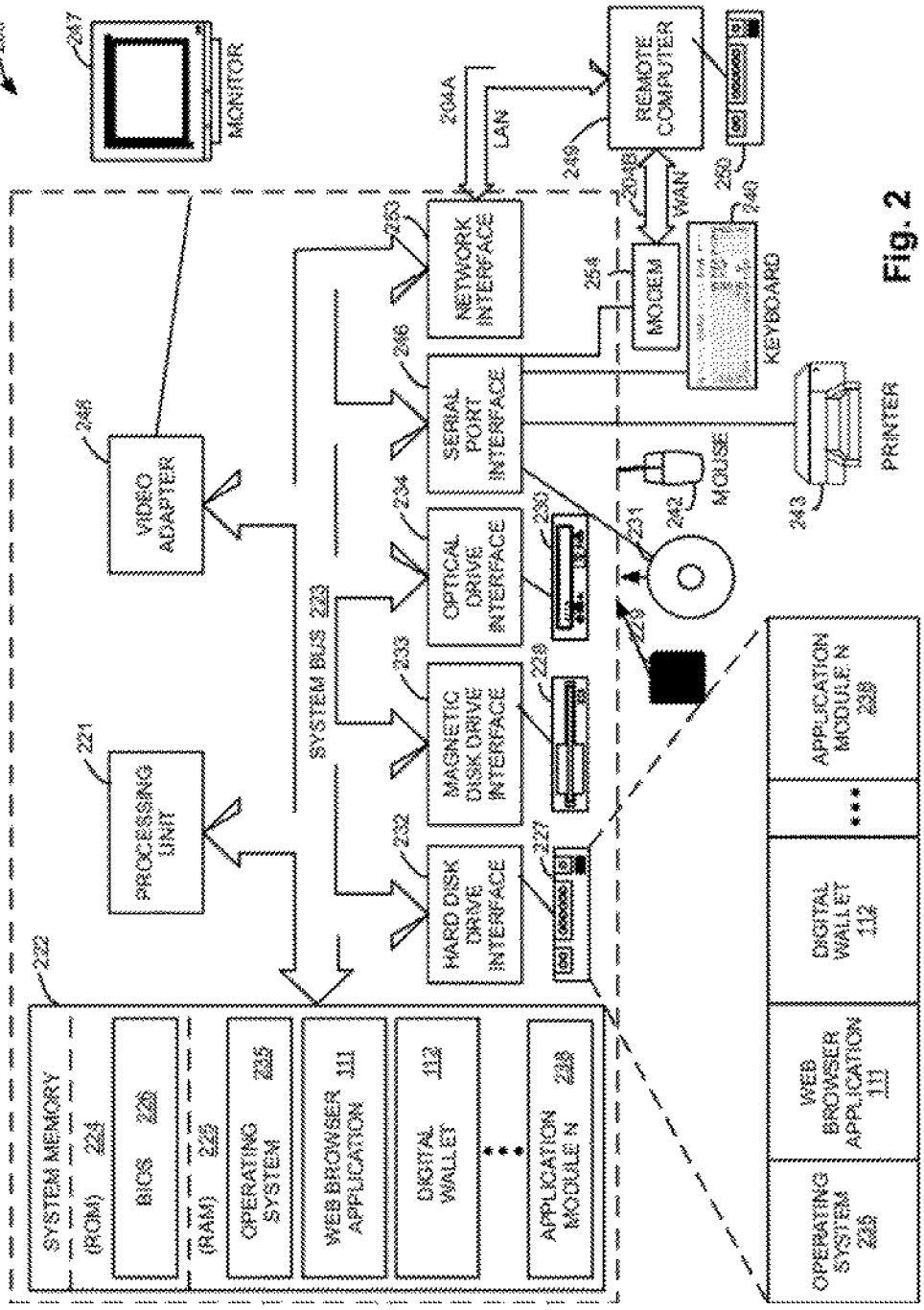

200
MONITOR
REMOTE COMPUTER
LAN
WAN
MODEM
KEYBOARD
PRINTER
MOUSE
NETWORK INTERFACE
SERIAL PORT INTERFACE
VIDEO ADAPTER
OPTICAL DRIVE INTERFACE
MAGNETIC DISK DRIVE INTERFACE
HARD DISK DRIVE INTERFACE
PROCESSING UNIT
SYSTEM BUS
SYSTEM MEMORY
(ROM)
BIOS
(RAM)
OPERATING SYSTEM
WEB BROWSER APPLICATION
DIGITAL WALLET
APPLICATION MODULE N
OPERATING SYSTEM
WEB BROWSER APPLICATION
DIGITAL WALLET
APPLICATION MODULE N

Fig. 2

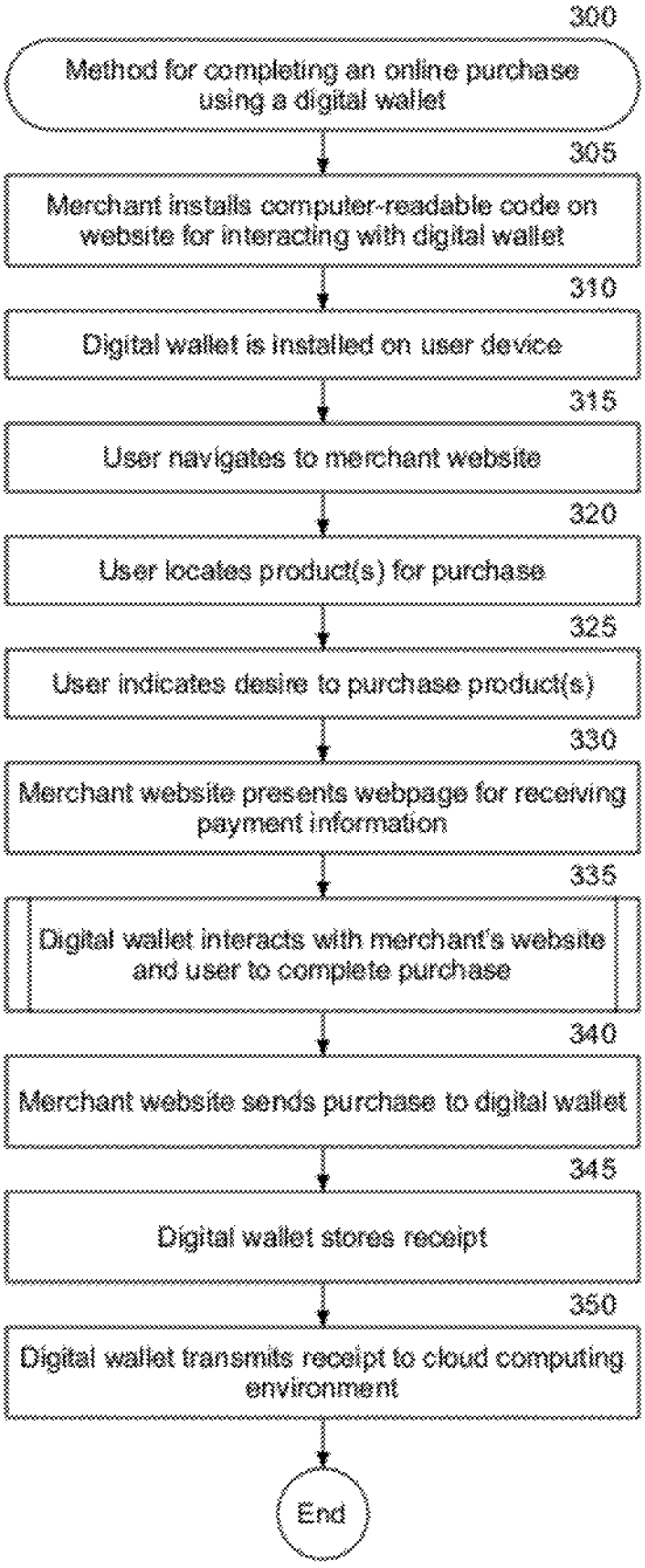

300
Method for completing an online purchase using a digital wallet
305
Merchant installs computer-readable code on website for interacting with digital wallet
310
Digital wallet is installed on user device
315
User navigates to merchant website
320
User locates product(s) for purchase
325
User indicates desire to purchase product(s)
330
Merchant website presents webpage for receiving payment information
335
Digital wallet interacts with merchant's website and user to complete purchase
340
Merchant website sends purchase to digital wallet
345
Digital wallet stores receipt
350
Digital wallet transmits receipt to cloud computing environment
End

Fig. 3

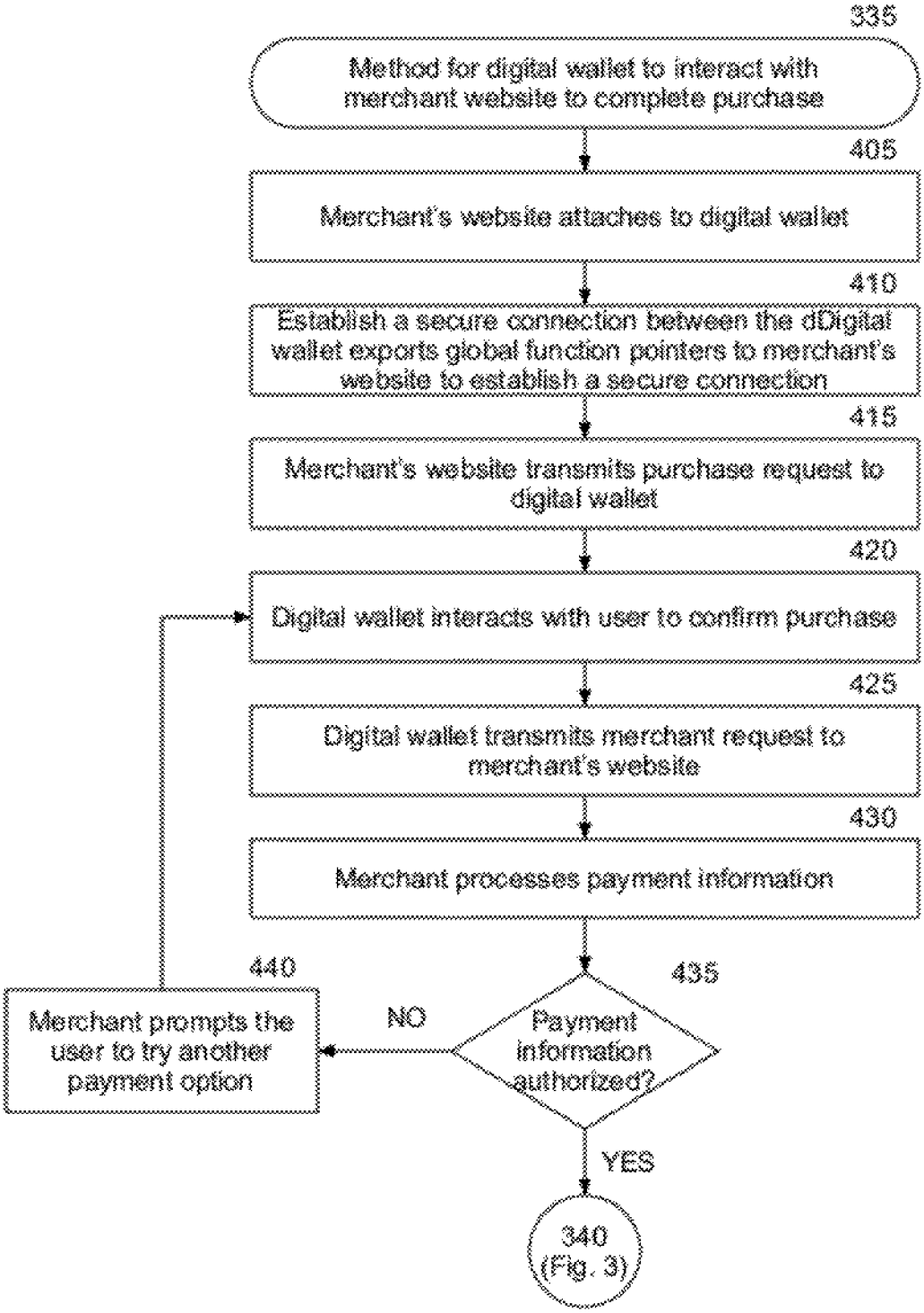

335
Method for digital wallet to interact with merchant website to complete purchase
405
Merchant's website attaches to digital wallet
410
Establish a secure connection between the dDigital wallet exports global function pointers to merchant's website to establish a secure connection
415
Merchant's website transmits purchase request to digital wallet
420
Digital wallet interacts with user to confirm purchase
425
Digital wallet transmits merchant request to merchant's website
430
Merchant processes payment information
435
Payment information authorized?
NO
440
Merchant prompts the user to try another payment option
YES
340 (Fig. 3)

Fig. 4

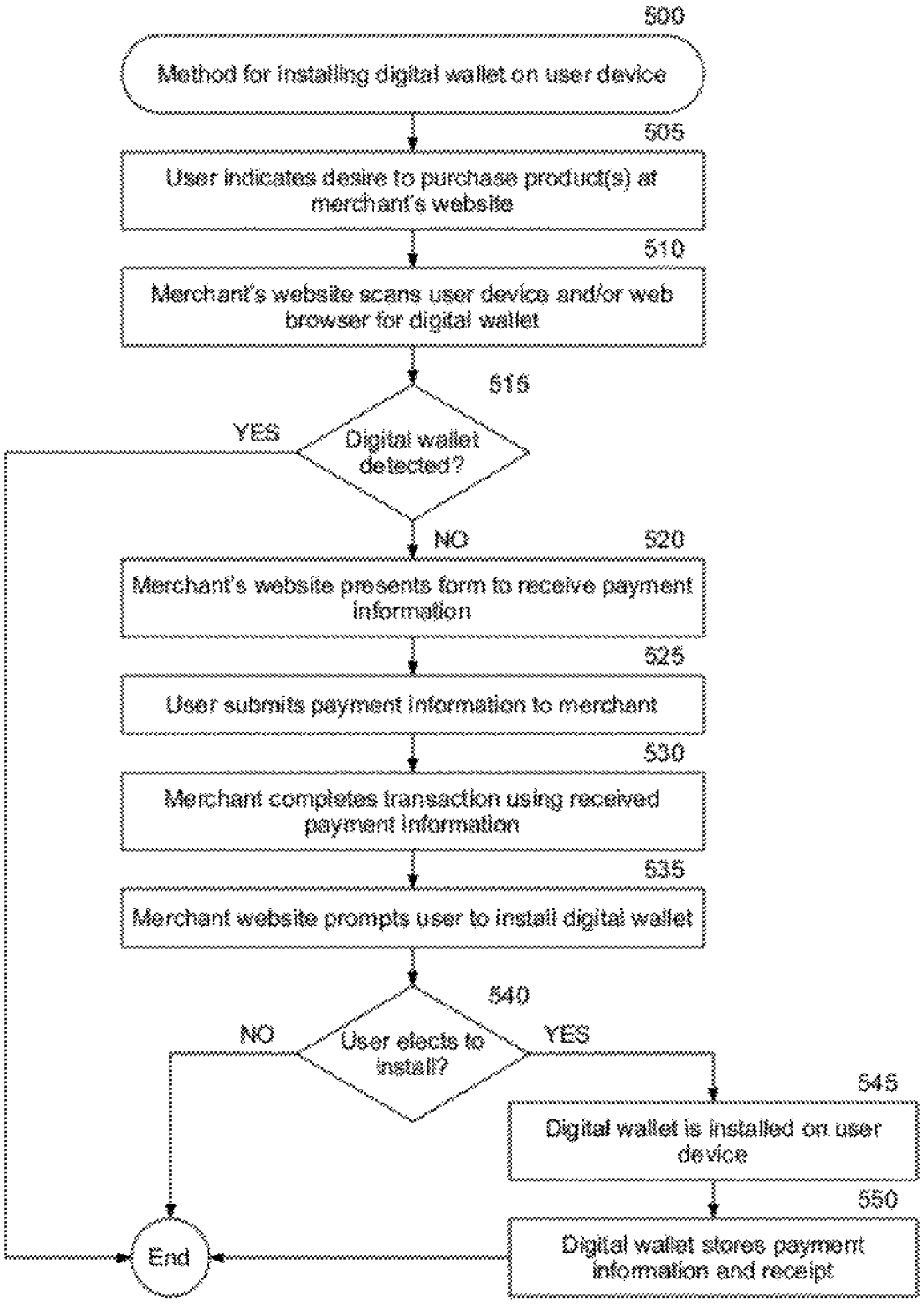

500
Method for installing digital wallet on user device
505
User indicates desire to purchase product(s) at merchant's website
510
Merchant's website scans user device and/or web browser for digital wallet
515
Digital wallet detected?
YES
NO
520
Merchant's website presents form to receive payment information
525
User submits payment information to merchant
530
Merchant completes transaction using received payment information
535
Merchant website prompts user to install digital wallet
540
User elects to install?
NO
YES
545
Digital wallet is installed on user device
550
Digital wallet stores payment information and receipt
End

Fig. 5

DIGITAL WALLET

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/424,611, filed Dec. 17, 2010 and entitled "Digital Wallet." The entire contents of the above-identified priority application are hereby fully incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates generally to electronic commerce, and more particularly to a digital wallet for facilitating transactions and storing information associated with transactions.

BACKGROUND

[0003] Electronic commerce, such as online shopping, has been increasingly common since the advent of the Internet. Online shopping websites generally provide a user interface for customers to select products to purchase. After the customer has selected products for purchase, the customer typically can choose from multiple payment options to purchase the products. Two conventional payment options generally supported by online merchants are using a financial account (for example, a credit card account or checking account) and using a third party payment processor, such as PAYPAL® or other processor.

[0004] To complete an online purchase using a credit card or other financial account, a consumer typically provides a significant amount of information to the merchant via the merchant's website. This information generally includes an account identifier (for example, credit card number, debit card number, etc.), shipping information, and the name, address, and contact information of the consumer. The requirement of entering this information for each merchant from which the consumer makes purchases can be cumbersome and frustrating to the consumers. This requirement can be particularly frustrating and difficult for consumers making online purchases using a mobile device, as many mobile devices do not include a user interface optimized to enter significant amounts of information. This deficiency for mobile devices results in substantially lower mobile browser conversion rates from product searching to product purchase compared to desktop browser conversion rates.

[0005] One conventional approach to alleviating the burden on the consumer involves a toolbar plug-in application for web browsers. Conventional toolbar applications are used to automatically populate web forms, such as a web form for receiving payment and consumer information for completing an online purchase, with stored information. However, these conventional toolbar applications often are inaccurate, as they merely attempt to predict which form is presented on a web page and then preload default values for the predicted form.

[0006] The use of a third party payment processor to complete online purchases is another approach to alleviating the burden of entering a significant amount of information at each merchant's website. Generally, a third party processor requires a consumer to register for an account and to provide one or more payment options. After registering, the consumer can use the payment options to complete purchases at participating merchants' websites. To complete an online purchase using the third party payment processor, the consumer generally selects a link at the merchant's website and, in response, the consumer is redirected from the merchant's website to a website of the third party payment processor. At this website, the consumer first has to provide login information and then can select one of the payment options to complete and confirm the purchase. After the purchase is confirmed, the consumer is directed back to the merchant's website. The third party payment processor then settles with the financial institution associated with the selected payment option and with the merchant to complete the transaction.

[0007] The use of a third party processor has several deficiencies. First, the process is disruptive to the consumer as the consumer is directed away from the merchant's website to the third party payment processor's website and then back to the merchant's website. Second, the use of a third party payment processor limits the amount of information that the merchant receives. For example, the merchant may not have access to information associated with the consumer or information regarding the payment method used. The use of a third party processor also presents an additional cost to the merchant.

[0008] Thus, a need in the art exists for systems and methods that overcome one or more of the above-described limitations.

SUMMARY

[0009] An aspect of the present invention provides a computer-implemented method for completing an online transaction. A digital wallet module resident on a client device receives a request for payment information to complete the transaction. The request originates from a website of a merchant. In response to receiving the request, the digital wallet module retrieves the payment information from a storage location on the client device and transmits the retrieved payment information to the merchant website.

[0010] Another aspect of the present invention provides a computer program product for completing an online transaction. The computer program product includes a computer-readable storage device having computer-readable program instructions stored therein. The computer-readable program instructions includes computer program instructions for receiving a request for payment information to complete the transaction, the request originating from a website of a merchant; computer program instructions for retrieving, in response to the request, the payment information; and computer program instructions for transmitting the retrieved payment information to the merchant website.

[0011] Another aspect of the present invention provides an apparatus for completing an electronic purchase from a merchant via a distributed network. The apparatus includes a web browser application a digital wallet module logically coupled to the web browser application. The digital wallet module is configured to receive a request for payment information to use in completing the purchase from the merchant website; retrieve payment information from a computer-readable storage device logically coupled to the digital wallet module; and transmit the retrieved payment information to the merchant.

[0012] Another aspect of the present invention provides a computer-implemented method for completing a purchase from a merchant via a website of the merchant. A digital wallet module embedded in a web browser in communication with the merchant website receives a purchase request message including a request for payment information for use in compensating the merchant for the purchase. In response to receiving the purchase request message, the digital wallet module presents a confirmation display requesting a user to

authorize the purchase. In response to receiving authorization from the user, the digital wallet module retrieves stored payment information and transmits a payment authorization message including the retrieved payment information to the merchant website.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. **1** is a block diagram depicting an operating environment of a digital wallet, in accordance with certain exemplary embodiments.

[0014] FIG. **2** is a block diagram depicting a general component architecture of a computer system, in accordance with certain exemplary embodiments.

[0015] FIG. **3** is a flow chart depicting a method for completing an online purchase using a digital wallet, in accordance with certain exemplary embodiments.

[0016] FIG. **4** is a flow chart depicting a method for a digital wallet to interact with a merchant website to complete a purchase, in accordance with certain exemplary embodiments.

[0017] FIG. **5** is a flow chart depicting a method for installing a digital wallet on a user device, in accordance with certain exemplary embodiments.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

Overview

[0018] The exemplary embodiments provide a digital wallet that can facilitate fast, convenient, and secure commerce using a mobile electronic device (or non-mobile electronic device) and that stores information associated with transactions, such as purchase confirmations and receipts. The digital wallet can provide a user interface for entering information for use in transactions, such as information associated with one or more financial accounts (for example, credit card or debit card information), contact information, and shipping information. The digital wallet can store this information for subsequent use in online (for example, via the Internet) and offline purchases (for example, via a merchant point of sale device, including a contactless payment device). The user can use the digital wallet to complete purchases by selecting a payment option stored by the digital wallet without the need to re-enter financial account information, contact information, or shipping information for each purchase. The user also may select a default payment option to use such that the user can confirm a purchase without making a payment option selection. The digital wallet can be particularly advantageous when utilized to complete a purchase using a mobile device, such as a mobile phone or other electronic device, having a limited user interface that may not be optimized to enter a significant amount of information.

[0019] The digital wallet can be embodied as a stand alone application program or as a companion program to a web browser, for example, as a companion program to a Hypertext Markup Language revision 5 ("HTML5") compliant web browser or other type of web browser having messaging and storage capabilities. In a web browser embodiment, the digital wallet can leverage the messaging and storage capabilities of the web browser to provide a consistent buying experience across multiple merchant websites. That is, the digital wallet can provide a consistent user interface independent of merchants' differing websites. The digital wallet also can allow a user to complete a purchase without navigating from the merchant's website as required by third party payment processors. While certain embodiments are described in which parts of the digital wallet are implemented in software, it will be appreciated that one or more acts or functions of the digital wallet may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems.

[0020] To complete an online transaction using the digital wallet, a user can navigate to a merchant's website using a web browser and locate one or more products. After the user indicates a desire to purchase one or more products, the digital wallet can interact with the merchant's website and with the user in a secure manner to complete the transaction. Once the transaction is completed, the digital wallet can receive or generate a confirmation or receipt for the transaction and can store the confirmation or receipt. The digital wallet also can synchronize the confirmation or receipt with a remote storage location, such as a cloud computing environment.

[0021] To complete an offline purchase at a merchant's store location, the digital wallet can interact with a merchant's point of sale device and with the user. The user can activate the digital wallet, for example, by launching an application, by pressing a physical or virtual button on the mobile device, or by making a gesture with the mobile device. The digital wallet can then communicate payment information to the point of sale device and, when the payment information is confirmed, receive a receipt from the point of sale device. The mobile device can communicate with the point of sale device using a wireless technology, such as near field communication technology (NFC), BLUETOOTH, or other suitable wireless technology.

[0022] The digital wallet can also store coupons or loyalty reward for use in transactions and can automatically apply the stored coupons during a purchase transaction, if appropriate. For example, a coupon for a product may be displayed to a user in response to an Internet search. The user can download the coupon to the digital wallet and store the coupon on the mobile device. The digital wallet can search the coupons during purchases to determine if one or more of the stored coupons may be applied to the purchase. If so, the digital wallet can automatically apply the stored coupon.

[0023] The digital wallet can communicate with a remote system to facilitate multiple functions. For example, the digital wallet can receive security information that identifies trusted merchants and non-trusted merchants from the remote system. The digital wallet can use this security information to prevent the user from providing financial account information or other information to non-trusted merchants. For example, the digital wallet may compare a merchant name, merchant website Uniform Resource Locator (URL), or Internet Protocol (IP) address to a list of known non-trusted merchants prior to passing information from the digital wallet to the merchant's website.

[0024] The remote system also can maintain an account for each individual user. This user account can include information associated with payment options for use in transactions and receipts or other information regarding completed transactions. The digital wallet can synchronize, for example, periodically, with the remote system to maintain current information at both locations. The remote system also may provide a user interface via a web browser that enables the user to modify information, such as financial account information of stored payment options and contact information for

use in transactions, and to access stored receipts. The user can access the stored receipts, for example, to determine when a certain purchase was made, to determine how much the user paid for an item, or for budgeting purposes. In certain implementations, the remote system or a third party having access to the receipts stored at the remote system can use the receipts to target advertisements or other promotional materials to the user.

[0025] Users may, in appropriate circumstances, be allowed to limit or otherwise affect the operation of the features disclosed in this specification. For example, users may be given an initial opportunity to opt-in or opt-out of the collection or use of certain data or the activation of certain features. In addition, users may be provided opportunities to change the manner in which the features are employed, including for situations in which users may have concerns regarding their privacy. Instructions also may be provided to users to notify the users regarding policies about the use of information, including personally identifiable information and receipt information, and manners in which the users may affect such use of information. Thus, sensitive personal information can be used to benefit a user, if desired, through receipt of targeted advertisements or other information, without risking disclosure of personal information or the user's identity.

[0026] One or more aspects of the invention may comprise a computer program that embodies the functions described and illustrated herein, wherein the computer program is implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions. However, it should be apparent that there could be many different ways of implementing the invention in computer programming, and the invention should not be construed as limited to any one set of computer program instructions. Further, a skilled programmer would be able to write such a computer program to implement an embodiment of the disclosed invention based on the appended flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the invention. Further, those skilled in the art will appreciate that one or more aspects of the invention described herein may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems. Moreover, any reference to an act being performed by a computer should not be construed as being performed by a single computer as the act may be performed by more than one computer. The inventive functionality of the invention will be explained in more detail in the following description, read in conjunction with the figures illustrating the program flow.

System Architecture

[0027] Turning now to the drawings, in which like numerals represent like (but not necessarily identical) elements throughout the figures, exemplary embodiments of the present invention are described in detail. FIG. **1** is a block diagram depicting an operating environment **100** for a digital wallet, in accordance with certain exemplary embodiments.

[0028] Referring to FIG. **1**, the exemplary operating environment **100** includes a merchant system **130**, a cloud computing environment **150**, and a user device **110** associated with a user **101**. The user device **110** may be a personal computer, mobile device, (for example, notebook computer, tablet computer, netbook computer, personal digital assistant (PDA), video game device, GPS locator device, cellular telephone, smartphone, or other mobile device), or other appropriate technology that includes or is coupled to a web browser application module **112**, such as GOOGLE'S CHROME, MICROSOFT'S INTERNET EXPLORER®, or MOZILLA'S FIREFOX®.

[0029] In certain exemplary embodiments, the web browser application **112** is an HTML5 compliant web browser. HTML5 compliant web browsers include a cross-document messaging application programming interface (API) and a local storage API that previous HTML versions did not have. The cross-document messaging API of HTML5 compliant web browsers enables documents, such as web pages, to communicate with each other. For example, a first document can send a message to a second document requesting information. In response, the second document can send a message including the requested information to the first document. The local storage API of HTML5 compliant web browsers enables the web browser to store information on a client device upon which the web browser is installed or is executing, such as the user device **110**. Websites also can employ the local storage API to store information on a client device. Other web browsers having cross-document messaging and/or local storage capabilities also may be used in certain exemplary embodiments.

[0030] The user **101** can use the web browser application **112** to view, download, upload, or otherwise access documents or web pages via a distributed network **105**. The network **105** includes a wired or wireless telecommunication system or device by which network devices (including devices **110**, **130**, and **150**) can exchange data. For example, the network **105** can include a local area network ("LAN"), a wide area network ("WAN"), an intranet, an Internet, or any combination thereof. Throughout the discussion of exemplary embodiments, it should be understood that the terms "data" and "information" are used interchangeably herein to refer to text, images, audio, video, or any other form of information that can exist in a computer based environment.

[0031] The web browser application **112** can interact with web servers (or other computing devices) connected to the network **105**, such as web server **132** of the merchant system **130** and/or web server **151** of the cloud computing environment **150**.

[0032] The user device **110** also includes a digital wallet application module **111**. The exemplary digital wallet **111** can interact with the web browser application **112** or can be embodied as a companion application of the web browser application **112**. As a companion application, the digital wallet **111** executes within the web browser application **112**. That is, the digital wallet **111** may be an application program embedded in the web browser application **112**.

[0033] The user device **110** also includes a data storage unit **113** accessible by the digital wallet **111** and the web browser application **112**. The exemplary data storage unit **113** can include one or more tangible computer-readable storage devices as discussed below with reference to FIG. **2**. The data storage unit **113** can be stored on the user device **110** or can be logically coupled to the user device **110**. For example, the data storage unit **113** can include on-board flash memory and/or one or more removable memory cards or removable flash memory.

[0034] The exemplary digital wallet **111** enables storage of one or more payment options that can be used for online purchases and offline purchases. Each payment option can

include or be associated with a financial account, such as a credit card account, a debit card account, a checking account, a savings account, a loyalty rewards account, or other type of account that can be used to make a purchase. The digital wallet **111** can store, for each payment option, information associated with the financial account for that payment option. This payment information can include a financial account identifier (for example, account number, card number), an expiration date of one or more financial cards associated with the financial account, and a billing address for the account. The payment information can also include information associated with the user **101**, such as name, contact information (for example, residential address, phone number, e-mail address), demographic information, or any other suitable information associated with the user **101**. The payment information also can include shipping information, such as one or more shipping addresses, preferred shipping provider(s), and preferred shipping method(s) (for example, ground, air, expedited, signature confirmation, or other shipping method). The payment information for each payment option can be maintained by the digital wallet **111** and stored in the data storage unit **113**.

[0035] The user **101** can interact with a user interface provided by the digital wallet **111** to add, modify, or remove payment information from the digital wallet **111**. In a web browser companion application embodiment, this user interface can be provided via the web browser application **112**. In addition or in the alternative, the payment information may be synchronized with a remote storage location, such as the cloud computing environment **150**. In such an embodiment, the user **101** can access the payment information stored at the remote location using another device, such as a desktop computer connected to the network **105**. The remote storage location can update the digital wallet **111** in response to any changes made at the remote storage location.

[0036] The payment option(s) stored in the digital wallet **111** can be used to complete purchases from merchants via a merchant's website **133** operating on the web server **131** or via a merchant's point of sale device **134**. In certain exemplary embodiments, each merchant's website **133** (operating on the web server **131**) that accepts payment via a digital wallet **111** can include a set of computer-readable program instructions, for example, using JavaScript, that enable the merchant's website **133** to interact with the digital wallet **111**. These program instructions can include program instructions for detecting whether the user device **110** includes a digital wallet **111** and program instructions for attaching to a detected digital wallet **111**. Once attached, the merchant's website **133** can communicate with the digital wallet **111**, for example, via cross-document messaging. In certain exemplary embodiments, the computer-readable instructions also include program instructions for downloading a digital wallet **111** onto a user device **110**. For example, if the merchant's website **133** detects that the user device **110** does not have a digital wallet **111**, the merchant's website **133** can prompt the user **101** to download and install the digital wallet **111**. If the user **101** elects to download the digital wallet **111**, the computer-readable program code can download and install the digital wallet **111** on the user device **101**. Embedding this computer-readable program instructions in a website **133** for interacting with a digital wallet **111** supports a simpler and efficient integration for the merchant system **130** compared to integrating with a third party payment processor.

[0037] The merchant's website **133** and the digital wallet **111** can communicate using a defined messaging protocol. The digital wallet **111** can encode a message using the protocol and send the encoded message to the merchant's website **133**, where the message is decoded using the protocol. Similarly, the merchant's website **133** can encode a message using the protocol and send the encoded message to the digital wallet **111** where the message is decoded using the protocol.

[0038] The merchant system **130** includes a payment processor **132** logically coupled to the web server **131**. The payment processor **132** can receive payment information via the web server **131** and interact with the financial institution (not shown) or an acquirer (not shown) to authorize payment information.

[0039] To complete an online purchase via the Internet, the digital wallet **111** can interact with a website **133** of the merchant system **130** and with the user **101**. The user **101** can browse the merchant's website **133** for products using the web browser **112** and indicate a desire to purchase one or more products. As used throughout the specification, the term "products" should be interpreted to include tangible and intangible products, as well as services. After the user **101** has indicated a desire to purchase the product(s) (for example, by actuating a "checkout" link), the merchant's website **133** can present a user interface in the form of a web page to receive payment information from the user **101**. The merchant's website **133** also can detect whether the user device **110** includes a digital wallet **111**. If the digital wallet **111** is detected, the merchant's website **133** can automatically attach to the digital wallet **111** as discussed in further detail below in connection with FIG. **4**. In addition or in the alternative, the merchant's website **133** can include a "pay with wallet" link or control that, when actuated, causes the merchant's website **133** to attach to the digital wallet **111**. Once attached, the merchant's website **133** sends a purchase request message to the digital wallet **111** requesting payment information. The purchase request message also can include information regarding the requested purchase, including information regarding the product(s) for purchase (for example, name and/or description of each product, price for each product, total price, etc.), information regarding the merchant system **130** (for example, merchant name, payment methods accepted by merchant, etc.), and requests for the user **101** to provide additional information. In response to receiving a purchase request message from the merchant's website **133**, the digital wallet **111** can present a user interface to the user **101** for the user **101** to confirm the purchase. This user interface can display all or a portion of the information in the purchase request and an actuatable button or link for the user **101** to confirm the purchase. This user interface also can allow the user **101** to select from multiple payment options stored by the digital wallet **111** to use as payment for the product(s) and from multiple shipping options. If the user **101** confirms the purchase, the digital wallet **111** can retrieve the information requested in the purchase request message, generate a merchant request message that contains the information and the confirmation, and transmit the merchant request message to the merchant's website **133**. If the purchase is authorized via the payment processor **132**, the merchant's website **133** can transmit an electronic confirmation and/or a receipt to the digital wallet **111** and then detach from the digital wallet **111**. The digital wallet **111** can store the confirmation and/or receipt at the user device **110** and also synchronize with the cloud computing environment **150**. An exemplary method for

completing an online purchase using the digital wallet **111** is illustrated in FIG. **3** and discussed below.

[0040] The receipt received by the digital wallet **111** can include line item details of the completed purchase. For example, the receipt can include a list of products purchased, a description of each product purchased, the price for each product purchased, a product category for each product purchased, a total price, a stock keeping unit (SKU) or similar identifier for each product purchased, taxes paid, rebates for one or more of the products purchased, payment method used, discounts applied, the time and/or date of purchase, warranty information for one or more of the products purchased, or other suitable information. The receipt also can include information regarding the merchant system **130**, including a name of the merchant associated with the merchant system **130**, a description of the **130**, the URL of the merchant's website **133**, and any other suitable information regarding the merchant system **130**.

[0041] In certain exemplary embodiments, the digital wallet **111** can generate a receipt for a purchase rather than or in addition to receiving a receipt from the merchant's website **133**. For example, the digital wallet **111** can generate the receipt using the information in the purchase request message received from the merchant's website **133** or from the merchant request message sent to the merchant's website **133**.

[0042] The exemplary cloud computing environment **150** includes the web server **151**, one or more data storage units **152**, and one or more application servers **153**. The cloud computing environment **150** may be provided by the provider of the digital wallet, by a merchant **130**, or by another party. In certain exemplary embodiments, multiple cloud computing environments **150** may be employed. For example, a first cloud computing environment may store receipt information and provide access to the receipts from a user device **110** connected to the first cloud computing environment, and a second cloud computing environment may provide security information, such as lists of non-trusted merchants, to the digital wallet **111**. Although the illustrated environment includes a cloud computing environment, other types of computing environments, such as a client-server environment may be used instead.

[0043] The application server **153** can maintain a digital wallet account for each user, including the user **101**. This digital wallet account can store (in the data storage unit **152**) the payment options created by the user **101** and their associated payment information and receipts and other information obtained by the digital wallet **111** in response to completed transactions. The application server **153** can synchronize this information with the digital wallet **111** periodically, on command (for example, by the user **101**), or in response to an update in information at the digital wallet **111** or at the cloud computing environment **150**.

[0044] The digital wallet **111** and the web browser application **112** can interact with the application server **151** via the web server **151**. The application server **153** can provide a user interface via the web server **151** that enables the user **101** to access, view, and/or modify content stored in the user's digital wallet account using the user device **110** or another device connected to the network. For example, the user **101** may add or modify payment information using a web browser application residing on a desktop computer having a better user interface for entering a significant amount of information.

[0045] The exemplary digital wallet **111** can include a user interface for accessing receipt information stored on the user device **110** or at the cloud computing environment **150** in a meaningful and useful way. One feature of this user interface enables the user **101** to search the receipts for information. For example, the user **101** may search for a product purchased to determine the price that was paid for the product or when the product was purchased. In another example, the user **101** may search for warranty information regarding a product to determine if the warranty has expired. In yet another example, the user **101** may search the receipts for merchant return policy information.

[0046] This digital wallet's user interface also includes a budgeting feature. This budgeting feature of the digital wallet **111** enables the user **101** to set a budget for expenditures associated with one or more products or product categories and to monitor this budget using the stored receipts. For example, the user **101** can set a budget of $200 to spend eating out each month. The digital wallet **111** can run a query on the receipts corresponding to transactions completed in the current month to identify receipts that correspond to a restaurant purchase or otherwise to eating out. The digital wallet **111** can then determine the total dollar amount of these receipts and the remaining budget for the current month.

[0047] The digital wallet's user interface also enables the user **101** to filter information associated with receipts and view the filtered information. The receipt information can be filtered by product category, merchant, time period, or any other receipt parameter or combination thereof. For example, the user **101** can use the digital wallet **111** to view the total amount spent at a particular merchant, such as the merchant associate with merchant system **130**, in the past three months or other desired time period.

[0048] One or more of the components of the exemplary operating environment **100**, such as the user device **110**, the web server **131**, the web server **151**, and the application server **153** can include one or more computer systems, such as the computer system **200** illustrated in FIG. **2**. Referring to FIG. **2**, the computer system **200** includes a processing unit **221**, a system memory **222**, and a system bus **223** that couples system components, including the system memory **222**, to the processing unit **221**. The system bus **223** can include any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, or a local bus, using any of a variety of bus architectures. The system memory **222** includes a read-only memory ("ROM") **224** and a random access memory ("RAM") **225**. A basic input/output system (BIOS) **226** containing the basic routines that help to transfer information between elements within the computer system **200**, such as during start-up, is stored in the ROM **224**.

[0049] The computer system **200** also includes a hard disk drive **227** for reading from and writing to a hard disk (not shown), a magnetic disk drive **228** for reading from or writing to a removable magnetic disk **229** such as a floppy disk, and an optical disk drive **230** for reading from or writing to a removable optical disk **231** such as a CD-ROM, compact disk-read/write (CD/RW), DVD, or other optical media. The hard disk drive **227**, magnetic disk drive **228**, and optical disk drive **230** are connected to the system bus **223** by a hard disk drive interface **232**, a magnetic disk drive interface **233**, and an optical disk drive interface **234**, respectively. Although the exemplary computer system **200** employs a ROM **224**, a RAM **225**, a hard disk drive **227**, a removable magnetic disk **229**, and a removable optical disk **231**, other types of computer-readable media also can be used in the exemplary computer system **200**. For example, the computer-readable media

can include any apparatus that can contain, store, communicate, propagate, or transport data for use by or in connection with one or more components of the computer system **200**, including any electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or propagation medium, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, and the like. The drives and their associated computer-readable media can provide nonvolatile storage of computer-executable instructions, data structures, program modules, and other data for the computer system **200**.

[0050] A number of modules can be stored on the ROM **224**, RAM **225**, hard disk drive **227**, magnetic disk **229**, or optical disk **231**, including an operating system **235**, an application module **238**, and the web browser application **112**, the digital wallet **111**, and the website application discussed above in connection with FIG. **1**. The web browser application **112**, the digital wallet **111**, website application, and application module **238** can include routines, sub-routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types.

[0051] A user, such as user **101**, can enter commands and information to the computer system **200** through input devices, such as a keyboard **240** and a pointing device **242**. The pointing device **242** can include a mouse, a trackball, an electronic pen that can be used in conjunction with an electronic tablet, or any other input device, such as a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit **222** through a serial port interface **246** that is coupled to the system bus **223**, but can be connected by other interfaces, such as a parallel port, game port, a universal serial bus (USB), or the like. A display device **247**, such as a monitor, also can be connected to the system bus **223** via an interface, such as video adapter **248**. In addition to the display device **247**, the computer **220** can include other peripheral output devices, such as speakers (not shown) and a printer **243**.

[0052] The computer system **200** is configured to operate in a networked environment using logical connections to one or more remote computers **249**. The remote computer **249** can be any network device, such as a personal computer, a server, a client, a router, a network PC, a peer device, or other device. While the remote computer **249** typically includes many or all of the elements described above relative to the computer system **200**, only a memory storage device **250** has been illustrated in FIG. **2** for simplicity. The logical connections depicted in FIG. **2** include a LAN **204**A and a WAN **204**B. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

[0053] When used in a LAN networking environment, the computer system **200** is often connected to the LAN **204**A through a network interface or adapter **253**. When used in a WAN networking environment, the computer system **200** typically includes a modem **254** or other means for establishing communications over the WAN **204**B, such as the Internet. The modem **254**, which can be internal or external, is connected to system bus **223** via a serial port interface **246**. In a networked environment, program modules depicted relative to computer system **200**, or portions thereof, can be stored in the remote memory storage device **250**.

[0054] It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used. Moreover, those having ordinary skill in the art having the benefit of the present disclosure will appreciate that the computer system **200** illustrated in FIG. **2** can have any of several other suitable computer system configurations. Furthermore, those skilled in the art having the benefit of the present disclosure will recognize that certain components of the computer system **200** may be added, deleted, or modified in certain alternative embodiments. For example a user device **101** embodied as a mobile phone or handheld computer may not include all the components depicted in FIG. **2** and/or described above.

System Process

[0055] The components of the exemplary operating environment **100** are described hereinafter with reference to the exemplary methods illustrated in FIGS. **3-5**. The exemplary embodiments can include one or more computer programs that embody the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing aspects of the exemplary embodiments in computer programming, and these aspects should not be construed as limited to one set of computer instructions. Further, a skilled programmer would be able to write such computer programs to implement exemplary embodiments based on the flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the exemplary embodiments. Further, those skilled in the art will appreciate that one or more acts described may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems.

[0056] FIG. **3** is a flow chart depicting a method **300** for completing an online purchase using a digital wallet **111**, in accordance with certain exemplary embodiments. With reference to FIGS. **1** and **3**, in block **305**, the merchant installs computer-readable program instructions on the merchant's website **133** for interacting with the digital wallet **111**. These computer-readable program instructions can be implemented as an embedded script, such as JavaScript, in a web page of the merchant system **130**. For example, the merchant system **130** can embed the computer-readable program instructions on a "checkout" web page of the merchant's website **133**.

[0057] The computer-readable program instructions can include program instructions for interacting with web browser applications, such as web browser application **112**, to determine whether the user device **110** has a digital wallet **111** installed thereon. The computer-readable program instructions also can include program instructions for attaching to a detected digital wallet **111** to exchange messages. In certain exemplary embodiments, the program instructions are configured to exchange messages with a digital wallet **111** embedded in an HTML5 compliant web browser **112**. In an exemplary embodiment, the computer-readable program instructions comprise execute when the browser application **112** on the user device **110** downloads a web page from the merchant's website **133**. The browser application **112** executes the code locally to search for an installed digital wallet **111** on the user device **110**. If a digital wallet **111** is installed, then the browser is instructed to surface a wallet control button for selection by the user. If a digital wallet **111** is not installed, then the browser is instructed to surface

another control for interaction with the user, such as an option to install a wallet application **111**.

[0058] In block **310**, the digital wallet **111** is installed on the user device **110**. In certain exemplary embodiments, the user **101** can navigate to a website **133** of a provider of the digital wallet **111** and download and install the digital wallet **111**. In certain exemplary embodiments, as discussed previously, a merchant's website **133** can prompt the user **101** to download and install the digital wallet **111**, for example, upon selecting the "checkout" option on the merchant's website **133**. In such an embodiment, the user **101** may provide payment information to the merchant's website **133** in a conventional manner and then download and install the digital wallet **111**. The payment information provided to the merchant's website **133** can then be automatically stored in the digital wallet **111** installed on the user device **101**. An exemplary method of installing a digital wallet **111** is discussed further in connection with FIG. **5**.

[0059] In block **315**, the user **101** navigates to the merchant's website **133** using the web browser application **112**. In block **320**, the user **101** browses the merchant's website **133** for one or more products to purchase. In block **325**, the user **101** indicates a desire to purchase one or more products. For example, the user **101** may browse the merchant's website **133** and add products to a virtual shopping cart. Once the user **101** is ready to checkout, the user **101** can actuate a "checkout" link on the merchant's website **133**.

[0060] In block **330**, the merchant's website **133** presents a web page via the web browser application **112** for obtaining payment information from the user **101**. This web page can include conventional payment options, such as a form for receiving payment information and contact information and/or a link to a third party payment processor. This web page also can include the computer-readable program instructions for detecting and interacting with the digital wallet **111**. Furthermore, this web page can include a "pay with wallet" link or button that the user **101** can select to pay using the digital wallet **111**.

[0061] In block **335**, the merchant's website **133** interacts with the digital wallet **111** to complete the purchase of the products selected by the user **101**. The merchant's website **133** can attach to the digital wallet **111** and send a purchase request message to the digital wallet **111**. As discussed above, the purchase request message can include a request for payment information and further include information regarding the requested purchase, such as information associated with the selected products and information associated with the merchant system **130**. In response to receiving the purchase request message, the digital wallet **111** can present a user interface to the user **101** for the user **101** to confirm the purchase. The user interface also can allow the user **101** to select from multiple payment options to send to the merchant's website **133**. If the user **101** confirms the purchase, the digital wallet **111** sends a merchant request message including the confirmation and payment information associated with the payment option to the merchant's website **133**. The payment processor **132** can interact with an acquirer or the financial institution associated with the payment information to authorize the purchase. Block **335** is discussed in further detail in connection with FIG. **4**.

[0062] In block **340**, the merchant's website **133** sends a message including a receipt to the digital wallet **111**. The receipt can include information associated with the purchase, such as a list of products purchased, a description of each product purchased, the price for each product purchased, a product category for each product purchased, a total price, a stock keeping unit (SKU) or similar product identifier for each product purchased, taxes paid, rebates for one or more of the products purchased, payment method used, discounts applied, the time and/or date of purchase, warranty information for one or more of the products purchased, or other suitable information. The receipt also can include information regarding the merchant associated with the merchant system **130**, including a name of the merchant, a description of the merchant, the URL of the merchant's website **133**, and other suitable information regarding the merchant or the merchant system **130**.

[0063] In block **345**, the digital wallet **111** stores the receipt in the data storage unit **113**. In an embodiment where the digital wallet **111** is embedded in an HTML5 compliant web browser application (or similar web browser application), the digital wallet **111** can employ the local storage functionality of the web browser application to store the receipt in the data storage unit **113**.

[0064] In block **350**, the digital wallet **111** synchronizes with the cloud computing environment **150** by sending the receipt to the web server **151**. The web server **151**, in turn, stores, in the data storage unit **152**, the received receipt in the user's digital wallet account with the cloud computing environment **150**. From step **350**, the method **300** ends.

[0065] FIG. **4** is a flow chart depicting a method **335** for a digital wallet to interact with a merchant website **133** to complete a purchase, in accordance with certain exemplary embodiments, as referenced in step **335** of FIG. **3**. With reference to FIGS. **1** and **4**, in block **405**, the merchant's website **133** attaches to the digital wallet **111** by establishing a connection between the website **133** and the digital wallet **111**.

[0066] In block **410**, the digital wallet **111** and the merchant's website **133** establish a secure connection for communication between the digital wallet **111** and the merchant's website **133**. In certain exemplary embodiments, the digital wallet **111** may authenticate the merchant's website **133** prior to establishing the secure connection. For example, the digital wallet **111** may compare the merchant name, the URL of the merchant's website **133**, or the IP address of the merchant's website **133** to a list of known trusted or known non-trusted merchants prior to establishing the secure connection. If the merchant system **130** is not trusted by the digital wallet **111**, then the digital wallet **111** will not authorize the secure connection, rather the digital wallet **111** detaches from the merchant's website **133** by disconnecting the connection between the website **133** and the digital wallet **111**.

[0067] After establishing the secure connection, in block **415**, the merchant's website **133** transmits a purchase request message to the digital wallet **111**. The purchase request message includes a request for payment information from the digital wallet **111** to complete the purchase. The purchase request message also can include information regarding the product(s) for purchase, such as a name and/or description of each product, a price for each product, a total price for all products, taxes, shipping charges, handling charges, other charges, a SKU or other product identifier for each product, shipping options and associated costs, and/or a discount amount for each product. The purchase request message also can include information regarding the merchant, such as the merchant's name, a description of the merchant, and/or payment methods accepted by the merchant (for example, VISA, MASTERCARD, debit card, or other payment method). In

certain exemplary embodiments, the purchase request message also can include a request for the user **101** to provide additional information. This request can be configured by the merchant to solicit additional information from the user **101**, such as an e-mail address or a loyalty rewards account number.

[0068] In block **420**, the digital wallet **111** receives the purchase request message from the merchant's website **133** and interacts with the user **101** to confirm the purchase. In certain exemplary embodiments, this interaction includes the digital wallet **111** presenting a user interface on the user device **110** that displays information associated with the purchase to the user **101** and requests confirmation to complete the purchase. The information displayed by the digital wallet **111** may include some or all of the information included in the purchase request message.

[0069] In certain exemplary embodiments, the user interface displayed by the digital wallet **111** also enables the user **101** to select from multiple payment options stored by the digital wallet **111**. The user interface also may allow the user **101** to select or update shipping information. The digital wallet **111** may block the user from using a payment option not accepted by the merchant system **130** as indicated in the purchase request message. The user interface also may prompt the user **101** to enter information requested by the merchant system **130** in the purchase request message. After reviewing the purchase information and/or selecting a payment method, updating shipping information, and/or providing additional information, the user **101** actuates a link or button control to confirm the purchase. If the user **101** does not want to confirm the purchase, the user **101** selects a "cancel" link or button control to cancel the purchase, thereby terminating the session between the digital wallet **111** and the website **133**.

[0070] In block **425**, if the user **101** confirmed the purchase in block **420**, the digital wallet **111** generates and transmits a merchant request message to the merchant's website **133**. The merchant request message includes confirmation of the purchase and payment information to use in completing the purchase. For example, the merchant request message can include the form of payment and all information needed to process that payment (for example, credit card number), shipping method, shipping address, e-mail address, user name, and any other information for the purchase transaction. The merchant request message also can include the information in the purchase request message and any information requested by the merchant system **130**. The digital wallet **111** can automatically retrieve payment information for a selected payment option from the data storage unit **113** to include in the merchant request message upon confirmation from the user **101** and/or a selection of a payment option by the user **101**.

[0071] In block **430**, the merchant's website **133** receives the merchant request message and sends the payment information to the payment processor **132** for processing. The payment processor **132** interacts with an acquirer or a financial institution associated with the payment information to authorize the payment information and to credit and debit the appropriate accounts for payment from the user **101** to the merchant.

[0072] In block **435**, the web server **131** receives a message from the payment processor **132** indicating whether the payment information was authorized. If the payment information was authorized, the method **335** follows the "YES" branch to step **340**, as referenced in FIG. **3**. Otherwise, the method **335** follows the "NO" branch to step **440**.

[0073] In step **440**, the merchant's website **133** notifies the user **101** that the payment information was not authorized and can prompt the user **101** to try another payment option. After block **440**, the method **335** returns to block **420** where the digital wallet **111** interacts with the user **101** to complete the purchase using a different payment option. The user **101** could cancel the purchase if the user **101** does not want to complete the purchase using a different payment option.

[0074] FIG. **5** is a flow chart depicting a method **500** for installing a digital wallet on a user device, in accordance with certain exemplary embodiments. With reference to FIGS. **1** and **5**, in block **505**, the user **101** indicates a desire to purchase one or more products at the merchant's website **133**. This act performed in block **505** can be substantially similar to steps **315-325** illustrated in FIG. **3** and discussed above.

[0075] In block **510**, the merchant's website **133** scans the user device **110** and/or the web browser application **112** to determine whether a digital wallet **111** is installed on the user device **110** or embedded in the web browser application **112**. In block **515**, if the merchant's website **133** detects a digital wallet **111**, then the method **500** follows the "YES" branch and ends as a digital wallet **111** is already installed on the user device **110**. If a digital wallet **111** is not detected by the merchant's website **133**, the method **500** follows the "NO" branch to block **520**.

[0076] In block **520**, the merchant's website **133** presents a form for the user **101** to provide payment information to complete the purchase of the one or more products. This form can be similar to a conventional web form having text entry fields for receiving credit card, debit card, or other payment information, shipping address, billing address, e-mail address, name, phone number, and other user information. The form also can include fields for receiving user information and user contact information.

[0077] In block **525**, the user **101** completes the form by providing the requested information and submits the form to the merchant's website **133**. In block **530**, the merchant system **130** processes the received payment information and completes the transaction. In block **535**, the merchant's website **133** prompts the user **101** to download and install the digital wallet **111** on the user device **110**.

[0078] In block **540**, if the user **101** elects to install the digital wallet **111**, the method **500** follows the "YES" branch to block **550**. Otherwise, the method **500** follows the "NO" branch and the method **500** ends.

[0079] In block **545**, the merchant's website **133** downloads and initiates the installation of the digital wallet **111** on the user device **110**. During the installation process, the digital wallet **111** can prompt the user **101** to set up a digital wallet account at the cloud computing environment. The user **101** can opt-in or opt-out of this feature and also can select to install or activate certain features only. If the user **101** opts-in to the digital wallet account, the digital wallet **111** can obtain information from the user **101** for the account, such as payment information, contact information, preferred shipping information, and a user name and password for security purposes.

[0080] The installed digital wallet **111** can interact with the merchant's website **133** to obtain the payment information used to complete the purchase and a receipt for the purchase. In block **550**, the digital wallet **111** stores the payment information and the receipt in the data storage unit **113**. If the user

101 elected to create a digital wallet account with the cloud computing environment, the digital wallet **111** synchronizes the receipt and the payment information with the digital wallet account.

[0081] In an alternative exemplary embodiment, the installation of the digital wallet **111** on user device **110** can occur prior to step **520**, whereby the user downloads the digital wallet application **111**, provides the payment and user information for storage by the digital wallet **111** on the date storage unit **113**, and then completes the purchase with the website **133** via the digital wallet **111**.

General

[0082] The exemplary embodiments described herein can be used with computer hardware and software that perform the methods and processing functions described previously. The systems, methods, and procedures described herein can be embodied in a programmable computer, computer-executable software, or digital circuitry. The software can be stored on computer-readable media. For example, computer-readable media can include a floppy disk, RAM, ROM, hard disk, removable media, flash memory, memory stick, optical media, magneto-optical media, CD-ROM, etc. Digital circuitry can include integrated circuits, gate arrays, building block logic, field programmable gate arrays (FPGA), etc.

[0083] The exemplary methods and acts described in the embodiments presented previously are illustrative, and, in alternative embodiments, certain acts can be performed in a different order, in parallel with one another, omitted entirely, and/or combined between different exemplary embodiments, and/or certain additional acts can be performed, without departing from the scope and spirit of the invention. Accordingly, such alternative embodiments are included in the inventions described herein.

[0084] Although specific embodiments have been described above in detail, the description is merely for purposes of illustration. It should be appreciated, therefore, that many aspects described above are not intended as required or essential elements unless explicitly stated otherwise. Modifications of, and equivalent acts corresponding to, the disclosed aspects of the exemplary embodiments, in addition to those described above, can be made by a person of ordinary skill in the art, having the benefit of the present disclosure, without departing from the spirit and scope of the invention defined in the following claims, the scope of which is to be accorded the broadest interpretation so as to encompass such modifications and equivalent structures.

1-31. (canceled)

32. A computer-implemented method for installing a digital wallet module on a user device, comprising:

reading, by a computer, information from a user device in response to receiving a request for payment information to complete an online transaction;

determining, by the computer, that a digital wallet module is not present on the user device based on the information read from the user device;

communicating, by the computer, a form for presentation on the user device in response to determining that a digital wallet module is not present on the user device, the form comprising a request for payment information to complete the transaction;

receiving, by the computer, the payment information from the user device;

communicating, by the computer, a request to install a digital wallet module on the user device based on determining that a digital wallet module is not present on the user device;

receiving, by the computer, an acceptance from the user device of the request to install the digital wallet module on the user device;

communicating, by the computer, the digital wallet module to the user device for installation on the user device in response to receiving the acceptance; and

communicating, by the computer, the payment information to the user device for storage in connection with the digital wallet module.

33. The computer-implemented method of claim **32**, wherein the computer is operated by the merchant website.

34. The computer-implemented method of claim **32**, further comprising submitting the payment information to the merchant website to complete the online transaction.

35. The computer-implemented method of claim **32**, further comprising retrieving the payment information from the merchant website, in response to receiving the acceptance from the user device of the request to install the digital wallet module on the user device.

36. The computer-implemented method of claim **32**, wherein the user device comprises a mobile telephone.

37. The computer-implemented method of claim **32**, wherein the user device comprises a computer.

38. A computer-implemented method for completing an online transaction, comprising:

reading, by a computer, a user device in response to receiving a request for payment information to complete the online transaction;

determining, by the computer, a digital wallet module is resident on the user device based on the information read from the user device, wherein the digital wallet module is embedded in the web browser;

authorizing, by the computer, a request to submit payment information from the digital wallet module resident on the user device;

establishing, by the computer, a secure connection with the digital wallet module resident on the user device;

submitting, by the computer, to the digital wallet module resident on the user device, a request for payment information to complete the transaction, the request originating from the merchant website;

receiving, by the computer, the payment information from the digital wallet module;

submitting, by the computer, a payment authorization request to a financial institution, wherein the financial institution corresponds to the payment information provided by the digital wallet module to pay for the transaction; and

receiving, by the computer, a payment authorization for the request from the financial institution authorizing the payment in accordance with the payment information.

39. The computer-implemented method of claim **38**, wherein the computer is operated by the merchant website.

40. The computer-implemented method of claim **38**, further comprising authorizing the online transaction in response to receiving the payment authorization.

41. The computer-implemented method of claim **38**, further comprising transmitting confirmation of an authorized online transaction to the digital wallet module resident on the user device.

42. The computer-implemented method of claim **41**, wherein the confirmation of the authorized online transaction comprises at least one of a total price for the transaction, a description of the product or service purchased, and a form of payment used to authorize the only transaction.

43. The computer-implemented method of claim **38**, wherein the user device comprises a mobile telephone.

44. The computer-implemented method of claim **38**, wherein the user device comprises a computer.

45. A computer-implemented method for completing an online transaction, comprising:

saving, by a digital wallet module resident on a user device, user information to a storage location on the user device, the user information comprising one or more payment options;

receiving, by the digital wallet module, authorization for a request from a merchant website to submit payment information from the digital wallet module;

establishing, by the digital wallet module, a secure connection with the merchant website in response to receiving authorization for the request to submit payment information from the digital wallet module;

receiving, by the digital wallet module, a request for payment information to complete the transaction, the request originating from the merchant website, wherein the digital wallet module executes within the same web browser application as the merchant website;

retrieving, by the digital wallet module, user information from the storage location on the user device in response to receiving the request for payment information;

presenting, by the digital wallet module, on the user device a request to confirm the transaction from the merchant website and to select a payment option to complete the transaction, wherein the payment option is selected from one of a plurality of payment options stored by the digital wallet module;

receiving, by the digital wallet module, confirmation of the transaction and the selection of payment option to complete the transaction from the user device; and

transmitting, by the digital wallet module, the selection of payment option to the merchant website.

46. The computer-implemented method of claim **45**, further comprising receiving a confirmation of an authorized online transaction to the digital wallet module resident on the user device.

47. The computer-implemented method of claim **46**, wherein the confirmation of the authorized online transaction comprises at least one of a total price for the transaction, a description of the product or service purchased, and a form of payment used to authorize the only transaction.

48. The computer-implemented method of claim **45**, wherein the user device comprises a mobile telephone.

49. The computer-implemented method of claim **45**, wherein the user device comprises a computer.

50. A computer program product, comprising:

a non-transitory computer-readable medium having computer-readable program code embodied therein for completing an online transaction, the computer-readable medium comprising:

computer-readable program code for reading a user device in response to receiving a request for payment information to complete the online transaction;

computer-readable program code for determining a digital wallet module is resident on the user device based on the information read from the user device, wherein the digital wallet module is embedded in the web browser;

computer-readable program code for authorizing a request to submit payment information from the digital wallet module resident on the user device;

computer-readable program code for establishing a secure connection with the digital wallet module resident on the user device;

computer-readable program code for submitting to the digital wallet module resident on the user device, a request for payment information to complete the transaction, the request originating from the merchant website;

computer-readable program code for receiving the payment information from the digital wallet module;

computer-readable program code for submitting a payment authorization request to a financial institution, wherein the financial institution corresponds to the payment information provided by the digital wallet module to pay for the transaction; and

computer-readable program code for receiving a payment authorization for the request from the financial institution authorizing the payment in accordance with the payment information.

51. The computer program product of claim **50**, further comprising computer-readable program code for authorizing the online transaction in response to receiving the payment authorization.

52. The computer program product of claim **50**, further comprising computer-readable program code for transmitting confirmation of an authorized online transaction to the digital wallet module resident on the user device.

53. The computer program product of claim **52**, wherein the confirmation of the authorized online transaction comprises at least one of a total price for the transaction, a description of the product or service purchased, and a form of payment used to authorize the only transaction.

54. The computer program product of claim **50**, wherein the user device comprises a mobile telephone.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

von Behren et al.

(10) **Pub. No.: US 2012/0166333 A1**

(43) **Pub. Date: Jun. 28, 2012**

(54) **DIGITAL WALLET**

(75) Inventors: **Rob von Behren**, Berkeley, CA (US); **Jonathan Wall**, San Francisco, CA (US)

(73) Assignee: **GOOGLE Inc.**, Mountain View, CA (US)

(21) Appl. No.: **13/412,957**

(22) Filed: **Mar. 6, 2012**

Related U.S. Application Data

(63) Continuation of application No. 13/277,182, filed on Oct. 19, 2011.

(60) Provisional application No. 61/424,611, filed on Dec. 17, 2010.

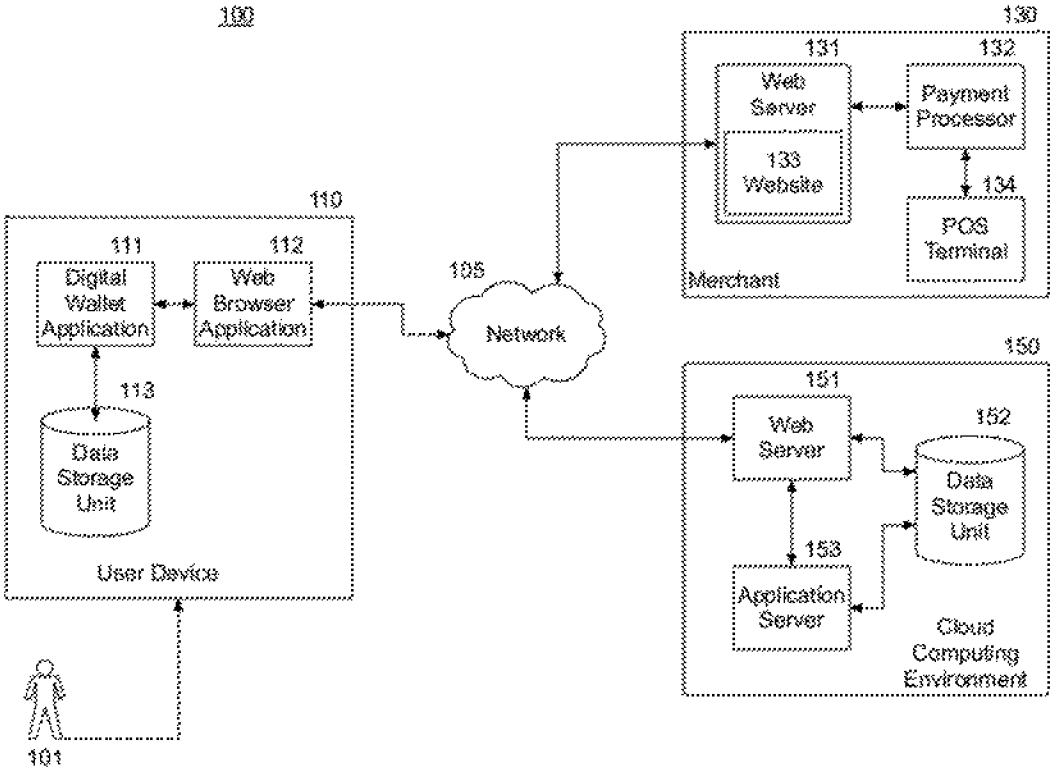
Publication Classification

(51) **Int. Cl.**
G06Q 20/36 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.** **705/41**

(57) **ABSTRACT**

A digital wallet that facilitates fast, convenient, and secure commerce using a mobile electronic device (or non-mobile electronic device) and stores information associated with transactions, such as purchase confirmations and receipts. The digital wallet can store information for use in transactions, including information associated with one or more financial accounts, user information, and shipping information. To complete an online purchase, the digital wallet can interact with a merchant's website to obtain information regarding the purchase. The digital wallet provides a user interface for the user to review and confirm the purchase information. The user interface also allows the user to select from multiple payment options, customize shipping information, or provide information requested by the merchant. The digital wallet can transmit user confirmation to the merchant's website and receive a receipt for the purchase. The digital wallet can store the receipt and synchronize the receipt with a remote storage location.



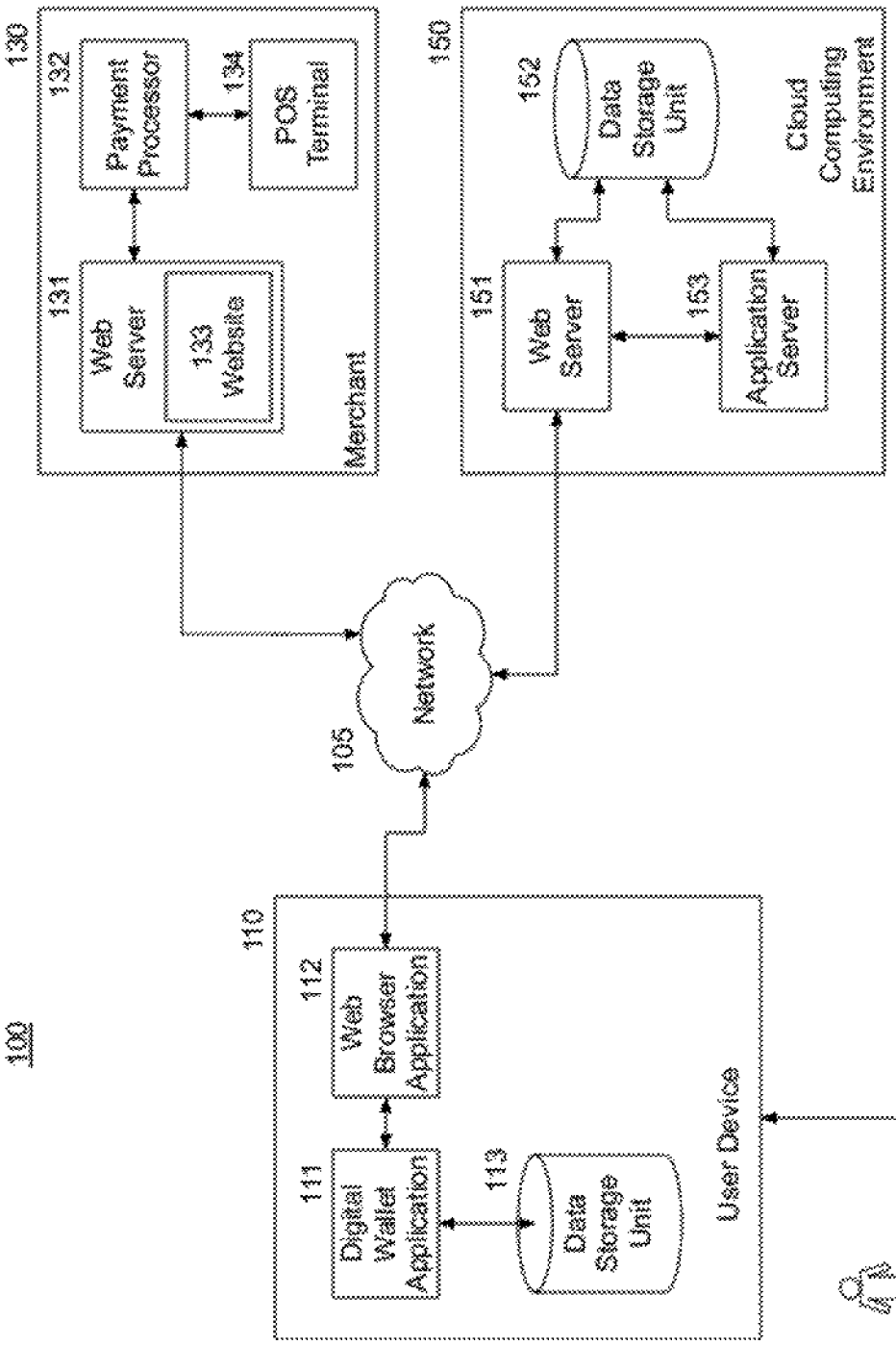

100
130
132
Payment Processor
134
POS Terminal
131
Web Server
133
Website
Merchant
150
152
Data Storage Unit
Cloud Computing Environment
151
Web Server
153
Application Server
105
Network
110
112
Web Browser Application
111
Digital Wallet Application
113
Data Storage Unit
User Device
101

Fig. 1

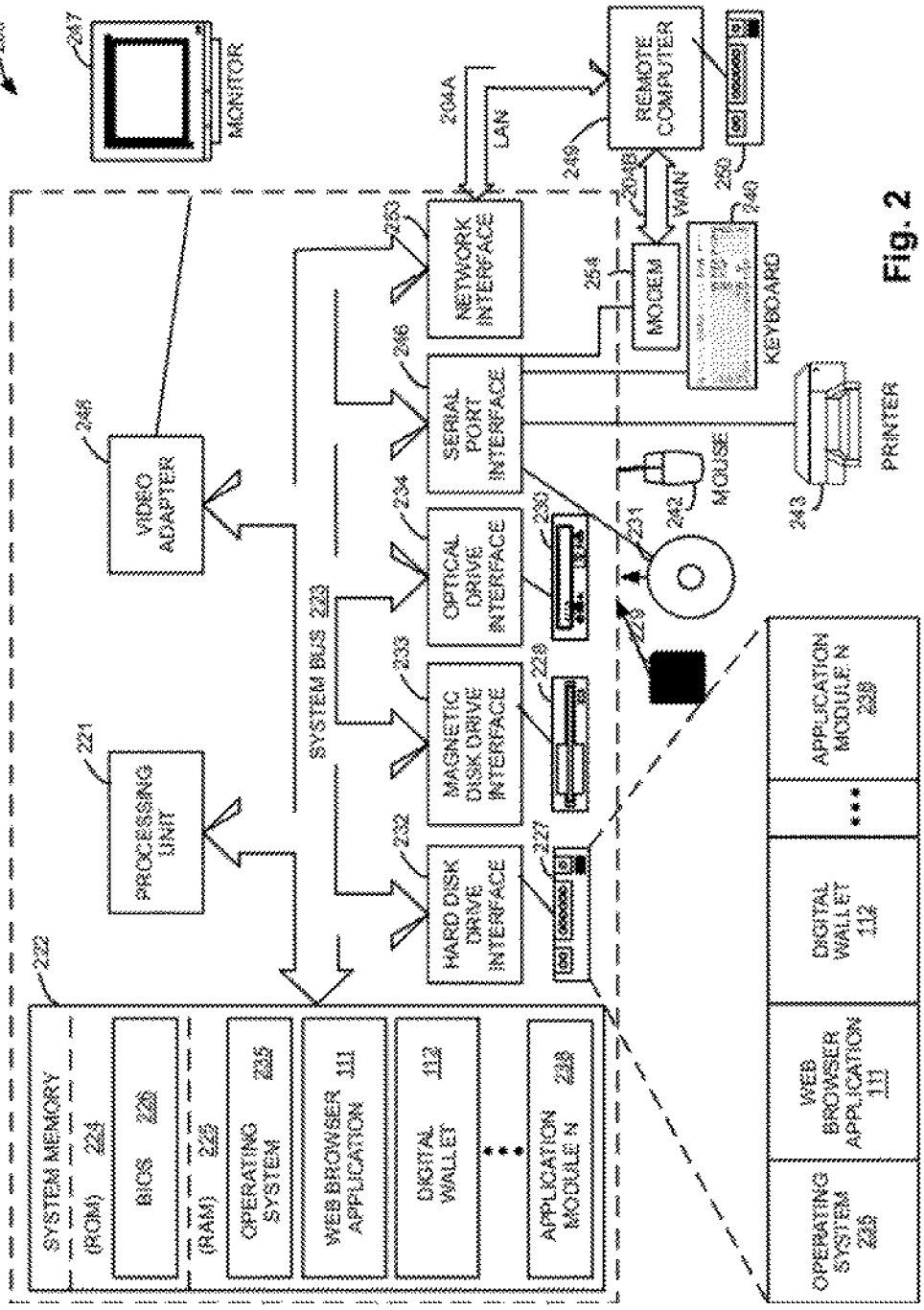

200
MONITOR
REMOTE COMPUTER
LAN
WAN
MODEM
KEYBOARD
PRINTER
MOUSE
NETWORK INTERFACE
SERIAL PORT INTERFACE
VIDEO ADAPTER
OPTICAL DRIVE INTERFACE
MAGNETIC DISK DRIVE INTERFACE
HARD DISK DRIVE INTERFACE
PROCESSING UNIT
SYSTEM BUS
SYSTEM MEMORY
(ROM)
BIOS
(RAM)
OPERATING SYSTEM
WEB BROWSER APPLICATION
DIGITAL WALLET
APPLICATION MODULE N
OPERATING SYSTEM 225
WEB BROWSER APPLICATION 111
DIGITAL WALLET 112
APPLICATION MODULE N 228

Fig. 2

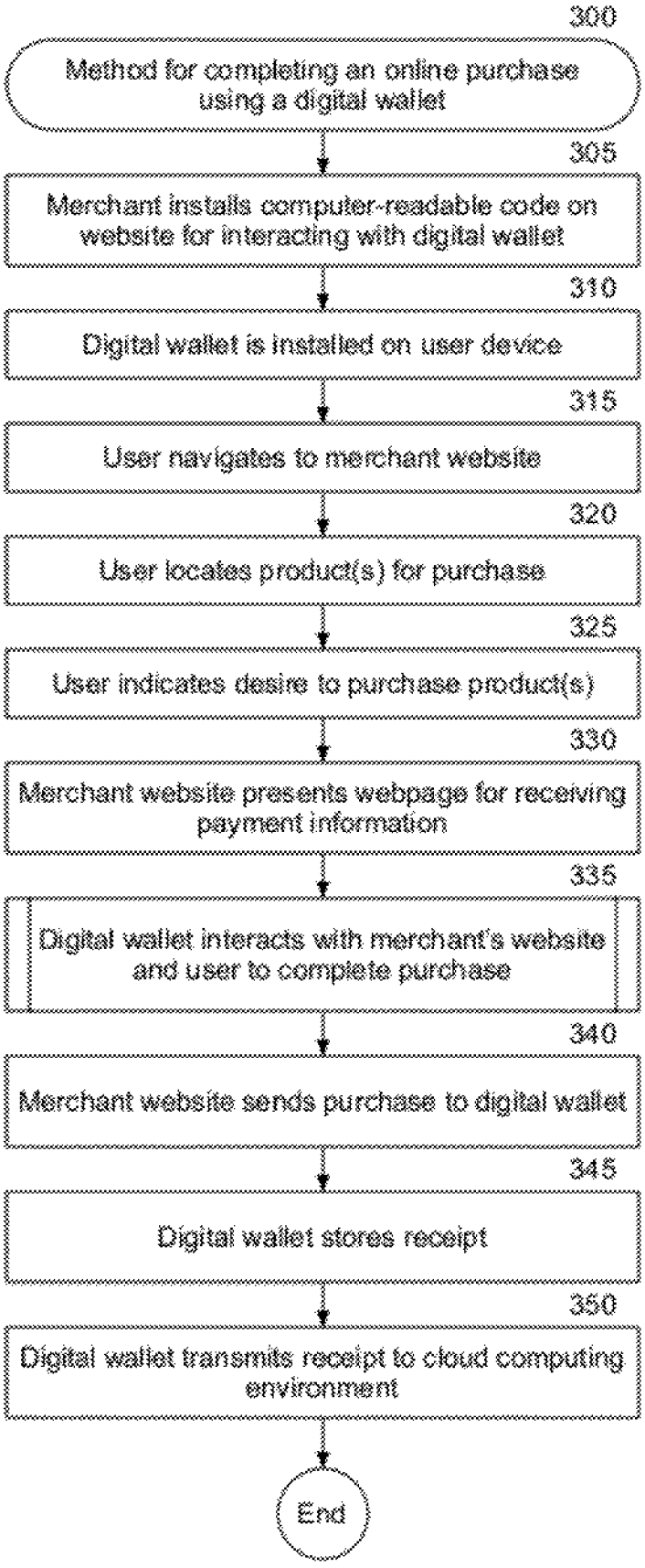

300
Method for completing an online purchase using a digital wallet
305
Merchant installs computer-readable code on website for interacting with digital wallet
310
Digital wallet is installed on user device
315
User navigates to merchant website
320
User locates product(s) for purchase
325
User indicates desire to purchase product(s)
330
Merchant website presents webpage for receiving payment information
335
Digital wallet interacts with merchant's website and user to complete purchase
340
Merchant website sends purchase to digital wallet
345
Digital wallet stores receipt
350
Digital wallet transmits receipt to cloud computing environment
End

Fig. 3

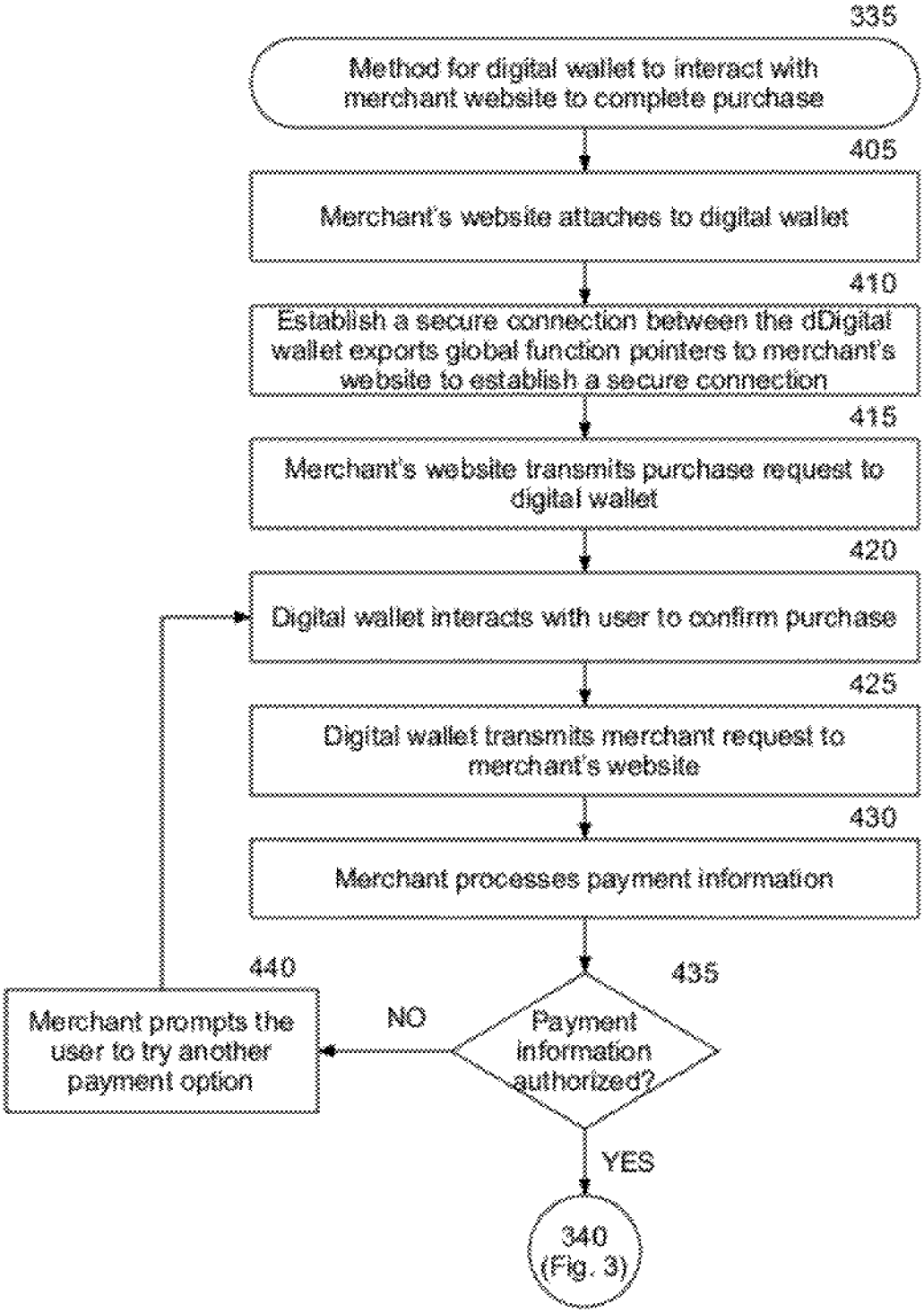

335
Method for digital wallet to interact with merchant website to complete purchase
405
Merchant's website attaches to digital wallet
410
Establish a secure connection between the dDigital wallet exports global function pointers to merchant's website to establish a secure connection
415
Merchant's website transmits purchase request to digital wallet
420
Digital wallet interacts with user to confirm purchase
425
Digital wallet transmits merchant request to merchant's website
430
Merchant processes payment information
435
Payment information authorized?
NO
440
Merchant prompts the user to try another payment option
YES
340 (Fig. 3)

Fig. 4

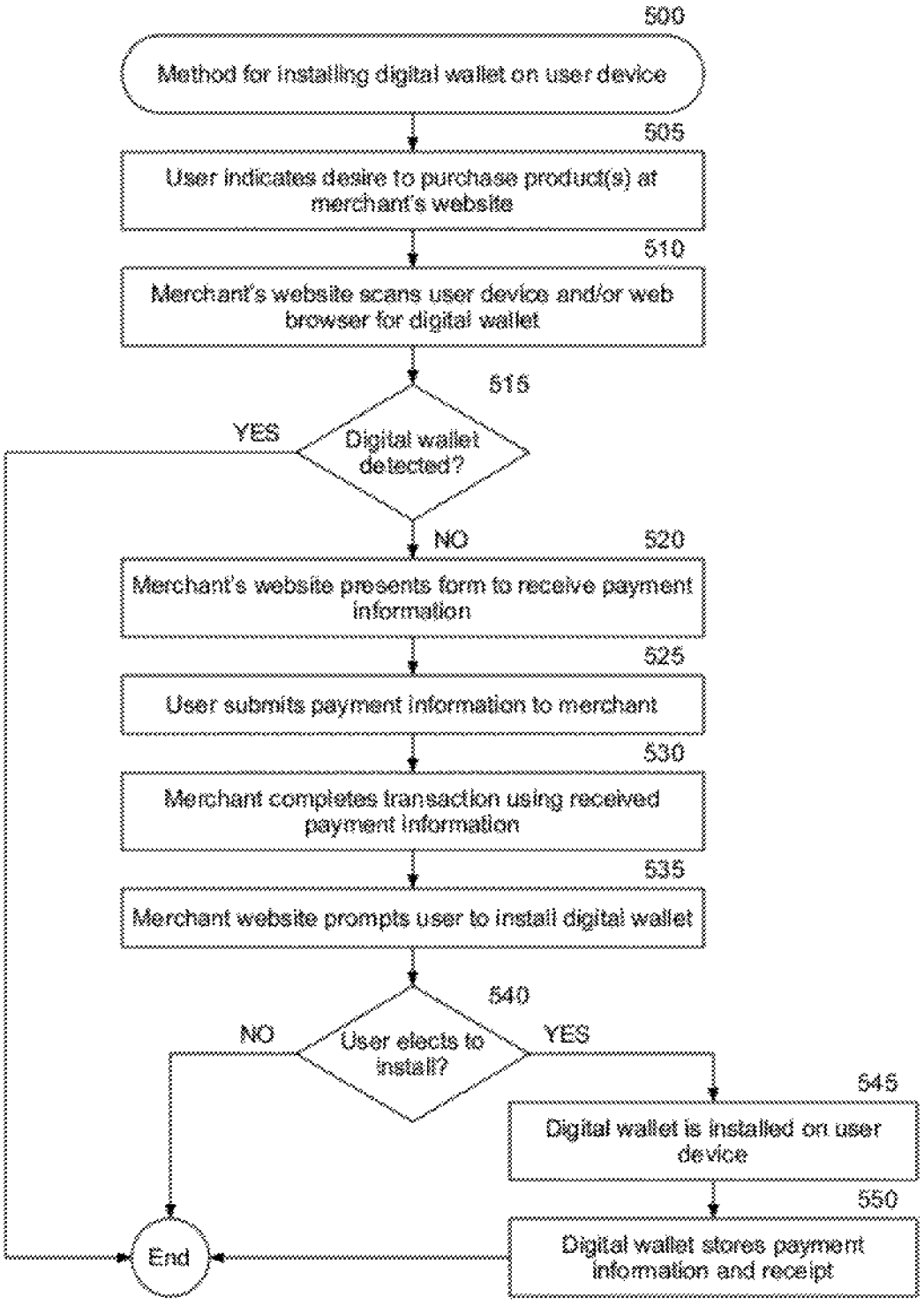

500
Method for installing digital wallet on user device
505
User indicates desire to purchase product(s) at merchant's website
510
Merchant's website scans user device and/or web browser for digital wallet
515
Digital wallet detected?
YES
NO
520
Merchant's website presents form to receive payment information
525
User submits payment information to merchant
530
Merchant completes transaction using received payment information
535
Merchant website prompts user to install digital wallet
540
User elects to install?
NO
YES
545
Digital wallet is installed on user device
550
Digital wallet stores payment information and receipt
End

Fig. 5

DIGITAL WALLET

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/424,611, filed Dec. 17, 2010 and entitled "Digital Wallet." The entire contents of the above-identified priority application are hereby fully incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates generally to electronic commerce, and more particularly to a digital wallet for facilitating transactions and storing information associated with transactions.

BACKGROUND

[0003] Electronic commerce, such as online shopping, has been increasingly common since the advent of the Internet. Online shopping websites generally provide a user interface for customers to select products to purchase. After the customer has selected products for purchase, the customer typically can choose from multiple payment options to purchase the products. Two conventional payment options generally supported by online merchants are using a financial account (for example, a credit card account or checking account) and using a third party payment processor, such as PAYPAL® or other processor.

[0004] To complete an online purchase using a credit card or other financial account, a consumer typically provides a significant amount of information to the merchant via the merchant's website. This information generally includes an account identifier (for example, credit card number, debit card number, etc.), shipping information, and the name, address, and contact information of the consumer. The requirement of entering this information for each merchant from which the consumer makes purchases can be cumbersome and frustrating to the consumers. This requirement can be particularly frustrating and difficult for consumers making online purchases using a mobile device, as many mobile devices do not include a user interface optimized to enter significant amounts of information. This deficiency for mobile devices results in substantially lower mobile browser conversion rates from product searching to product purchase compared to desktop browser conversion rates.

[0005] One conventional approach to alleviating the burden on the consumer involves a toolbar plug-in application for web browsers. Conventional toolbar applications are used to automatically populate web forms, such as a web form for receiving payment and consumer information for completing an online purchase, with stored information. However, these conventional toolbar applications often are inaccurate, as they merely attempt to predict which form is presented on a web page and then preload default values for the predicted form.

[0006] The use of a third party payment processor to complete online purchases is another approach to alleviating the burden of entering a significant amount of information at each merchant's website. Generally, a third party processor requires a consumer to register for an account and to provide one or more payment options. After registering, the consumer can use the payment options to complete purchases at participating merchants' websites. To complete an online purchase using the third party payment processor, the consumer generally selects a link at the merchant's website and, in response, the consumer is redirected from the merchant's website to a website of the third party payment processor. At this website, the consumer first has to provide login information and then can select one of the payment options to complete and confirm the purchase. After the purchase is confirmed, the consumer is directed back to the merchant's website. The third party payment processor then settles with the financial institution associated with the selected payment option and with the merchant to complete the transaction.

[0007] The use of a third party processor has several deficiencies. First, the process is disruptive to the consumer as the consumer is directed away from the merchant's website to the third party payment processor's website and then back to the merchant's website. Second, the use of a third party payment processor limits the amount of information that the merchant receives. For example, the merchant may not have access to information associated with the consumer or information regarding the payment method used. The use of a third party processor also presents an additional cost to the merchant.

[0008] Thus, a need in the art exists for systems and methods that overcome one or more of the above-described limitations.

SUMMARY

[0009] An aspect of the present invention provides a computer-implemented method for completing an online transaction. A digital wallet module resident on a client device receives a request for payment information to complete the transaction. The request originates from a website of a merchant. In response to receiving the request, the digital wallet module retrieves the payment information from a storage location on the client device and transmits the retrieved payment information to the merchant website.

[0010] Another aspect of the present invention provides a computer program product for completing an online transaction. The computer program product includes a computer-readable storage device having computer-readable program instructions stored therein. The computer-readable program instructions includes computer program instructions for receiving a request for payment information to complete the transaction, the request originating from a website of a merchant; computer program instructions for retrieving, in response to the request, the payment information; and computer program instructions for transmitting the retrieved payment information to the merchant website.

[0011] Another aspect of the present invention provides an apparatus for completing an electronic purchase from a merchant via a distributed network. The apparatus includes a web browser application a digital wallet module logically coupled to the web browser application. The digital wallet module is configured to receive a request for payment information to use in completing the purchase from the merchant website; retrieve payment information from a computer-readable storage device logically coupled to the digital wallet module; and transmit the retrieved payment information to the merchant.

[0012] Another aspect of the present invention provides a computer-implemented method for completing a purchase from a merchant via a website of the merchant. A digital wallet module embedded in a web browser in communication with the merchant website receives a purchase request message including a request for payment information for use in compensating the merchant for the purchase. In response to receiving the purchase request message, the digital wallet module presents a confirmation display requesting a user to

authorize the purchase. In response to receiving authorization from the user, the digital wallet module retrieves stored payment information and transmits a payment authorization message including the retrieved payment information to the merchant website.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. **1** is a block diagram depicting an operating environment of a digital wallet, in accordance with certain exemplary embodiments.

[0014] FIG. **2** is a block diagram depicting a general component architecture of a computer system, in accordance with certain exemplary embodiments.

[0015] FIG. **3** is a flow chart depicting a method for completing an online purchase using a digital wallet, in accordance with certain exemplary embodiments.

[0016] FIG. **4** is a flow chart depicting a method for a digital wallet to interact with a merchant website to complete a purchase, in accordance with certain exemplary embodiments.

[0017] FIG. **5** is a flow chart depicting a method for installing a digital wallet on a user device, in accordance with certain exemplary embodiments.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

Overview

[0018] The exemplary embodiments provide a digital wallet that can facilitate fast, convenient, and secure commerce using a mobile electronic device (or non-mobile electronic device) and that stores information associated with transactions, such as purchase confirmations and receipts. The digital wallet can provide a user interface for entering information for use in transactions, such as information associated with one or more financial accounts (for example, credit card or debit card information), contact information, and shipping information. The digital wallet can store this information for subsequent use in online (for example, via the Internet) and offline purchases (for example, via a merchant point of sale device, including a contactless payment device). The user can use the digital wallet to complete purchases by selecting a payment option stored by the digital wallet without the need to re-enter financial account information, contact information, or shipping information for each purchase. The user also may select a default payment option to use such that the user can confirm a purchase without making a payment option selection. The digital wallet can be particularly advantageous when utilized to complete a purchase using a mobile device, such as a mobile phone or other electronic device, having a limited user interface that may not be optimized to enter a significant amount of information.

[0019] The digital wallet can be embodied as a stand alone application program or as a companion program to a web browser, for example, as a companion program to a Hypertext Markup Language revision 5 ("HTML5") compliant web browser or other type of web browser having messaging and storage capabilities. In a web browser embodiment, the digital wallet can leverage the messaging and storage capabilities of the web browser to provide a consistent buying experience across multiple merchant websites. That is, the digital wallet can provide a consistent user interface independent of merchants' differing websites. The digital wallet also can allow a user to complete a purchase without navigating from the merchant's website as required by third party payment processors. While certain embodiments are described in which parts of the digital wallet are implemented in software, it will be appreciated that one or more acts or functions of the digital wallet may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems.

[0020] To complete an online transaction using the digital wallet, a user can navigate to a merchant's website using a web browser and locate one or more products. After the user indicates a desire to purchase one or more products, the digital wallet can interact with the merchant's website and with the user in a secure manner to complete the transaction. Once the transaction is completed, the digital wallet can receive or generate a confirmation or receipt for the transaction and can store the confirmation or receipt. The digital wallet also can synchronize the confirmation or receipt with a remote storage location, such as a cloud computing environment.

[0021] To complete an offline purchase at a merchant's store location, the digital wallet can interact with a merchant's point of sale device and with the user. The user can activate the digital wallet, for example, by launching an application, by pressing a physical or virtual button on the mobile device, or by making a gesture with the mobile device. The digital wallet can then communicate payment information to the point of sale device and, when the payment information is confirmed, receive a receipt from the point of sale device. The mobile device can communicate with the point of sale device using a wireless technology, such as near field communication technology (NFC), BLUETOOTH, or other suitable wireless technology.

[0022] The digital wallet can also store coupons or loyalty reward for use in transactions and can automatically apply the stored coupons during a purchase transaction, if appropriate. For example, a coupon for a product may be displayed to a user in response to an Internet search. The user can download the coupon to the digital wallet and store the coupon on the mobile device. The digital wallet can search the coupons during purchases to determine if one or more of the stored coupons may be applied to the purchase. If so, the digital wallet can automatically apply the stored coupon.

[0023] The digital wallet can communicate with a remote system to facilitate multiple functions. For example, the digital wallet can receive security information that identifies trusted merchants and non-trusted merchants from the remote system. The digital wallet can use this security information to prevent the user from providing financial account information or other information to non-trusted merchants. For example, the digital wallet may compare a merchant name, merchant website Uniform Resource Locator (URL), or Internet Protocol (IP) address to a list of known non-trusted merchants prior to passing information from the digital wallet to the merchant's website.

[0024] The remote system also can maintain an account for each individual user. This user account can include information associated with payment options for use in transactions and receipts or other information regarding completed transactions. The digital wallet can synchronize, for example, periodically, with the remote system to maintain current information at both locations. The remote system also may provide a user interface via a web browser that enables the user to modify information, such as financial account information of stored payment options and contact information for

use in transactions, and to access stored receipts. The user can access the stored receipts, for example, to determine when a certain purchase was made, to determine how much the user paid for an item, or for budgeting purposes. In certain implementations, the remote system or a third party having access to the receipts stored at the remote system can use the receipts to target advertisements or other promotional materials to the user.

[0025] Users may, in appropriate circumstances, be allowed to limit or otherwise affect the operation of the features disclosed in this specification. For example, users may be given an initial opportunity to opt-in or opt-out of the collection or use of certain data or the activation of certain features. In addition, users may be provided opportunities to change the manner in which the features are employed, including for situations in which users may have concerns regarding their privacy. Instructions also may be provided to users to notify the users regarding policies about the use of information, including personally identifiable information and receipt information, and manners in which the users may affect such use of information. Thus, sensitive personal information can be used to benefit a user, if desired, through receipt of targeted advertisements or other information, without risking disclosure of personal information or the user's identity.

[0026] One or more aspects of the invention may comprise a computer program that embodies the functions described and illustrated herein, wherein the computer program is implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions. However, it should be apparent that there could be many different ways of implementing the invention in computer programming, and the invention should not be construed as limited to any one set of computer program instructions. Further, a skilled programmer would be able to write such a computer program to implement an embodiment of the disclosed invention based on the appended flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the invention. Further, those skilled in the art will appreciate that one or more aspects of the invention described herein may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems. Moreover, any reference to an act being performed by a computer should not be construed as being performed by a single computer as the act may be performed by more than one computer. The inventive functionality of the invention will be explained in more detail in the following description, read in conjunction with the figures illustrating the program flow.

System Architecture

[0027] Turning now to the drawings, in which like numerals represent like (but not necessarily identical) elements throughout the figures, exemplary embodiments of the present invention are described in detail. FIG. **1** is a block diagram depicting an operating environment **100** for a digital wallet, in accordance with certain exemplary embodiments.

[0028] Referring to FIG. **1**, the exemplary operating environment **100** includes a merchant system **130**, a cloud computing environment **150**, and a user device **110** associated with a user **101**. The user device **110** may be a personal computer, mobile device, (for example, notebook computer, tablet computer, netbook computer, personal digital assistant (PDA), video game device, GPS locator device, cellular telephone, smartphone, or other mobile device), or other appropriate technology that includes or is coupled to a web browser application module **112**, such as GOOGLE'S CHROME, MICROSOFT'S INTERNET EXPLORER®, or MOZILLA'S FIREFOX®.

[0029] In certain exemplary embodiments, the web browser application **112** is an HTML5 compliant web browser. HTML5 compliant web browsers include a cross-document messaging application programming interface (API) and a local storage API that previous HTML versions did not have. The cross-document messaging API of HTML5 compliant web browsers enables documents, such as web pages, to communicate with each other. For example, a first document can send a message to a second document requesting information. In response, the second document can send a message including the requested information to the first document. The local storage API of HTML5 compliant web browsers enables the web browser to store information on a client device upon which the web browser is installed or is executing, such as the user device **110**. Websites also can employ the local storage API to store information on a client device. Other web browsers having cross-document messaging and/or local storage capabilities also may be used in certain exemplary embodiments.

[0030] The user **101** can use the web browser application **112** to view, download, upload, or otherwise access documents or web pages via a distributed network **105**. The network **105** includes a wired or wireless telecommunication system or device by which network devices (including devices **110**, **130**, and **150**) can exchange data. For example, the network **105** can include a local area network ("LAN"), a wide area network ("WAN"), an intranet, an Internet, or any combination thereof. Throughout the discussion of exemplary embodiments, it should be understood that the terms "data" and "information" are used interchangeably herein to refer to text, images, audio, video, or any other form of information that can exist in a computer based environment.

[0031] The web browser application **112** can interact with web servers (or other computing devices) connected to the network **105**, such as web server **132** of the merchant system **130** and/or web server **151** of the cloud computing environment **150**.

[0032] The user device **110** also includes a digital wallet application module **111**. The exemplary digital wallet **111** can interact with the web browser application **112** or can be embodied as a companion application of the web browser application **112**. As a companion application, the digital wallet **111** executes within the web browser application **112**. That is, the digital wallet **111** may be an application program embedded in the web browser application **112**.

[0033] The user device **110** also includes a data storage unit **113** accessible by the digital wallet **111** and the web browser application **112**. The exemplary data storage unit **113** can include one or more tangible computer-readable storage devices as discussed below with reference to FIG. **2**. The data storage unit **113** can be stored on the user device **110** or can be logically coupled to the user device **110**. For example, the data storage unit **113** can include on-board flash memory and/or one or more removable memory cards or removable flash memory.

[0034] The exemplary digital wallet **111** enables storage of one or more payment options that can be used for online purchases and offline purchases. Each payment option can

include or be associated with a financial account, such as a credit card account, a debit card account, a checking account, a savings account, a loyalty rewards account, or other type of account that can be used to make a purchase. The digital wallet **111** can store, for each payment option, information associated with the financial account for that payment option. This payment information can include a financial account identifier (for example, account number, card number), an expiration date of one or more financial cards associated with the financial account, and a billing address for the account. The payment information can also include information associated with the user **101**, such as name, contact information (for example, residential address, phone number, e-mail address), demographic information, or any other suitable information associated with the user **101**. The payment information also can include shipping information, such as one or more shipping addresses, preferred shipping provider(s), and preferred shipping method(s) (for example, ground, air, expedited, signature confirmation, or other shipping method). The payment information for each payment option can be maintained by the digital wallet **111** and stored in the data storage unit **113**.

[0035] The user **101** can interact with a user interface provided by the digital wallet **111** to add, modify, or remove payment information from the digital wallet **111**. In a web browser companion application embodiment, this user interface can be provided via the web browser application **112**. In addition or in the alternative, the payment information may be synchronized with a remote storage location, such as the cloud computing environment **150**. In such an embodiment, the user **101** can access the payment information stored at the remote location using another device, such as a desktop computer connected to the network **105**. The remote storage location can update the digital wallet **111** in response to any changes made at the remote storage location.

[0036] The payment option(s) stored in the digital wallet **111** can be used to complete purchases from merchants via a merchant's website **133** operating on the web server **131** or via a merchant's point of sale device **134**. In certain exemplary embodiments, each merchant's website **133** (operating on the web server **131**) that accepts payment via a digital wallet **111** can include a set of computer-readable program instructions, for example, using JavaScript, that enable the merchant's website **133** to interact with the digital wallet **111**. These program instructions can include program instructions for detecting whether the user device **110** includes a digital wallet **111** and program instructions for attaching to a detected digital wallet **111**. Once attached, the merchant's website **133** can communicate with the digital wallet **111**, for example, via cross-document messaging. In certain exemplary embodiments, the computer-readable instructions also include program instructions for downloading a digital wallet **111** onto a user device **110**. For example, if the merchant's website **133** detects that the user device **110** does not have a digital wallet **111**, the merchant's website **133** can prompt the user **101** to download and install the digital wallet **111**. If the user **101** elects to download the digital wallet **111**, the computer-readable program code can download and install the digital wallet **111** on the user device **101**. Embedding this computer-readable program instructions in a website **133** for interacting with a digital wallet **111** supports a simpler and efficient integration for the merchant system **130** compared to integrating with a third party payment processor.

[0037] The merchant's website **133** and the digital wallet **111** can communicate using a defined messaging protocol. The digital wallet **111** can encode a message using the protocol and send the encoded message to the merchant's website **133**, where the message is decoded using the protocol. Similarly, the merchant's website **133** can encode a message using the protocol and send the encoded message to the digital wallet **111** where the message is decoded using the protocol.

[0038] The merchant system **130** includes a payment processor **132** logically coupled to the web server **131**. The payment processor **132** can receive payment information via the web server **131** and interact with the financial institution (not shown) or an acquirer (not shown) to authorize payment information.

[0039] To complete an online purchase via the Internet, the digital wallet **111** can interact with a website **133** of the merchant system **130** and with the user **101**. The user **101** can browse the merchant's website **133** for products using the web browser **112** and indicate a desire to purchase one or more products. As used throughout the specification, the term "products" should be interpreted to include tangible and intangible products, as well as services. After the user **101** has indicated a desire to purchase the product(s) (for example, by actuating a "checkout" link), the merchant's website **133** can present a user interface in the form of a web page to receive payment information from the user **101**. The merchant's website **133** also can detect whether the user device **110** includes a digital wallet **111**. If the digital wallet **111** is detected, the merchant's website **133** can automatically attach to the digital wallet **111** as discussed in further detail below in connection with FIG. **4**. In addition or in the alternative, the merchant's website **133** can include a "pay with wallet" link or control that, when actuated, causes the merchant's website **133** to attach to the digital wallet **111**. Once attached, the merchant's website **133** sends a purchase request message to the digital wallet **111** requesting payment information. The purchase request message also can include information regarding the requested purchase, including information regarding the product(s) for purchase (for example, name and/or description of each product, price for each product, total price, etc.), information regarding the merchant system **130** (for example, merchant name, payment methods accepted by merchant, etc.), and requests for the user **101** to provide additional information. In response to receiving a purchase request message from the merchant's website **133**, the digital wallet **111** can present a user interface to the user **101** for the user **101** to confirm the purchase. This user interface can display all or a portion of the information in the purchase request and an actuatable button or link for the user **101** to confirm the purchase. This user interface also can allow the user **101** to select from multiple payment options stored by the digital wallet **111** to use as payment for the product(s) and from multiple shipping options. If the user **101** confirms the purchase, the digital wallet **111** can retrieve the information requested in the purchase request message, generate a merchant request message that contains the information and the confirmation, and transmit the merchant request message to the merchant's website **133**. If the purchase is authorized via the payment processor **132**, the merchant's website **133** can transmit an electronic confirmation and/or a receipt to the digital wallet **111** and then detach from the digital wallet **111**. The digital wallet **111** can store the confirmation and/or receipt at the user device **110** and also synchronize with the cloud computing environment **150**. An exemplary method for

completing an online purchase using the digital wallet **111** is illustrated in FIG. **3** and discussed below.

[0040] The receipt received by the digital wallet **111** can include line item details of the completed purchase. For example, the receipt can include a list of products purchased, a description of each product purchased, the price for each product purchased, a product category for each product purchased, a total price, a stock keeping unit (SKU) or similar identifier for each product purchased, taxes paid, rebates for one or more of the products purchased, payment method used, discounts applied, the time and/or date of purchase, warranty information for one or more of the products purchased, or other suitable information. The receipt also can include information regarding the merchant system **130**, including a name of the merchant associated with the merchant system **130**, a description of the **130**, the URL of the merchant's website **133**, and any other suitable information regarding the merchant system **130**.

[0041] In certain exemplary embodiments, the digital wallet **111** can generate a receipt for a purchase rather than or in addition to receiving a receipt from the merchant's website **133**. For example, the digital wallet **111** can generate the receipt using the information in the purchase request message received from the merchant's website **133** or from the merchant request message sent to the merchant's website **133**.

[0042] The exemplary cloud computing environment **150** includes the web server **151**, one or more data storage units **152**, and one or more application servers **153**. The cloud computing environment **150** may be provided by the provider of the digital wallet, by a merchant **130**, or by another party. In certain exemplary embodiments, multiple cloud computing environments **150** may be employed. For example, a first cloud computing environment may store receipt information and provide access to the receipts from a user device **110** connected to the first cloud computing environment, and a second cloud computing environment may provide security information, such as lists of non-trusted merchants, to the digital wallet **111**. Although the illustrated environment includes a cloud computing environment, other types of computing environments, such as a client-server environment may be used instead.

[0043] The application server **153** can maintain a digital wallet account for each user, including the user **101**. This digital wallet account can store (in the data storage unit **152**) the payment options created by the user **101** and their associated payment information and receipts and other information obtained by the digital wallet **111** in response to completed transactions. The application server **153** can synchronize this information with the digital wallet **111** periodically, on command (for example, by the user **101**), or in response to an update in information at the digital wallet **111** or at the cloud computing environment **150**.

[0044] The digital wallet **111** and the web browser application **112** can interact with the application server **151** via the web server **151**. The application server **153** can provide a user interface via the web server **151** that enables the user **101** to access, view, and/or modify content stored in the user's digital wallet account using the user device **110** or another device connected to the network. For example, the user **101** may add or modify payment information using a web browser application residing on a desktop computer having a better user interface for entering a significant amount of information.

[0045] The exemplary digital wallet **111** can include a user interface for accessing receipt information stored on the user device **110** or at the cloud computing environment **150** in a meaningful and useful way. One feature of this user interface enables the user **101** to search the receipts for information. For example, the user **101** may search for a product purchased to determine the price that was paid for the product or when the product was purchased. In another example, the user **101** may search for warranty information regarding a product to determine if the warranty has expired. In yet another example, the user **101** may search the receipts for merchant return policy information.

[0046] This digital wallet's user interface also includes a budgeting feature. This budgeting feature of the digital wallet **111** enables the user **101** to set a budget for expenditures associated with one or more products or product categories and to monitor this budget using the stored receipts. For example, the user **101** can set a budget of $200 to spend eating out each month. The digital wallet **111** can run a query on the receipts corresponding to transactions completed in the current month to identify receipts that correspond to a restaurant purchase or otherwise to eating out. The digital wallet **111** can then determine the total dollar amount of these receipts and the remaining budget for the current month.

[0047] The digital wallet's user interface also enables the user **101** to filter information associated with receipts and view the filtered information. The receipt information can be filtered by product category, merchant, time period, or any other receipt parameter or combination thereof. For example, the user **101** can use the digital wallet **111** to view the total amount spent at a particular merchant, such as the merchant associate with merchant system **130**, in the past three months or other desired time period.

[0048] One or more of the components of the exemplary operating environment **100**, such as the user device **110**, the web server **131**, the web server **151**, and the application server **153** can include one or more computer systems, such as the computer system **200** illustrated in FIG. **2**. Referring to FIG. **2**, the computer system **200** includes a processing unit **221**, a system memory **222**, and a system bus **223** that couples system components, including the system memory **222**, to the processing unit **221**. The system bus **223** can include any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, or a local bus, using any of a variety of bus architectures. The system memory **222** includes a read-only memory ("ROM") **224** and a random access memory ("RAM") **225**. A basic input/output system (BIOS) **226** containing the basic routines that help to transfer information between elements within the computer system **200**, such as during start-up, is stored in the ROM **224**.

[0049] The computer system **200** also includes a hard disk drive **227** for reading from and writing to a hard disk (not shown), a magnetic disk drive **228** for reading from or writing to a removable magnetic disk **229** such as a floppy disk, and an optical disk drive **230** for reading from or writing to a removable optical disk **231** such as a CD-ROM, compact disk-read/write (CD/RW), DVD, or other optical media. The hard disk drive **227**, magnetic disk drive **228**, and optical disk drive **230** are connected to the system bus **223** by a hard disk drive interface **232**, a magnetic disk drive interface **233**, and an optical disk drive interface **234**, respectively. Although the exemplary computer system **200** employs a ROM **224**, a RAM **225**, a hard disk drive **227**, a removable magnetic disk **229**, and a removable optical disk **231**, other types of computer-readable media also can be used in the exemplary computer system **200**. For example, the computer-readable media

can include any apparatus that can contain, store, communicate, propagate, or transport data for use by or in connection with one or more components of the computer system **200**, including any electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or propagation medium, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, and the like. The drives and their associated computer-readable media can provide nonvolatile storage of computer-executable instructions, data structures, program modules, and other data for the computer system **200**.

[0050] A number of modules can be stored on the ROM **224**, RAM **225**, hard disk drive **227**, magnetic disk **229**, or optical disk **231**, including an operating system **235**, an application module **238**, and the web browser application **112**, the digital wallet **111**, and the website application discussed above in connection with FIG. **1**. The web browser application **112**, the digital wallet **111**, website application, and application module **238** can include routines, sub-routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types.

[0051] A user, such as user **101**, can enter commands and information to the computer system **200** through input devices, such as a keyboard **240** and a pointing device **242**. The pointing device **242** can include a mouse, a trackball, an electronic pen that can be used in conjunction with an electronic tablet, or any other input device, such as a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit **222** through a serial port interface **246** that is coupled to the system bus **223**, but can be connected by other interfaces, such as a parallel port, game port, a universal serial bus (USB), or the like. A display device **247**, such as a monitor, also can be connected to the system bus **223** via an interface, such as video adapter **248**. In addition to the display device **247**, the computer **220** can include other peripheral output devices, such as speakers (not shown) and a printer **243**.

[0052] The computer system **200** is configured to operate in a networked environment using logical connections to one or more remote computers **249**. The remote computer **249** can be any network device, such as a personal computer, a server, a client, a router, a network PC, a peer device, or other device. While the remote computer **249** typically includes many or all of the elements described above relative to the computer system **200**, only a memory storage device **250** has been illustrated in FIG. **2** for simplicity. The logical connections depicted in FIG. **2** include a LAN **204**A and a WAN **204**B. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

[0053] When used in a LAN networking environment, the computer system **200** is often connected to the LAN **204**A through a network interface or adapter **253**. When used in a WAN networking environment, the computer system **200** typically includes a modem **254** or other means for establishing communications over the WAN **204**B, such as the Internet. The modem **254**, which can be internal or external, is connected to system bus **223** via a serial port interface **246**. In a networked environment, program modules depicted relative to computer system **200**, or portions thereof, can be stored in the remote memory storage device **250**.

[0054] It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used. Moreover, those having ordinary skill in the art having the benefit of the present disclosure will appreciate that the computer system **200** illustrated in FIG. **2** can have any of several other suitable computer system configurations. Furthermore, those skilled in the art having the benefit of the present disclosure will recognize that certain components of the computer system **200** may be added, deleted, or modified in certain alternative embodiments. For example a user device **101** embodied as a mobile phone or handheld computer may not include all the components depicted in FIG. **2** and/or described above.

System Process

[0055] The components of the exemplary operating environment **100** are described hereinafter with reference to the exemplary methods illustrated in FIGS. **3-5**. The exemplary embodiments can include one or more computer programs that embody the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing aspects of the exemplary embodiments in computer programming, and these aspects should not be construed as limited to one set of computer instructions. Further, a skilled programmer would be able to write such computer programs to implement exemplary embodiments based on the flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the exemplary embodiments. Further, those skilled in the art will appreciate that one or more acts described may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems.

[0056] FIG. **3** is a flow chart depicting a method **300** for completing an online purchase using a digital wallet **111**, in accordance with certain exemplary embodiments. With reference to FIGS. **1** and **3**, in block **305**, the merchant installs computer-readable program instructions on the merchant's website **133** for interacting with the digital wallet **111**. These computer-readable program instructions can be implemented as an embedded script, such as JavaScript, in a web page of the merchant system **130**. For example, the merchant system **130** can embed the computer-readable program instructions on a "checkout" web page of the merchant's website **133**.

[0057] The computer-readable program instructions can include program instructions for interacting with web browser applications, such as web browser application **112**, to determine whether the user device **110** has a digital wallet **111** installed thereon. The computer-readable program instructions also can include program instructions for attaching to a detected digital wallet **111** to exchange messages. In certain exemplary embodiments, the program instructions are configured to exchange messages with a digital wallet **111** embedded in an HTML5 compliant web browser **112**. In an exemplary embodiment, the computer-readable program instructions comprise execute when the browser application **112** on the user device **110** downloads a web page from the merchant's website **133**. The browser application **112** executes the code locally to search for an installed digital wallet **111** on the user device **110**. If a digital wallet **111** is installed, then the browser is instructed to surface a wallet control button for selection by the user. If a digital wallet **111** is not installed, then the browser is instructed to surface

another control for interaction with the user, such as an option to install a wallet application **111**.

[0058] In block **310**, the digital wallet **111** is installed on the user device **110**. In certain exemplary embodiments, the user **101** can navigate to a website **133** of a provider of the digital wallet **111** and download and install the digital wallet **111**. In certain exemplary embodiments, as discussed previously, a merchant's website **133** can prompt the user **101** to download and install the digital wallet **111**, for example, upon selecting the "checkout" option on the merchant's website **133**. In such an embodiment, the user **101** may provide payment information to the merchant's website **133** in a conventional manner and then download and install the digital wallet **111**. The payment information provided to the merchant's website **133** can then be automatically stored in the digital wallet **111** installed on the user device **101**. An exemplary method of installing a digital wallet **111** is discussed further in connection with FIG. **5**.

[0059] In block **315**, the user **101** navigates to the merchant's website **133** using the web browser application **112**. In block **320**, the user **101** browses the merchant's website **133** for one or more products to purchase. In block **325**, the user **101** indicates a desire to purchase one or more products. For example, the user **101** may browse the merchant's website **133** and add products to a virtual shopping cart. Once the user **101** is ready to checkout, the user **101** can actuate a "checkout" link on the merchant's website **133**.

[0060] In block **330**, the merchant's website **133** presents a web page via the web browser application **112** for obtaining payment information from the user **101**. This web page can include conventional payment options, such as a form for receiving payment information and contact information and/or a link to a third party payment processor. This web page also can include the computer-readable program instructions for detecting and interacting with the digital wallet **111**. Furthermore, this web page can include a "pay with wallet" link or button that the user **101** can select to pay using the digital wallet **111**.

[0061] In block **335**, the merchant's website **133** interacts with the digital wallet **111** to complete the purchase of the products selected by the user **101**. The merchant's website **133** can attach to the digital wallet **111** and send a purchase request message to the digital wallet **111**. As discussed above, the purchase request message can include a request for payment information and further include information regarding the requested purchase, such as information associated with the selected products and information associated with the merchant system **130**. In response to receiving the purchase request message, the digital wallet **111** can present a user interface to the user **101** for the user **101** to confirm the purchase. The user interface also can allow the user **101** to select from multiple payment options to send to the merchant's website **133**. If the user **101** confirms the purchase, the digital wallet **111** sends a merchant request message including the confirmation and payment information associated with the payment option to the merchant's website **133**. The payment processor **132** can interact with an acquirer or the financial institution associated with the payment information to authorize the purchase. Block **335** is discussed in further detail in connection with FIG. **4**.

[0062] In block **340**, the merchant's website **133** sends a message including a receipt to the digital wallet **111**. The receipt can include information associated with the purchase, such as a list of products purchased, a description of each product purchased, the price for each product purchased, a product category for each product purchased, a total price, a stock keeping unit (SKU) or similar product identifier for each product purchased, taxes paid, rebates for one or more of the products purchased, payment method used, discounts applied, the time and/or date of purchase, warranty information for one or more of the products purchased, or other suitable information. The receipt also can include information regarding the merchant associated with the merchant system **130**, including a name of the merchant, a description of the merchant, the URL of the merchant's website **133**, and other suitable information regarding the merchant or the merchant system **130**.

[0063] In block **345**, the digital wallet **111** stores the receipt in the data storage unit **113**. In an embodiment where the digital wallet **111** is embedded in an HTML5 compliant web browser application (or similar web browser application), the digital wallet **111** can employ the local storage functionality of the web browser application to store the receipt in the data storage unit **113**.

[0064] In block **350**, the digital wallet **111** synchronizes with the cloud computing environment **150** by sending the receipt to the web server **151**. The web server **151**, in turn, stores, in the data storage unit **152**, the received receipt in the user's digital wallet account with the cloud computing environment **150**. From step **350**, the method **300** ends.

[0065] FIG. **4** is a flow chart depicting a method **335** for a digital wallet to interact with a merchant website **133** to complete a purchase, in accordance with certain exemplary embodiments, as referenced in step **335** of FIG. **3**. With reference to FIGS. **1** and **4**, in block **405**, the merchant's website **133** attaches to the digital wallet **111** by establishing a connection between the website **133** and the digital wallet **111**.

[0066] In block **410**, the digital wallet **111** and the merchant's website **133** establish a secure connection for communication between the digital wallet **111** and the merchant's website **133**. In certain exemplary embodiments, the digital wallet **111** may authenticate the merchant's website **133** prior to establishing the secure connection. For example, the digital wallet **111** may compare the merchant name, the URL of the merchant's website **133**, or the IP address of the merchant's website **133** to a list of known trusted or known non-trusted merchants prior to establishing the secure connection. If the merchant system **130** is not trusted by the digital wallet **111**, then the digital wallet **111** will not authorize the secure connection, rather the digital wallet **111** detaches from the merchant's website **133** by disconnecting the connection between the website **133** and the digital wallet **111**.

[0067] After establishing the secure connection, in block **415**, the merchant's website **133** transmits a purchase request message to the digital wallet **111**. The purchase request message includes a request for payment information from the digital wallet **111** to complete the purchase. The purchase request message also can include information regarding the product(s) for purchase, such as a name and/or description of each product, a price for each product, a total price for all products, taxes, shipping charges, handling charges, other charges, a SKU or other product identifier for each product, shipping options and associated costs, and/or a discount amount for each product. The purchase request message also can include information regarding the merchant, such as the merchant's name, a description of the merchant, and/or payment methods accepted by the merchant (for example, VISA, MASTERCARD, debit card, or other payment method). In

certain exemplary embodiments, the purchase request message also can include a request for the user **101** to provide additional information. This request can be configured by the merchant to solicit additional information from the user **101**, such as an e-mail address or a loyalty rewards account number.

[0068] In block **420**, the digital wallet **111** receives the purchase request message from the merchant's website **133** and interacts with the user **101** to confirm the purchase. In certain exemplary embodiments, this interaction includes the digital wallet **111** presenting a user interface on the user device **110** that displays information associated with the purchase to the user **101** and requests confirmation to complete the purchase. The information displayed by the digital wallet **111** may include some or all of the information included in the purchase request message.

[0069] In certain exemplary embodiments, the user interface displayed by the digital wallet **111** also enables the user **101** to select from multiple payment options stored by the digital wallet **111**. The user interface also may allow the user **101** to select or update shipping information. The digital wallet **111** may block the user from using a payment option not accepted by the merchant system **130** as indicated in the purchase request message. The user interface also may prompt the user **101** to enter information requested by the merchant system **130** in the purchase request message. After reviewing the purchase information and/or selecting a payment method, updating shipping information, and/or providing additional information, the user **101** actuates a link or button control to confirm the purchase. If the user **101** does not want to confirm the purchase, the user **101** selects a "cancel" link or button control to cancel the purchase, thereby terminating the session between the digital wallet **111** and the website **133**.

[0070] In block **425**, if the user **101** confirmed the purchase in block **420**, the digital wallet **111** generates and transmits a merchant request message to the merchant's website **133**. The merchant request message includes confirmation of the purchase and payment information to use in completing the purchase. For example, the merchant request message can include the form of payment and all information needed to process that payment (for example, credit card number), shipping method, shipping address, e-mail address, user name, and any other information for the purchase transaction. The merchant request message also can include the information in the purchase request message and any information requested by the merchant system **130**. The digital wallet **111** can automatically retrieve payment information for a selected payment option from the data storage unit **113** to include in the merchant request message upon confirmation from the user **101** and/or a selection of a payment option by the user **101**.

[0071] In block **430**, the merchant's website **133** receives the merchant request message and sends the payment information to the payment processor **132** for processing. The payment processor **132** interacts with an acquirer or a financial institution associated with the payment information to authorize the payment information and to credit and debit the appropriate accounts for payment from the user **101** to the merchant.

[0072] In block **435**, the web server **131** receives a message from the payment processor **132** indicating whether the payment information was authorized. If the payment information was authorized, the method **335** follows the "YES" branch to step **340**, as referenced in FIG. **3**. Otherwise, the method **335** follows the "NO" branch to step **440**.

[0073] In step **440**, the merchant's website **133** notifies the user **101** that the payment information was not authorized and can prompt the user **101** to try another payment option. After block **440**, the method **335** returns to block **420** where the digital wallet **111** interacts with the user **101** to complete the purchase using a different payment option. The user **101** could cancel the purchase if the user **101** does not want to complete the purchase using a different payment option.

[0074] FIG. **5** is a flow chart depicting a method **500** for installing a digital wallet on a user device, in accordance with certain exemplary embodiments. With reference to FIGS. **1** and **5**, in block **505**, the user **101** indicates a desire to purchase one or more products at the merchant's website **133**. This act performed in block **505** can be substantially similar to steps **315-325** illustrated in FIG. **3** and discussed above.

[0075] In block **510**, the merchant's website **133** scans the user device **110** and/or the web browser application **112** to determine whether a digital wallet **111** is installed on the user device **110** or embedded in the web browser application **112**. In block **515**, if the merchant's website **133** detects a digital wallet **111**, then the method **500** follows the "YES" branch and ends as a digital wallet **111** is already installed on the user device **110**. If a digital wallet **111** is not detected by the merchant's website **133**, the method **500** follows the "NO" branch to block **520**.

[0076] In block **520**, the merchant's website **133** presents a form for the user **101** to provide payment information to complete the purchase of the one or more products. This form can be similar to a conventional web form having text entry fields for receiving credit card, debit card, or other payment information, shipping address, billing address, e-mail address, name, phone number, and other user information. The form also can include fields for receiving user information and user contact information.

[0077] In block **525**, the user **101** completes the form by providing the requested information and submits the form to the merchant's website **133**. In block **530**, the merchant system **130** processes the received payment information and completes the transaction. In block **535**, the merchant's website **133** prompts the user **101** to download and install the digital wallet **111** on the user device **110**.

[0078] In block **540**, if the user **101** elects to install the digital wallet **111**, the method **500** follows the "YES" branch to block **550**. Otherwise, the method **500** follows the "NO" branch and the method **500** ends.

[0079] In block **545**, the merchant's website **133** downloads and initiates the installation of the digital wallet **111** on the user device **110**. During the installation process, the digital wallet **111** can prompt the user **101** to set up a digital wallet account at the cloud computing environment. The user **101** can opt-in or opt-out of this feature and also can select to install or activate certain features only. If the user **101** opts-in to the digital wallet account, the digital wallet **111** can obtain information from the user **101** for the account, such as payment information, contact information, preferred shipping information, and a user name and password for security purposes.

[0080] The installed digital wallet **111** can interact with the merchant's website **133** to obtain the payment information used to complete the purchase and a receipt for the purchase. In block **550**, the digital wallet **111** stores the payment information and the receipt in the data storage unit **113**. If the user

101 elected to create a digital wallet account with the cloud computing environment, the digital wallet **111** synchronizes the receipt and the payment information with the digital wallet account.

[0081] In an alternative exemplary embodiment, the installation of the digital wallet **111** on user device **110** can occur prior to step **520**, whereby the user downloads the digital wallet application **111**, provides the payment and user information for storage by the digital wallet **111** on the date storage unit **113**, and then completes the purchase with the website **133** via the digital wallet **111**.

General

[0082] The exemplary embodiments described herein can be used with computer hardware and software that perform the methods and processing functions described previously. The systems, methods, and procedures described herein can be embodied in a programmable computer, computer-executable software, or digital circuitry. The software can be stored on computer-readable media. For example, computer-readable media can include a floppy disk, RAM, ROM, hard disk, removable media, flash memory, memory stick, optical media, magneto-optical media, CD-ROM, etc. Digital circuitry can include integrated circuits, gate arrays, building block logic, field programmable gate arrays (FPGA), etc.

[0083] The exemplary methods and acts described in the embodiments presented previously are illustrative, and, in alternative embodiments, certain acts can be performed in a different order, in parallel with one another, omitted entirely, and/or combined between different exemplary embodiments, and/or certain additional acts can be performed, without departing from the scope and spirit of the invention. Accordingly, such alternative embodiments are included in the inventions described herein.

[0084] Although specific embodiments have been described above in detail, the description is merely for purposes of illustration. It should be appreciated, therefore, that many aspects described above are not intended as required or essential elements unless explicitly stated otherwise. Modifications of, and equivalent acts corresponding to, the disclosed aspects of the exemplary embodiments, in addition to those described above, can be made by a person of ordinary skill in the art, having the benefit of the present disclosure, without departing from the spirit and scope of the invention defined in the following claims, the scope of which is to be accorded the broadest interpretation so as to encompass such modifications and equivalent structures.

1-31. (canceled)

32. A computer-implemented method for installing a digital wallet module on a user device, comprising:

reading, by a computer, information from a user device in response to receiving a request for payment information to complete an online transaction;

determining, by the computer, that a digital wallet module is not present on the user device based on the information read from the user device;

communicating, by the computer, a form for presentation on the user device in response to determining that a digital wallet module is not present on the user device, the form comprising a request for payment information to complete the transaction;

receiving, by the computer, the payment information from the user device;

communicating, by the computer, a request to install a digital wallet module on the user device based on determining that a digital wallet module is not present on the user device;

receiving, by the computer, an acceptance from the user device of the request to install the digital wallet module on the user device;

communicating, by the computer, the digital wallet module to the user device for installation on the user device in response to receiving the acceptance; and

communicating, by the computer, the payment information to the user device for storage in connection with the digital wallet module.

33. The computer-implemented method of claim **32**, wherein the computer is operated by the merchant website.

34. The computer-implemented method of claim **32**, further comprising submitting the payment information to the merchant website to complete the online transaction.

35. The computer-implemented method of claim **32**, further comprising retrieving the payment information from the merchant website, in response to receiving the acceptance from the user device of the request to install the digital wallet module on the user device.

36. The computer-implemented method of claim **32**, wherein the user device comprises a mobile telephone.

37. The computer-implemented method of claim **32**, wherein the user device comprises a computer.

38. A computer-implemented method for completing an online transaction, comprising:

reading, by a computer, a user device in response to receiving a request for payment information to complete the online transaction;

determining, by the computer, a digital wallet module is resident on the user device based on the information read from the user device, wherein the digital wallet module is embedded in the web browser;

authorizing, by the computer, a request to submit payment information from the digital wallet module resident on the user device;

establishing, by the computer, a secure connection with the digital wallet module resident on the user device;

submitting, by the computer, to the digital wallet module resident on the user device, a request for payment information to complete the transaction, the request originating from the merchant website;

receiving, by the computer, the payment information from the digital wallet module;

submitting, by the computer, a payment authorization request to a financial institution, wherein the financial institution corresponds to the payment information provided by the digital wallet module to pay for the transaction; and

receiving, by the computer, a payment authorization for the request from the financial institution authorizing the payment in accordance with the payment information.

39. The computer-implemented method of claim **38**, wherein the computer is operated by the merchant website.

40. The computer-implemented method of claim **38**, further comprising authorizing the online transaction in response to receiving the payment authorization.

41. The computer-implemented method of claim **38**, further comprising transmitting confirmation of an authorized online transaction to the digital wallet module resident on the user device.

42. The computer-implemented method of claim **41**, wherein the confirmation of the authorized online transaction comprises at least one of a total price for the transaction, a description of the product or service purchased, and a form of payment used to authorize the only transaction.

43. The computer-implemented method of claim **38**, wherein the user device comprises a mobile telephone.

44. The computer-implemented method of claim **38**, wherein the user device comprises a computer.

45. A computer-implemented method for completing an online transaction, comprising:

saving, by a digital wallet module resident on a user device, user information to a storage location on the user device, the user information comprising one or more payment options;

receiving, by the digital wallet module, authorization for a request from a merchant website to submit payment information from the digital wallet module;

establishing, by the digital wallet module, a secure connection with the merchant website in response to receiving authorization for the request to submit payment information from the digital wallet module;

receiving, by the digital wallet module, a request for payment information to complete the transaction, the request originating from the merchant website, wherein the digital wallet module executes within the same web browser application as the merchant website;

retrieving, by the digital wallet module, user information from the storage location on the user device in response to receiving the request for payment information;

presenting, by the digital wallet module, on the user device a request to confirm the transaction from the merchant website and to select a payment option to complete the transaction, wherein the payment option is selected from one of a plurality of payment options stored by the digital wallet module;

receiving, by the digital wallet module, confirmation of the transaction and the selection of payment option to complete the transaction from the user device; and

transmitting, by the digital wallet module, the selection of payment option to the merchant website.

46. The computer-implemented method of claim **45**, further comprising receiving a confirmation of an authorized online transaction to the digital wallet module resident on the user device.

47. The computer-implemented method of claim **46**, wherein the confirmation of the authorized online transaction comprises at least one of a total price for the transaction, a description of the product or service purchased, and a form of payment used to authorize the only transaction.

48. The computer-implemented method of claim **45**, wherein the user device comprises a mobile telephone.

49. The computer-implemented method of claim **45**, wherein the user device comprises a computer.

50. A computer program product, comprising:

a non-transitory computer-readable medium having computer-readable program code embodied therein for completing an online transaction, the computer-readable medium comprising:

computer-readable program code for reading a user device in response to receiving a request for payment information to complete the online transaction;

computer-readable program code for determining a digital wallet module is resident on the user device based on the information read from the user device, wherein the digital wallet module is embedded in the web browser;

computer-readable program code for authorizing a request to submit payment information from the digital wallet module resident on the user device;

computer-readable program code for establishing a secure connection with the digital wallet module resident on the user device;

computer-readable program code for submitting to the digital wallet module resident on the user device, a request for payment information to complete the transaction, the request originating from the merchant website;

computer-readable program code for receiving the payment information from the digital wallet module;

computer-readable program code for submitting a payment authorization request to a financial institution, wherein the financial institution corresponds to the payment information provided by the digital wallet module to pay for the transaction; and

computer-readable program code for receiving a payment authorization for the request from the financial institution authorizing the payment in accordance with the payment information.

51. The computer program product of claim **50**, further comprising computer-readable program code for authorizing the online transaction in response to receiving the payment authorization.

52. The computer program product of claim **50**, further comprising computer-readable program code for transmitting confirmation of an authorized online transaction to the digital wallet module resident on the user device.

53. The computer program product of claim **52**, wherein the confirmation of the authorized online transaction comprises at least one of a total price for the transaction, a description of the product or service purchased, and a form of payment used to authorize the only transaction.

54. The computer program product of claim **50**, wherein the user device comprises a mobile telephone.

* * * * *

US 20120239529A1

(19) **United States**

(12) **Patent Application Publication**

Low et al.

(10) **Pub. No.: US 2012/0239529 A1**

(43) **Pub. Date: Sep. 20, 2012**

(54) **SINGLE DIGITAL WALLET ACROSS MULTIPLE PAYMENT PLATFORMS**

(75) Inventors: **Gak Wee Low**, Sunnyvale, CA (US); **Mark Wenger**, San Francisco, CA (US); **Prashant Jamkhedkar**, Sunnyvale, CA (US)

(73) Assignee: **eBay Inc.**, San Jose, CA (US)

(21) Appl. No.: **13/420,663**

(22) Filed: **Mar. 15, 2012**

Related U.S. Application Data

(60) Provisional application No. 61/453,843, filed on Mar. 17, 2011.

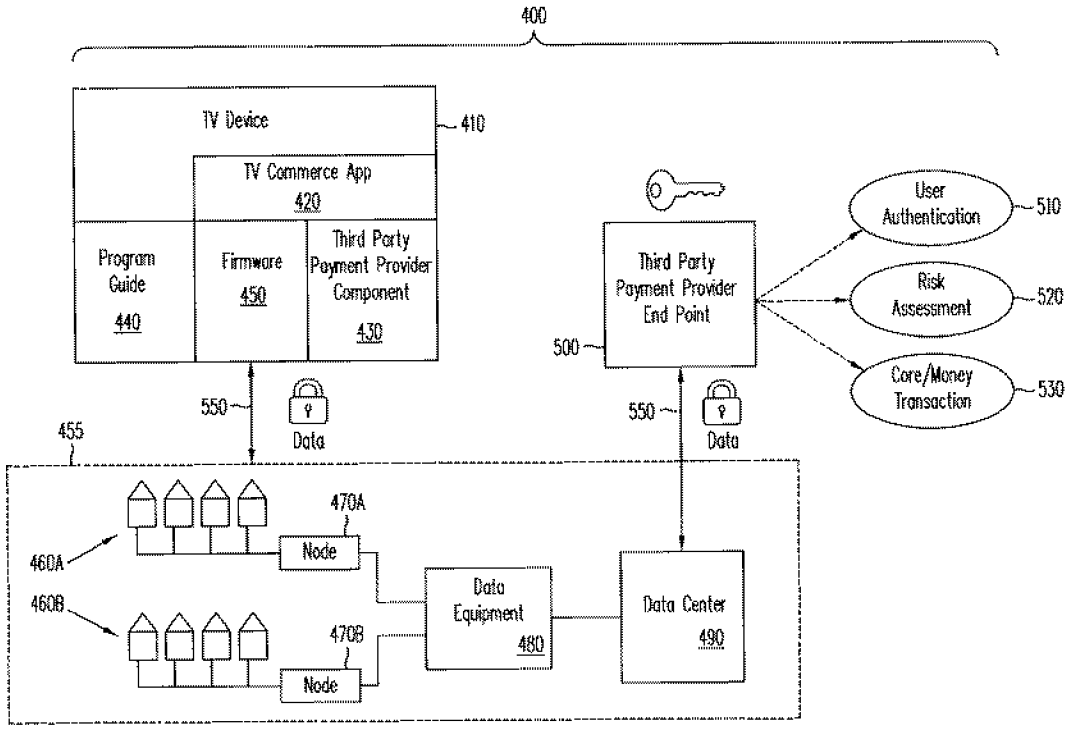
Publication Classification

(51) **Int. Cl.**
G06Q 20/02 (2012.01)
G06Q 20/40 (2012.01)

(52) **U.S. Cl.** **705/26.41**; 705/39

(57) **ABSTRACT**

The present disclosure involves a method of conducting a transaction. In one aspect, the method includes: displaying a media program on a media display device; indicating, while the media program is being displayed, an item associated with the media program is available for purchase; receiving authentication information of a prospective purchaser of the item; and completing a purchase of the item in response to the authentication information. In another aspect, the method includes: receiving, from a media display device, a user authentication request that contains user login credentials; granting the user authentication request in response to the user login credentials; and sending an authentication permission to the media display device; wherein the receiving and the sending are each performed such that the user login credentials and the authentication permission are sent through one or more intermediate hops without being inspected by any of the intermediate hops.



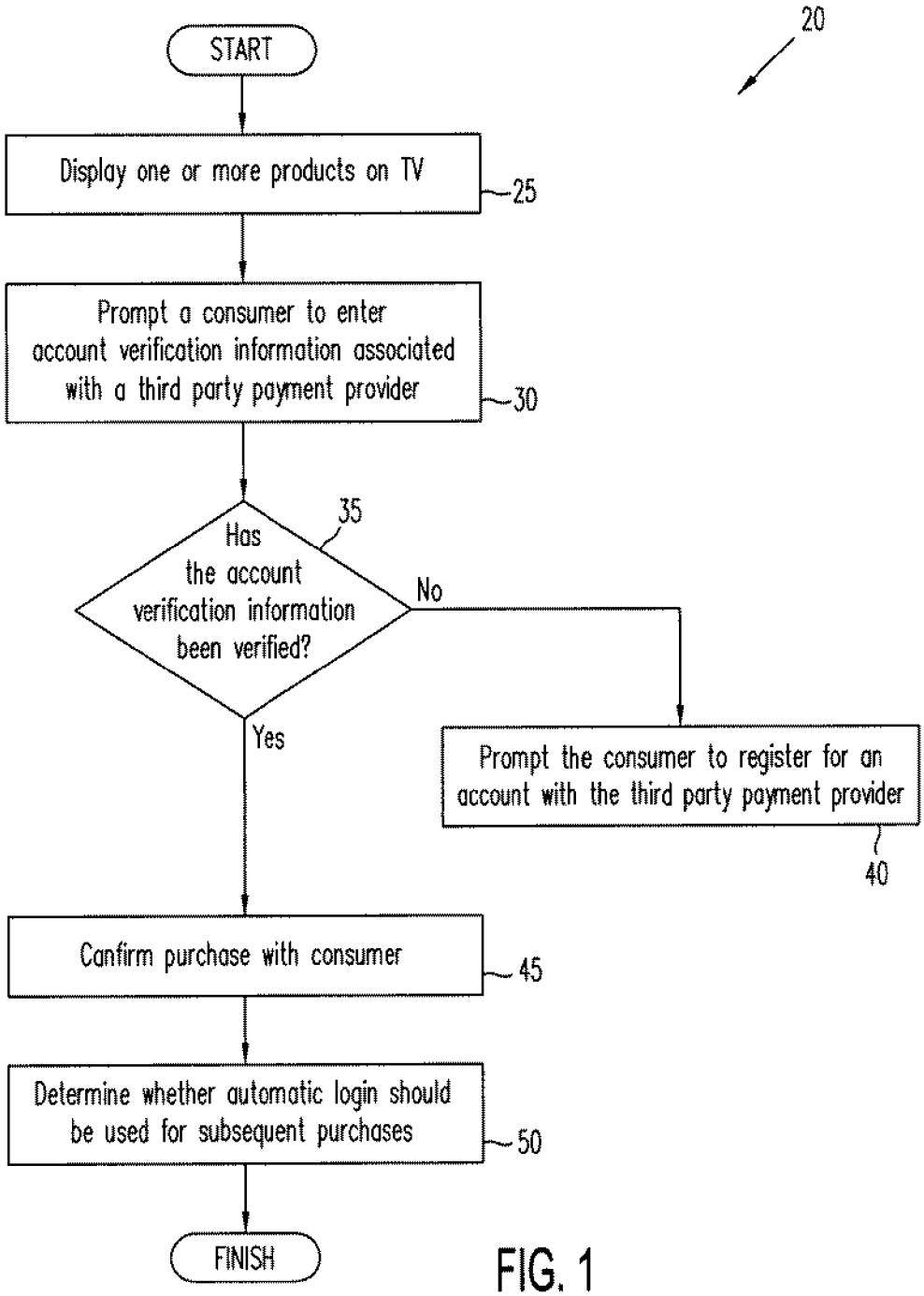

20
START
Display one or more products on TV
25
Prompt a consumer to enter account verification information associated with a third party payment provider
30
35
Has the account verification information been verified?
No
Yes
Prompt the consumer to register for an account with the third party payment provider
40
Confirm purchase with consumer
45
Determine whether automatic login should be used for subsequent purchases
50
FINISH

FIG. 1

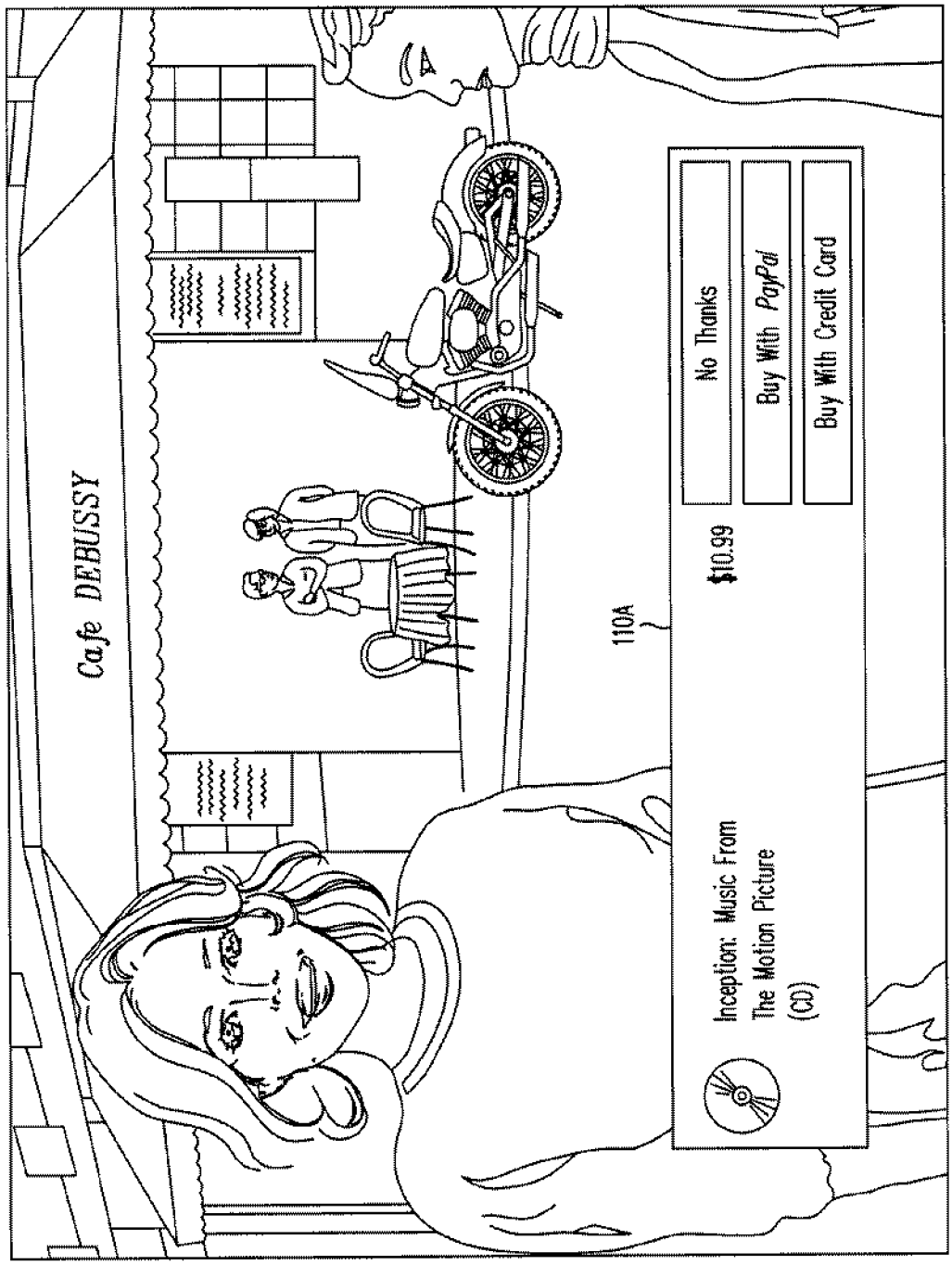

Cafe DEBUSSY
No Thanks
Buy With PayPal
Buy With Credit Card
$10.99
Inception: Music From
The Motion Picture
(CD)
110A
100A

FIG. 2

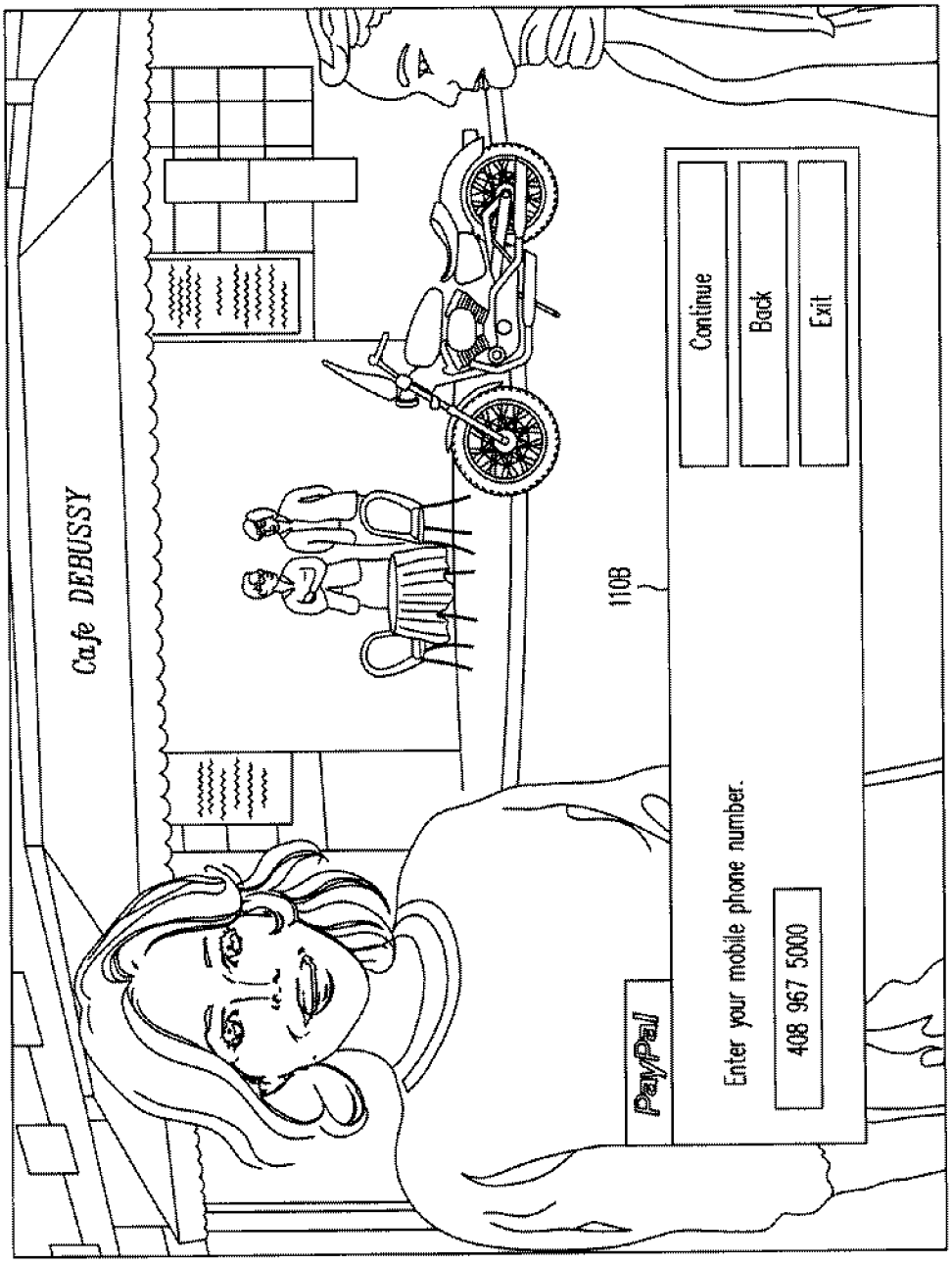

Cafe DEBUSSY
110B
Continue
Back
Exit
PayPal
Enter your mobile phone number.
408 967 5000
100B

FIG. 3

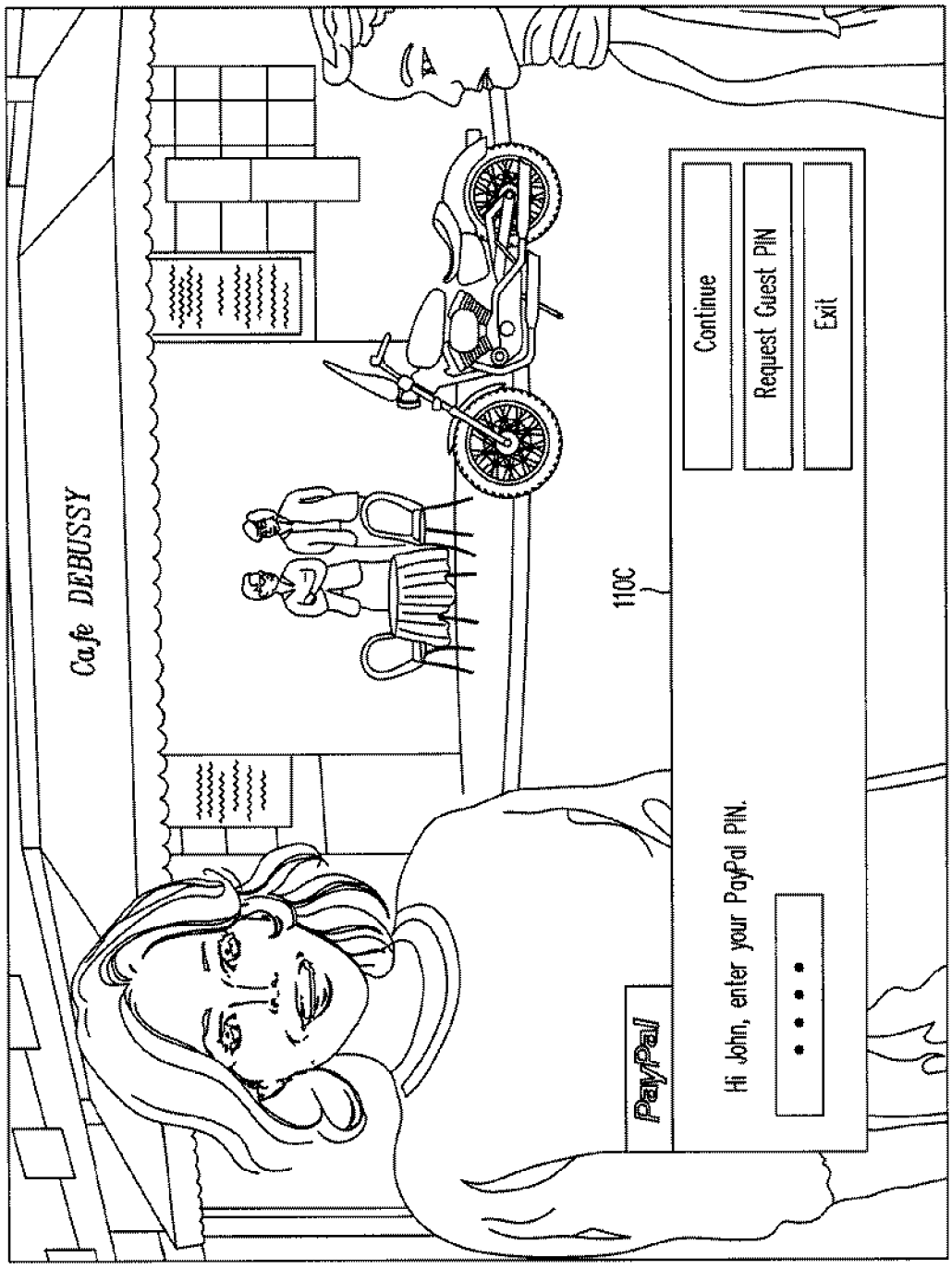

100C
Cafe DEBUSSY
110C
Continue
Request Guest PIN
Exit
PayPal
Hi John, enter your PayPal PIN.
• • • •

FIG. 4

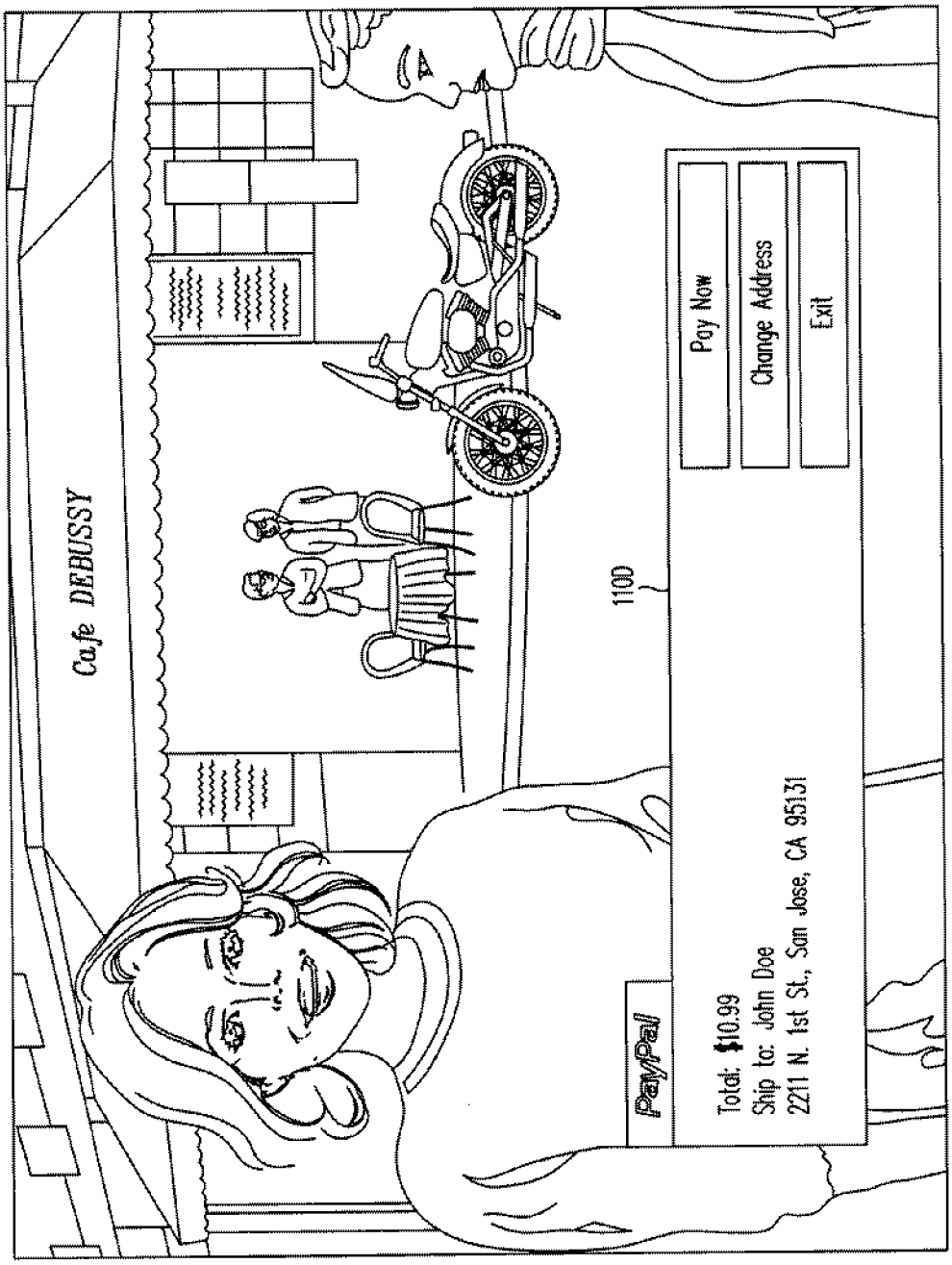

Cafe DEBUSSY
1100
Pay Now
Change Address
Exit
PayPal
Total: $10.99
Ship to: John Doe
2211 N. 1st St., San Jose, CA 95131
1000

FIG. 5

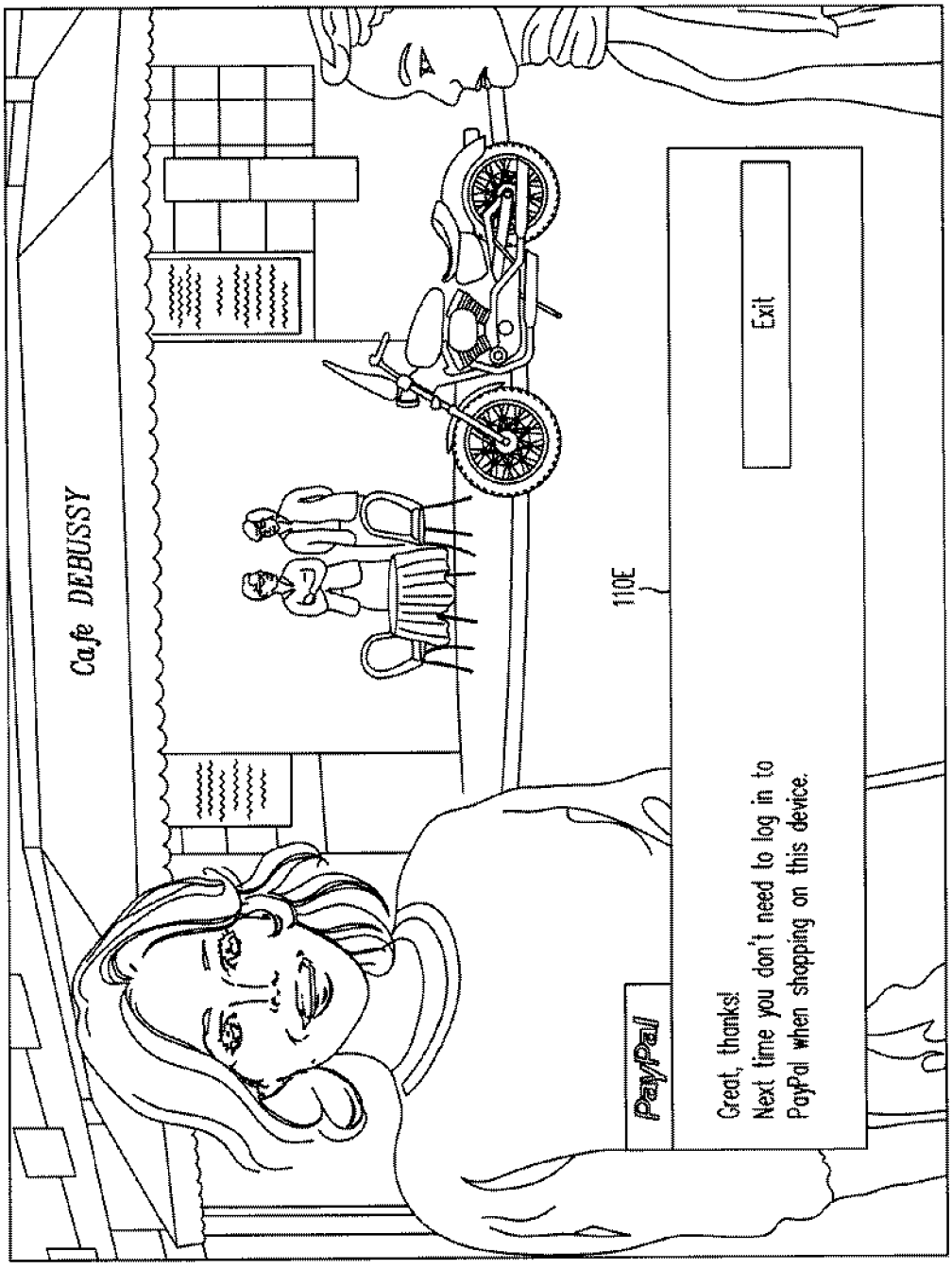

Cafe DEBUSSY
110E
Exit
PayPal
Great, thanks!
Next time you don't need to log in to
PayPal when shopping on this device.
100E

FIG. 6

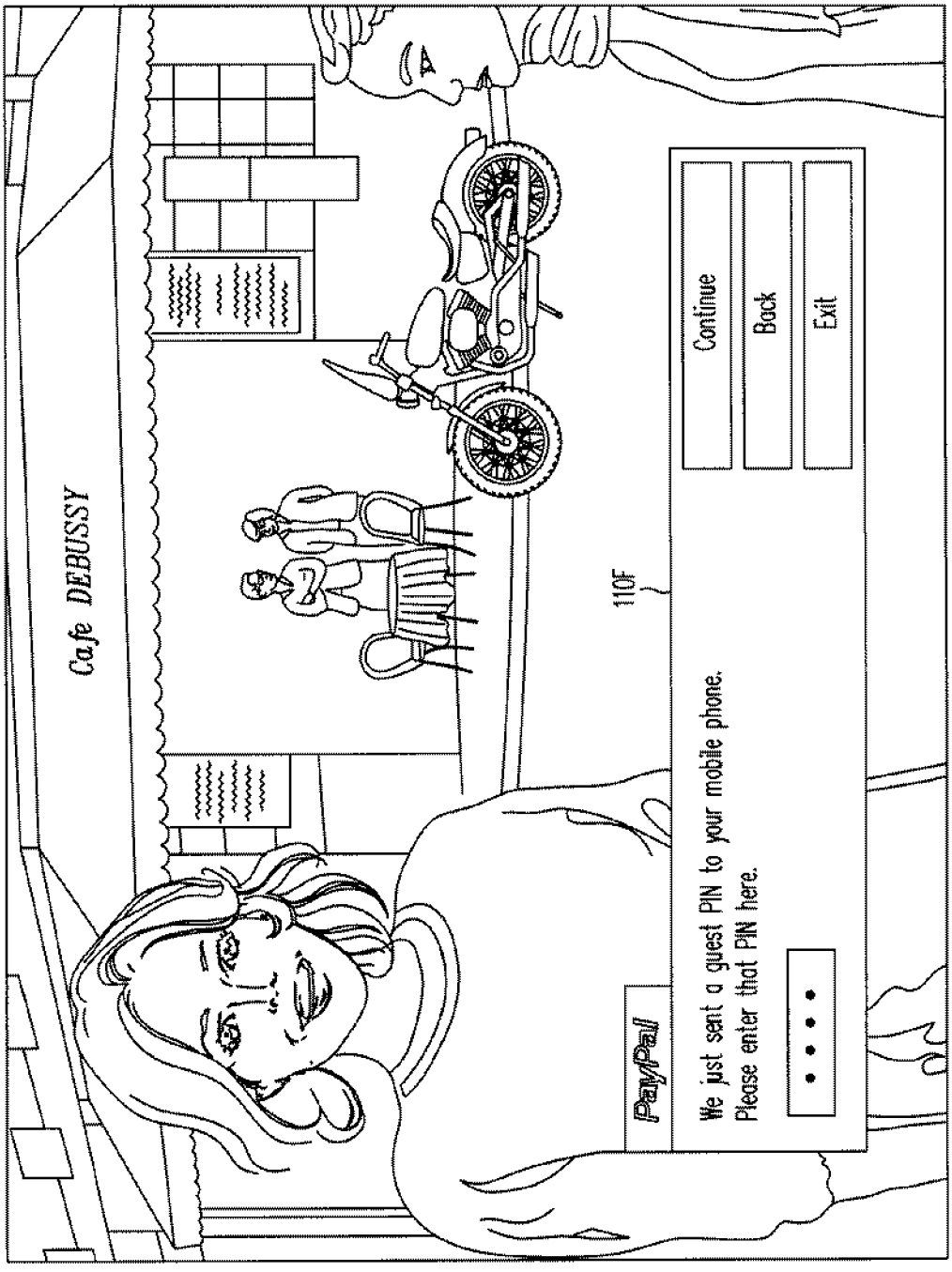

Cafe DEBUSSY
110F
Continue
Back
Exit
PayPal
We just sent a guest PIN to your mobile phone.
Please enter that PIN here.
• • • •
100F

FIG. 7

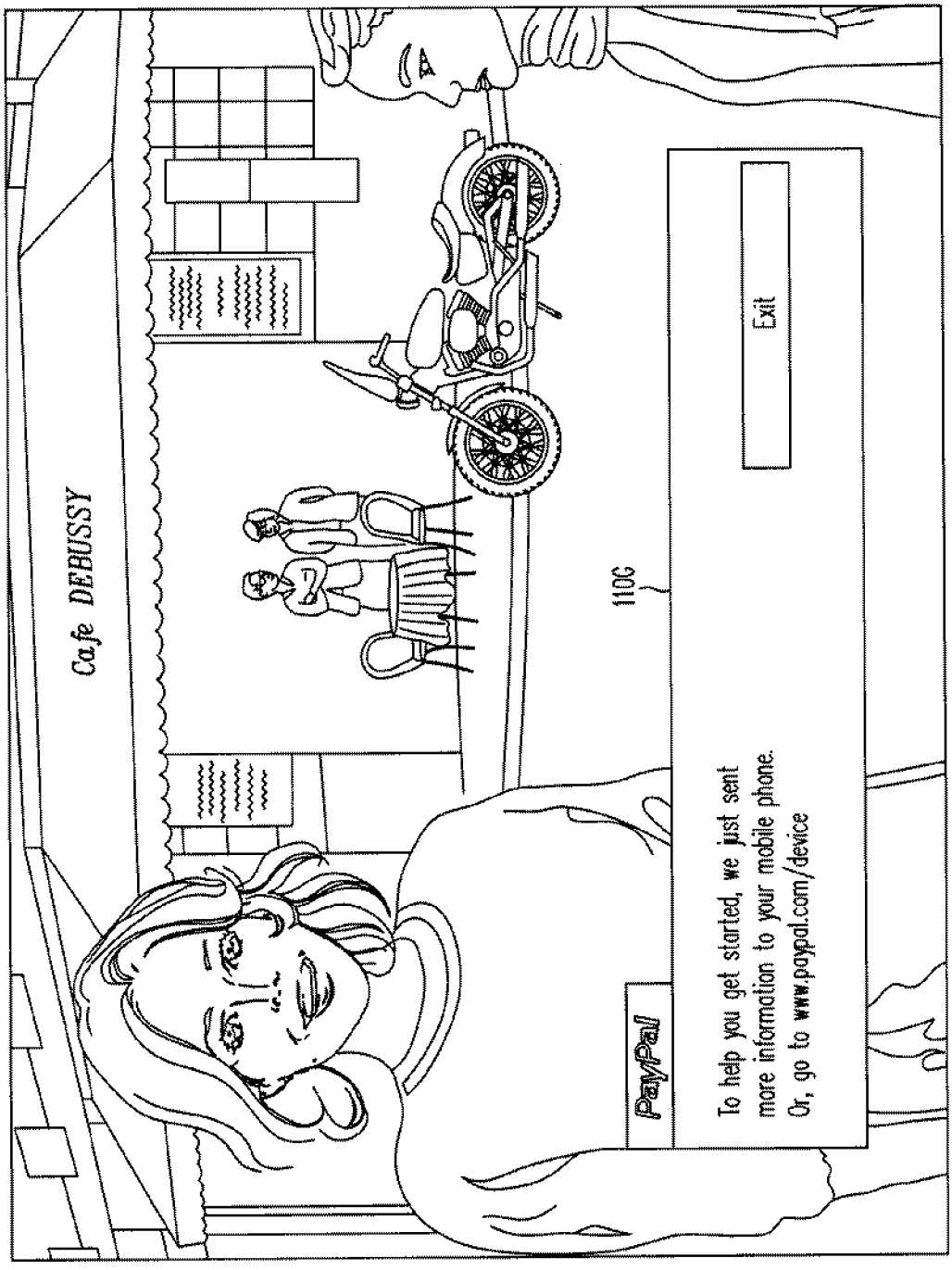

Cafe DEBUSSY
Exit
PayPal
To help you get started, we just sent more information to your mobile phone. Or, go to www.paypal.com/device
110C
100C

FIG. 8

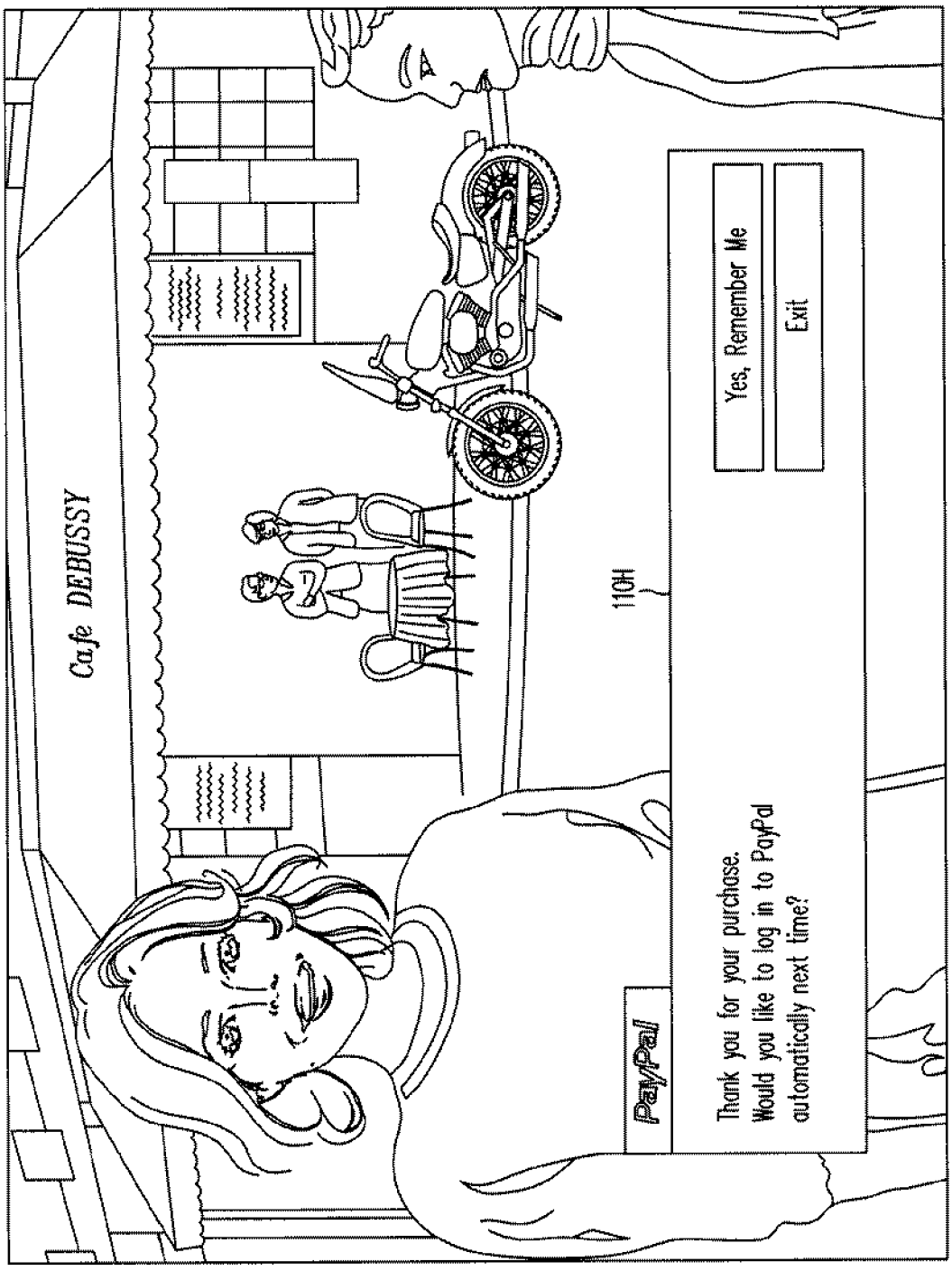

100H
Cafe DEBUSSY
110H
PayPal
Thank you for your purchase.
Would you like to log in to PayPal
automatically next time?
Yes, Remember Me
Exit

FIG. 9

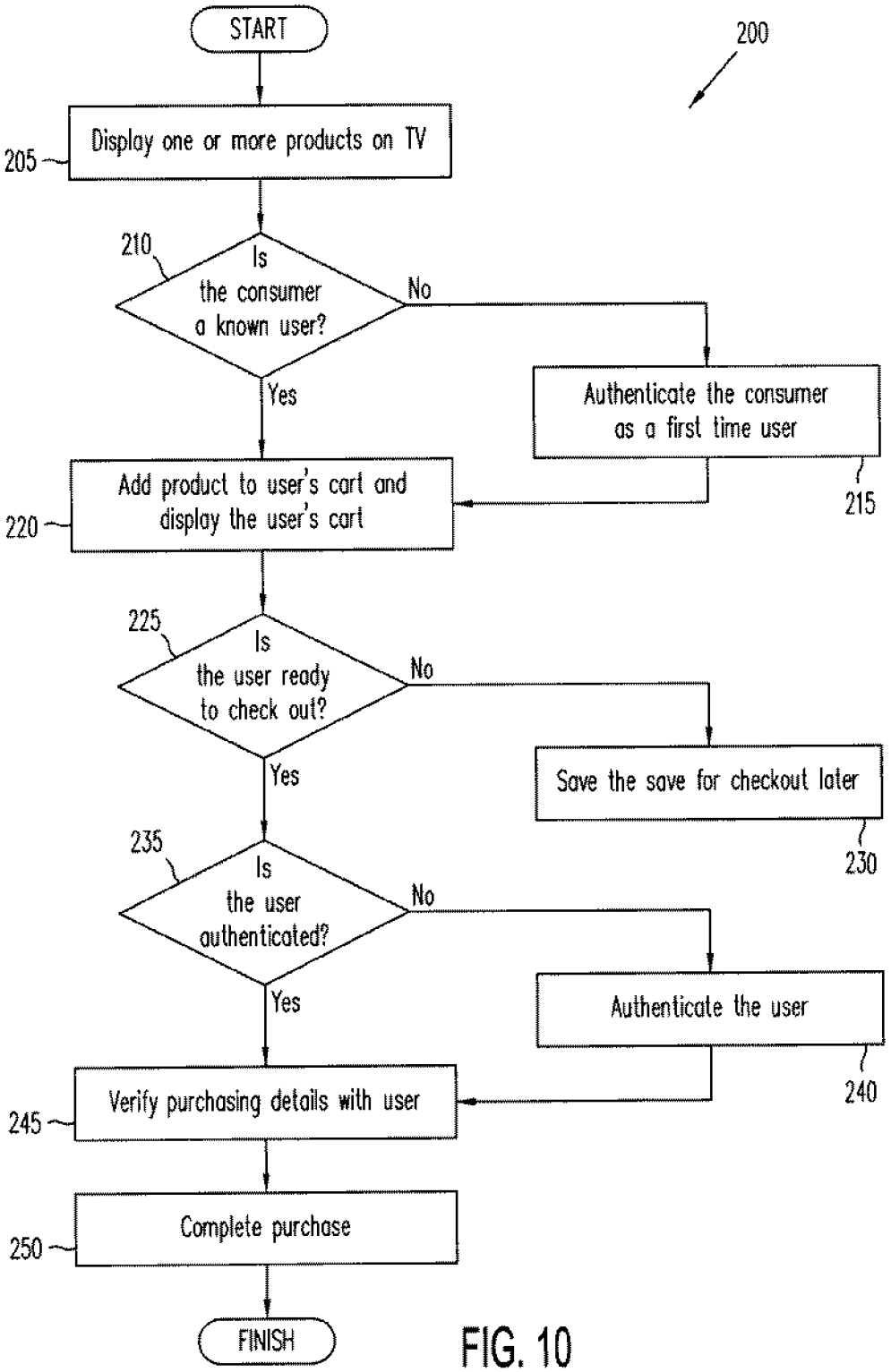

START
200
Display one or more products on TV
205
210
Is the consumer a known user?
No
Yes
Authenticate the consumer as a first time user
215
Add product to user's cart and display the user's cart
220
225
Is the user ready to check out?
No
Yes
Save the save for checkout later
230
235
Is the user authenticated?
No
Yes
Authenticate the user
240
Verify purchasing details with user
245
Complete purchase
250
FINISH

FIG. 10

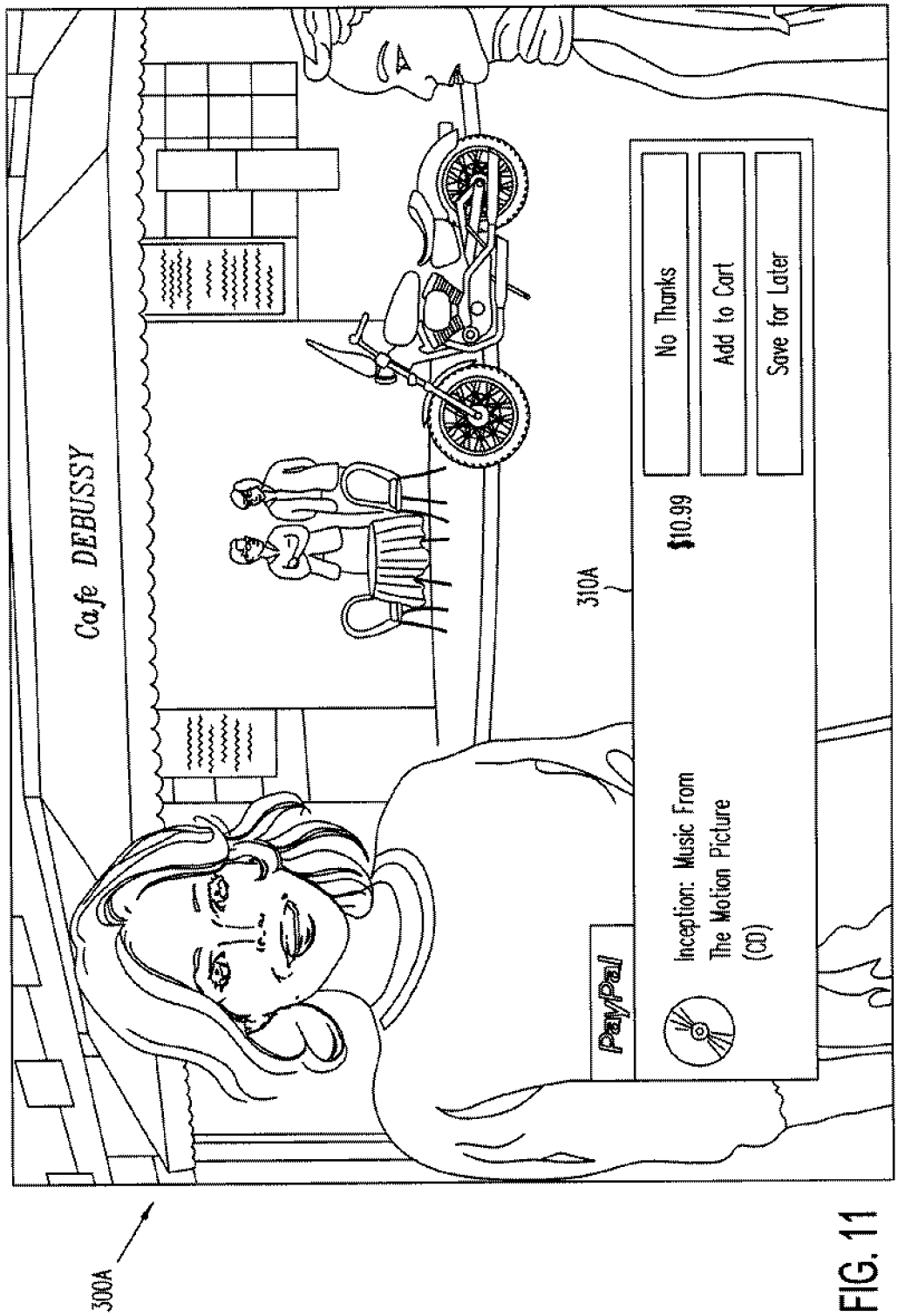

300A
Cafe DEBUSSY
310A
$10.99
No Thanks
Add to Cart
Save for Later
PayPal
Inception: Music From
The Motion Picture
(CD)

FIG. 11

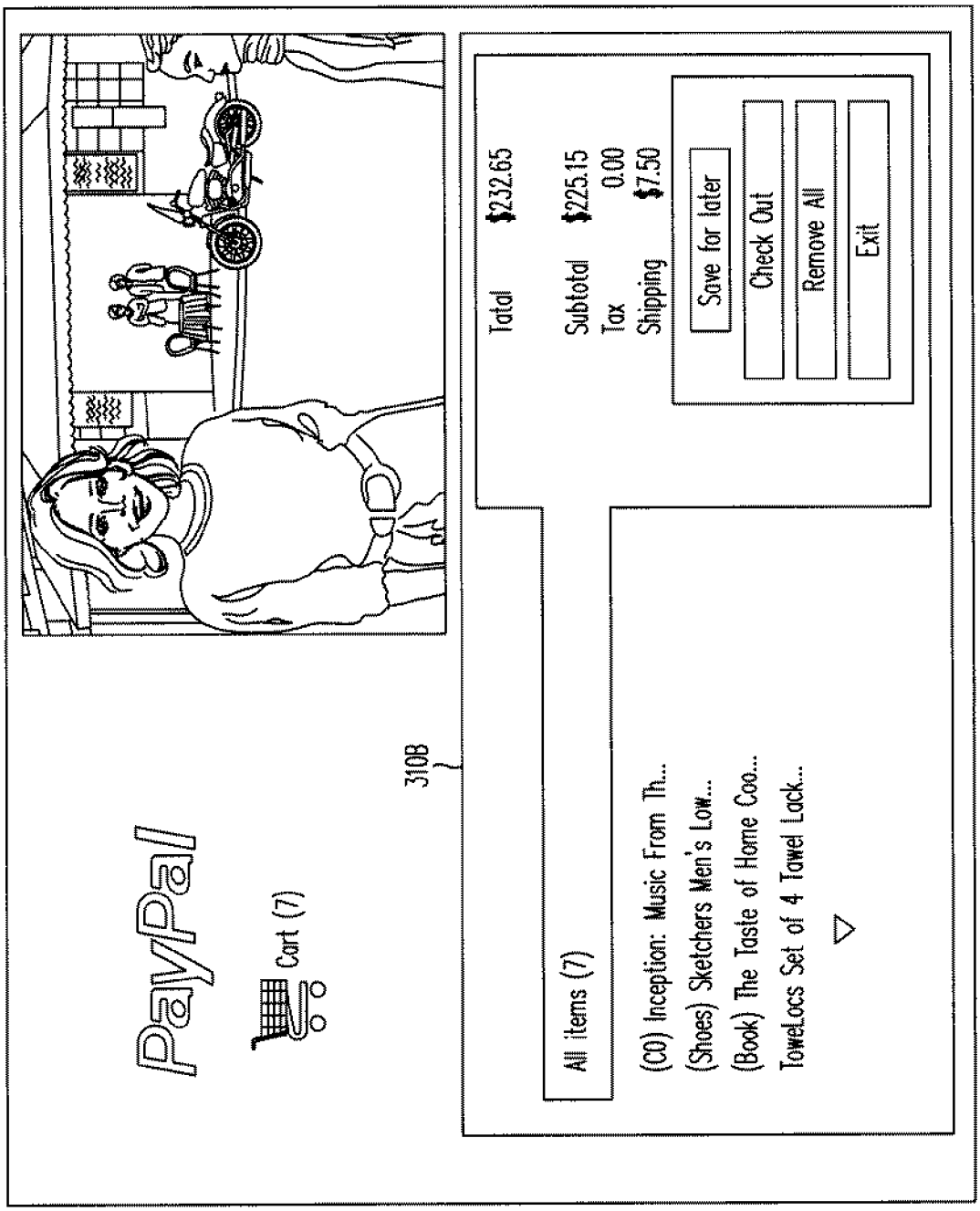

300B
PayPal
Cart (7)
310B
All items (7)
(CO) Inception: Music From Th...
(Shoes) Sketchers Men's Low...
(Book) The Taste of Home Coo...
TowelLocs Set of 4 Towel Lack...
Total $232.65
Subtotal $225.15
Tax 0.00
Shipping $7.50
Save for later
Check Out
Remove All
Exit

FIG. 12

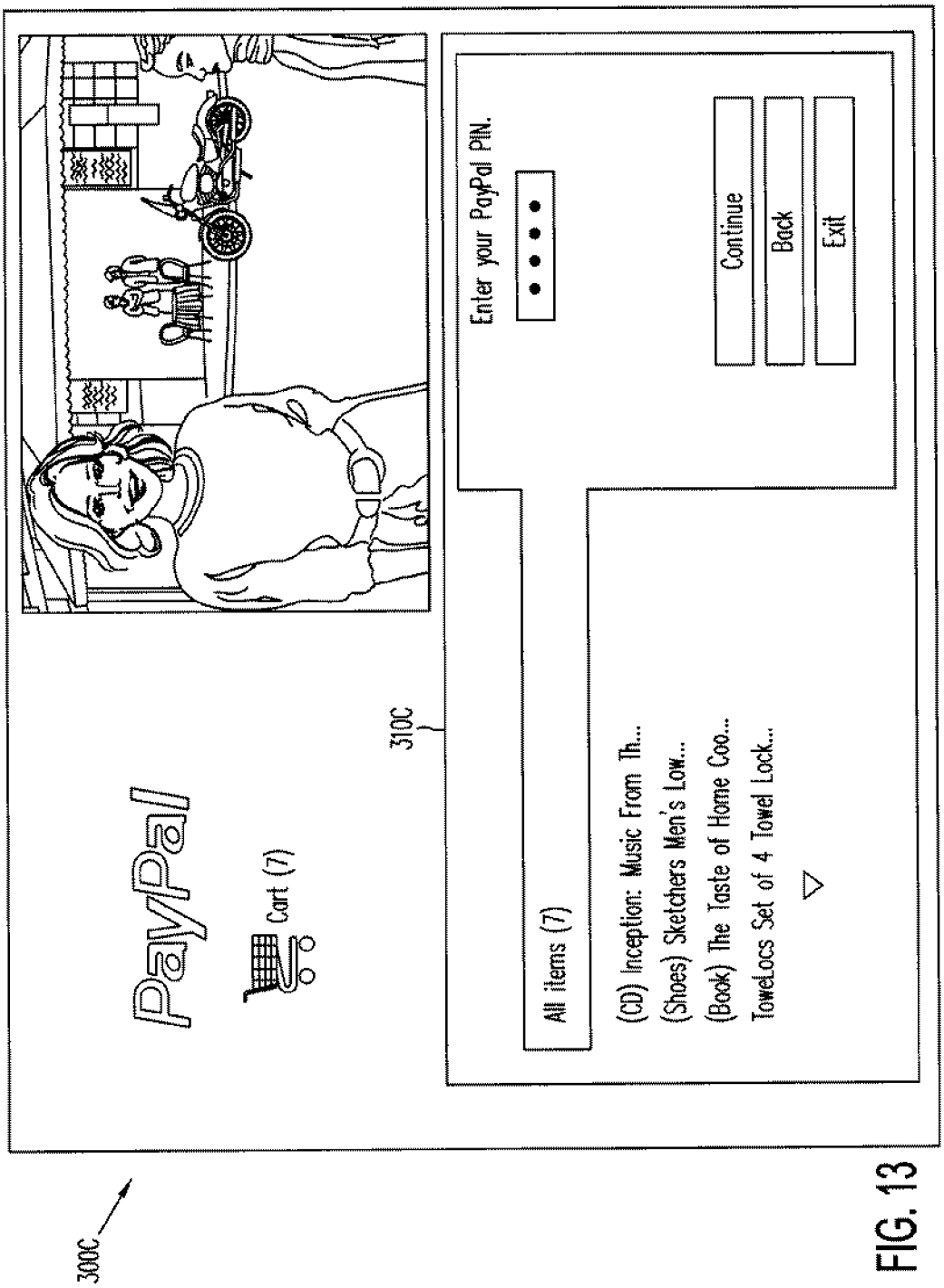

300C
PayPal
Cart (7)
310C
All items (7)
(CD) Inception: Music From Th...
(Shoes) Sketchers Men's Low...
(Book) The Taste of Home Coo...
TowelLocs Set of 4 Towel Lock...
Enter your PayPal PIN.
Continue
Back
Exit

FIG. 13

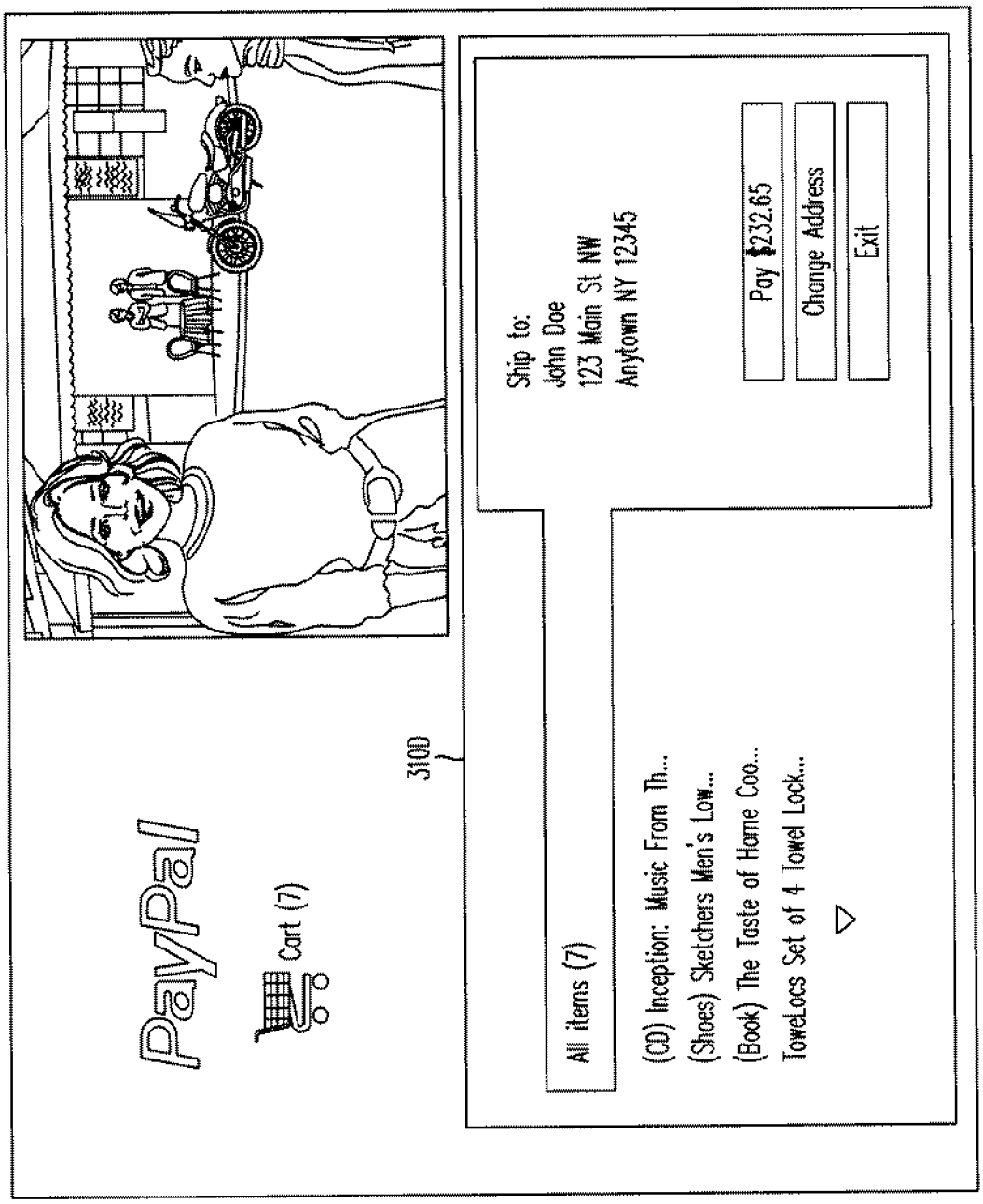

300D
PayPal
Cart (7)
310D
All items (7)
(CD) Inception: Music From Th...
(Shoes) Sketchers Men's Low...
(Book) The Taste of Home Coo...
TowelLocs Set of 4 Towel Lock...
Ship to:
John Doe
123 Main St NW
Anytown NY 12345
Pay $232.65
Change Address
Exit

FIG. 14

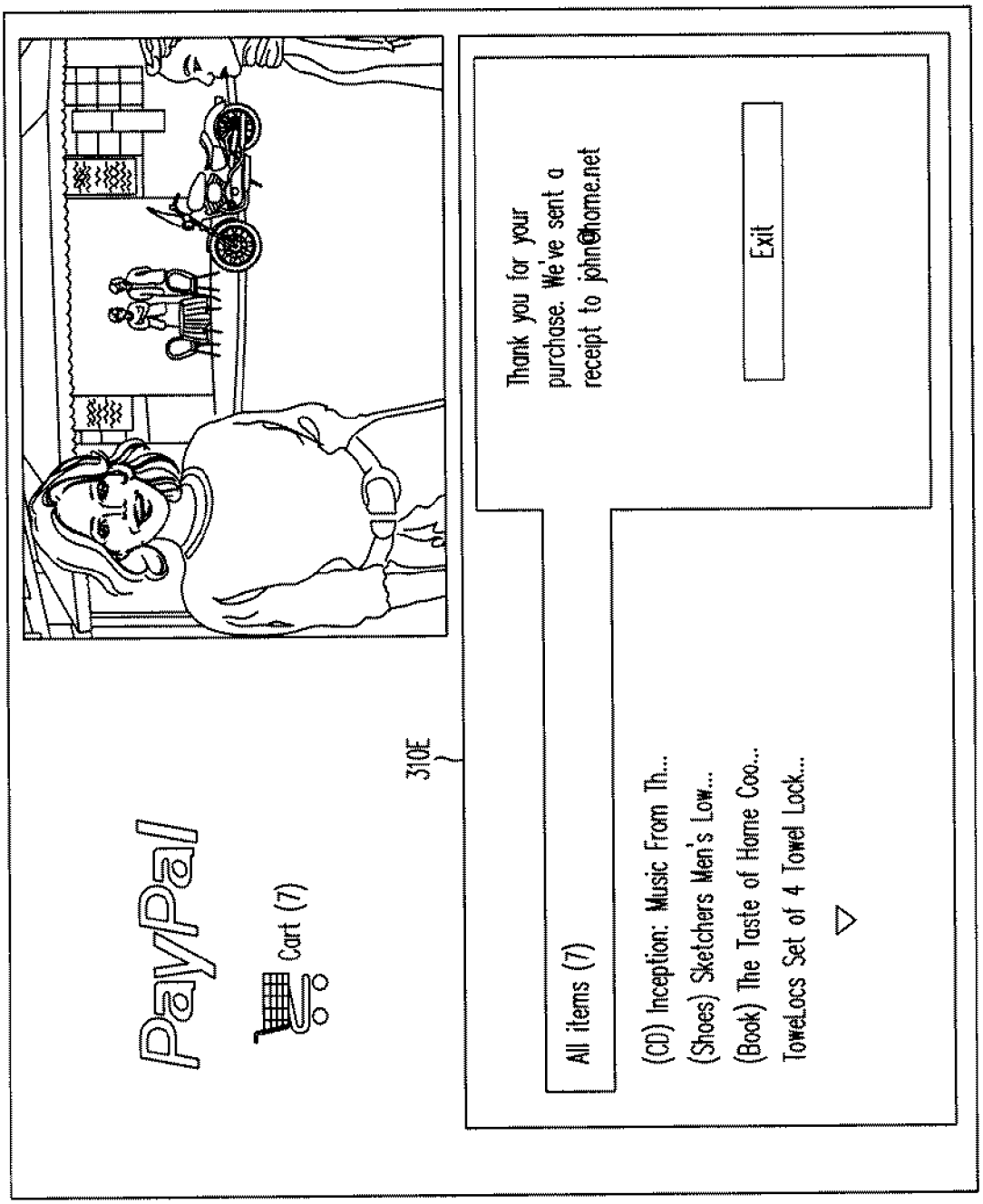

300E
PayPal
Cart (7)
310E
All items (7)
(CD) Inception: Music From Th...
(Shoes) Sketchers Men's Low...
(Book) The Taste of Home Coo...
TowelLocs Set of 4 Towel Lock...
Thank you for your purchase. We've sent a receipt to john@home.net
Exit

FIG. 15

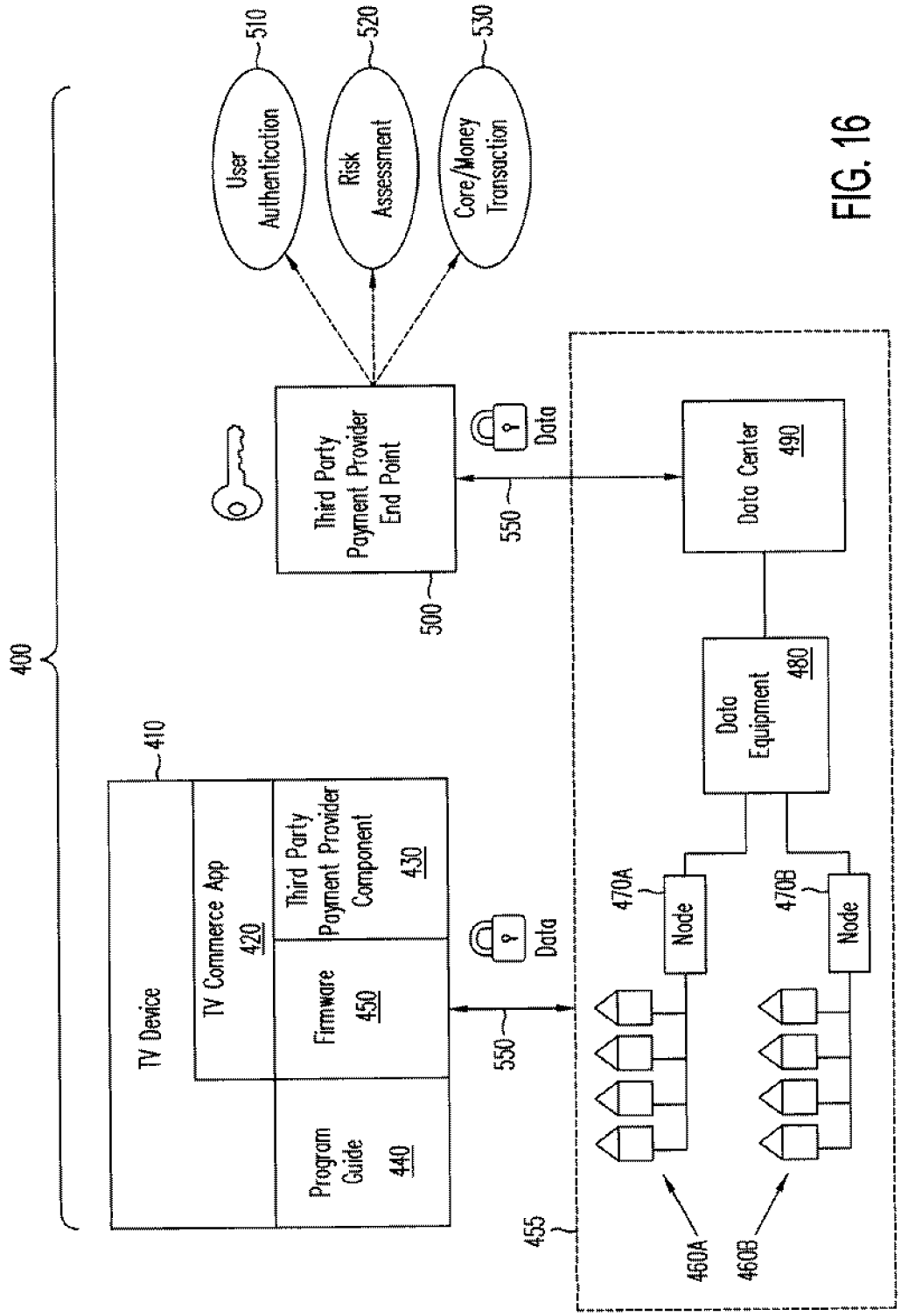

400
410
TV Device
TV Commerce App
420
Third Party
Payment Provider
Component
430
Firmware
450
Program
Guide
440
550
Data
550
Data
455
Third Party
Payment Provider
End Point
500
User
Authentication
510
Risk
Assessment
520
Core/Money
Transaction
530
Data Center
490
Data
Equipment
480
470A
Node
470B
Node
460A
460B

FIG. 16

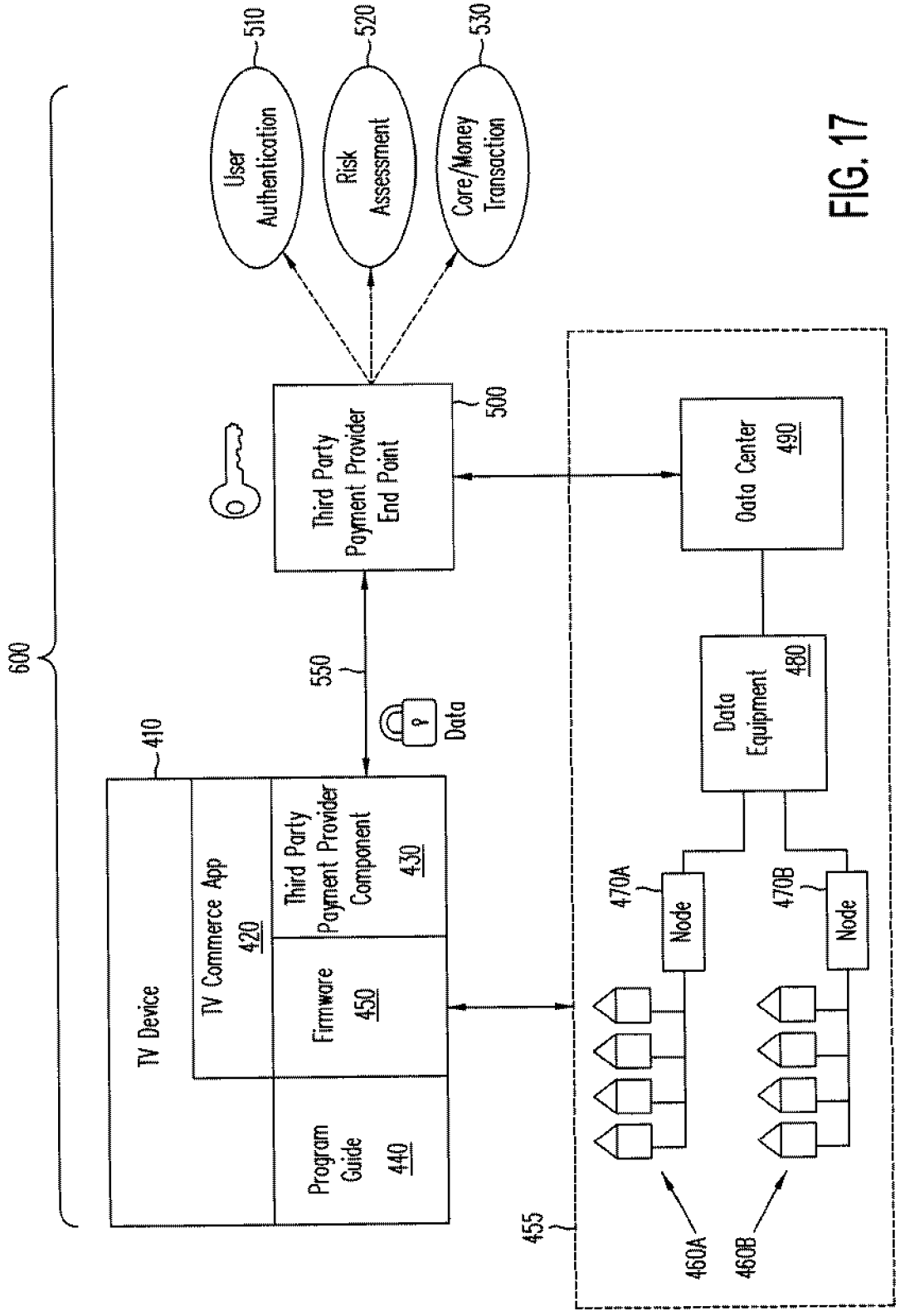

600
TV Device
410
TV Commerce App
420
Third Party
Payment Provider
Component
430
Firmware
450
Program
Guide
440
550
Data
Third Party
Payment Provider
End Point
500
User
Authentication
510
Risk
Assessment
520
Core/Money
Transaction
530
Data Center
490
Data
Equipment
480
470A
Node
470B
Node
460A
460B
455

FIG. 17

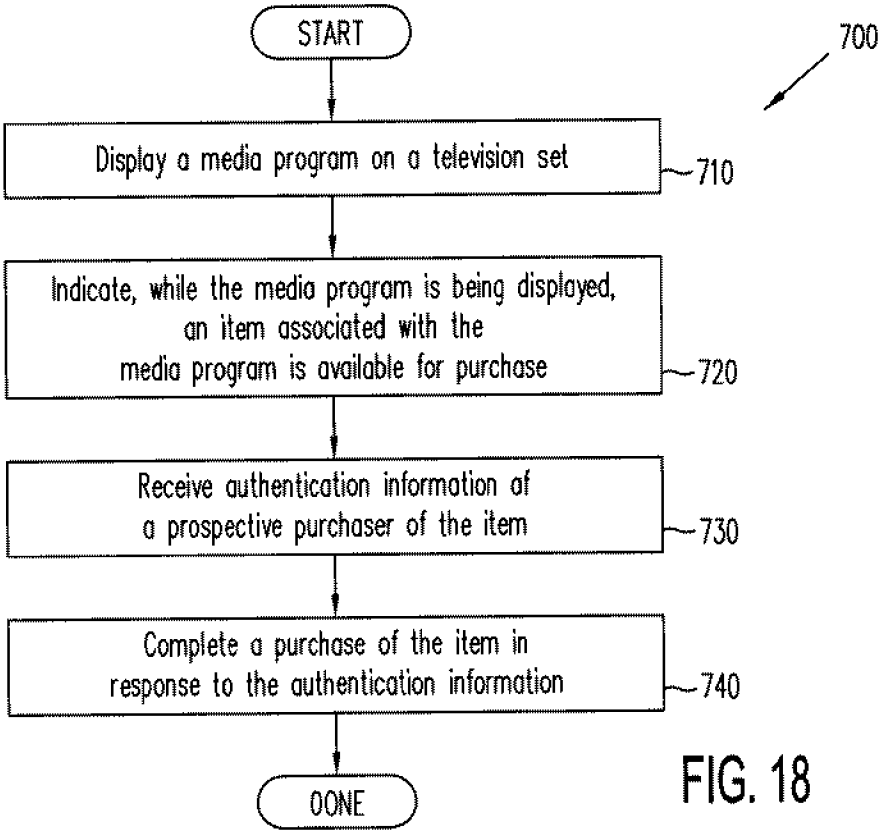

START
700
Display a media program on a television set
710
Indicate, while the media program is being displayed, an item associated with the media program is available for purchase
720
Receive authentication information of a prospective purchaser of the item
730
Complete a purchase of the item in response to the authentication information
740
DONE

FIG. 18

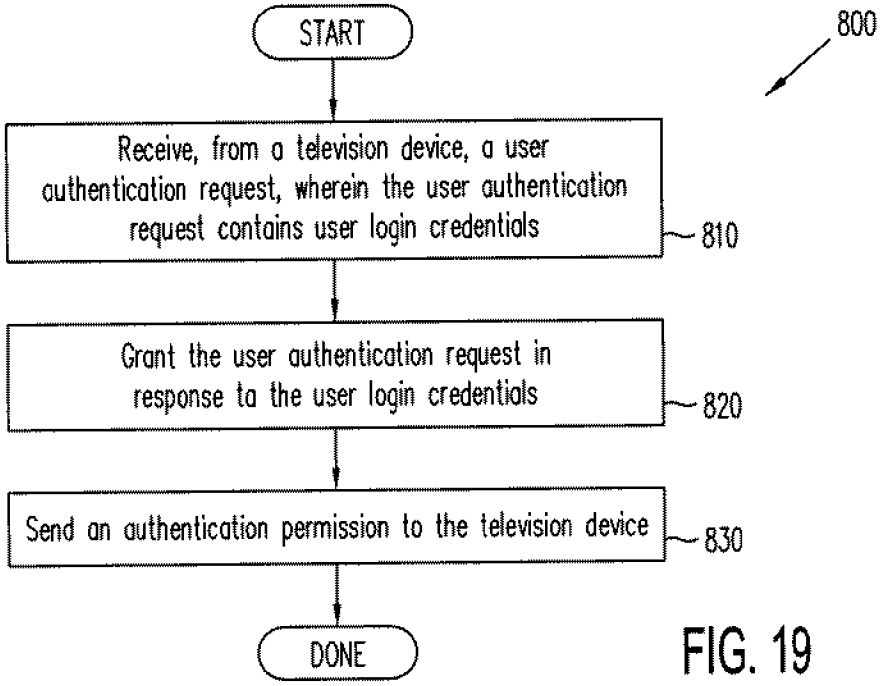

START
800
Receive, from a television device, a user authentication request, wherein the user authentication request contains user login credentials
810
Grant the user authentication request in response to the user login credentials
820
Send an authentication permission to the television device
830
DONE

FIG. 19

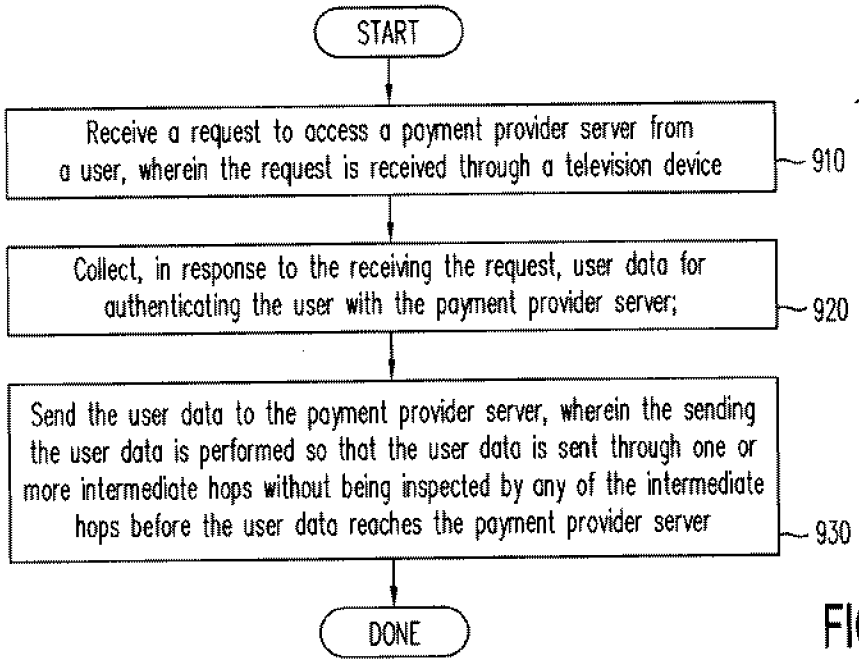

START
900
Receive a request to access a payment provider server from a user, wherein the request is received through a television device
910
Collect, in response to the receiving the request, user data for authenticating the user with the payment provider server;
920
Send the user data to the payment provider server, wherein the sending the user data is performed so that the user data is sent through one or more intermediate hops without being inspected by any of the intermediate hops before the user data reaches the payment provider server
930
DONE

FIG. 20

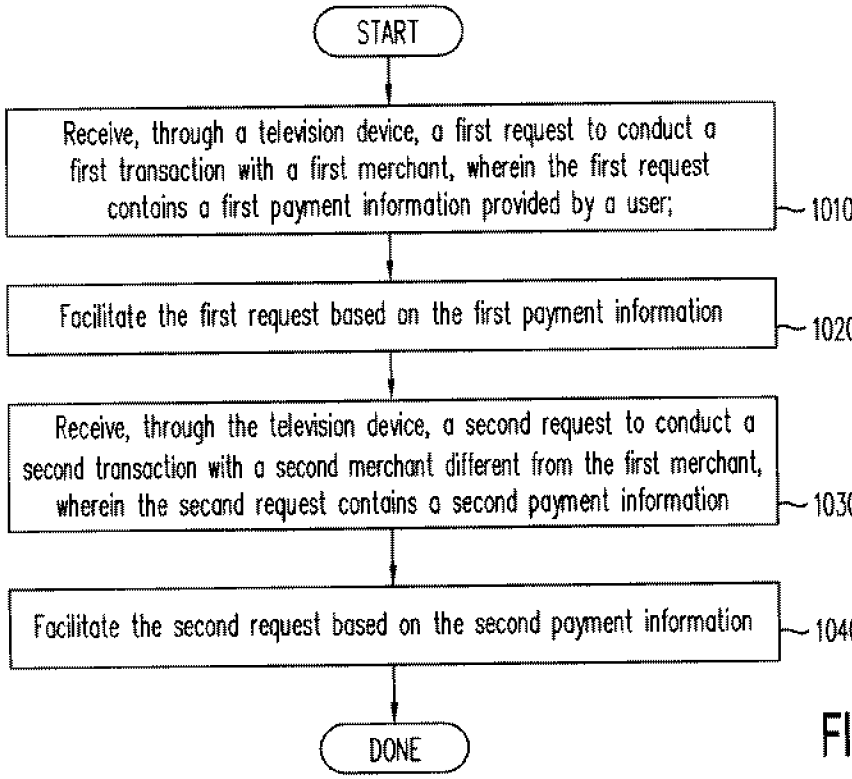

START
1000
Receive, through a television device, a first request to conduct a first transaction with a first merchant, wherein the first request contains a first payment information provided by a user;
1010
Facilitate the first request based on the first payment information
1020
Receive, through the television device, a second request to conduct a second transaction with a second merchant different from the first merchant, wherein the second request contains a second payment information
1030
Facilitate the second request based on the second payment information
1040
DONE

FIG. 21

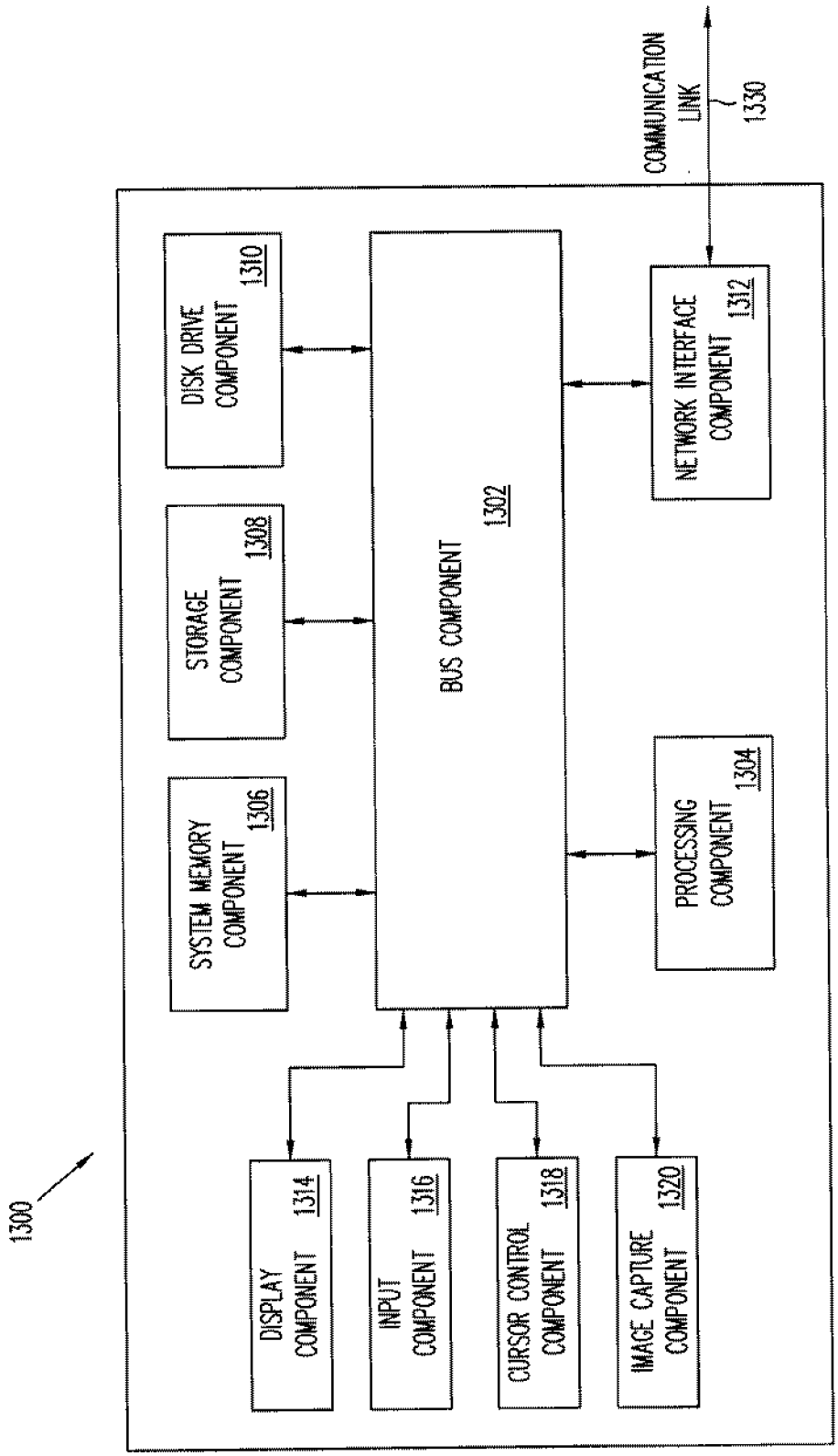

1300
COMMUNICATION LINK
1330
DISK DRIVE COMPONENT
1310
STORAGE COMPONENT
1308
SYSTEM MEMORY COMPONENT
1306
BUS COMPONENT
1302
NETWORK INTERFACE COMPONENT
1312
PROCESSING COMPONENT
1304
DISPLAY COMPONENT
1314
INPUT COMPONENT
1316
CURSOR CONTROL COMPONENT
1318
IMAGE CAPTURE COMPONENT
1320

FIG. 22

SINGLE DIGITAL WALLET ACROSS MULTIPLE PAYMENT PLATFORMS

CROSS REFERENCE TO RELATED APPLICATION

[0001] The present application claims priority to U.S. Provisional Patent Appl. Ser. No. 61/453,843, filed Mar. 17, 2011 and titled "PAYMENT AUTHENTICATION AND AUTHORIZATION NON-WEB DEVICES," which is incorporated by reference in its entirety. The present application is also related to concurrently filed U.S. Applications entitled "MAKING INTERACTIVE PURCHASES THROUGH A MEDIA DISPLAY DEVICE," bearing attorney docket number 70481.478, and "SINGLE DIGITAL WALLET ACROSS MULTIPLE PAYMENT PLATFORMS," bearing attorney docket number 70481.520, both of which are incorporated by reference in their entirety.

BACKGROUND

[0002] 1. Technical Field

[0003] The present disclosure generally relates to conducting electronic transactions and, more particularly, to conducting transactions using a media display device such as a television set.

[0004] 2. Related Art

[0005] Before the rise of electronic media, consumers usually go to physical "brick and mortar" stores to conduct their purchases. As electronic commerce became increasingly popular in recent years, consumers have been given more options to complete their shopping without leaving their homes. For example, the consumer may see a product advertised during a TV infomercial. If the consumer wishes to purchase the product, he may then call the merchant selling the product or go to the merchant's website to complete the purchase. However, transactions like the one described above may be cumbersome (for example, they require the consumer to leave the TV), may not be interactive enough, and may also lack sufficient security.

[0006] Therefore, while existing electronic commerce transactions involving TVs have been generally adequate for their intended purposes, they have not been entirely satisfactory in every aspect. It would be advantageous to make it easier for prospective consumers to conduct secure transactions through a TV.

SUMMARY

[0007] One of the broader forms of the present disclosure involves a method. The method involves: initializing a digital check-in chain for a venue; expanding, electronically by a processor, the check-in chain with a plurality of check-in entries that each correspond to a visit to the venue by a respective user, wherein each check-in entry on the check-in chain is generated in response to one or more preceding check-in entries on the check-in chain; detecting fraudulent check-in entries in response to a split in the check-in chain; and removing the fraudulent check-in entries from the check-in chain.

[0008] Another one of the broader forms of the present disclosure involves an apparatus comprising a non-transitory, tangible computer readable storage medium storing a computer program. The computer program has instructions that when executed, perform: initializing a digital check-in chain for a venue; expanding, electronically by a processor, the check-in chain with a plurality of check-in entries that each correspond to a visit to the venue by a respective user, wherein each check-in entry on the check-in chain is generated in response to one or more preceding check-in entries on the check-in chain; detecting fraudulent check-in entries in response to a split in the check-in chain; and removing the fraudulent check-in entries from the check-in chain.

[0009] Yet another one of the broader forms of the present disclosure involves a method. The method involves: providing a check-in seed for a venue; receiving a first check-in entry, the first check-in entry being a function of the check-in seed; verifying, electronically by a processor, the first check-in entry; forming a check-in chain by appending the first check-in entry after the check-in seed if the first check-in entry is successfully verified; receiving a second check-in entry, the second check-in entry being a function of the check-in seed and the first check-in entry; verifying, electronically by the processor, the second check-in entry; and expanding the check-in chain by appending the second check-in entry after the first check-in entry if the second check-in entry is successfully verified.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. **1** illustrates an example flowchart for performing a transaction according to various aspects of the present disclosure.

[0011] FIGS. **2-9** illustrate example user interfaces for conducting a transaction through a television according to various aspects of the present disclosure.

[0012] FIG. **10** illustrates an example flowchart for performing a transaction according to various aspects of the present disclosure.

[0013] FIGS. **11-15** illustrate example user interfaces for conducting a transaction through a television according to various aspects of the present disclosure.

[0014] FIGS. **16-17** illustrate example media infrastructures for enabling the conducting the transactions through a television according to various aspects of the present disclosure.

[0015] FIGS. **18-21** illustrate example flowcharts for performing a transaction according to various aspects of the present disclosure.

[0016] FIG. **22** illustrates a block diagram of a computer system for implementing various methods and devices described according to various aspects of the present disclosure.

DETAILED DESCRIPTION

[0017] It is to be understood that the following disclosure provides many different embodiments, or examples, for implementing different features of the present disclosure. Specific examples of components and arrangements are described below to simplify the present disclosure. These are, of course, merely examples and are not intended to be limiting. Various features may be arbitrarily drawn in different scales for simplicity and clarity.

[0018] Before the rise of electronic media, consumers usually had to conduct their shopping outside their homes. A prospective consumer would have to go visit one or more physical "brick and mortar" stores to survey the merchandise available at each store. If the consumer is interested in a piece of merchandise, he then buys and pays for the merchandise at the store that offers it for sale.

[0019] As electronic commerce became more popular in recent years, consumers have been given more flexibility regarding being able to do shopping without having to leave their homes. For example, a consumer may see a product being advertised while watching an infomercial on television (TV). The infomercial may display the merchant's phone number and/or website address. If the consumer is interested in purchasing the product, he may call the merchant or log on to the merchant's website to complete the purchase. However, these types of transactions may be inconvenient to the consumer, as the consumer may not be able to instantly buy the product but may be forced to leave the TV. In addition, these transactions may not be secure enough.

[0020] According to the various aspects of the present disclosure, an improved method of conducting a transaction through a TV is disclosed, as discussed in more detail below.

[0021] FIG. **1** is a flowchart illustrating a method **20** of purchasing a product via a TV set through a third party payment provider/platform. For example, the third party payment provider may be PAYPAL, INC®. of San Jose, Calif. or another suitable financial institution. The method **20** includes a step **25**, in which one or more products or pieces of merchandise is displayed on TV during a TV program. The products may include physical and tangible goods, including (but not limited to) clothing, electronics, tools, toys, household appliances, books, movies, automotive components, sporting goods, groceries, etc. The products may also include digital goods, which include goods that are stored, delivered, and/or used in an electronic format. As non-limiting examples, digital goods may include electronic-books, digital music, digital images, digital videos, virtual items, etc. The virtual items may be virtual currency or other types of precious items (e.g., virtual gold, virtual weapons/armor, virtual medicine, virtual gems) that can be obtained and used in a virtual reality role-playing computer game. In some cases, the "product" being offered may even include an opportunity to donate to a charity.

[0022] The method **20** continues with a step **30**, in which a consumer is prompted to enter his account verification information associated with the third party payment provider. In some embodiments, the consumer may be prompted to enter his mobile telephone number (or another suitable personal identification number (PIN)) linked to his account with the third party payment provider. In other embodiments, the consumer may be prompted to enter a username and a password that are associated with his account with the third party payment provider. In certain embodiments, the consumer may be allowed to choose to enter either the mobile telephone number, or the username and password, or another suitable identifier associated with his account.

[0023] The method **20** continues with a decision step **35** to determine if the account information has been verified. In embodiments where the consumer chooses to enter a mobile telephone number (or another suitable PIN), the decision step **35** checks to see if the entered mobile telephone number or PIN matches any existing numbers associated with the third party payment provider. If the answer is no, then the method **20** may proceed to a step **40**, in which the consumer is prompted to register for an account with the third party payment provider. In some embodiments, if the consumer wishes not to register for an account, a guest PIN may be sent to the consumer (e.g., as a text message to the consumer's mobile telephone or as an email to the consumer's email address) upon the consumer's request. The guest PIN provides a temporary login for the consumer to complete the transaction.

[0024] In a similar manner, in embodiments where the consumer chooses to enter a username and a password, the decision step **35** checks to see if the combination of entered username and password matches an existing account with the third party payment provider. If the answer is no, then the method **20** proceeds to the step **40**, in which the consumer is prompted to register for an account with the third party payment provider. Once again, if the consumer chooses not to register for an account at this time, a temporary guest login may be sent to the consumer to complete the transaction.

[0025] If the answer from the decision step **35** is yes—whether as a result of a matched mobile phone number or a correct combination of username and password being entered—the method **20** continues with a step **45** in which the purchase is confirmed with the consumer. In various embodiments, the purchase confirmation may display to the consumer information such as the consumer's name and address as well as the product's name, quantity, and price. In some embodiments, as a part of the execution of the step **45**, the consumer may be given an option to change one or more aspects of the purchase, including but not limited to the quantity or the consumer's shipping address.

[0026] The method **20** continues with a step **50**, in which it is determined whether automatic login should be used for subsequent purchases. In some embodiments, the consumer may be specifically prompted as to whether he would prefer to have the login information "remembered" for his subsequent purchases. Having the login information "remembered" is convenient when the consumer lives alone and/or is using his own TV at home. On the other hand, if the consumer is traveling (e.g., watching a TV program at a hotel at which he is staying) or has to share the TV with other roommates, then the consumer may choose not to have his login information remembered for security purposes. Based on the answer received form the consumer, the method **20** may either "remember" or discard the login information.

[0027] It is understood that the method **20** discussed above merely illustrates an example process flow and is not intended to be limiting, and that additional steps may be performed before, during, or after the steps **25-50** of the method **20**. To facilitate a better understanding of the various aspects of the method **20**, FIGS. **2-9** are provided to graphically illustrate some embodiments of the method **20**.

[0028] Referring to FIG. **2**, an example user interface **100**A is displayed. According to the various aspects of the present disclosure, the user interface **100**A is a screenshot of a TV program that the consumer is watching. In some embodiments, the TV program may be a movie, a TV show, a music video, a commercial, a documentary, an educational program, a sporting event, a video game, or another suitable media program displayed on the consumer's TV set. According to certain aspects of the present disclosure, the TV program is being displayed to the TV set through a video stream (or data stream). At various points of the video stream, there are embedded trigger points in the video stream to notify the consumer that an offer for a merchandise is available.

[0029] In some embodiments, the offer may be displayed as a text box (or a dialog box) **110**A, which contains a brief description of the product being offered. As discussed above with reference to FIG. **1**, the product being offered may be a tangible piece of merchandise or a digital item. As an example, the product being offered in FIG. **2** is the musical

soundtrack from the TV program, which is a movie. As other non-limiting examples, the product being offered may be a piece of clothing (e.g., for a specific brand name) that the actor/actress is wearing, a coupon for a restaurant or store shown in the background, or a deal to buy an item appearing in the scene of the TV program (e.g., a 20% off offer to buy a motorcycle that is shown in the scene). In other words, the product being offered is integrated into or "embedded" within the TV program. At predetermined times while the TV is program is being shown to the consumer, the right offers will be triggered and be displayed to the consumer.

[0030] In some embodiments, the availability of the offer will initially be displayed as a small icon (not illustrated herein), which may be shown unobtrusively near a corner of the screen so as to not disrupt the consumer's viewing of the TV program. The icon may or may not indicate what the product being offered will be. If the consumer is interested in finding ont more abont the offer, he can click on the icon, which may then expand into the text box **110**A shown in FIG. **2**. In certain embodiments, the consumer may be given a choice with respect to how he wishes to be notified of the offer: he may elect not to be notified of any offers at all, or he may elect to be first notified of an availability of an offer with the small unobtrusive icon, or he may elect to be notified of the offer with a text box such as the text box **110**A of FIG. **2**. The consumer may set these preferences before or during the TV program is being played.

[0031] In addition to displaying the description of the product being offered, the text box **110**A may also display the price and/or quantity of the product, as well as one or more payment options. For example, a logo of the third party payment provider (e.g., PAYPAL) may be displayed as one of the payment options.

[0032] Referring now to FIG. **3**, once the consumer chooses to pay with the third party payment provider, an example user interface **100**B is displayed to the consumer, in which the consumer is prompted to enter suitable identification information associated with his account with the third party payment provider. In the embodiment illustrated in FIG. **3**, the user interface **100**B contains a text box **110**B that prompts the consumer to enter a mobile telephone number that is linked to his third party payment provider accounnt. In some embodiments, the consumer may enter the mobile telephone number through a suitable mechanism such as a TV remote.

[0033] Referring now to FIG. **4**, after the consumer inputs his mobile telephone number, an example user interface **100**C is displayed to the consumer. In this case, it has been verified that the mobile telephone number that the consumer has entered does match a telephone number for an existing user in the third party payment provider's system. Consequently, the user interface **100**C displays a text box **110**C that prompts the consumer to enter a secret code or a PIN associated with the correct user. For example, the secret code or PIN may be a multi-digit number.

[0034] Referring now to FIG. **5**, the consumer has entered the correct secret code or PIN and has been successfully verified, and he is now considered "logged-in" to the system. It is understood that in some embodiments, the consumer may also log in to the system using an email address and a password, rather than the mobile phone number and a PIN. The consumer may be given the option to choose a preferred login method. For reasons of simplicity, the user interfaces pertaining to the email/password login method is not illustrated herein. Regardless of which method the consumer chooses to log in to the system, once he has been correctly verified, an example user interface **100**D then displays a text box **110**D to the consumer. The text box **110**D may contain details regarding the transaction, such as the amonnt total of the purchase and/or the shipping address of the purchaser. The text box **110**D may also allow the consumer to change the shipping address.

[0035] Referring now to FIG. **6**, once the consumer confirms that all the purchasing information is correct and follows throngh with the purchase, an example user interface **100**E is then displayed to the consumer. The example user interface **100**E includes a text box **110**E that informs the consumer that the transaction is successful and that the consumer need not login to the third party payment platform for subsequent purchases. The text box **110**E may also optionally inform the consumer that an electronic confirmation (such as an email confirmation) regarding the purchase may be sent to the consumer soon.

[0036] As discnssed above with reference to FIG. **1**, if the consumer does not have an account with the third party payment provider and does not wish to register for an account, he may be given a temporary guest login to complete the transaction. An example of this sitnation is graphically illustrated in FIG. **7**, in which a user interface **100**F displays a text box **110**F to the consumer. The text box **110**F may inform the consumer that a guest PIN or temporary secret code has been sent to the consumer's mobile phone (or email address), and the consumer is prompted to enter that guest PIN. Once the correct PIN is entered, the purchasing transaction may resume in a similar manner as discussed above with reference to FIGS. **5**-**6**.

[0037] On the other hand, if the consumer does not have an account with the third party payment provider but is ready to register for an account, an example user interface **100**G may be displayed to the consumer, as illustrated in FIG. **8**. The user interface **100**G may include a text box **110**G that informs the consumer that additional account signup information has been sent to his mobile phone or email address. In addition, the consumer may also visit a website of the third party payment provider in order to sign up for an account.

[0038] Also as discussed above with reference to FIG. **1**, the consumer may be given an option to log in to the third party payment provider automatically for the subsequent purchases. This aspect of the present disclosure is graphically illustrated in FIG. **9**, which asks the consumer such question in a text box **110**H. If the consumer chooses yes, then he no long needs to perform a login to the third party payment provider every time. Instead, his login information will be "remembered" for subsequent purchases.

[0039] The discussions above pertain to the purchase of a single item as an example. According to the various aspects of the present disclosure, the consumer may indeed purchase multiple products in the same transaction. FIG. **10** is a flowchart of a method **200** that illustrates an example process flow for performing a purchasing transaction involving multiple products.

[0040] Referring to FIG. **10**, the method **200** includes a step **205**, in which one or more products are displayed on TV. This step is similar to the step **25** of FIG. **1**. For example, as a live TV program is being displayed to the consumer, the consumer is notified that a product may be available. The product may be associated with or embedded as an element within the TV program.

[0041] The method **200** continues with a decision step **210** to determine whether or not the consumer is a known user once the consumer decides to purchase the product. In some embodiments, the consumer may add the product to a virtual or digital "shopping cart." As the consumer performs this transaction, the method **200** will determine if the consumer is a known user (e.g., a consumer who has been authenticated previously) or is a new user. If the answer from the decision step is no—meaning the user has not been previously authenticated—then the method proceeds to a step **215** to authenticate the consumer. The execution of the step **215** may involve substantially similar processes as those discussed above with reference to FIG. **1**, where a consumer is authenticated for the first time.

[0042] On the other hand, if the decision step confirms that the consumer had already been authenticated as a known user for the third party payment provider, the method **200** proceeds to step **220**, in which the product selected by the consumer/user is added to his digital shopping cart. The cart may or may not include other products previously selected and added to the cart by the consumer. In some embodiments, the products in the cart may be displayed as a list, and the consumer may be able to scroll up and down the list to view the details of each product. The consumer may also be given the option to edit the cart, for example changing the quantity of each item in the cart.

[0043] The method **200** then proceeds to a decision step **225** to determine if the consumer is ready to check out. If the answer is no, the method **200** then proceeds to a step **230**, in which the products in the cart are saved for a later checkout, and the consumer may resume watching the TV program. If the decision step **225** determines that the consumer is ready to check out, the method **200** proceeds to a decision step **225** to determine if the consumer has been authenticated. If the answer is no, the method **200** proceeds to a step **240** in which the consumer is authenticated in a procedure similar to that discussed above with reference to FIG. **1**. For example, the consumer may be authenticated using a mobile phone number and a PIN linked to the third party payment provider account, or using the correct combination of a username and a password.

[0044] If the consumer had already been authenticated (or after the consumer finishes the authenticated process in step **240**), the method **200** proceeds to a step **245**, in which the purchasing details are verified with the user. For example, the consumer may be prompted to confirm that the quantity and price of the products in the cart are correct, and/or that his shipping address is correct. After the consumer confirms the purchasing details, the method **200** proceeds to a step **250** to complete the purchase.

[0045] The method **200** discussed above merely illustrates an example process flow and is not intended to be limiting, and additional steps may be performed before, during, or after the steps **205-250** of the method **200**. To facilitate a better understanding of the various aspects of the method **200**, FIGS. **11-15** are provided to graphically illustrate some embodiments of the method **200**.

[0046] Referring to FIG. **11**, an example user interface **300**A is displayed. The user interface **300**A is similar to the user interface **100**A of FIG. **2**. For example, it may be a screenshot of a TV program that the consumer is watching. And similarly, an offer may be communicated to the consumer at various points of the TV program. The offer may be displayed as a text box (or a dialog box) **310**A, which contains a brief description of the product being offered. The text box **310**A gives the consumer an option to add the product to a digital or virtual shopping cart or save it for a later purchase.

[0047] Referring now to FIG. **12**, an example user interface **300**B is displayed to the consumer after the consumer adds the product to the cart. The user interface **300**B shows a text box **310**B, in which the consumer's shopping cart is displayed. The consumer may be able to scroll through the shopping cart to view the details associated with each item in the cart. In some embodiments, the consumer may be able to edit the shopping cart, such as changing the quantity of the items in the cart. The consumer can initiate the checkout process, or alternatively save one or more items in the cart for a later purchase.

[0048] Referring now to FIG. **13**, as the consumer initiates the checkout process, an example user interface **300**C is displayed. The user interface **300**C includes a text box **310**C that prompts the consumer to enter his login information for a third party payment provider. In some embodiments, the consumer can choose to enter a mobile number and a PIN to authenticate himself. In other embodiments, the consumer can choose to enter a username and a password to authenticate himself.

[0049] Referring now to FIG. **14**, the transaction details are displayed to the consumer in a text box **310**D in an example user interface **300**D. The consumer is asked to verify details such as the consumer's shipping address and/or the price/quantity in the cart. Thereafter, in FIG. **15**, an example user interface **300**E includes a text box **310**E that displays a confirmation for the purchasing transaction.

[0050] In all the above examples, the consumer may interact with the TV (for example selecting different options or inputting text) in a variety of ways. In some embodiments, the consumer may use a remote control to perform the transaction. In other embodiments, the consumer may use a gesture-based mechanism to perform the transaction. The gesture-based mechanism may include a sensor device coupled to the TV, where the sensor device can detect gestures or physical movements of the consumer and interpret the corresponding meaning of the gestures. For example, a particular hand waving motion may correspond to an "enter" or "yes" command, while a different hand waving motion may correspond to a "cancel" or "no" command. In yet other embodiments, the TV screen itself may be touch-sensitive, so that the user can interact with the TV set through the touch-sensitive controls.

[0051] Compared to conventional shopping experiences, the purchasing scheme described above offers the consumers greater flexibility and a more interactive shopping experience. For example, the products can be offered to the consumer throughout a TV program that the consumer is watching. If the consumer is interested in a product, he need not leave his couch (or bed) and go make a phone call or log online to contact the merchant. Rather, he can browse through the available products and make a purchase while he is watching the TV program. Of course, the user may have the option to pause the TV program as he is making the purchase. The user may also choose to configure the notification icon of a product availability to be unobtrusive so as to not diminish his TV viewing experience. In addition, the TV program containing offers may or may not be live. The consumer may still interact with the TV the same way even if the TV program is on tape delay or is a digitally pre-recorded program.

[0052] Moreover, while the consumer may initiate and complete the purchase through a TV, he is not required to do

so. In some embodiments, the consumer may just manipulate his third party payment shopping cart (e.g., add or delete items to his cart) by interacting with the TV, and he can finish the checkout process on any computing device later, for example after he has finished watching the TV program. Stated differently, the consumer can initiate a commercial transaction through TV, but he is not necessarily required to finish that commercial transaction through TV.

[0053] Furthermore, since the products being offered are integrated into (or embedded within) the TV program (e.g., an article of clothing worn by the lead actress or a car driven by the actor), the product is discretely and yet efficiently advertised to the consumer. As such, the consumer may be able to better gauge his interest level of the product. For example, the consumer might decide that the dress or jewelry worn by the actress would look very good on his wife, or that the soundtrack from the movie is really enjoyable. Because the consumer can more accurately gauge his interest level in the product, and because he can make a purchase instantly using the TV, the consumer is more likely to follow through with the purchase. Hence, the type of advertising platform discussed above not only offers convenience to the consumers, but also offers advantages to merchants as well.

[0054] The discussions above have used an example of a single user conducting a transaction securely through a TV. However, a single user case is merely one of many example scenarios according to various aspects of the present disclosure, and some additional multi-user scenarios are briefly discussed below.

[0055] In one multi-user scenario, a father logs into his XBOX® account and decides to make a purchase in the XBOX market place. The father chooses a sports game that he would like to play with his son over the weekend. On a payment option screen, he may select to pay with a third party provider, with which he has an account. This may be the first time that the father is using his third party payment provider account in the XBOX marketplace. After the father enters his security credentials to log in the third party payment provider, he is given an option to add an account for other eligible users. The father may then set up an account for his son and enters the required information for his son's account. The father can then fund his son's account after it is set up. Thereafter, the son may make purchases from the XBOX marketplace using the balance in his new account with the third party payment provider. The son may also make purchases through the TV in the interactive manner described above.

[0056] In another multi-user scenario, user A and user B are roommates living together and thus share the same TV (though the TV may be owned by either the user A or the user B). Suppose that while watching a TV program together, the user A sees a product that she would like to purchase but is not sure as to how to conduct the purchasing transaction. The user A asks the user B to make the purchase for her. The user B initiates the transaction using the third party payment provider, and during the login process, the user B is given an option to "switch users." By choosing this option, a mobile phone number for the user A may be entered. If the user A does not have an account with the third party payment provider, the TV will display a notification message indicating that a message has been sent to the user A's phone. The user A may then set up her account with the third party payment provider, which may be done using any suitable computing device. Thereafter, both the users A and B may conduct purchasing transactions interactively through the TV in the manner described above. During the purchasing transaction, the users A and B may switch back and forth between their third party payment provider accounts, depending on who is making the purchase.

[0057] The infrastructure of implementing the interactive shopping through a TV will now be described. Referring to FIG. **16**, a simplified block diagram of a media infrastructure **400** is illustrated. The media infrastructure **400** includes a TV device **410**. The TV device **410** may include a television set, which may be an analog TV set or a digital TV set. The TV device **410** may also include a set-top box (STB).

[0058] The TV device **410** includes software (e.g., STB software) that supports various applications. Examples of STB software include applications based on an Enhanced TV Binary Interchange Format specification (EBIF). EBIF is a multimedia content format defined by a specification developed under the OpenCable project. The primary purpose of the EBIF content format is to represent an optimized collection of widget and byte code specifications that define one or more multimedia pages, similar to web pages, but specialized for use within an enhanced television or interactive television system. An EBIF resource (file), i.e., a sequence of bytes that conforms to the EBIF content format, forms the primary information contained in an ETV Application. An ETV User Agent acquires, decodes, presents (widgets), and executes (actions) contained in an EBIF resource in order to present a multimedia page to an end-user.

[0059] Of course, EBIF is just one of the many ways that can enable the media infrastructure **400**. Other standards or specifications may also be used to enable an interactive TV infrastructure.

[0060] In the embodiment illustrated in FIG. **16**, a TV commerce app **420** is implemented as software on the TV device **410**. The TV commerce app **420** may pertain to one or more specific merchants. In some embodiments, the TV commerce app **420** comes pre-installed on the TV device **410**. In other embodiments, the user of the TV device **410** may install the TV commerce app **420** after the TV device **410** has been purchased and installed. The TV commerce app **420** may be invoked when the TV is displaying a TV program. For example, as a video stream comes through the TV device **410**, there may be one or more trigger points embedded in the video stream. These trigger points may be capable of invoking one or more specific TV commerce apps such as the TV commerce app **420**.

[0061] A third party payment provider component **430** is also implemented as software on the TV device **410**. The third party payment provider component **430** will handle security tasks such as verifying username and passwords or PINs (or the temporary login information) entered by the user. The third party payment provider component **430** can also handle user presentation. The third party payment provider component **430** communicates securely with the third party payment provider. For example, the third party payment provider component **430** may encrypt the communication taking place between itself and external devices. In some embodiments, the third party payment provider and a vendor for the TV device **410** may agree on public keys bundled with a library of the third party payment provider. The third party payment provider component **430** interacts with device specific intelligence and collects device data.

[0062] In some embodiments, the third party payment provider component **430** includes a front end component that resides on a TV set and a back end component that resides on

a set top box. The front end component is configured for direct interaction with the user. For example, the front end component may display the various user interfaces discussed above in association with FIG. **2-9** or **11-15**. The front end component may instruct the TV set to display a text box of 300 pixels by 500 pixels, with the texts being a certain font. The back end component is a lower level component and handles tasks such as encryption algorithms and encryption keys. In some embodiments, the back end component includes a library, for example an EBIF library. The user may interact with the front end component, and the front end component communicates with the back end component, and the back end component communicates with a third party payment provider server discussed later.

[0063] Similar to the TV commerce app **420**, the third party payment provider component **430** may also be pre-installed on the TV device **410** or may be installed on the TV device **410** afterwards. The third party payment provider component **430** interacts with the TV commerce app **420** to facilitate an interactive commercial transaction through TV as discussed above.

[0064] The TV device **410** may also contain a program guide app **440** and firmware **450**. The program guide app **440** is shown herein to illustrate the internal workings of a cable set top box. The firmware **450** is a component that exists in many set top boxes and that controls the communication and other functions of the set top box. The firmware **450** may interact with the third party payment provider component **430** in order to perform certain tasks of the set top box.

[0065] The media infrastructure **400** includes a network **455**. In the embodiment illustrated in FIG. **16**, the network **455** is a cable TV network. The cable TV network **455** includes a plurality of homes **460**. A TV device like the TV device **410** may be implemented inside each of the homes **460**. The homes **460** may be divided into different groups, where the homes in each group share a common node **470**. For example, as illustrated in FIG. **16**, a subset of the homes **460**A may be connected to a node **470**A through common cabling, while a different subset of the homes **460**B may be connected to a node **470**B through common cabling.

[0066] In a hierarchical manner, a group of the nodes **470** are then connected to a data equipment **480**. The data equipment **480** is then connected to a data center **490**. Data communication may take place between the nodes **470** and the data equipment **480**, and between the data equipment **480** and the data center **490**. The data center **490** may generate media content or media programs by itself, or may receive media programs generated by a media provider (not illustrated herein) and relay the media programs to the TV device **410**, which is done through the data equipment **480**, the node **470**A, and the homes **460**A. The nodes **470**, the data equipment **480**, and the data center **490** may contain suitable machines or equipment for carrying or delivering the media content. For example, the nodes **470** may include multiplexers for multiplexing or consolidating signals. The data equipment **480** and the data center **490** may include may include computer servers for processing signals.

[0067] The cable TV network **455** serves as a "bridge" for connecting the TV device **410** to the Internet, since the TV device **410** itself otherwise lacks Internet connection capabilities. It is also understood that other types of networks may also be used to provide Internet access to the TV device **410**. For example, a satellite TV network may be used in place of the cable TV network **455**. The satellite TV network may include appropriate equipment such as satellite dishes, transmitters, receivers, etc. Other alternative networks (such as IPTV networks) may also be implemented, but they are not discussed in detail herein for reasons of simplicity.

[0068] In the embodiment illustrated in FIG. **16**, the data center **490** communicates with a third party payment provider end point **500**. In some embodiments, the third party payment provider end point **500** includes an application programming interface (API) system built with intelligence to understand what device(s) is interacting with it. Based on the device data and type, the third party payment provider end point **500** will present users with the appropriate presentation and security challenge. Also based on device data and type, the third party payment provider end point **500** will allow or deny certain types of transaction. The third party payment provider end point **500** may also apply the corresponding risk models/rules based on the device data and type. The third party payment provider end point **500** may include one or more computer or data servers for processing these various tasks.

[0069] As examples, the third party payment provider end point **500** includes software modules or software engines such as a user authentication software module **510**, a risk assessment software module **520**, and a core/money transaction software module **530**. The user authentication software module **510** can interact with the third party payment provider component **430** to verify the security credentials entered by a user. The risk assessment software module **520** can monitor the purchasing history of a user and detect anomalous purchases. For example, if the user has never bought any merchandise exceeding 100 dollars, then a supposed purchase of 5,000 dollars may be flagged by the risk assessment software module **520**, which can then send an alert to the user and/or appropriate financial institutions. The core/money transaction software module **530** represents a merchant infrastructure in some embodiments. For example, the core/money transaction software module **530** may facilitate the movement and transfer of funds between a merchant and users' accounts.

[0070] It is understood that the third party payment provider end point **500** may include a plurality of additional software or hardware modules that are designed and configured to accomplish specific tasks, but they are not discussed herein for reasons of simplicity.

[0071] As discussed above, a user may stream media programs to his TV device **410** from a media content or media program provider. For example, the media programs may be streamed from the data center **490**, to the data equipment, to the node **470**, to the home **460**, and then to the TV device **410**. In some embodiments, the video stream is an analog video stream. Offer trigger mechanisms are embedded at various points in the analog video stream. For example, the media program may be a commercial for a clothing apparel. The trigger mechanisms communicate with the TV commerce app **420**. In some embodiments, the TV commerce app **420** is customized for a specific type of media program, and the TV commerce app actively "listens" for the right trigger mechanism as the media program is being streamed to the TV device **410**.

[0072] Once a trigger mechanism is identified, the TV commerce app **420** may display a small icon or a larger pop-up window on a viewing screen of the TV device **410**, which indicates to the user watching the TV program that an offer to purchase one or more specific types of cloth apparel is available. When the user is ready to make a purchase based on the displayed offer, the TV commerce app **420** interacts with the

third party payment provider component **430** to facilitate the transaction. For example, the TV commerce app **420** may request the third party payment provider component **430** to display a login screen overlying the TV program screen itself, so that the user can enter his login credentials (i.e., PIN, username/password, etc) for the third party payment provider.

[0073] Data **550**—which may contain the user's login credentials and/or other sensitive information such as the user's credit card or bank account numbers—is then sent to the third party payment provider end point **500** for verification. As discussed above, since the TV device **410** itself lacks Internet connectivity, the data **550** is delivered to the third party provider end point **500** through the network **455**. In the embodiment illustrated in FIG. **16**, the data **550** is routed outside the home **460** (inside which the TV device **410** is located) and travels through the node **470**, the data equipment **480**, and thereafter the data center **490**, before eventually reaching the third party payment provider end point **500**. The node **470**, the data equipment **480**, and the data center **490** may each be referred to as an "intermediate hop," since they are intermediate relay points between the TV device **410** and the third party payment provider end point **500**.

[0074] When the third party payment provider end point **500** receives the data **550** from the TV device **410**, the third party payment provider end point **500** determines whether the credentials entered by the user matches with an existing user's account. If not, the third party payment provider end point **500** may send a message back to the TV device **410** through the network **455** to prompt the user to either re-enter his login information or to register for an account with the third party payment provider end point **500** in case the user has not registered for one yet. If the user credentials are correct, the third party payment provider end point **500** may grant the user's authentication request to log in to the server of the third party payment provider end point **500**. The third party payment provider end point **500** may then send the TV device **410** data **550** that contains an authentication permission. For example, the authentication permission may include an authentication token. The authentication token allows the user operating the TV device **410** to gain access to the third party payment provider end point **500**, but may impose limitations on such access. For example, the authentication token may restrict such access to a specific time period or other session related elements, or even for a specific device type.

[0075] After the user has been authenticated, the third party payment provider component **430** may also display a user authorization screen to collect the user's authorization for the purchasing transaction. The relevant request is sent to the third party payment provider end point **500**, along with the authentication token. The third party payment provider end point **500** may respond back with an authorization token. The third party payment provider component (specifically, the back end component) may then make a request (along with the authorization token) to the third party payment provider end point **500** to execute the payment

[0076] Thus, it can be seen that the communication between the TV device **410** and the third party payment provider end point **500** is a two-way communication, as each entity may send and receive data **550** from the other. As discussed above, such data is delivered through the intermediate hops of the network **455**. Due to these intermediate hops, high levels of security measures will be taken to ensure that the data **550** is not compromised while it is in transit from the TV device **410** to the third party payment provider end point **500**, or vice versa. In various embodiments, these security measures include channel encryption and/or message encryption. Also, in certain embodiments, the communication between the data center **490** and the third party payment provider end point **500** is based on client mutual authentication, for example through a Secure Sockets Layer (SSL) handshake, so as to authenticate the data center. Also because of the intermediate hops, the third party payment provider end point **500** will possess intelligence to know the specific route taken by the data **550** to reach the third party payment provider end point **500**.

[0077] Based on the discussions above, it can be seen that one aspect of the media infrastructure **400** involves implementing a secure digital technology component on a TV device (which may includes a set top box), and enabling the digital technology component to securely communicate with a server on the Internet. The communication takes place by propagating data through a network with intermediate hops without any of the intermediate hops "looking side" or inspecting the data. Stated differently, the intermediate hops of the network merely forwards the data to its next destination. In various embodiments, the secure digital technology component is the third party payment provider component **430** (which may contain Internet-related security mechanisms), whereas the intermediate hops of the network include the nodes **470**, the data equipment **480**, and the data center **490** when the network is a cable TV network.

[0078] FIG. **17** illustrates a simplified block diagram of a media infrastructure **600** that can be used to implement the interactive shopping throngh a TV as discussed above. For reasons of consistency and clarity, similar components of the media infrastructure **400** and the media infrastructure **600** are labeled the same in FIGS. **16** and **17**.

[0079] Referring to FIG. **17**, the media infrastructure **600** includes a TV device **410**, which contains a TV commerce app **420**, a third party payment provider component **430**, a program gnide **440**, and firmware **450**. The media infrastructure **600** also includes homes **460**, nodes **470**, the data equipment **480**, the data center **490**, and the third party payment provider end point **500**. Similar to the media infrastructure **400** of FIG. **16**, the nodes **470**, the data equipment **480**, and the data center **490** are parts of a layered analog media network. Unlike the media infrastructure **400**, however, the TV device **410** is Internet-capable. The TV device **410** directly communicates with the third party payment provider end point **500**, without any terminations on any of the intermediate hops (e.g., the nodes **470**, the data equipment **480**, the data center **490**). In some embodiments, the TV device **410** communicates with the third party payment provider end point **500** in a secure manner such as throngh a SSL handshake. And since there are no terminations in the intermediate hops, the security measures herein may not be as strict as in the media infrastructure **400**. For example, channel encryption alone may be sufficient for the communication between the TV device **410** and the third party payment provider endpoint **500**.

[0080] Thus, according to various aspects of the present disclosure, a user (or a plurality of users) is allowed to make an instant purchase from a TV device without requiring an account set-up or the use of a personal computer (or other computing device). In certain embodiments, a third party payment provider digital component based on an STB ecosystem (e.g., EBIF Application) is embedded into STB (based

EWS-004193

on EBIF runtime). Changes are made to the EBIF specifications to enable security and to embed the interactive functionality into runtime. The interactive functionality enables an end user to directly make payments through a TV. These aspects of the present disclosure may involve one or more of the following elements:

[0081] User/Device registration to associate a user with a device.

[0082] Site key management to associate a user with a third party payment provider, which enables a user to enter user credentials in a secure way.

[0083] User authentication/authorization for a user to authenticate with their credentials (e.g., mobile number/PIN, username/password) and to authorize the payment.

[0084] Application authorization to authorize applications using third party payment provider applications for basic or advanced level functionality.

[0085] Third party payment provider controlled user interface and interaction to dynamically determine the authentication schemes.

[0086] Ability to execute in-line payments (simple, split payments), without being re-directed to the third party payment provider.

[0087] These elements offer enhanced security (e.g., site key and message encryption) and allow full control of the user interaction, including multiple users on a single device.

[0088] According to various aspects of the present disclosure, an example use case scenario for conducting a simple commercial transaction through a TV device is described below with the following steps:

[0089] 1. A user clicks a "Pay" button shown in an STB application (e.g., an STB EBIF application).

[0090] 2. The STB EBIF application sends the "Pay" request (Pay $10 to "ABC"), to the third party payment provider (e.g., PAYPAL) EBIF Library.

[0091] 3. The third party payment provider EBIF library communicates with the EBIF runtime to authenticate, so as to use/enable message and channel encryption. (Note: the third party payment provider and STB vendor may have already agreed upon public keys to be bundled with the library, so as to enable encryption).

[0092] 4. The third party payment provider EBIF library communicates with the third party payment provider service to register the device.

[0093] 5. The third party payment provider responds with a device token and the meta-data of painting the authentication/authorization screens.

[0094] 6. The third party payment provider EBIF expects the end user to register with the third party payment provider site key to personalize, so as to make sure that the end user is comfortable to enter their credentials.

[0095] 7. The third party payment provider EBIF library displays a user authentication screen, to collect the login credentials to authenticate the user. With the authentication credentials, it also collects details of the environment for risk and fraud analysis.

[0096] 8. The user enters the credentials, and an authentication request is sent to the third party payment provider along with the device token and additional data.

[0097] 9. The third party payment provider responds with an authentication token (AuthN).

[0098] 10. The third party payment provider EBIF library displays a user authorization screen, to collect the user authorization for the activity (e.g., pay). The relevant request with the AuthN Token is sent to the third party payment provider, which responds back with an Authorization Token (AuthZ).

[0099] 11. The third party payment provider EBIF library makes a request to the third party payment provider service (e.g., adaptive payments), to execute the pay call with the authorization token (e.g., AuthZ).

[0100] 12. The third party payment provider EBIF library returns the payment status to the application, with is displayed on the TV screen.

[0101] In the manner described above, the third party payment provider is able to provide secure on-device payments within a TV device ecosystem (e.g., set top boxes). Thus, the users will be able to purchase products and services directly from their TV and TV devices without any further interaction with their computing devices (e.g., PC, laptop, or mobile phones).

[0102] According to various aspects of the present disclosure, a single digital wallet can also be used to conduct electronic transactions across with different merchants and across different platforms. Such digital wallet may be referred to as a "white label" wallet. Traditionally, when a user or consumer sees a product that he wishes to buy, he can go to that merchant who is offering the product and set up an account with the merchant. His subsequent transactions with that merchant may be done through this account with the merchant. However, if the user wishes to buy a product from a different merchant, the account he set up with the first merchant is useless, and he would have to set up a different account with the second merchant to conduct transactions with the second merchant.

[0103] Here, the user can set up an account with the third party payment provider. Once that account is set up, he may use that account to conduct different transactions with different merchants across different platforms. For example, say the user is watching a TV program and sees a first product (e.g., clothing worn by the actor) that he wishes to buy from a first merchant. He can then log in to the third party payment provider in the manner described above to complete the purchase. If the user does not have an account with the third party payment provider, he only needs to set it up once. Afterwards, his login information can be remembered by the TV device (for example, by the set top box) for future transactions.

[0104] Thereafter, while watching the same TV program or even a different TV program, if the user sees another product (e.g., a motorcycle that the actor is riding) that he wishes to buy from a different merchant, the same login information for the user can be used to access his account with the third party payment provider again. In some embodiments, the user need not re-enter his login information if it is already remembered. The third party payment provider may complete the user's purchase with the second merchant seamlessly without requiring the user to supply additional data, thereby simplifying the transaction for the user.

[0105] In some cases, the user may also wish to supply other types of payment information other than his account access information with the third party payment provider. For example, the user may elect to enter his credit card number or a band account number through the TV device. However, the third party payment provider may still be the back engine that operates "behind the scenes" to facilitate the transaction. For example, if the user has entered a credit card number, from the user's perspective, it is the credit card company who is handling the transaction with a given merchant. In actuality, that

merchant may delegate the responsibilities of handling the transaction to the third party payment provider. The third party payment provider may then forward the credit card information supplied by the user to a suitable credit card network. Similarly, had the user provided a bank account number (or an account number with another financial institution), the third party payment provider may forward the bank account number to the appropriate bank or financial institution. This is done without requiring the user to understand what is going on behind the scenes. In other words, the user may be interacting with the third party payment provider without realizing that he is doing so. In this manner, the third party payment provider serves as a "one-size-fits-all" payment platform.

[0106] FIG. **18** is a flowchart of a method **700** for performing a transaction according to various aspects of the present disclosure. The method **700** includes a step **710**, in which a media program is displayed on a television set. The media program may be streamed from a media content provider. The method **700** includes a step **720**, in which a purchasing availability of an item associated with the media program is indicated. The indication occurs while the media program is being displayed. In some embodiments, the indication includes showing an interactive graphical component on the television set. The item could include physical merchandise or digital merchandise. The item is embedded in the media program. In some embodiments, the item includes a product that appears in a scene of the media program while the media program is being displayed. The method **700** includes a step **730**, in which authentication information of a prospective purchaser of the item is received. The authentication information may be received through a television remote control. The method **700** includes a step **740**, in which a purchase of the item is completed in response to the authentication information. The receiving authentication information and the completing the purchase are performed without exiting the media program.

[0107] FIG. **19** is a flowchart of a method **800** for performing a transaction according to various aspects of the present disclosure. The method **800** includes a step **810**, in which a user authentication request is received from a television device. The user authentication request contains user login credentials. The method **800** includes a step **820**, in which the user authentication request is granted in response to the user login credentials. The method **800** includes a step **830**, in which an authentication permission is sent to the television device. The steps **810**, **820**, and **830** are all performed such that the user login credentials and the authentication permission are sent through one or more intermediate hops without being inspected by any of the intermediate hops. In some embodiments, the steps **810**, **820**, and **830** are all performed by a payment provider server, and the user login credentials are login credentials for accessing a user account with the payment provider server. The intermediate hops may be components of a network for providing Internet access to the television device.

[0108] FIG. **20** is a flowchart of a method **900** for performing a transaction according to various aspects of the present disclosure. The method **900** includes a step **910**, in which a request to access a payment provider server is received from a user. The request is received through a television device. The request is also electronically processed by a payment provider software application that resides on the television device. The television device may include a television display and a set top box. The method **900** includes a step **920**, in which user data for authenticating the user with the payment provider server is collected in response to the receiving the request. The user data contains login credentials of the user for accessing an account of the user with the payment provider. The method **900** includes a step **920**, in which the user data is sent to the payment provider server. The step **930** is performed so that the user data is sent through one or more intermediate hops without being inspected by any of the intermediate hops before the user data reaches the payment provider server. The user data is encrypted before it is sent. The intermediate hops are components of a network for providing Internet access to the television device.

[0109] FIG. **21** is a flowchart of a method **1000** for performing a transaction according to various aspects of the present disclosure. The method **1000** includes a step **1010**, in which a first request to conduct a first transaction with a first merchant is received through a television device. The first request contains a first payment information provided by a user. The method **1000** includes a step **1020**, in which the first request is facilitated based on the first payment information. The method **1000** includes a step **1030**, in which the second request to conduct a second transaction with a second merchant is received through the television device. The second merchant is different from the first merchant. The second request contains a second payment information. The method **1000** includes a step **1040**, in which the second request is facilitated based on the second payment information. The facilitating the first request and the facilitating the second request are both performed by a third party payment provider.

[0110] FIG. **22** is a block diagram of a computer system **1300** suitable for implementing various methods and devices described herein, for example, the various method steps of the methods **700**, **800**, **900**, or **1000**. In various implementations, the devices capable of performing the steps may comprise a network communications device (e.g., mobile cellular phone, laptop, personal computer, tablet, etc.), a network computing device (e.g., a network server, a computer processor, an electronic communications interface, etc), or another suitable device. Accordingly, it should be appreciated that the devices capable of implementing the methods **700**, **800**, **900**, and **1000** may be implemented as the computer system **1300** in a manner as follows.

[0111] In accordance with various embodiments of the present disclosure, the computer system **1300**, such as a network server or a mobile communications device, includes a bus component **1302** or other communication mechanisms for communicating information, which interconnects subsystems and components, such as processing component **1304** (e.g., processor, micro-controller, digital signal processor (DSP), etc.), system memory component **1306** (e.g., RAM), static storage component **1308** (e.g., ROM), disk drive component **1310** (e.g., magnetic or optical), network interface component **1312** (e.g., modem or Ethernet card), display component **1314** (e.g., cathode ray tube (CRT) or liquid crystal display (LCD)), input component **1316** (e.g., keyboard), cursor control component **1318** (e.g., mouse or trackball), and image capture component **1320** (e.g., analog or digital camera). In one implementation, disk drive component **1310** may comprise a database having one or more disk drive components.

[0112] In accordance with embodiments of the present disclosure, computer system **1300** performs specific operations by processor **1304** executing one or more sequences of one or

more instructions contained in system memory component **1306**. Such instructions may be read into system memory component **1306** from another computer readable medium, such as static storage component **1308** or disk drive component **1310**. In other embodiments, hard-wired circuitry may be used in place of (or in combination with) software instructions to implement the present disclosure.

[0113] Logic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to processor **1304** for execution. Such a medium may take many forms, including but not limited to, non-volatile media and volatile media. In one embodiment, the computer readable medium is non-transitory. In various implementations, non-volatile media includes optical or magnetic disks, such as disk drive component **1310**, and volatile media includes dynamic memory, such as system memory component **1306**. In one aspect, data and information related to execution instructions may be transmitted to computer system **1300** via a transmission media, such as in the form of acoustic or light waves, including those generated during radio wave and infrared data communications. In various implementations, transmission media may include coaxial cables, copper wire, and fiber optics, including wires that comprise bus **1302**.

[0114] Some common forms of computer readable media includes, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, PROM, EPROM, FLASH-EPROM, any other memory chip or cartridge, carrier wave, or any other medium from which a computer is adapted to read.

[0115] In various embodiments of the present disclosure, execution of instruction sequences to practice the present disclosure may be performed by computer system **1300**. In various other embodiments of the present disclosure, a plurality of computer systems **1300** coupled by communication link **1330** (e.g., a communications network, such as a LAN, WLAN, PTSN, and/or various other wired or wireless networks, including telecommunications, mobile, and cellular phone networks) may perform instruction sequences to practice the present disclosure in coordination with one another.

[0116] Computer system **1300** may transmit and receive messages, data, information and instructions, including one or more programs (i.e., application code) through communication link **1330** and communication interface **1312**. Received program code may be executed by processor **1304** as received and/or stored in disk drive component **1310** or some other non-volatile storage component for execution.

[0117] Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa.

[0118] Software, in accordance with the present disclosure, such as computer program code and/or data, may be stored on one or more computer readable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

[0119] It should be appreciated that like reference numerals are used to identify like elements illustrated in one or more of the figures, wherein these labeled figures are for purposes of illustrating embodiments of the present disclosure and not for purposes of limiting the same.

[0120] It is also understood that although a television device has been used to illustrate the various concepts of the present disclosure, other types of media display devices may also be used in different embodiments. For example, a computer tablet or a smart phone may also be used to perform the various functions of the television set discussed above (e.g., displaying a media program, etc).

[0121] One of the broader forms of the present disclosure involves a method of conducting a transaction. The method includes: displaying a media program on a television set; indicating, while the media program is being displayed, an item associated with the media program is available for purchase; receiving authentication information of a prospective purchaser of the item; and completing a purchase of the item in response to the authentication information.

[0122] In some embodiments, the displaying the media program comprises streaming the media program from a media content provider to the television set.

[0123] In some embodiments, the indicating comprises showing an interactive graphical component on the television set.

[0124] In some embodiments, the item comprises one of: physical merchandise and digital merchandise.

[0125] In some embodiments, the item is embedded in the media program.

[0126] In some embodiments, the item comprises a product that appears in a scene of the media program while the media program is being displayed.

[0127] In some embodiments, the receiving the authentication information and the completing the purchase are each performed without exiting the media program.

[0128] In some embodiments, the receiving the authentication information is performed through a television remote control.

[0129] Another one of the broader forms of the present disclosure involves an apparatus comprising a non-transitory, tangible machine-readable storage medium storing a computer program, wherein the computer program contains machine-readable instructions that when executed electronically by processors, perform: displaying a media program on a television set; indicating, while the media program is being displayed, an item associated with the media program is available for purchase; receiving authentication information of a prospective purchaser of the item; and completing a purchase of the item in response to the authentication information.

[0130] In some embodiments, the instructions for displaying the media program comprise instructions for streaming the media program from a media content provider to the television set.

[0131] In some embodiments, the instructions for indicating the item is available for purchase comprise instructions for showing an interactive graphical component on the television set.

[0132] In some embodiments, the item comprises one of: physical merchandise and digital merchandise.

[0133] In some embodiments, the item is embedded in the media program.

[0134] In some embodiments, the item comprises a product that appears in a scene of the media program while the media program is being displayed.

[0135] In some embodiments, the instructions for receiving the authentication information and the instructions for completing the purchase are each executed without forcing the media program to exit.

[0136] In some embodiments, the instructions for receiving the authentication information comprise instructions for receiving the authentication information through a television remote control.

[0137] Yet another one of the broader forms of the present disclosure involves an apparatus. The apparatus includes: a television set operable to: display a media program; and indicate, while the media program is being displayed, an item associated with the media program is available for purchase; and a set top box coupled to the television set, wherein the set top box is operable to: receive authentication information of a prospective purchaser of the item; and complete a purchase of the item in response to the authentication information.

[0138] In some embodiments, the television set is operable to show an interactive graphical component to the prospective purchase to indicate the item is available for purchase.

[0139] In some embodiments, the item comprises one of: physical merchandise and digital merchandise.

[0140] In some embodiments, the item is embedded in the media program.

[0141] In some embodiments, the set top box is operable to receive the authentication information and to complete the purchase without causing the television set to exit the media program.

[0142] In some embodiments, the set top box is operable to stream the media program from a media content provider to the television set.

[0143] Another one of the broader forms of the present disclosure involves a method of conducting an electronic transaction. The method includes: receiving, from a television device, a user authentication request, wherein the user authentication request contains user login credentials; granting the user authentication request in response to the user login credentials; and thereafter sending an authentication permission to the television device; wherein the receiving the user authentication request and the sending the authentication permission are each performed such that the user login credentials and the authentication permission are sent through one or more intermediate hops without being inspected by any of the intermediate hops.

[0144] In some embodiments, the receiving, the granting, and the sending are performed by a payment provider server; and the user login credentials are login credentials for accessing a user account with the payment provider server.

[0145] In some embodiments, the granting of the user authentication request comprises generating an authentication token; and the sending the authentication permission comprises sending the authentication token to the television device.

[0146] In some embodiments, the user authentication request is encrypted when it is received, and the method further includes: decrypting the user authentication request after it is received; and encrypting the authentication permission before it is sent.

[0147] In some embodiments, the intermediate hops are components of a network for providing Internet access to the television device.

[0148] In some embodiments, the network comprises one of: a cable television network and a satellite television network.

[0149] In some embodiments, the sending the authentication permission is performed such that the authentication permission is sent to a payment provider software application that resides on the television device.

[0150] In some embodiments, the television device comprises a television display and a set top box.

[0151] Another one of the broader forms of the present disclosure involves an apparatus comprising a non-transitory, tangible machine-readable storage medium storing a computer program, wherein the computer program contains machine-readable instructions that when executed electronically by processors, perform: receiving, from a television device, a user authentication request, wherein the user authentication request contains user login credentials; granting the user authentication request in response to the user login credentials; and thereafter sending an authentication permission to the television device; wherein the receiving the user authentication request and the sending the authentication permission are each performed such that the user login credentials and the authentication permission are sent through one or more intermediate hops without being inspected by any of the intermediate hops.

[0152] In some embodiments, the instructions for the receiving, the granting, and the sending are executed by a payment provider server; and the user login credentials are login credentials for accessing a user account with the payment provider server.

[0153] In some embodiments, the instructions for granting the user authentication request comprise instructions for generating an authentication token; and the instructions for sending the authentication permission comprise instructions for sending the authentication token to the television device.

[0154] In some embodiments, the user authentication request is encrypted when it is received, and wherein the instructions further comprise: instructions for decrypting the user authentication request after it is received; and instructions for encrypting the authentication permission before it is sent.

[0155] In some embodiments, the intermediate hops are components of a network for providing Internet access to the television device.

[0156] In some embodiments, the network comprises one of: a cable television network and a satellite television network.

[0157] In some embodiments, the instructions for sending the authentication permission are executed such that the authentication permission is sent to a payment provider software application that resides on the television device.

[0158] In some embodiments, the television device comprises a television display and a set top box.

[0159] Yet another one of the broader forms of the present disclosure involves a method of conducting an electronic transaction. The method includes: receiving a request to access a payment provider server from a user, wherein the request is received through a television device; collecting, in response to the receiving the request, user data for authenticating the user with the payment provider server; and sending the user data to the payment provider server, wherein the sending the user data is performed so that the user data is sent through one or more intermediate hops without being inspected by any of the intermediate hops before the user data reaches the payment provider server.

[0160] In some embodiments, the user data comprises login credentials of the user for accessing an account of the user with the payment provider.

[0161] In some embodiments, the receiving of the request is performed such that the request is electronically processed by a payment provider software application that resides on the television device.

[0162] In some embodiments, the sending of the user data comprises encrypting the user data.

[0163] In some embodiments, the method further includes: receiving user authentication information from the payment provider server after the sending the user data.

[0164] In some embodiments, the television device comprises a television display and a set top box.

[0165] In some embodiments, the intermediate hops are components of a network for providing Internet access to the television device.

[0166] Another one of the broader forms of the present disclosure involves a method of conducting a transaction. The method includes: receiving, through a television device, a first request to conduct a first transaction with a first merchant, wherein the first request contains a first payment information provided by a user; facilitating the first request based on the first payment information; receiving, through the television device, a second request to conduct a second transaction with a second merchant different from the first merchant, wherein the second request contains a second payment information; and facilitating the second request based on the second payment information; wherein the facilitating the first request and the facilitating the second request are both performed by a third party payment provider.

[0167] In some embodiments, the first payment information and the second payment information each include at least one of: credentials for accessing an account of the user with the third party payment provider, and a credit card number of the user, and a bank account of the user.

[0168] In some embodiments, the facilitating of the first request and the facilitating of the second request include granting the first request and granting the second request, if the first payment information and the second payment information include the credentials for accessing the account of the user with the third party payment provider.

[0169] In some embodiments, the facilitating of the first request and the facilitating of the second request include forwarding the first request and forwarding the second request to a respective financial institution, if the first payment information and the second payment information include the credit card number or the bank account of the user.

[0170] In some embodiments, the first payment information and the second payment information are the same.

[0171] In some embodiments, the method further includes: remembering at least one of the first payment information and the second payment information for future transactions of the user.

[0172] In some embodiments, the first transaction is a purchase of a first product offered by the first merchant in response to the first product being displayed on the television device; and the second transaction is a purchase of a second product offered by the second merchant in response to the second product being displayed on the television device.

[0173] In some embodiments, the first product and the second product are each integrated in one or more television programs being displayed on the television device.

[0174] Yet another one of the broader forms of the present disclosure involves an apparatus comprising a non-transitory, tangible machine-readable storage medium storing a computer program, wherein the computer program contains machine-readable instructions that when executed electronically by processors, perform: receiving, through a television device, a first request to conduct a first transaction with a first merchant, wherein the first request contains a first payment information provided by a user; facilitating the first request based on the first payment information; receiving, through the television device, a second request to conduct a second transaction with a second merchant different from the first merchant, wherein the second request contains a second payment information; and facilitating the second request based on the second payment information; wherein the facilitating the first request and the facilitating the second request are both performed by a third party payment provider.

[0175] In some embodiments, the first payment information and the second payment information each include at least one of: credentials for accessing an account of the user with the third party payment provider, and a credit card number of the user, and a bank account of the user.

[0176] In some embodiments, the instructions for facilitating the first request and the instructions for facilitating the second request include instructions for granting the first request and instructions for granting the second request, if the first payment information and the second payment information include the credentials for accessing the account of the user with the third party payment provider.

[0177] In some embodiments, the instructions for facilitating the first request and the instructions for facilitating the second request include instructions for forwarding the first request and instructions for forwarding the second request to a respective financial institution, if the first payment information and the second payment information include the credit card number or the bank account of the user.

[0178] In some embodiments, the first payment information and the second payment information are the same.

[0179] In some embodiments, the computer program further contains: instructions for remembering at least one of the first payment information and the second payment information for future transactions of the user.

[0180] In some embodiments, the first transaction is a purchase of a first product offered by the first merchant in response to the first product being displayed on the television device; and the second transaction is a purchase of a second product offered by the second merchant in response to the second product being displayed on the television device.

[0181] In some embodiments, the first product and the second product are each integrated in one or more television programs being displayed on the television device.

[0182] Yet another one of the broader forms of the present disclosure involves a method of conducting a transaction. The method includes: receiving, from a user, a first purchasing request to buy a first product from a first merchant, wherein the first purchasing request is entered through a television device and contains login credentials for accessing an account of the user with a payment provider; authorizing the first purchasing request based on the login credentials; receiving, from the user, a second purchasing request to buy a second product from a second merchant different from the first merchant, wherein the second purchasing request is entered through the television device and contains the login credentials for accessing the account of the user; and authorizing the second purchasing request based on the login credentials.

[0183] In some embodiments, the authorizing the first purchasing request and the authorizing the second purchasing request are both performed by a server of the payment provider.

[0184] In some embodiments, the login credentials are remembered for the second purchasing request.

[0185] In some embodiments, the first purchasing request is received in response to the first product being demonstrated in a television program playing on the television device; and the second purchasing request is received in response to the second product being demonstrated in the television program playing on the television device.

[0186] The foregoing disclosure is not intended to limit the present disclosure to the precise forms or particular fields of use disclosed. As such, it is contemplated that various alternate embodiments and/or modifications to the present disclosure, whether explicitly described or implied herein, are possible in light of the disclosure. Having thus described embodiments of the present disclosure, persons of ordinary skill in the art will recognize that changes may be made in form and detail without departing from the scope of the present disclosure. Thus, the present disclosure is limited only by the claims.

What is claimed is:

1. A method of conducting a transaction, comprising:

receiving, through a media display device, a first request to conduct a first transaction with a first merchant, wherein the first request contains a first payment information provided by a user;

facilitating the first request based on the first payment information;

receiving, through the media display device, a second request to conduct a second transaction with a second merchant different from the first merchant, wherein the second request contains a second payment information; and

facilitating the second request based on the second payment information;

wherein the facilitating the first request and the facilitating the second request are both performed by a third party payment provider.

2. The method of claim **1**, wherein the first payment information and the second payment information each include at least one of: credentials for accessing an account of the user with the third party payment provider, and a credit card number of the user, and a bank account of the user.

3. The method of claim **2**, wherein the facilitating the first request and the facilitating the second request include granting the first request and granting the second request, if the first payment information and the second payment information include the credentials for accessing the account of the user with the third party payment provider.

4. The method of claim **2**, wherein the facilitating the first request and the facilitating the second request include forwarding the first request and forwarding the second request to a respective financial institution, if the first payment information and the second payment information include the credit card number or the bank account of the user.

5. The method of claim **1**, wherein the first payment information and the second payment information are the same.

6. The method of claim **1**, further comprising: remembering at least one of the first payment information and the second payment information for future transactions of the user.

7. The method of claim **1**, wherein:

the first transaction is a purchase of a first product offered by the first merchant in response to the first product being displayed on the media display device; and

the second transaction is a purchase of a second product offered by the second merchant in response to the second product being displayed on the media display device.

8. The method of claim **7**, wherein the first product and the second product are each integrated in one or more media programs being displayed on the media display device.

9. An apparatus comprising a non-transitory, tangible machine-readable storage medium storing a computer program, wherein the computer program contains machine-readable instructions that when executed electronically by processors, perform:

receiving, through a media display device, a first request to conduct a first transaction with a first merchant, wherein the first request contains a first payment information provided by a user;

facilitating the first request based on the first payment information;

receiving, through the media display device, a second request to conduct a second transaction with a second merchant different from the first merchant, wherein the second request contains a second payment information; and

facilitating the second request based on the second payment information;

wherein the facilitating the first request and the facilitating the second request are both performed by a third party payment provider.

10. The apparatus of claim **9**, wherein the first payment information and the second payment information each include at least one of: credentials for accessing an account of the user with the third party payment provider, and a credit card number of the user, and a bank account of the user.

11. The apparatus of claim **10**, wherein the instructions for facilitating the first request and the instructions for facilitating the second request include instructions for granting the first request and instructions for granting the second request, if the first payment information and the second payment information include the credentials for accessing the account of the user with the third party payment provider.

12. The apparatus of claim **10**, wherein the instructions for facilitating the first request and the instructions for facilitating the second request include instructions for forwarding the first request and instructions for forwarding the second request to a respective financial institution, if the first payment information and the second payment information include the credit card number or the bank account of the user.

13. The apparatus of claim **9**, wherein the first payment information and the second payment information are the same.

14. The apparatus of claim **9**, further comprising: instructions for remembering at least one of the first payment information and the second payment information for future transactions of the user.

15. The apparatus of claim **9**, wherein:

the first transaction is a purchase of a first product offered by the first merchant in response to the first product being displayed on the media display device; and

the second transaction is a purchase of a second product offered by the second merchant in response to the second product being displayed on the media display device.

16. The apparatus of claim **15**, wherein the first product and the second product are each integrated in one or more media programs being displayed on the media display device.

17. A method of conducting a transaction, comprising:

receiving, from a user, a first purchasing request to buy a first product from a first merchant, wherein the first purchasing request is entered through a media display device and contains login credentials for accessing an account of the user with a payment provider;

authorizing the first purchasing request based on the login credentials;

receiving, from the user, a second purchasing request to buy a second product from a second merchant different from the first merchant, wherein the second purchasing request is entered through the media display device and contains the login credentials for accessing the account of the user; and

authorizing the second purchasing request based on the login credentials.

18. The method of claim **17**, wherein the authorizing the first purchasing request and the authorizing the second purchasing request are both performed by a server of the payment provider.

19. The method of claim **17**, wherein the login credentials are remembered for the second purchasing request.

20. The method of claim **17**, wherein:

the first purchasing request is received in response to the first product being demonstrated in a media program playing on the media display device; and

the second purchasing request is received in response to the second product being demonstrated in the media program playing on the media display device.

21. The method of claim **17**, wherein the media display device includes a television set.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Dryer et al.

(10) **Pub. No.: US 2012/0290376 A1**

(43) **Pub. Date: Nov. 15, 2012**

(54) **PROCESSING ELECTRONIC PAYMENT INVOLVING MOBILE COMMUNICATION DEVICE**

(75) Inventors: **Trevor D. Dryer**, San Francisco, CA (US); **Eran Arbel**, Los Altos, CA (US); **Alexander S. Ran**, Palo Alto, CA (US); **Ajay Tripathi**, San Ramon, CA (US); **Douglas Lethin**, Rading, MA (US); **Bennett R. Blank**, San Diego, CA (US); **Eugene Krivopaltsev**, San Jose, CA (US)

(73) Assignee: **INTUIT INC.**, Mountain View, CA (US)

(21) Appl. No.: **13/103,957**

(22) Filed: **May 9, 2011**

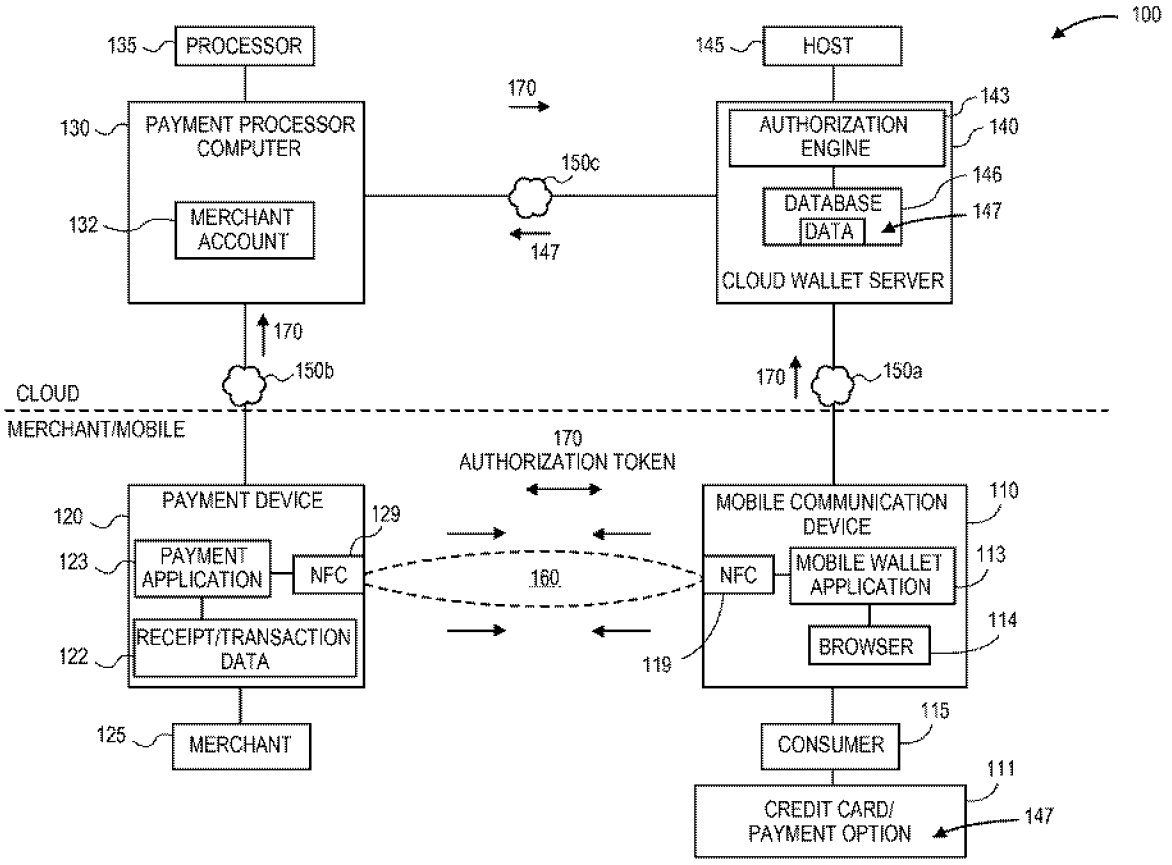
Publication Classification

(51) **Int. Cl.**
G06Q 30/00 (2006.01)

(52) **U.S. Cl.** **705/14.23**; 705/26.41

(57) **ABSTRACT**

Mobile payments and processing data related to electronic transactions. A near field communication connection is established between a mobile communication device of a consumer that serves as a mobile wallet and an electronic payment device of a merchant. Authorization data is shared between the mobile communication device and the electronic payment device without providing electronic payment instrument (e.g. credit card) data to the merchant. Authorization data is transmitted from the mobile communication device to a cloud computer or resource that serves as a cloud wallet and hosts respective data of respective electronic payment instruments of respective consumers, and from the electronic payment device a payment processor computer. The payment processor computer presents the authorization data to the cloud wallet, and in response, the cloud wallet transmits the credit card data to the payment processor computer, which processes the transaction.



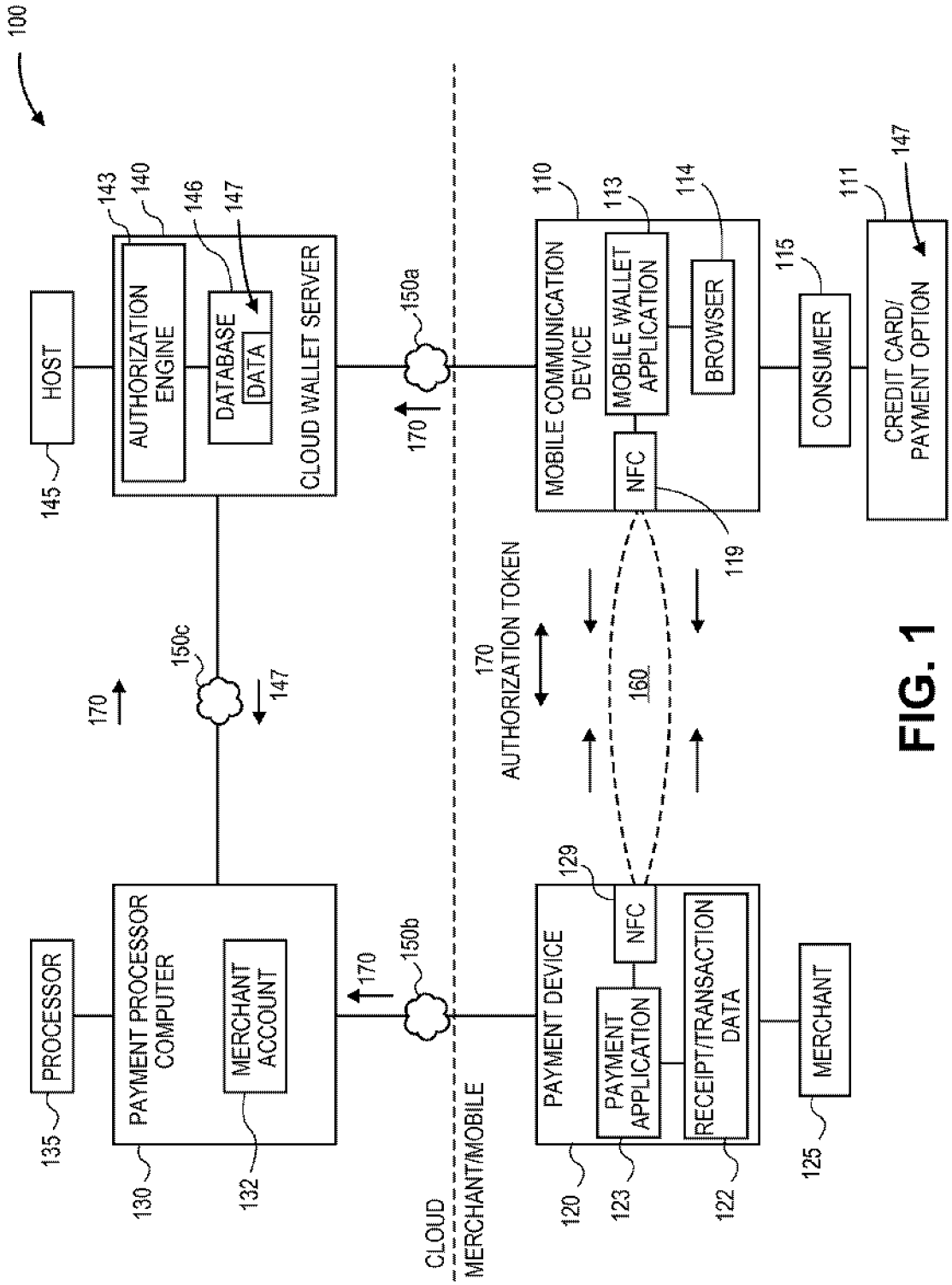

100
HOST
145
AUTHORIZATION ENGINE
143
140
DATABASE
DATA
146
147
CLOUD WALLET SERVER
150a
170
MOBILE COMMUNICATION DEVICE
110
MOBILE WALLET APPLICATION
113
NFC
BROWSER
114
119
CONSUMER
115
CREDIT CARD/ PAYMENT OPTION
111
147
170
150c
147
170
AUTHORIZATION TOKEN
160
PROCESSOR
135
PAYMENT PROCESSOR COMPUTER
MERCHANT ACCOUNT
130
132
170
150b
CLOUD
MERCHANT/MOBILE
PAYMENT DEVICE
129
NFC
PAYMENT APPLICATION
RECEIPT/TRANSACTION DATA
120
123
122
MERCHANT
125

FIG. 1

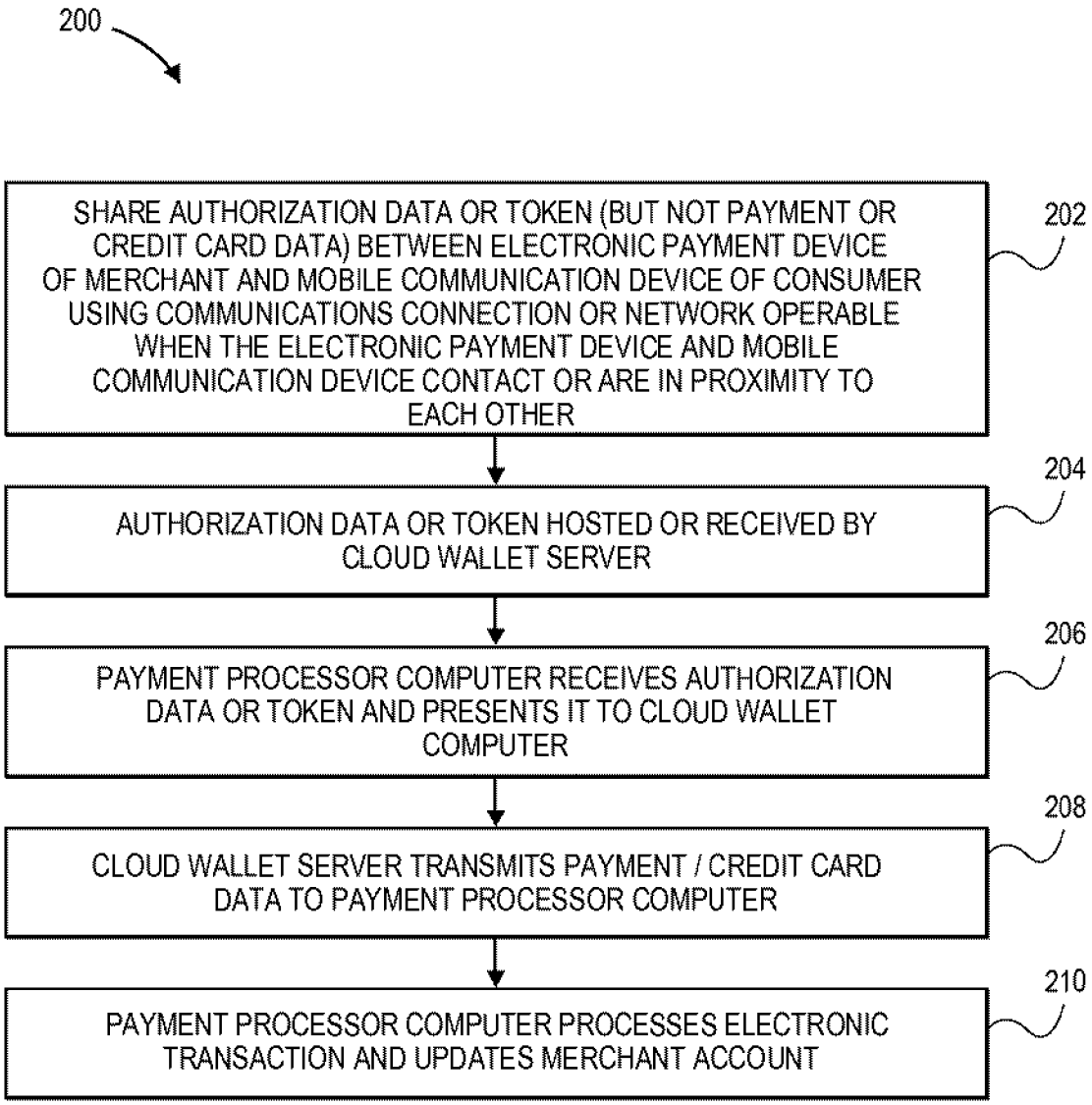

200
SHARE AUTHORIZATION DATA OR TOKEN (BUT NOT PAYMENT OR CREDIT CARD DATA) BETWEEN ELECTRONIC PAYMENT DEVICE OF MERCHANT AND MOBILE COMMUNICATION DEVICE OF CONSUMER USING COMMUNICATIONS CONNECTION OR NETWORK OPERABLE WHEN THE ELECTRONIC PAYMENT DEVICE AND MOBILE COMMUNICATION DEVICE CONTACT OR ARE IN PROXIMITY TO EACH OTHER
202
AUTHORIZATION DATA OR TOKEN HOSTED OR RECEIVED BY CLOUD WALLET SERVER
204
PAYMENT PROCESSOR COMPUTER RECEIVES AUTHORIZATION DATA OR TOKEN AND PRESENTS IT TO CLOUD WALLET COMPUTER
206
CLOUD WALLET SERVER TRANSMITS PAYMENT / CREDIT CARD DATA TO PAYMENT PROCESSOR COMPUTER
208
PAYMENT PROCESSOR COMPUTER PROCESSES ELECTRONIC TRANSACTION AND UPDATES MERCHANT ACCOUNT
210

FIG. 2

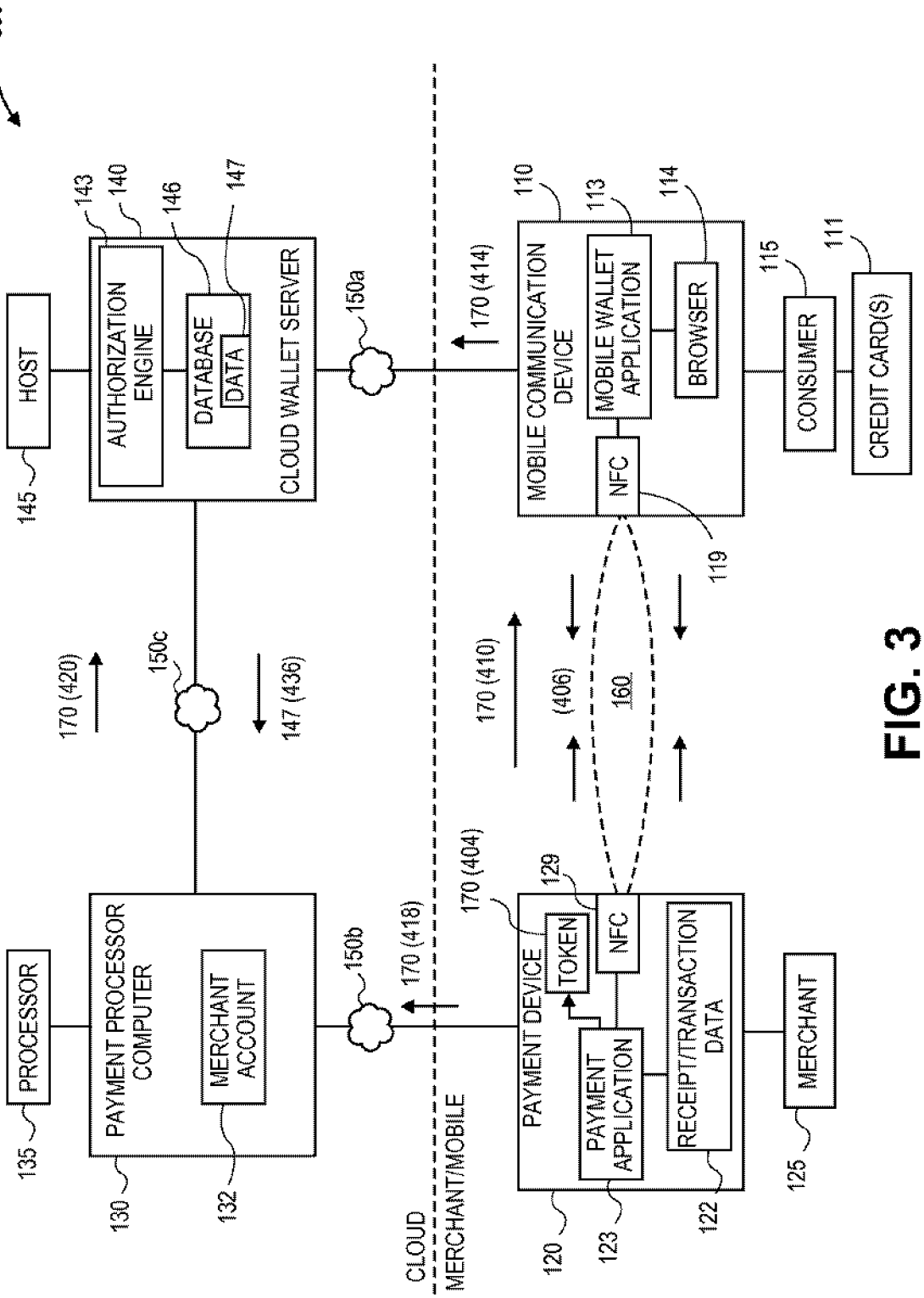

300
HOST
145
AUTHORIZATION ENGINE
143
140
DATABASE
DATA
146
147
CLOUD WALLET SERVER
150a
170 (414)
MOBILE COMMUNICATION DEVICE
110
MOBILE WALLET APPLICATION
113
BROWSER
114
NFC
119
CONSUMER
115
CREDIT CARD(S)
111
170 (420)
150c
147 (436)
170 (410)
(406)
160
PROCESSOR
135
PAYMENT PROCESSOR COMPUTER
130
MERCHANT ACCOUNT
132
150b
170 (418)
170 (404)
CLOUD
MERCHANT/MOBILE
PAYMENT DEVICE
129
TOKEN
NFC
PAYMENT APPLICATION
120
123
RECEIPT/TRANSACTION DATA
122
MERCHANT
125

FIG. 3

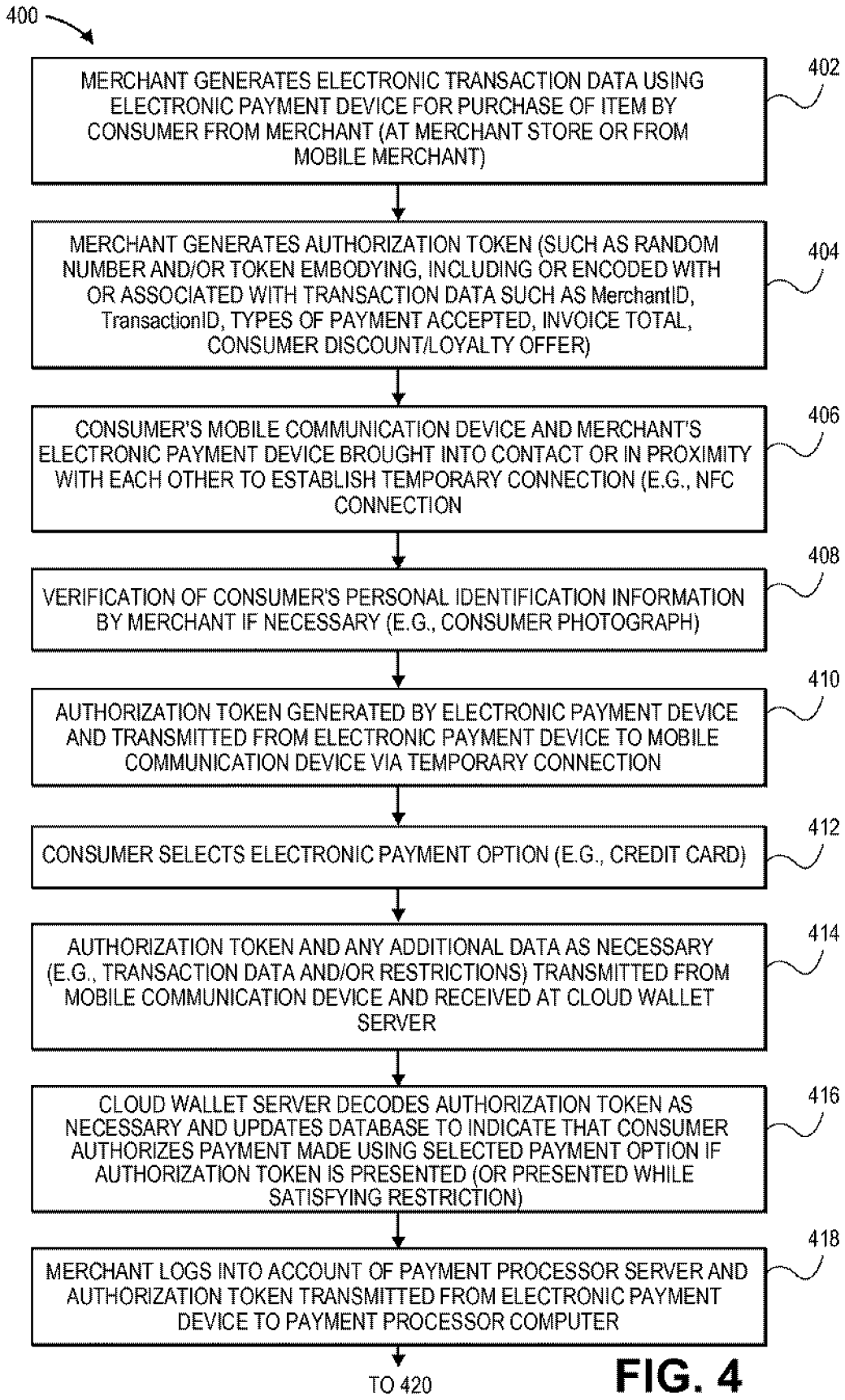

400
MERCHANT GENERATES ELECTRONIC TRANSACTION DATA USING ELECTRONIC PAYMENT DEVICE FOR PURCHASE OF ITEM BY CONSUMER FROM MERCHANT (AT MERCHANT STORE OR FROM MOBILE MERCHANT)
402
MERCHANT GENERATES AUTHORIZATION TOKEN (SUCH AS RANDOM NUMBER AND/OR TOKEN EMBODYING, INCLUDING OR ENCODED WITH OR ASSOCIATED WITH TRANSACTION DATA SUCH AS MerchantID, TransactionID, TYPES OF PAYMENT ACCEPTED, INVOICE TOTAL, CONSUMER DISCOUNT/LOYALTY OFFER)
404
CONSUMER'S MOBILE COMMUNICATION DEVICE AND MERCHANT'S ELECTRONIC PAYMENT DEVICE BROUGHT INTO CONTACT OR IN PROXIMITY WITH EACH OTHER TO ESTABLISH TEMPORARY CONNECTION (E.G., NFC CONNECTION
406
VERIFICATION OF CONSUMER'S PERSONAL IDENTIFICATION INFORMATION BY MERCHANT IF NECESSARY (E.G., CONSUMER PHOTOGRAPH)
408
AUTHORIZATION TOKEN GENERATED BY ELECTRONIC PAYMENT DEVICE AND TRANSMITTED FROM ELECTRONIC PAYMENT DEVICE TO MOBILE COMMUNICATION DEVICE VIA TEMPORARY CONNECTION
410
CONSUMER SELECTS ELECTRONIC PAYMENT OPTION (E.G., CREDIT CARD)
412
AUTHORIZATION TOKEN AND ANY ADDITIONAL DATA AS NECESSARY (E.G., TRANSACTION DATA AND/OR RESTRICTIONS) TRANSMITTED FROM MOBILE COMMUNICATION DEVICE AND RECEIVED AT CLOUD WALLET SERVER
414
CLOUD WALLET SERVER DECODES AUTHORIZATION TOKEN AS NECESSARY AND UPDATES DATABASE TO INDICATE THAT CONSUMER AUTHORIZES PAYMENT MADE USING SELECTED PAYMENT OPTION IF AUTHORIZATION TOKEN IS PRESENTED (OR PRESENTED WHILE SATISFYING RESTRICTION)
416
MERCHANT LOGS INTO ACCOUNT OF PAYMENT PROCESSOR SERVER AND AUTHORIZATION TOKEN TRANSMITTED FROM ELECTRONIC PAYMENT DEVICE TO PAYMENT PROCESSOR COMPUTER
418
TO 420

FIG. 4

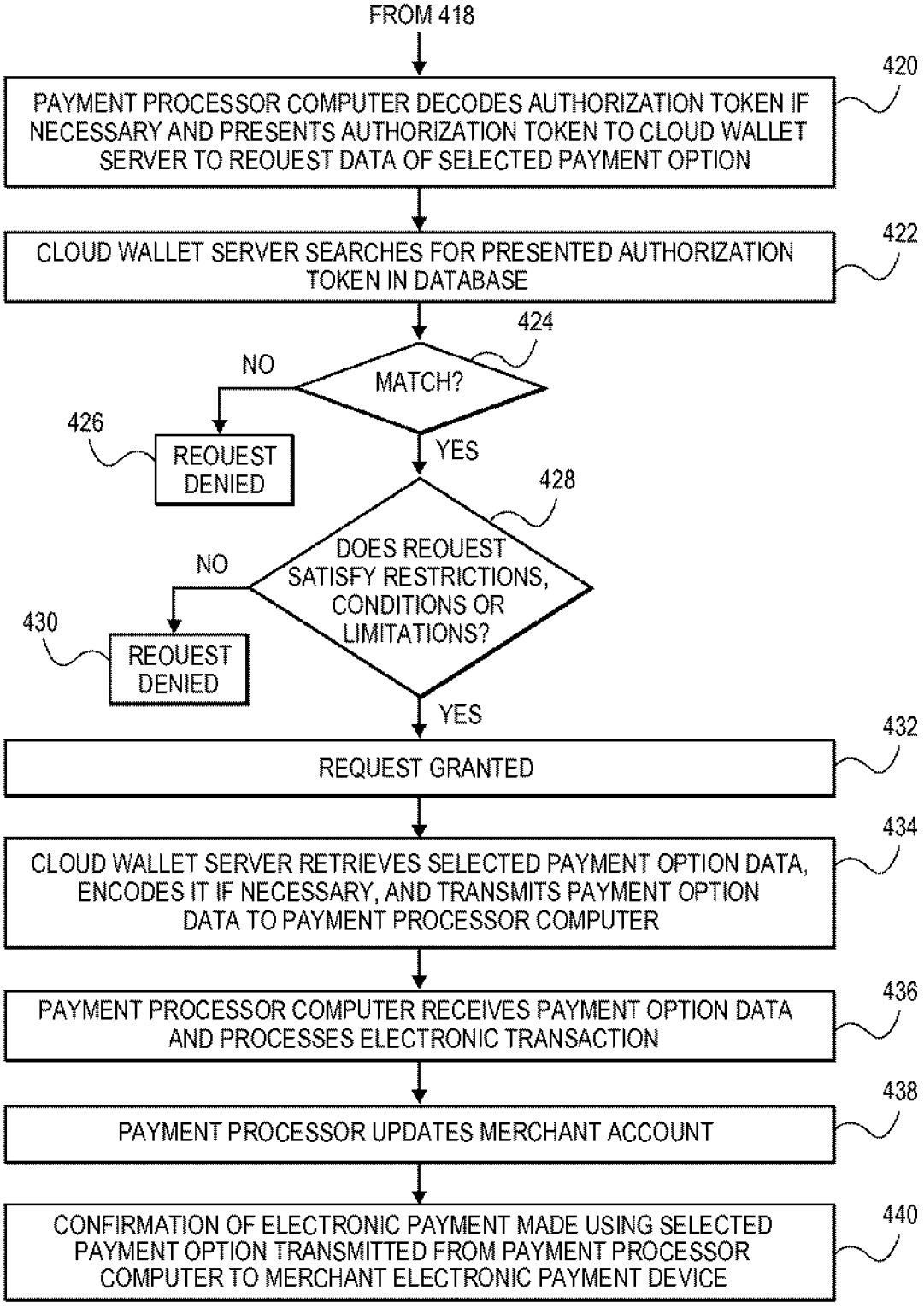

FROM 418
420
PAYMENT PROCESSOR COMPUTER DECODES AUTHORIZATION TOKEN IF NECESSARY AND PRESENTS AUTHORIZATION TOKEN TO CLOUD WALLET SERVER TO REOUEST DATA OF SELECTED PAYMENT OPTION
422
CLOUD WALLET SERVER SEARCHES FOR PRESENTED AUTHORIZATION TOKEN IN DATABASE
424
MATCH?
NO
426
REOUEST DENIED
YES
428
DOES REOUEST SATISFY RESTRICTIONS, CONDITIONS OR LIMITATIONS?
NO
430
REOUEST DENIED
YES
432
REQUEST GRANTED
434
CLOUD WALLET SERVER RETRIEVES SELECTED PAYMENT OPTION DATA, ENCODES IT IF NECESSARY, AND TRANSMITS PAYMENT OPTION DATA TO PAYMENT PROCESSOR COMPUTER
436
PAYMENT PROCESSOR COMPUTER RECEIVES PAYMENT OPTION DATA AND PROCESSES ELECTRONIC TRANSACTION
438
PAYMENT PROCESSOR UPDATES MERCHANT ACCOUNT
440
CONFIRMATION OF ELECTRONIC PAYMENT MADE USING SELECTED PAYMENT OPTION TRANSMITTED FROM PAYMENT PROCESSOR COMPUTER TO MERCHANT ELECTRONIC PAYMENT DEVICE

FIG. 4 (CONT.)

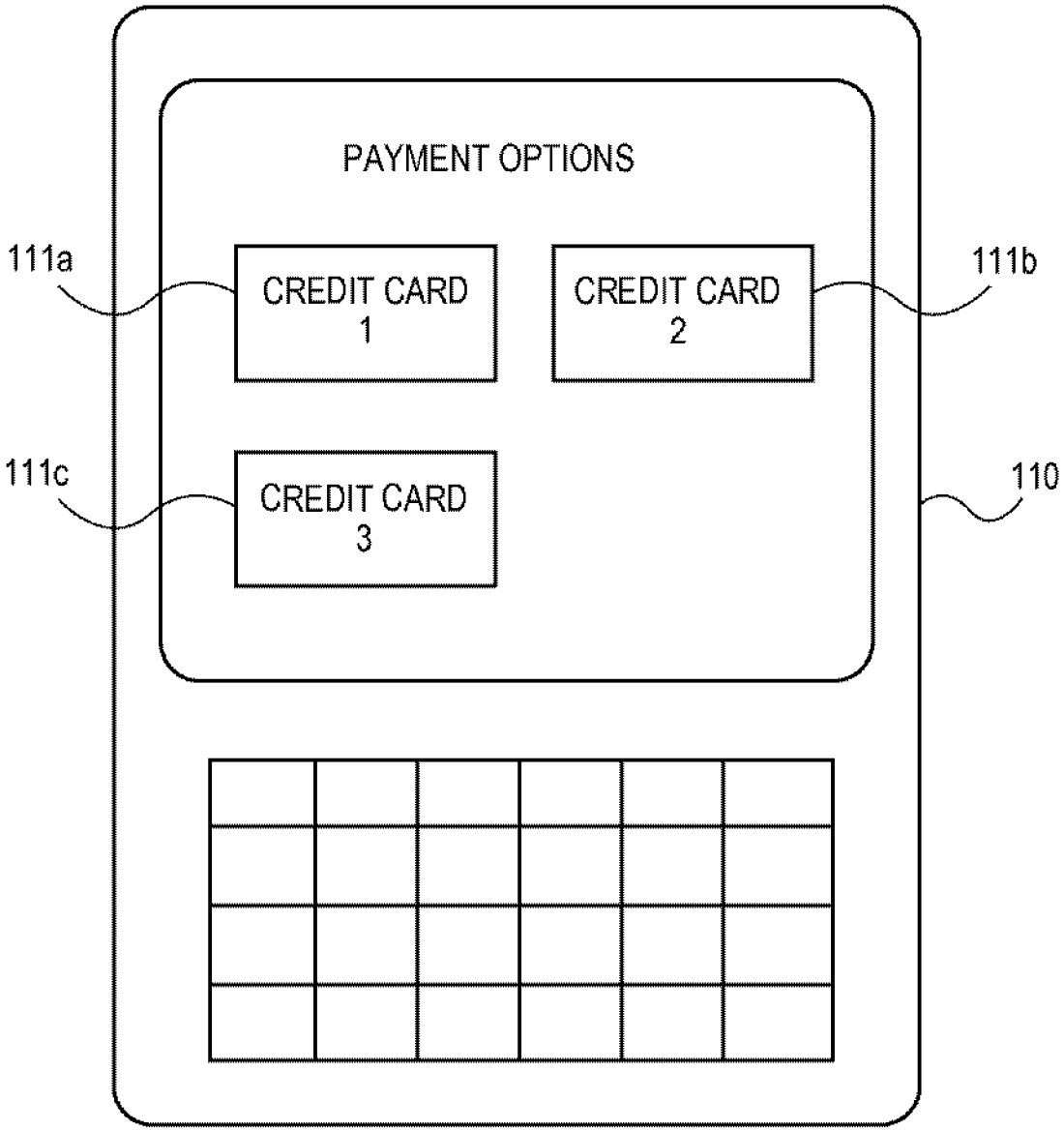

PAYMENT OPTIONS
111a
CREDIT CARD 1
CREDIT CARD 2
111b
111c
CREDIT CARD 3
110

FIG. 5

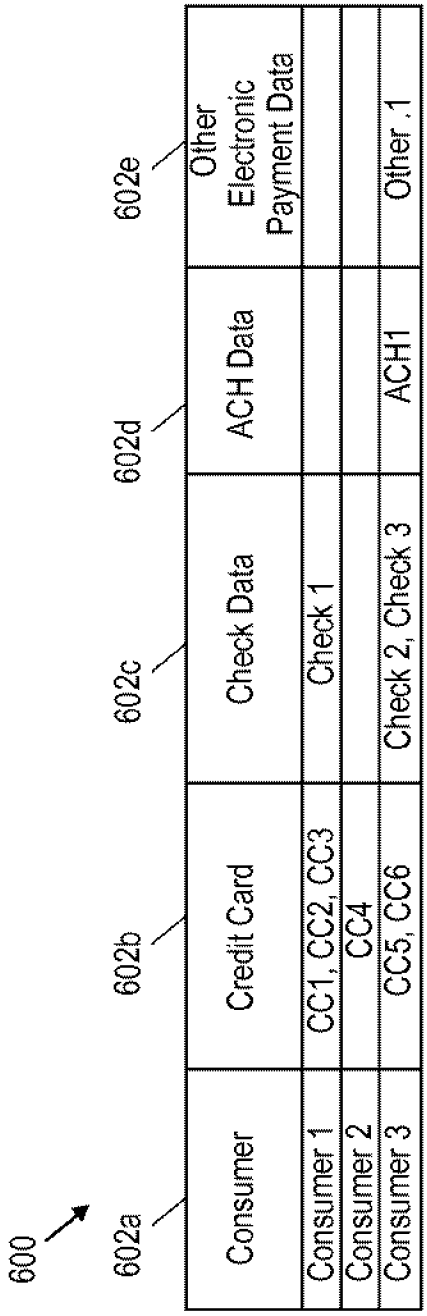

600
602a
602b
602c
602d
602e
Consumer
Credit Card
Check Data
ACH Data
Other Electronic Payment Data
Consumer 1
CC1, CC2, CC3
Check 1
Consumer 2
CC4
Consumer 3
CC5, CC6
Check 2, Check 3
ACH1
Other ,1

FIG. 6A

610
612a
612b
612c
612d
612e
612f
Credit Card
Authorization Token
Authorized Amount
Token Date/Time
Time Token Valid
MerchantID
CC1
Token 1
Amount1
CC1
Token 2
Date/Time2
6 hours
CC1
CC2
Token 4
Amount4
Date/Time4
2 hours
MerchantID4
CC3
Token 5
Amount5
CC4

FIG. 6B

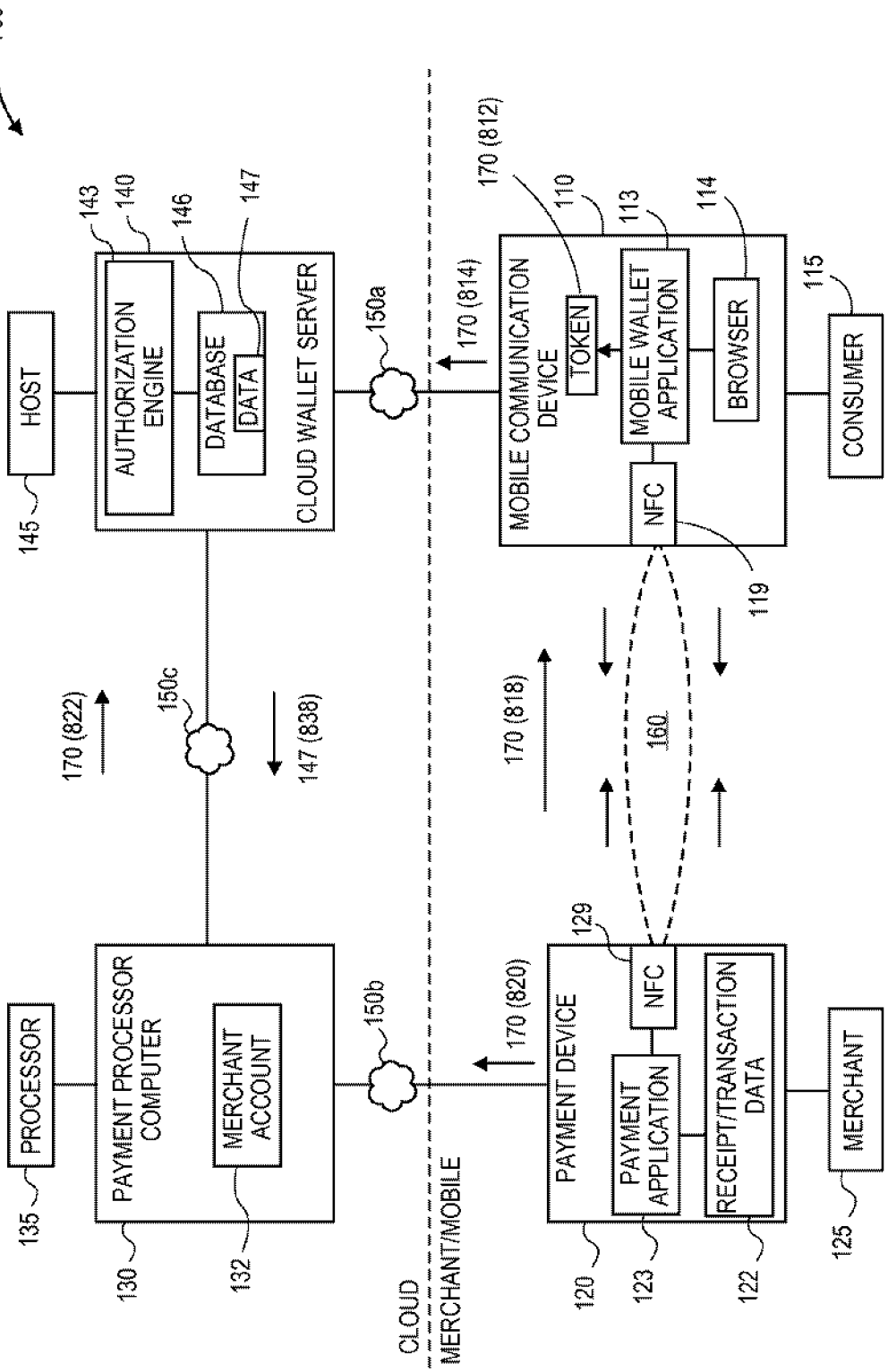

700
HOST
145
AUTHORIZATION ENGINE
143
140
DATABASE
DATA
146
147
CLOUD WALLET SERVER
150a
170 (814)
170 (812)
MOBILE COMMUNICATION DEVICE
110
TOKEN
MOBILE WALLET APPLICATION
113
BROWSER
114
NFC
119
CONSUMER
115
170 (822)
150c
147 (838)
170 (818)
160
PROCESSOR
135
PAYMENT PROCESSOR COMPUTER
MERCHANT ACCOUNT
130
132
150b
CLOUD
MERCHANT/MOBILE
170 (820)
PAYMENT DEVICE
129
NFC
PAYMENT APPLICATION
RECEIPT/TRANSACTION DATA
120
123
122
MERCHANT
125

FIG. 7

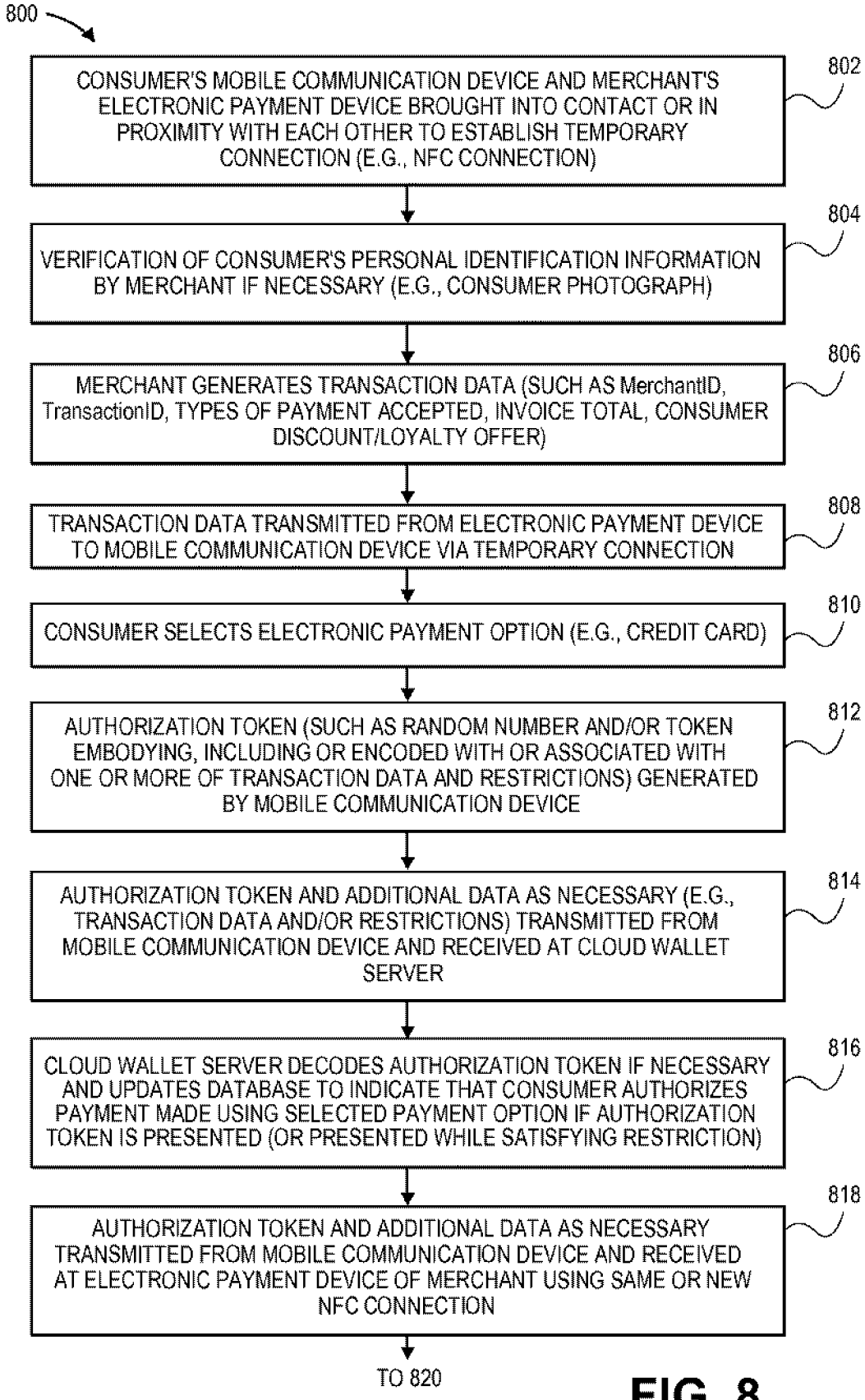

800
CONSUMER'S MOBILE COMMUNICATION DEVICE AND MERCHANT'S ELECTRONIC PAYMENT DEVICE BROUGHT INTO CONTACT OR IN PROXIMITY WITH EACH OTHER TO ESTABLISH TEMPORARY CONNECTION (E.G., NFC CONNECTION)
802
VERIFICATION OF CONSUMER'S PERSONAL IDENTIFICATION INFORMATION BY MERCHANT IF NECESSARY (E.G., CONSUMER PHOTOGRAPH)
804
MERCHANT GENERATES TRANSACTION DATA (SUCH AS MerchantID, TransactionID, TYPES OF PAYMENT ACCEPTED, INVOICE TOTAL, CONSUMER DISCOUNT/LOYALTY OFFER)
806
TRANSACTION DATA TRANSMITTED FROM ELECTRONIC PAYMENT DEVICE TO MOBILE COMMUNICATION DEVICE VIA TEMPORARY CONNECTION
808
CONSUMER SELECTS ELECTRONIC PAYMENT OPTION (E.G., CREDIT CARD)
810
AUTHORIZATION TOKEN (SUCH AS RANDOM NUMBER AND/OR TOKEN EMBODYING, INCLUDING OR ENCODED WITH OR ASSOCIATED WITH ONE OR MORE OF TRANSACTION DATA AND RESTRICTIONS) GENERATED BY MOBILE COMMUNICATION DEVICE
812
AUTHORIZATION TOKEN AND ADDITIONAL DATA AS NECESSARY (E.G., TRANSACTION DATA AND/OR RESTRICTIONS) TRANSMITTED FROM MOBILE COMMUNICATION DEVICE AND RECEIVED AT CLOUD WALLET SERVER
814
CLOUD WALLET SERVER DECODES AUTHORIZATION TOKEN IF NECESSARY AND UPDATES DATABASE TO INDICATE THAT CONSUMER AUTHORIZES PAYMENT MADE USING SELECTED PAYMENT OPTION IF AUTHORIZATION TOKEN IS PRESENTED (OR PRESENTED WHILE SATISFYING RESTRICTION)
816
AUTHORIZATION TOKEN AND ADDITIONAL DATA AS NECESSARY TRANSMITTED FROM MOBILE COMMUNICATION DEVICE AND RECEIVED AT ELECTRONIC PAYMENT DEVICE OF MERCHANT USING SAME OR NEW NFC CONNECTION
818
TO 820

FIG. 8

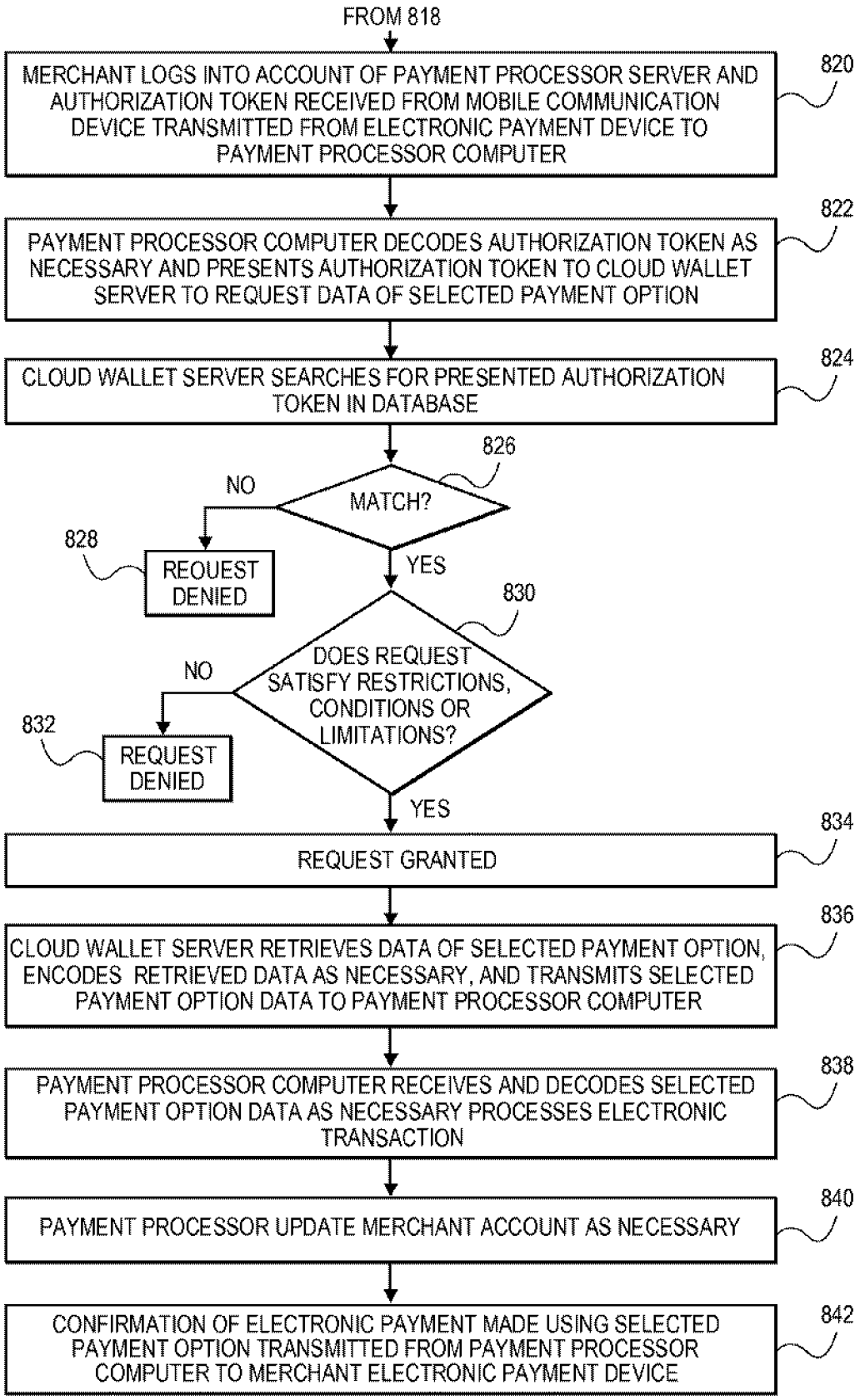

FROM 818
MERCHANT LOGS INTO ACCOUNT OF PAYMENT PROCESSOR SERVER AND AUTHORIZATION TOKEN RECEIVED FROM MOBILE COMMUNICATION DEVICE TRANSMITTED FROM ELECTRONIC PAYMENT DEVICE TO PAYMENT PROCESSOR COMPUTER
820
PAYMENT PROCESSOR COMPUTER DECODES AUTHORIZATION TOKEN AS NECESSARY AND PRESENTS AUTHORIZATION TOKEN TO CLOUD WALLET SERVER TO REQUEST DATA OF SELECTED PAYMENT OPTION
822
CLOUD WALLET SERVER SEARCHES FOR PRESENTED AUTHORIZATION TOKEN IN DATABASE
824
826
MATCH?
NO
828
REQUEST DENIED
YES
830
DOES REQUEST SATISFY RESTRICTIONS, CONDITIONS OR LIMITATIONS?
NO
832
REQUEST DENIED
YES
REQUEST GRANTED
834
CLOUD WALLET SERVER RETRIEVES DATA OF SELECTED PAYMENT OPTION, ENCODES RETRIEVED DATA AS NECESSARY, AND TRANSMITS SELECTED PAYMENT OPTION DATA TO PAYMENT PROCESSOR COMPUTER
836
PAYMENT PROCESSOR COMPUTER RECEIVES AND DECODES SELECTED PAYMENT OPTION DATA AS NECESSARY PROCESSES ELECTRONIC TRANSACTION
838
PAYMENT PROCESSOR UPDATE MERCHANT ACCOUNT AS NECESSARY
840
CONFIRMATION OF ELECTRONIC PAYMENT MADE USING SELECTED PAYMENT OPTION TRANSMITTED FROM PAYMENT PROCESSOR COMPUTER TO MERCHANT ELECTRONIC PAYMENT DEVICE
842

FIG. 8 (CONT.)

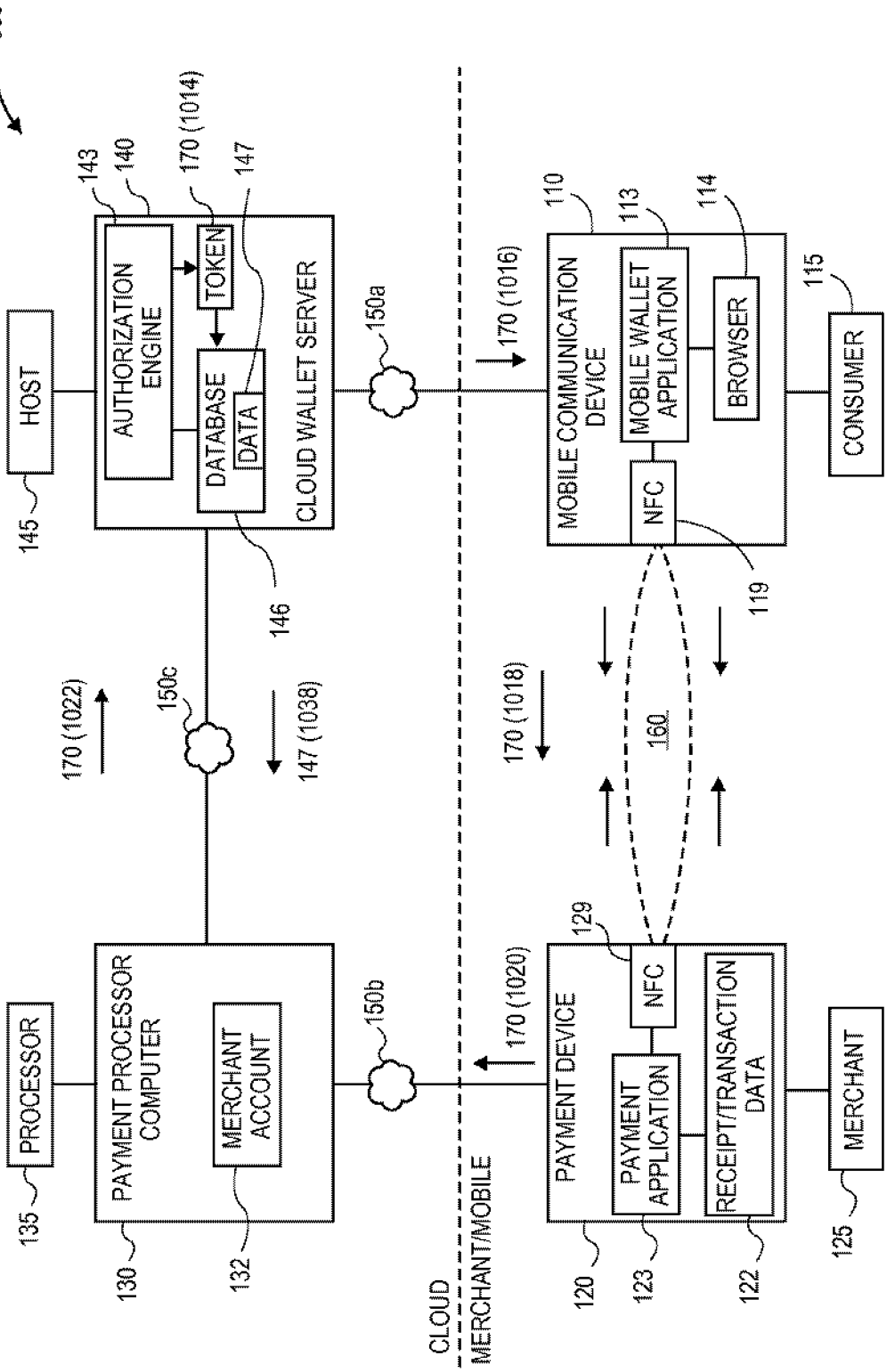

900
143
140
170 (1014)
147
AUTHORIZATION ENGINE
TOKEN
DATABASE
DATA
CLOUD WALLET SERVER
HOST
145
146
150a
170 (1016)
110
MOBILE COMMUNICATION DEVICE
113
MOBILE WALLET APPLICATION
114
BROWSER
115
CONSUMER
NFC
119
170 (1022)
150c
147 (1038)
170 (1018)
160
PROCESSOR
135
PAYMENT PROCESSOR COMPUTER
MERCHANT ACCOUNT
130
132
150b
170 (1020)
CLOUD
MERCHANT/MOBILE
129
PAYMENT DEVICE
NFC
PAYMENT APPLICATION
RECEIPT/TRANSACTION DATA
MERCHANT
120
123
122
125

FIG. 9

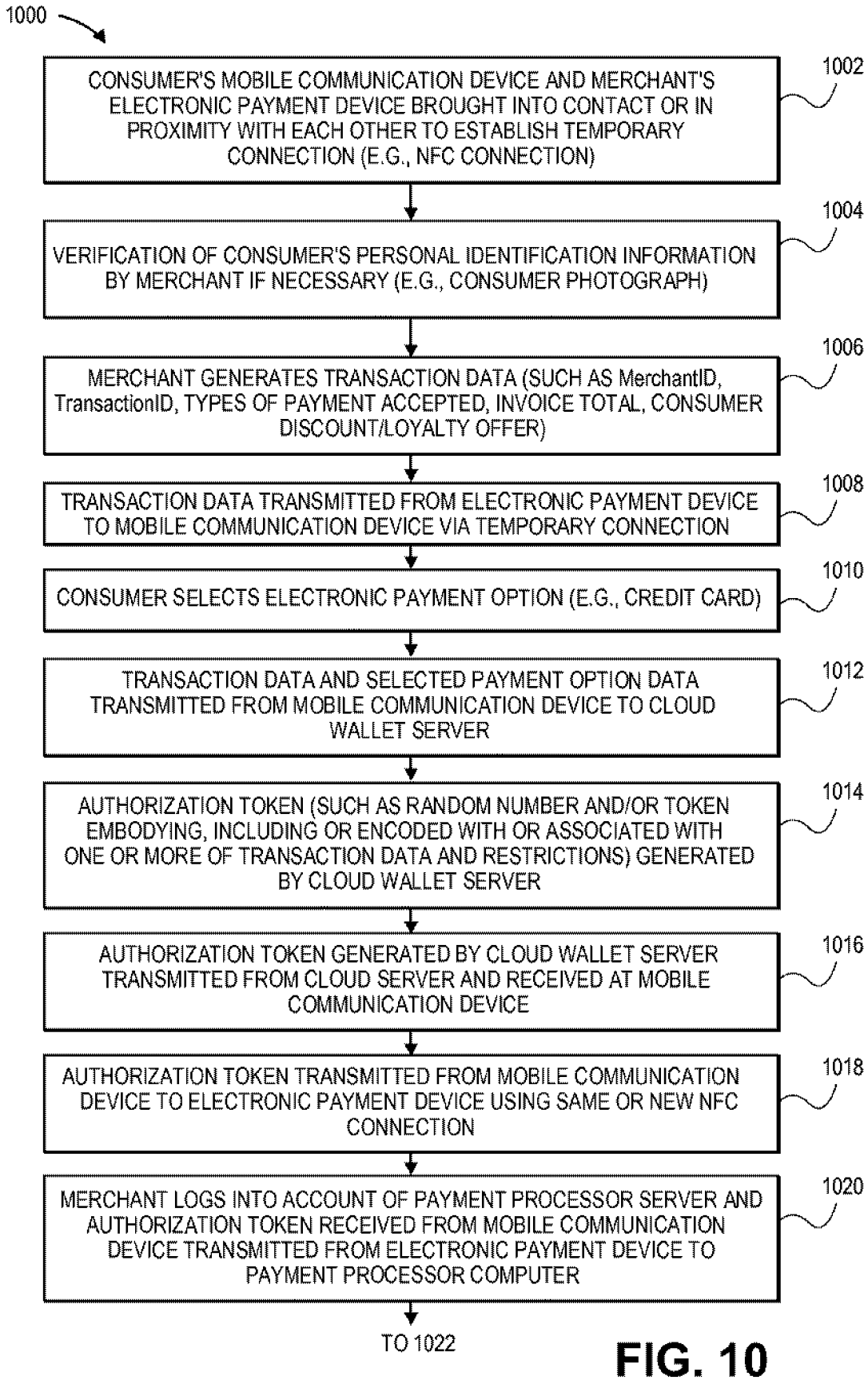

1000
CONSUMER'S MOBILE COMMUNICATION DEVICE AND MERCHANT'S ELECTRONIC PAYMENT DEVICE BROUGHT INTO CONTACT OR IN PROXIMITY WITH EACH OTHER TO ESTABLISH TEMPORARY CONNECTION (E.G., NFC CONNECTION)
1002
VERIFICATION OF CONSUMER'S PERSONAL IDENTIFICATION INFORMATION BY MERCHANT IF NECESSARY (E.G., CONSUMER PHOTOGRAPH)
1004
MERCHANT GENERATES TRANSACTION DATA (SUCH AS MerchantID, TransactionID, TYPES OF PAYMENT ACCEPTED, INVOICE TOTAL, CONSUMER DISCOUNT/LOYALTY OFFER)
1006
TRANSACTION DATA TRANSMITTED FROM ELECTRONIC PAYMENT DEVICE TO MOBILE COMMUNICATION DEVICE VIA TEMPORARY CONNECTION
1008
CONSUMER SELECTS ELECTRONIC PAYMENT OPTION (E.G., CREDIT CARD)
1010
TRANSACTION DATA AND SELECTED PAYMENT OPTION DATA TRANSMITTED FROM MOBILE COMMUNICATION DEVICE TO CLOUD WALLET SERVER
1012
AUTHORIZATION TOKEN (SUCH AS RANDOM NUMBER AND/OR TOKEN EMBODYING, INCLUDING OR ENCODED WITH OR ASSOCIATED WITH ONE OR MORE OF TRANSACTION DATA AND RESTRICTIONS) GENERATED BY CLOUD WALLET SERVER
1014
AUTHORIZATION TOKEN GENERATED BY CLOUD WALLET SERVER TRANSMITTED FROM CLOUD SERVER AND RECEIVED AT MOBILE COMMUNICATION DEVICE
1016
AUTHORIZATION TOKEN TRANSMITTED FROM MOBILE COMMUNICATION DEVICE TO ELECTRONIC PAYMENT DEVICE USING SAME OR NEW NFC CONNECTION
1018
MERCHANT LOGS INTO ACCOUNT OF PAYMENT PROCESSOR SERVER AND AUTHORIZATION TOKEN RECEIVED FROM MOBILE COMMUNICATION DEVICE TRANSMITTED FROM ELECTRONIC PAYMENT DEVICE TO PAYMENT PROCESSOR COMPUTER
1020
TO 1022

FIG. 10

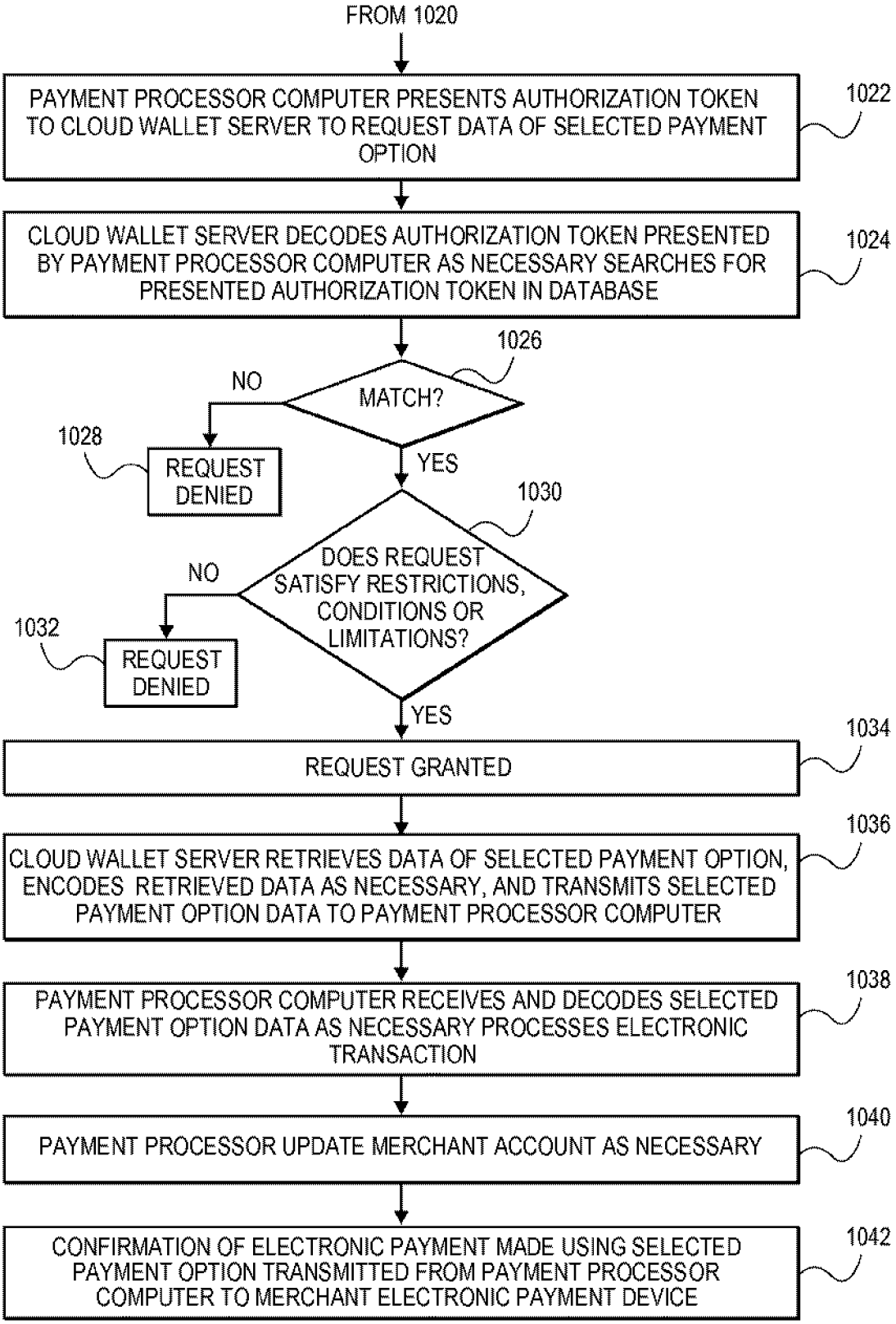

FROM 1020
PAYMENT PROCESSOR COMPUTER PRESENTS AUTHORIZATION TOKEN TO CLOUD WALLET SERVER TO REQUEST DATA OF SELECTED PAYMENT OPTION
1022
CLOUD WALLET SERVER DECODES AUTHORIZATION TOKEN PRESENTED BY PAYMENT PROCESSOR COMPUTER AS NECESSARY SEARCHES FOR PRESENTED AUTHORIZATION TOKEN IN DATABASE
1024
1026
MATCH?
NO
1028
REQUEST DENIED
YES
1030
DOES REQUEST SATISFY RESTRICTIONS, CONDITIONS OR LIMITATIONS?
NO
1032
REQUEST DENIED
YES
1034
REQUEST GRANTED
1036
CLOUD WALLET SERVER RETRIEVES DATA OF SELECTED PAYMENT OPTION, ENCODES RETRIEVED DATA AS NECESSARY, AND TRANSMITS SELECTED PAYMENT OPTION DATA TO PAYMENT PROCESSOR COMPUTER
1038
PAYMENT PROCESSOR COMPUTER RECEIVES AND DECODES SELECTED PAYMENT OPTION DATA AS NECESSARY PROCESSES ELECTRONIC TRANSACTION
1040
PAYMENT PROCESSOR UPDATE MERCHANT ACCOUNT AS NECESSARY
1042
CONFIRMATION OF ELECTRONIC PAYMENT MADE USING SELECTED PAYMENT OPTION TRANSMITTED FROM PAYMENT PROCESSOR COMPUTER TO MERCHANT ELECTRONIC PAYMENT DEVICE

FIG. 10 (CONT.)

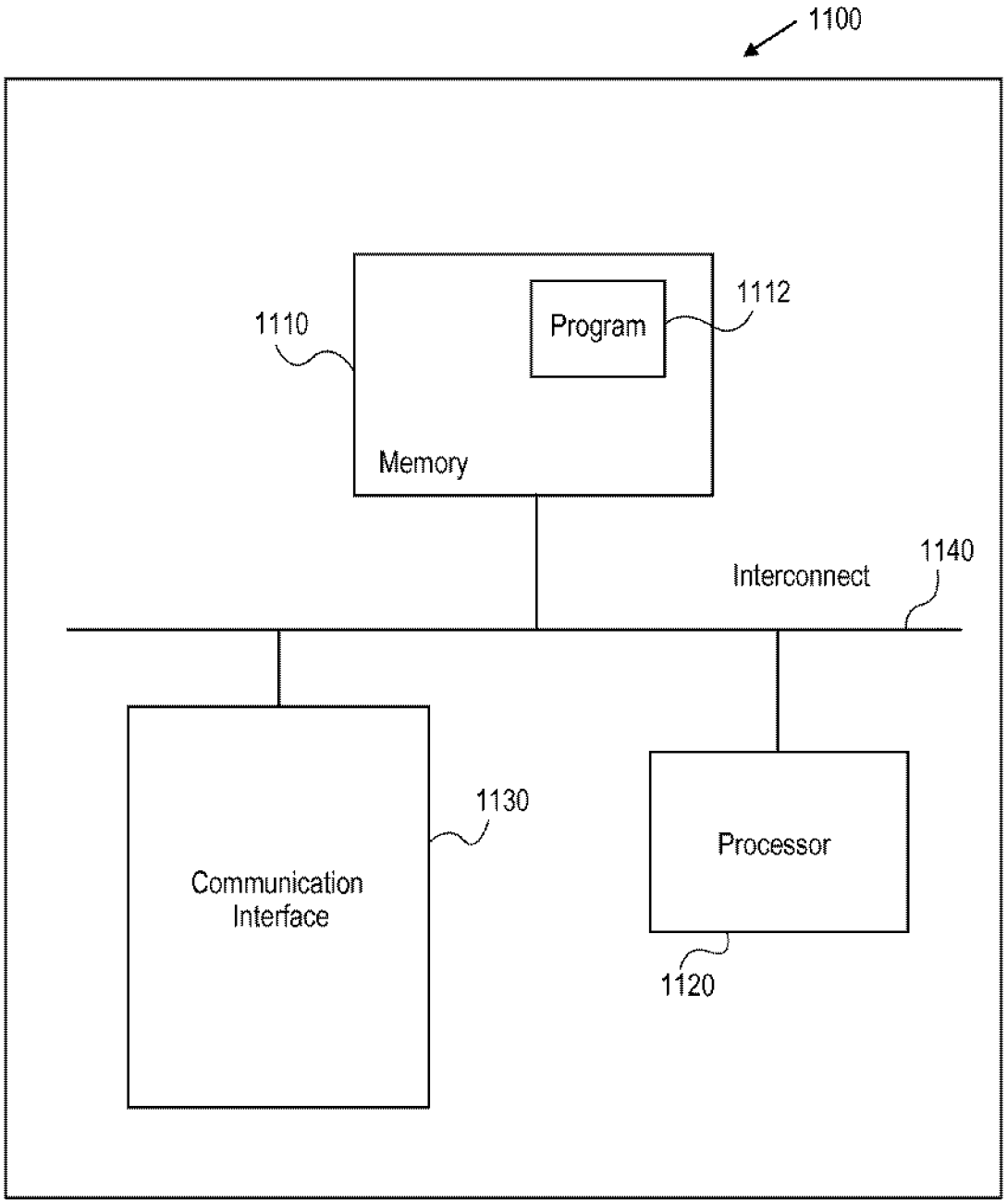

1100
1110
Program
1112
Memory
Interconnect
1140
1130
Communication Interface
Processor
1120

FIG. 11

PROCESSING ELECTRONIC PAYMENT INVOLVING MOBILE COMMUNICATION DEVICE

BACKGROUND

[0001] Embodiments of the invention are generally related to electronic commerce and, more particularly, to electronic payments made utilizing a mobile communication device. Customers or consumers of merchant stores or retail establishments often pay for goods or services using a payment or transaction card such as a credit card. Some merchants utilize mobile communication devices for accepting payment, and for this purpose, they may utilize a Smartphone including a payment application or software program that is operable by the merchant for electronically accepting payment from a consumer. Payments can be accepted at various locations including various residential and commercial locations, houses, offices, job sites, cities, states and countries at various times.

[0002] For example, during a transaction, the merchant may manually enter credit card data into a payment terminal or the consumer or merchant may swipe the card through a payment terminal. If the merchant utilizes a mobile device, the merchant may enter data into the mobile device or swipe the card if the mobile device is so equipped. Transaction data is sent to a third party payment processor that serves as an intermediary to process the transaction.

[0003] While many transactions are successfully completed using credit cards, entry of credit card data can be time consuming and inconvenient. Mobile wallets are being developed to facilitate electronic payments. Rather than payment by cash, check or credit card, a consumer utilizes a mobile communication device for payment. For example, mobile wallets are utilized in Japan to purchase train tickets and in Europe to pay for parking, but implementation of mobile wallets in the United States for electronic payment in merchant stores has been slow and limited due to various concerns and limitations such as consumer security and privacy concerns and lack of supporting infrastructure. For example, certain studies have estimated only a small fraction of the about 105 million mobile payment users in the world are located in North America. Given these concerns and limitations, consumers may be more inclined to continue using traditional credit card and check payments until mobile wallet applications are more developed and secure such that consumers, merchants and payment processors can all be confident that mobile wallet payments can be reliably processed.

SUMMARY

[0004] Embodiments relate to processing electronic transactions in which a consumer tenders electronic payment to a merchant using a mobile communication device such as a Smartphone that is a mobile wallet, a near field communication (NFC) connection between the consumer's mobile communication device and a merchant's electronic payment device, which may also be a Smartphone, and a cloud computer, server or resource. The cloud computer hosts or accesses a database storing the consumer's mobile wallet data (e.g., credit card data) and releases credit card data to a payment processor to complete the transaction if the payment processor presents an authorization token to the cloud resource. For this purpose, according to embodiments, the authorization token is generated, exchanged between the merchant and consumer using a communication protocol such as peer-to-peer communication, and provided to a payment processor and the cloud computer. The payment processor, after receiving the authorization token from the merchant's electronic payment device, requests electronic payment data (e.g., credit card number, expiration, etc.) from the cloud resource. Assuming the authorization token is valid, the payment processor receives the electronic payment data, processes the transaction, and updates a merchant account.

[0005] Embodiments are directed to methods performed by or involving, systems of or utilized by, and articles of manufacture or computer program products or applications of or utilized by one or multiple parties of involved in the electronic transaction. According to embodiments, the parties involved include a consumer who carries a mobile communication device serving as a mobile wallet, a merchant utilizing an electronic payment device, a host or computer or cloud resource including respective payment or credit card data of respective consumers, and an intermediate party or host that processes the electronic transaction on behalf of a merchant utilizing payment data received from the cloud resource.

[0006] One embodiment is directed to a computer-implemented method for processing data related to an electronic transaction involving a consumer and a merchant and comprises establishing a NFC connection between an electronic payment device of the merchant and a mobile communication of the consumer. The short range NFC connection is established when the electronic payment device and the mobile communication device contact or are placed sufficiently close to each other. Authorization data such as a token or other data known to the merchant and consumer devices is sent from one and received by the other. Thus, authorization data is shared between the mobile communication device and the electronic payment device using the NFC connection. However, electronic payment data, such as credit card data number and expiration date, is not transmitted to the merchant. Instead, the authorization data is transmitted from the mobile communication device through a first network to a cloud computer, server or resource, which may host respective data of respective payment cards of respective consumers, and also transmitted from the electronic payment device through a second network to an electronic payment processor. Having the authorization data, the payment processor computer can retrieve electronic payment data by presenting the authorization data to the cloud computer, and then process the transaction with the electronic payment data and update a merchant account.

[0007] According to another embodiment, the authorization data or token embodies, or is encoded with, data of the merchant and/or transaction (generally, transaction data). For example, transaction data encoded may include one or more of a merchant identification, transaction identification, an invoice, receipt or transaction amount, a transaction date, etc. An encoded authorization token can be decoded to determine the token and associated transaction data. In this embodiment, a NFC connection is established between an electronic payment device of the merchant and a mobile communication of the consumer when the electronic payment device and the mobile communication device contact or are located in proximity to each other. The authorization data or a token is generated and embodies data of a transaction involving the consumer and the merchant. For this purpose, the merchant may generate the authorization data embodying or encoded with transaction data, or transaction data can be sent to the

consumer's mobile communication device, which generates authorization data embodying or encoded with transaction data. The authorization data or token is transmitted from the mobile communication device through a first network to a first computer or cloud computer hosting respective data of respective payment cards of respective consumers, and from the electronic payment device through a second network to a second computer of an electronic payment processor. The payment processor presents the authorization data to the cloud computer to request electronic payment data of the consumer associated with the authorization data, which may be decoded by the first computer if necessary, compared with the authorization data received from the consumer, e.g., by accessing a database or record for that consumer or authorization data, and if the transaction data matches, the payment processor can be provided with the electronic payment data to complete the transaction.

[0008] A further embodiment is directed to a system for processing data related to an electronic transaction involving a consumer and a merchant and comprises a mobile communication device carried by a consumer used to establish a NFC connection with an electronic payment device of a merchant. A mobile wallet application executing on the mobile communication device generates or receives authorization data that is also shared with the electronic payment device utilizing the NFC connection, but without transmitting payment data (e.g., credit card number) to the merchant. The mobile communication device is also configured or operable to transmit the authorization data through a first network to a first computer hosting respective data of respective payment cards of respective consumers so that when the authorization data is transmitted from the electronic payment device through a second network to a second computer of an electronic payment processor and presented by the second computer to the first computer, which can return payment card data to the payment processor to allow the payment processor to complete the transaction.

[0009] Other system embodiments include one or more or all of the merchant's electronic payment device, the first or cloud computer and the second or payment processor computer. In certain system embodiments, the mobile communication device of the consumer and/or the electronic payment device of the merchant is configured or operable to generate authorization data or a token encoded with or embodying transaction data such as a merchant identification or transaction amount. Other embodiments are directed to a merchant's electronic payment device configured to implemented method embodiments, a first or payment processor computer configured to implement method embodiments, and a second or cloud wallet computer configured to implement embodiments.

[0010] Other embodiments are directed to applications and articles of manufacture or computer program products comprising a non-transitory, computer readable storage medium having instructions which, when executed by a first computer of a consumer or other computer of system embodiments, cause the one or more processors to execute a method for processing data related to an electronic transaction involving a consumer and a merchant.

[0011] In a single or multiple embodiments, the electronic payment device is a Point Of Sale (POS) device located at the merchant location. In other embodiments, the merchant utilizes a mobile communication device such as a Smartphone that includes a mobile payment application executing thereon that allows the merchant to accept payment from the consumer without receiving payment data such as credit card data.

[0012] In a single or multiple embodiments, the second or payment processor computer presents authorization data received from the merchant to the first or cloud computer to request electronic payment data such as credit card data of the consumer. In response, the payment processor computer receives the requested credit card data from the first computer so that the second computer processes the transaction using the received credit card data and updates a merchant account hosted or accessible by the second computer.

[0013] In a single or multiple embodiments, the electronic payment device and the mobile communication device are connected to each other in a peer-to-peer configuration so that authorization data can be generated by either of the electronic payment device or the mobile communication device and transmitted to the other. This is in contrast to certain systems that utilize restrictive or one-way communications (e.g., transmitting a tag from a mobile communication device to a merchant payment device).

[0014] In a single or multiple embodiments, the authorization data is a random number. The random number may be generated by a mobile wallet application or payment application, or by a separate random number generator or a controller of a NFC chip. According to one embodiment, authorization data generated according to embodiments is dynamic such that different authorization data or tokens are utilized for different purchases by a consumer. In a further embodiment, the authorization data or token is a single use token such that once generated and provided to the cloud computer, only a single request for the data may be presented by the payment processor. The authorization data or token may also be encoded with or associated with date or time restrictions, conditions or limitations. One example restriction is that the token is valid for a limited time and must be utilized by the payment processor within a certain time from generation of the token or receipt of the token.

[0015] In a single or multiple embodiments, the merchant transmits an offer, advertisement, coupon, discount or loyalty incentive to the consumer, e.g., to encourage the consumer to select a certain type of payment or certain credit card on behalf of an issuer of the credit card. For example, the merchant may have an arrangement with VISA or another issuer so that the merchant offers a discount to the consumer if the consumer utilizes a VISA credit card.

[0016] In a single or multiple embodiments, authorization data or tokens that embody or are encoded with transaction data may be encoded with one or more or all of a merchant identification, a transaction identification, a transaction amount, and accepted forms or types of electronic payment. Encoding authorization data or utilizing additional data in this manner provides additional security and assurances to the parties involved in the transaction that the payment processing involves the correct consumer and the correct transaction amount. Thus, when the cloud computer receives an encoded token, the cloud computer can decode the token if necessary, e.g., using a key shared with the consumer, to determine the transaction data, store the transaction data in a database so that the transaction data is associated with the authorization token. In this manner, when the payment processor presents the authorization token to the cloud wallet, the cloud wallet can provide the credit card data and specify what amount is

properly charged to the credit card, instead of relying on the merchant and/or payment processor to charge the correct amount.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The foregoing and other aspects of embodiments are described in further detail with reference to the accompanying drawings, wherein:

[0018] FIG. **1** is a block diagram of a system constructed according to one embodiment for generating an authentication token for use in processing an electronic transaction without providing electronic payment data to a merchant;

[0019] FIG. **2** is a flow diagram of one embodiment of a method for generating an authentication token for use in processing an electronic transaction without providing electronic payment data to a merchant;

[0020] FIG. **3** is a block diagram of a system constructed according to one embodiment in which an authentication token is generated by a payment application executing on an electronic payment device of a merchant that is in communication with a consumer mobile communication device and a payment processor computer for use in processing an electronic transaction without providing electronic payment data to the merchant;

[0021] FIG. **4** is a flow diagram of one embodiment of a method for generating an authentication token with an electronic payment device of a merchant for use in processing an electronic transaction without providing electronic payment data to the merchant;

[0022] FIG. **5** generally illustrates a display generated by a mobile payment application to allow a consumer to select which form of electronic payment should be utilized for payment to a merchant and generation of an authorization token;

[0023] FIGS. **6**A-B illustrate examples of how embodiments may be implemented to manage and update a cloud database that hosts electronic payment data of consumers;

[0024] FIG. **7** is a block diagram of a system constructed according to one embodiment in which an authentication token is generated by a mobile wallet application executing on a mobile communication device of a consumer that is in communication with a cloud resource or computer and an electronic payment device of a merchant for use in processing an electronic transaction without providing electronic payment data to the merchant;

[0025] FIG. **8** is a flow diagram of one embodiment of a method for generating an authentication token with a mobile communication device of a consumer for use in processing an electronic transaction without providing electronic payment data to the merchant;

[0026] FIG. **9** is a block diagram of a system constructed according to one embodiment in which an authentication token is generated by a cloud computer or resource that is in communication with a mobile communication device of a consumer and a payment processor computer for use in processing an electronic transaction without providing electronic payment data to a merchant;

[0027] FIG. **10** is a flow diagram of one embodiment of a method for generating an authentication token with a cloud resource or computer for use in processing an electronic transaction without providing electronic payment data to the merchant; and

[0028] FIG. **11** is a block diagram of components of a computing apparatus in which embodiments may be implemented or that may be utilized in or by embodiments.

[0029] In order to better appreciate how to obtain the above-recited and other advantages and objects of various embodiments, a more detailed description of embodiments is provided with reference to the accompanying drawings. It should be noted that the drawings are not drawn to scale and that elements of similar structures or functions are represented by like reference numerals throughout. It will be understood that these drawings depict only certain illustrated embodiments and are not therefore to be considered limiting of scope of embodiments.

DETAILED DESCRIPTION OF ILLUSTRATED EMBODIMENTS

[0030] Embodiments relate to processing of electronic transactions involving a merchant and a consumer that pays for an item purchased from the merchant using a mobile communication device while not providing data of the form of payment (e.g., credit card number) to the merchant. Embodiments involve or are executed by mobile communication device of the consumer that has an application that transforms the mobile communication into a mobile wallet. The mobile wallet is tendered by the consumer to pay for an item from the merchant without tendering a physical credit card or providing credit card data to the merchant. Instead, embodiments involve sharing of authorization data or a token by the merchant and the consumer, e.g., using peer-to-peer communications. The authorization data or token is provided to a cloud wallet server and to a payment processor. The cloud wallet server stores data about the types or forms of electronic payment available to the consumer, and which form of electronic payment was selected by the consumer for a particular transaction authorized by the consumer according to the authorization data or token. To process the transaction, the authorization data or token is provided to a payment processor, which presents the authorization data or token to the cloud wallet server. If the presented authorization data or token is valid or matches records of the cloud wallet server, the cloud wallet server provides payment data (e.g., credit card data such as credit card number, expiration date and security code) to the payment processor computer, which processes the transaction with the received payment data so that the consumer's credit card is charged, and a merchant account is updated to reflect the completed transaction. A merchant account is a type of bank account that allows a merchant to accept electronic payment by credit or debit card, for example, and is utilized for settlement of credit card and/or debit card transactions.

[0031] Thus, with embodiments, consumer credit card information is stored securely on a server of the cloud that serves as a cloud wallet server, consumers are not required to provide credit card data to merchants, and consumers can be more confident about utilizing mobile communication devices as mobile wallets since their credit card information is safeguarded by the cloud wallet server. Further, merchants, consumers and payment processors can be confident that mobile wallet transactions can be securely and efficiently processed in a secure manner. Further aspects of embodiments are described with reference to FIGS. **1-2**, and examples of how embodiments may be implemented are described in further detail with reference to FIGS. **3-11**.

[0032] Referring to FIG. **1**, a system **100** constructed according to one embodiment involves or comprises one or more or all of a mobile communication device **110** of a consumer **115**, an electronic payment device **120** of a mer-

chant **125**, a computer or server **130** of a payment processor **135** that processes transactions and manages or accesses a merchant account **132** on behalf of the merchant **125**, and a cloud computer, server or resource (generally, cloud computer **140**) of a host **145** that manages a database **146** containing electronic payment data **147** (e.g., credit card number, expiration date, security code) utilized by the consumer **115**. Mobile communication device **110** and cloud computer **140** are in communication with each other via network **150***a*, electronic payment device **120** and payment processor computer **130** are in communication with each other via network **150***b*, and payment processor computer **130** and cloud computer **140** are in communication with each other via network **150***c*. In the illustrated embodiment, the consumer has one or more forms of electronic payment **111** (three credit cards **111***a-c* are illustrated as an example), and registers with cloud computer **140**, which serves as a cloud wallet resource or computer and stores consumer's credit card data in a database **142**.

[0033] In the illustrated embodiment, the consumer **110** tenders the mobile communication device **110**, which serves as a mobile wallet, to pay for an item, good or service (generally, item) offered by the merchant **125**. For this purpose, the mobile communication device or mobile wallet **110** may involve or authorize various types of electronic payments including, but not limited to credit card, debit card, ATM card, ACH, eCheck, PAYPAL and other forms of payment capable of being made or authorized using the mobile communication device **110**. For ease of explanation, reference is made generally to a mobile communication device **110** or mobile wallet and a credit card **111**. Mobile communication devices **110** that may be utilized in embodiments include a cellular telephone, a Smartphone, and a Personal Digital Assistant (PDA) that has cellular telephone or wireless communication capabilities. In the illustrated embodiment, the mobile communication device **110** is a Smartphone that includes a native application or application **113** (generally, mobile wallet application) downloaded from a source such as the cloud wallet computer **140** for making electronic payments utilizing the mobile communication device **110**.

[0034] Depending on the type and capabilities of mobile communication device **110** and mobile wallet application **113** utilized, a web browser **114** may execute on the mobile communications device **110** to allow the consumer **110** to navigate screens or pages generated by the mobile wallet application **113**, e.g., to select a form of electronic payment such as selecting a credit card **111**. Examples of web browsers **114** that may be used for this purpose include, for example, INTERNET EXPLORER, NETSCAPE NAVIGATOR, FIREFOX, OPERA, AVANT Browser, GOOGLE CHROME, and FLOCK. Non-web browser software that is also capable of displaying payment options and receiving consumer input utilizing the mobile communication device **110** may also be utilized for this purpose. Embodiments may also utilize a dedicated mobile wallet application **113** or other application capable of executing and navigating a mobile wallet application **113**. While various mobile communication devices and browsers **114** may be utilized, reference is made to a mobile communication device **110** and mobile wallet application **113** executing thereon.

[0035] According to one embodiment, the merchant **125** is an in-store or brick and mortar merchant. In these embodiments, the merchant **125** may utilize an electronic payment device **120** in the form of a Point Of Sale (POS) terminal. According to other embodiments, the merchant **125** utilizes an electronic payment device **120** in the form of a mobile communication device configured for processing electronic transactions so that a transaction involves multiple mobile communication devices. The electronic payment device **120**, whether a POS terminal or mobile communication device, includes or accesses a payment program or application **123** for generating transaction data **122** and communicating with the consumer's mobile communication device **110** via a temporary, close proximity or short range connection such as a NFC connection **160**.

[0036] When using a mobile communication device as the electronic payment device **120**, the merchant **125** can be in-store or at a remote location and accept payment using merchant and consumer mobile communication devices. For example, both the consumer **115** and the merchant **125** may be in the merchant store or office, or the consumer **115** and merchant **125** may be at a location other than the merchant store or office, e.g., at various residential, commercial and retail locations, offices, job sites, etc. Further, such mobile merchants **125** can accept payments at various times including at times during which a retail establishment of the merchant **125** is closed. For this purpose, the mobile payment application **152** can be downloaded onto the mobile device, and a web browser may execute on the merchant's mobile communications device to allow the merchant **125** to navigate screens or pages generated by the mobile payment application **123**. Embodiments may also utilize a dedicated mobile payment application or other application capable of executing and navigating a mobile payment application **123**. Thus, a merchant **125** who utilizes a mobile device for payment is not restricted to operating from a retail establishment. However, since such merchants **125** are mobile, they may conduct business from various locations at various times, including at or near at or near retail establishments during or after business hours. Examples of mobile payment applications **123** that can utilized or configured for use in embodiments include GOPAYMENT, available from Intuit Inc., CHARGE ANYWHERE Mobile POS software, Transaction Wireless and AIR CHARGE. For ease of explanation, reference is made to a consumer's mobile communication device **110** including a mobile wallet application **113** and a merchant's mobile communication device or electronic payment device **120** including a mobile payment application **123**, one example of which is GOPAYMENT.

[0037] The payment processor **135** provides services of processing transactions involving forms of electronic payment such as a credit card **111** and serves as an intermediary between the consumer **115** and an issuing bank (not illustrated in FIG. **1**). The issuing bank acts as a recipient of proceeds of the transaction. For this purpose, the payment processor **135** hosts or manages a merchant account **132** on behalf of the merchant **125**. The merchant account **132** allows the merchant **125** to accept payment using a credit card and other forms of payment. Examples of payment processors or payment processing systems **130** that provide these types of services include, for example, Innovative Merchant Solutions (an Intuit Inc. company), CHASE PAYMENTECH and EVALON.

[0038] In the illustrated embodiment, the merchant account **132** resides on the payment processor computer **130**, but the merchant account **132** may also reside on another computer that is accessed by the payment processor **130**. For example, the other computer may host a financial management system

(FMS), an example of which is an on-line accounting program such as quickbooks.com, available from Intuit, Inc. A merchant account **132** managed using the FMS can be updated by the payment processor computer **130**. Thus, it should be understood that FIG. **1** illustrates one system **100** configuration that may be utilized, and that one or more system components, such as the merchant account **132**, may be on different computers and/or on different networks.

[0039] The cloud computer, server or resource **140** (generally, cloud server) includes an authorization application or program (generally, authorization program **113**) and manages or hosts a database **146** including payment data **147** of respective consumers **115** that can be accessed by mobile communication devices **110** serving as mobile wallets. The "cloud" server may be one or multiple servers, but in the illustrated embodiment, at least one server includes payment data of respective consumers **115**, and "cloud" in embodiments refers to the cloud wallet server **140** and the payment processor computer **130** that serve as on-demand resources that may be utilized by various consumers **115** and merchants **125** to process respective electronic transactions.

[0040] Examples of networks **150***a-c* that may be utilized for communications between the mobile communication device **110** and the cloud wallet server **140**, between the electronic payment device **120** and the payment processor computer **130**, and between the payment processor computer **130** and the cloud wallet server **140** include but are not limited to a Local Area Network (LAN), a Wide Area Network (WAN), Metropolitan Area Network (MAN), a wireless network, other suitable networks capable of transmitting data, and a combination of such networks. For ease of explanation, reference is made to a network **150** generally, but various networks **150** and communication methods may be utilized.

[0041] Referring to FIG. **2**, and with continuing reference to FIG. **1**, a method **200** for processing an electronic transaction involving a mobile communication device **110** that serves as a mobile wallet comprises, at **202**, the electronic payment device **120** and the mobile communication device **110** sharing a secret or transaction specific authorization data or token **170** (without transmitting credit card data to the merchant **125**). According to embodiments, this is accomplished using a near field communications (NFC) **160** or other suitable close proximity connection (generally, NFC). For this purpose, the mobile communication device **110** and the electronic payment device **120** are equipped with respective NFC chips or cards **119**, **129** (generally, NFC chip), which are utilized to establish a NFC connection **160** (represented by arrows in FIG. **1**) with each other when they are brought together or sufficiently close to each other. According to embodiments, the mobile communication device **110** and electronic payment device **120** communicate with each other using a peer-to-peer configuration so that data can originate from or be generated by either of the mobile communication device **110** or electronic payment device **120** and be transmitted to the other via the NFC connection **160**.

[0042] Authorization data or an authorization token **170** (generally, authorization token) is generated and shared between the merchant's electronic payment device **120** and the consumer's mobile communication device **110**. Use of peer-to-peer communications between the electronic payment device **120** and the mobile communication device **110** is in contrast to certain systems that utilize restrictive or one-way communications (e.g., transmitting a tag from a mobile communication device to a merchant payment device) such that, as described in further detail below, embodiments provide a flexible system architecture that accommodates multi-directional communications between system components such that multiple components may generate an authorization token and transmit the authorization token to other system components for use in processing an electronic transaction.

[0043] At **204**, the authorization token **170** is transmitted from the mobile communication device **110** to the cloud wallet server **140**, and at **206**, transmitted from the electronic payment device **120** to the payment processor computer **130**, which presents the authorization token **170** to the cloud wallet server **140**. At **208**, the authorization program **143** of the cloud wallet server **140** looks up the received authorization token **170** in the database **146**, identifies the associated data **147** of the credit card **111** of the consumer **115** for which the authorization token **170** was generated, and sends the associated credit card data **147** to the payment processor computer **130** at **208**, which then processes electronic transaction, updates merchant account **132** and notifies merchant **125** as necessary at **210**. Further embodiments and aspects thereof are described with reference to FIGS. **3-11**. Embodiments in which the authorization token **170** is generated by the electronic payment device **120** of the merchant **125** are described with reference to FIGS. **3-6**, embodiments in which the authorization token **170** is generated by or using the mobile communication device **110** of the consumer **115** are described with reference to FIGS. **7-8**, and embodiments in which the authorization token **170** is generated by the cloud wallet server **140** are described with reference to FIGS. **9-10**.

Authorization Token Generated by Electronic Payment Device of Merchant/Payment Application

[0044] Referring to FIG. **3**, a system **300** constructed according to one embodiment comprises or involves one or more or all of the system components described above (aspects of which are not repeated), and the authorization token **170** that is generated by a merchant's electronic payment device **120**, e.g., by a payment application or program **125**, a controller of the NFC chip **129** or by a separate authorization token generator.

[0045] With further reference to FIG. **4**, and with continuing reference to FIG. **3**, a method **400** for processing an electronic transaction using a merchant-generated authorization token **170** comprises, at **402**, the merchant **125** generating invoice, receipt or transaction data **122** using electronic payment device **120** for purchase of item by the consumer **115** from the merchant **125** (at merchant store or from mobile merchant). Examples of transaction data **122** (generally, "transaction data") include merchant identification (MerchantID) (such as a merchant name, store number, location or zip code), a transaction identification (TransactionID), types of electronic payment accepted by the merchant (e.g., VISA, MASTERCARD, AMERICAN EXPRESS, electronic check, debit card, ACH, etc.).

[0046] At **404**, the payment application **123** executing on the electronic payment device **120** generates an authorization token **170**. According to one embodiment, the authorization token **170** is a random number. According to a further embodiment, the authorization token **170** embodies, includes or is encoded with transaction data **122** such as merchant identification (MerchantID) (merchant name, store number, location or zip code or other identifier), a transaction identification (TransactionID), types of electronic payment accepted by the merchant (e.g., VISA, MASTERCARD,

AMERICAN EXPRESS, electronic check, debit card, ACH, etc.), an invoice amount and, in certain embodiments, consumer discount/loyalty offers. For example, a discount or loyalty offer may offer a 2% credit or discount to the consumer **115** if the consumer **115** utilizes a credit card **111** of a certain issuer with whom the merchant **125** has a relationship. The credit or discount can be applied in real time during the transaction or issued later (e.g., in the form of a check or credit card credit) after the transaction has been completed.

[0047] At **406**, the consumer's mobile communication device **110** and the merchant's electronic payment device **120** brought into contact or in proximity with each other to establish a temporary connection, e.g., a NFC connection **160**, between the devices so they can communicate with each other. According to one embodiment, the electronic payment device **120** is a stationary POS terminal such that the mobile communication device **110** is brought into contact or in proximity with the POS terminal by the consumer **115**. According to another embodiment, the electronic payment device **120** is also a mobile communication device such that one or both of the mobile communication devices may be into contact or in proximity with the other.

[0048] At **408**, in certain embodiments, the merchant **125** verifies the identity of the consumer **115**. For this purpose, a photograph of the consumer **115** may be displayed to the merchant **125** on the merchant's electronic payment device **120** or on the consumer's mobile communication device **110**. For example, in one embodiment, the mobile wallet application **115** may be operable to access a photograph stored locally on the mobile communication device **110** after a NFC connection **160** is established. The initial or a new NFC connection may be utilized for this purpose of the photograph is displayed on the merchant's electronic payment device **120**.

[0049] In another embodiment, the consumer **115** logs into the cloud wallet server **140**, which stores the photograph in the database **146** with associated credit card data **147** of the consumer **110**, downloads the photograph to the mobile communication device **110**, which is then displayed to the merchant **125**. Other types of biometric data may also be utilized to verify the identity of the consumer **115** including fingerprints and voice samples acquired at the point of sale, which may be compared with fingerprints and voice samples previously provided by the consumer **115** and stored in the database **146** of the cloud wallet server **140**.

[0050] In further embodiments, the consumer may also allow contact information to be communicated to the electronic payment device **120** to allow the merchant **125** to communicate with the consumer **115** at a later time, e.g., so that the consumer **115** may receive promotional offers from the merchant **125**.

[0051] Continuing with FIG. **4**, at **410**, the payment application **123** executing on the electronic payment device **120** or a controller of the NFC chip **129** if so configured generates the authorization token **170**, which is transmitted from the electronic payment device **120** to the mobile communication **110** device via the temporary NFC connection **160**. As discussed above with reference to FIGS. **1-2**, the authorization token **170** may be a randomly generated number. The authorization token **170** may also be a use token. The authorization token **170**, or data transmitted with the authorization token **170**, may also indicate or be decoded to indicate transaction data **122**, e.g., which types of payment are accepted by the merchant **125**.

[0052] At **412**, the consumer **115** selects an electronic payment option (e.g., selects a credit card, checking account, etc.) based at least in part upon data **122** received from merchant **125** (if merchant specifies types of payment) and electronic payment option data **147** stored locally on mobile communication device **110** indicating which credit cards can be used, or by logging into consumer account hosted by the cloud wallet server **140** and accessing stored electronic payment options. For example, referring to FIG. **5**, the consumer may execute the mobile wallet application **113**, which generates a screen **500** displayed on the mobile communication device **110** with images or representations of the available payment options (e.g., credit cards **111***a-c*) that can be selected for payment. In the illustrated example, three credit cards **111** are displayed, but it will be understood that the consumer **110** may have other numbers of credit cards, other forms of electronic payment and combinations of electronic payments may be presented to the consumer **115**.

[0053] Referring again to FIGS. **3-4**, at **414**, the authorization token **170** and any additional data as necessary (e.g., transaction data **122** such as one or more of MerchantID, TransactionID, accepted payment options, invoice amount), are transmitted from mobile communication device **110** to the cloud wallet server **140** via network **150** and received at the cloud wallet server **140**.

[0054] According to one embodiment, the authorization token **170** as generated by the merchant's electronic payment device **120** is transmitted to the cloud wallet server **140** through the mobile communication device **140**. In other embodiments, the payment application **123** executing on the electronic payment device **120** or the mobile wallet application **113** executing on the mobile communication device **110** transforms or encodes the merchant-generated authorization token. The encoded authorization token **170** may embody or be encoded with transaction data **122**, and may be decoded by the cloud wallet server **140** using an appropriate key or decoding mechanism. The ability to encode and decode the authorization data provides for more flexibility and inclusion of additional information associated with the merchant **125** and/or transaction to ensure that the credit card data **147** to be utilized is utilized for payment is for the correct amount, e.g., if the invoice or receipt amount **122** is encoded within or transmitted with the authorization token **170**, and that the payment request is for a particular merchant **125** for that specified amount. Further, use of single-use authorization tokens **170** that are dynamically generated for a particular transaction provide for enhanced security compared to systems that assign and utilize the same data or tag to a consumer's mobile communication device **110** since loss or theft of that data or tag may result in fraudulent activity.

[0055] At **416**, the cloud wallet server **140** decodes the authorization token **170** if necessary and updates database **146** to indicate that consumer **115** authorizes payment made using selected payment option if that authorization token **170** is presented (or presented while satisfying pre-determined restrictions, conditions or limitations).

[0056] For example, referring to FIG. **6A**, the cloud wallet server **140** may store data **147** of credit cards or other forms of electronic payment of various consumers **115**. With credit cards, the credit card data may include one or more or all of the name of an issuer bank, a credit card number, expiration date, name as it appears on the credit card, and card verification code (CVC).

[0057] In the illustrated example, the cloud wallet server database **146** includes a table **600** having a columns **602***a*-**602***e* identifying consumers **115** and data **147** of their respective options for electronic payment. For example, the data **147** includes data (e.g., one or more of credit card number, expiration date, cardholder name, credit verification code, etc.) of three credit cards (CC**1**-**3**) for Consumer **1**, data of one credit card (CC**4**) for Consumer **2**, and data of two credit cards (CC**5**-**6**) for Consumer **3**. The database **146** may also store data **147** of other types of electronic payment that may be utilized such as electronic check data, ACH and other data.

[0058] FIG. **6**B further illustrates the database **146** including a table **610** structured for a particular consumer **115** to include columns indicating which authorization token **170** has been received for a particular payment option, and associated authorization token restrictions and transaction data **122**. For example, column **612***a* includes data specifying a consumer's payment option, e.g., credit cards, column **612***b* indicates that the cloud wallet server **140** has received authorization tokens **170** from the consumer's mobile communication device **110** for some, but not all of the credit cards. Column **612***c* indicates a transaction, invoice or receipt amount authorized to be charged on a credit card as determined by data transmitted with the authorization token **170** or when the authorization application **143** decoded an authorization token encoded with that data. Data in column **612***d* indicates when a token **170** was generated, and data in column **612***e* indicates the time the token **170** is valid such that the token **170** would have to be presented by a payment processor **130** within that time (e.g., 10 minutes, 30 minutes, 60 minutes) to request credit card data **147**, as explained in further detail below. Column **612***f* identifies the merchant for whom credit card data **147** can be released for payment.

[0059] It will be understood that table **610** may include some or all of these types of data for all or some of various types of electronic payment options, and that the table **610** is provided as an example of how embodiments may be implemented. For example, while FIG. **6**B illustrates a table **610** including data of a condition, restriction or limitation of a time during which an authorization token **170** is valid, other or additional conditions, restrictions and limitations may be imposed and recorded in the database **146**.

[0060] Referring again to FIGS. **3**-**4**, after generating the authorization token **170**, at **418**, the merchant **125** logs into an account with the payment processor computer **130** if necessary, and transmits the authorization token **170** from the electronic payment device **120** to the payment processor computer **130**. At **420**, the payment processor computer **130** decodes authorization token if necessary, authenticates itself to the cloud wallet server **140** as necessary, and transmits and presents the authorization token **170** to the cloud wallet server **140** to request data **147** of the credit card **111** selected by the consumer **115**.

[0061] At **422**, the authorization application or program **143** of the cloud wallet server **140** searches the database **146** (e.g., tables **600**, **610** shown in FIGS. **6**A-B) for data **147** linked to or associated with the authorization token **170** received from the payment processor computer **130**. At **424**, the authorization application or program **143** determines whether the authorization token **170** received from payment processor computer **130** matches an authorization token **170** that was received from the consumer's mobile communication device **100** and stored in the database **146**. If not, then the payment processor's request is denied at **426**, no credit card data **147** is provided by the cloud wallet server **140** to the payment processor computer **130**.

[0062] If so, then proceeding to FIG. **4**, **428**, the authorization engine **143** of the cloud wallet server **140** determines whether the authorization token **170** received from the payment processor computer **130** satisfies restrictions, conditions or limitations. If not, then at **430**, the payment processor's request is denied, no credit card data **147** is provided by the cloud wallet server **140** to the payment processor computer **130**. If so, then at **432**, the cloud wallet server **140** proceeds to **434** and retrieves data **147** (e.g., one or more of issuer bank name, credit card number, cardholder name, expiration date, CVD data etc.) of the elected payment option, encodes retrieved data **147** if necessary, and transmits selected payment option data **147** to the payment processor computer **130**.

[0063] For example, FIG. **4**, **428**, may involve the authorization token **170** being generated at 1:00 pm, and a restriction specifies that the token **170** is valid for only one hour and thus must be presented by the payment processor computer **130** within that time. If the payment processor computer **130** presents an authorization token **170** that matches a token **170** provided by the mobile communication device **110**, and it was presented within the one hour time frame, then the cloud wallet server **140** returns data **147** of the credit card **111** associated with that valid authorization token **170**, and the database can be updated to reflect that a valid authorization token **170** was presented and credit card data **147** was sent to the payment processor **130**. This ensures that the authorization token **170** that is generated is only valid for a limited time and thus reduces the chance that the same authorization token **170** may be utilized again or for a fraudulent purchase.

[0064] According to another embodiment, the authorization token **170** received at the cloud wallet server **140** from the mobile communication device **110** can be encoded with or be transmitted with data indicating an amount of an invoice or receipt. When the payment processor **130** presents the authorization token **170** to the cloud wallet server **140**, the cloud wallet server **140** may return data **147** of the credit card **111** associated with that valid authorization token **170** and authorize a charge for that specified invoice or receipt amount. Or, the invoice or receipt amount may be transmitted as part of or with the authorization token **170** to the payment processor **130**, which transmits the same authorization token **170** and/or invoice amount to the cloud wallet server **140**. If the authorization engine **143** determines that the invoice amount received from the payment processor computer **130** and the invoice amount received from the mobile communication device **110** match, then data **147** of the credit card **111** for that authorization token **170** can be sent by the cloud wallet server **140** to the payment processor computer **130**. If they do not match, then data **147** of the credit card **111** for that authorization token **170** is not provided to the payment processor **135**. In these cases, the payment processor **135** may inquire with the merchant **125** regarding the discrepancy. Thus, embodiments ensure that the correct amount is charged to the consumer's credit card **111**, and neither the merchant **125** nor the payment processor **135** can charge an incorrect or higher amount after the consumer **115** has left the merchant **125** or merchant store.

[0065] In yet another embodiment, the restriction or limitation can be based on an identification (e.g., name or store number) and/or location of the merchant **125** so that the cloud wallet server **140** authorizes use of credit card data **147** for

that identified merchant or location. In these embodiments, the authorization token **170** may have been encoded with or transmitted with data specifying that the authorization token **170** is valid for payment made to a particular merchant **125** identified by name, store number, location or other identifying data, and that presentation of the authorization token **170** on behalf of another merchant would not be accepted.

[0066] Embodiments may involve one or multiple types of restrictions, conditions or limitations and combinations thereof, and such data may be stored in table **610** or other table or data structure of database **146**. For example, embodiments may involve a time during which the authorization token **170** is valid and must be presented, an invoice amount, a merchant identification, both a time the authorization token **170** is valid and an invoice amount, both a time the token is valid and a merchant identification, both an invoice amount and a merchant identification, all of a time the authorization token **170** is valid, invoice amount and merchant identification, and other types, numbers and combination of restrictions. Further, it will be understood that depending on the type of restriction, the restriction may be selected by the authorization engine **143** according to a pre-determined standard or selected or specified by the consumer **115** as part of the process when the consumer **115** selects a credit card **111** to utilize. It will also be understood that such restrictions may be encoded within the authorization token **170**, which is decoded by the authorization engine **143** to determine the restrictions, transmitted with the authorization token **170** that is encoded with other data, or transmitted with an unencoded or unmodified authorization token **170** as generated by the merchant **115**.

[0067] Referring again to FIGS. **3-4**, if the authorization token **170** matches a token stored in the database **146**, and the token **170** satisfies any restrictions such that at **434**, the cloud wallet server **140** transmits selected payment option data **147** to the payment processor computer **130**, then at **436**, the payment processor computer **130** receives the data **147** and decodes it if necessary, and processes the electronic transaction. At **438**, the merchant account **132** is updated and a confirmation is sent to the electronic payment device **120** at **440**.

Authorization Token Generated Using Mobile Communication Device Of Consumer/Mobile Wallet Application

[0068] Referring to FIGS. **7-8**, a system **700** constructed according to another embodiment comprises or involves system components described above (aspects of which and embodiments are not repeated), and is utilized to execute a method **800** for processing an electronic transaction using authorization token **170** generated by a consumer's mobile communication device **110**. It will be understood that various aspects of the system **300** and method **400** described above also apply to the system **700** and method **800** described with reference to FIGS. **7-8**, and thus are not repeated in full detail. Further, it will be understood that while certain embodiments are described with reference to certain steps performed in a certain order or at a certain stage of a method, other steps may be performed in different orders and at different method stages.

[0069] In the illustrated embodiment, the method **800** comprises bringing the consumer's mobile communication device **110** and merchant's electronic payment device **120** into contact or in proximity with each other to establish a temporary connection (e.g., a NFC connection **160** as discussed above) between the mobile communication device **110** and electronic payment device **120**. At **804**, the consumer **115** may by verified by the merchant **125**, e.g., based on personal identification information of the consumer **115** such as a photograph or other biometric data acquired or displayed at the point of sale. At **806**, the merchant **125** generates data **122** of an invoice or receipt that includes one or more types of electronic transaction data such as MerchantID, TransactionID, Types of Payment Accepted, Invoice Total and consumer discount/loyalty offer. At **808**, the transaction data **122** is transmitted from the electronic payment device **120** to mobile communication device **110** via the same or a new NFC connection **160**, and at **810**, the mobile wallet application **113** displays a list of available payment options to the consumer **115** (e.g., as shown in FIG. **5**) so that the consumer **115** selects an option (e.g., selects a credit card, checking account, etc. accepted by merchant). The consumer's selection may be based at least in part upon one or more of data received from electronic payment device **120** (if merchant **125** specified an acceptable form of payment) and electronic payment option data **147** stored locally on mobile communication device **110** or accessed by logging into consumer account hosted by cloud wallet server **140**. At **812**, an authorization token **170** (such as random number and/or token embodying, including or encoded with or associated with one or one of transaction data and selected payment option data) is generated by the mobile wallet application **113** executing on mobile communication device **110**, and at **814**, the token **170** and additional data (e.g., selected payment option and authorized payment/invoice amount and restrictions, conditions or limitations as necessary) are transmitted from the mobile communication device **110** and received at cloud wallet server **140** via network **150**.

[0070] At **816**, the authorization engine **143** decodes the authorization token **170** if necessary and updates the database **146** to indicate that consumer **115** authorizes payment made using selected payment option upon presentation of the received authorization token **170** (or presented while satisfying pre-determined restrictions, conditions or limitations as discussed above with reference to FIG. 6B). At **818**, the authorization token **170** generated by the mobile communication device **110** and any additional merchant for transaction data as necessary (e.g., selected payment option and authorized payment/invoice amount and restrictions, conditions or limitations) are transmitted from the mobile communication device **110** and received at electronic payment device **120** of the merchant **125** using the same or new NFC connection **160**.

[0071] At **820**, the merchant **125** logs into an account at the payment processor computer **130**, and the authorization token **170** received from the mobile communication device **110** is transmitted from the electronic payment device **120** to the payment processor computer **130**, which decodes the authorization token **170** if necessary and presents the authorization token **130** to the cloud wallet server **140** to request data **147** of selected payment option at **822**. At **824**, the authorization engine **143** of the cloud wallet server **140** searches the database **146** to determine, at **826**, whether there is a match in the database **146**. If the authorization token **170** is not located, there is no match at **828** and the request for credit card data **147** is denied. If the presented authorization token **170** is located in the database **146**, there is a match, and at **830**, the authorization engine **143** determines whether the request satisfies any restrictions, conditions or limitations. If not, then at **832**, the request for credit card data **147** is denied.

If so, then the request is granted at **834**, and at **836**, the authorization engine **143** retrieves data **147** of the selected credit card **111** from the database **146**, encodes the data **147** if necessary, and transmits the data **147** to the payment processor computer **130** at **836**. At **838**, the payment processor computer **130** receives the credit card data **147**, decodes it if necessary, and processes electronic transaction. The merchant account **132** is updated at **840**, and confirmation of the electronic payment is sent from the payment processor computer **130** to the merchant electronic payment device at **842**.

Authorization Token Generated by Clond Wallet Server/ Cloud Wallet Application

[0072] Referring to FIGS. **9-10**, a system **900** constructed according to another embodiment comprises or involves system components described above (aspects of which and embodiments are not repeated), and is ntilized to execute a method **1000** for processing an electronic transaction using authorization token **170** generated by a cloud wallet server **140**. It will be understood that various aspects of the systems **300**, **700** and methods **400**,**800** described above also apply to the system **900** and method **1000** described with reference to FIGS. **9-10**, and thus are not repeated in full detail. Further, it will be understood that while certain embodiments are described with reference to certain steps performed in a certain order or at a certain stage of a method, other steps may be performed in different orders and at different method stages.

[0073] In the illustrated embodiment, the method **1000** comprises, at **1002**, the consumer's mobile communication device **110** and merchant's electronic payment device **120** brought into contact or in proximity with each other to establish temporary connection (e.g., NFC comection **160** between the mobile communication device **110** and the electronic payment device **120**. At **1004**, the merchant **125** may verify the identity of the consumer **115** using a photograph or other biometric data acquired or displayed at the point of sale. At **1006**, the merchant **125** generates electronic receipt, transaction data **122** that may include one or more of MerchantID, TransactionID, Types of Payment Accepted, Invoice Total, and a consumer discount/loyalty offer, and at **1008**, the data **122** is transmitted from the electronic payment device **120** to the mobile communication device **110** via the NFC comection **160**. At **1010**, the mobile wallet application **113** displays possible payment options to the consumer **115** (e.g., as described with reference to FIG. **5**) who selects an option, e.g., a particnlar credit card.

[0074] At **1012**, the transaction data **122** if applicable and the selected payment option are transmitted from the mobile communication device **110** to cloud wallet server **140**, and the authorization engine **143** generates an authorization token **170** at **1014**. The authorization token generated by the authorization engine **143** is transmitted from the clond wallet server **140** via network **150** to the mobile communication device **110** at **1016**.

[0075] At **1018**, the authorization token **170** is transmitted from the mobile communication device **110** to the electronic payment device **120** using the same or new NFC connection **160**, and at **1020**, the merchant **125** logs into an account at the payment processor computer **130** if necessary. The authorization token **170** received from the mobile communication device **110** is transmitted from the electronic payment device **120** to the payment processor computer **130**, which presents the authorization token **170** to the cloud wallet server **140** at **1022** to request data **147** of the credit card **111** selected by the consumer **115**. At **1024**, the authorization engine **143**, which generated the authorization token **170**, decodes the authorization token **170** if necessary and searches the database **146** for a match at **1026**. If not, the payment processor's request is denied at **1028**. If so, then at **1030**, the authorization engine **143** determines whether the request by the payment processor **130** satisfies any restrictions, conditions or limitations (generally, restrictions) such as one or more of a time restriction during which the authorization token is valid, payment of a specified amount, and payment to a particular merchant, as discussed above. If the restriction is not satisfied, then at **1032**, the request is denied, but if satisfied, at **1034**, the request is granted, and at **1036**, the authorization engine **143** retrieves data **147** of selected credit card **111**, encodes the data **147** if necessary, and transmits the data **147** to payment processor computer **130**. At **1038**, the payment processor computer **130** receives the requested credit card data **147**, decodes it if necessary, and processes the electronic transaction. At **1040**, the payment processor computer **130** updates the merchant account **132** as necessary, and at **1042**, sends a confirmation to merchant electronic payment device **120** that the transaction has been completed.

[0076] FIG. **11** generally illustrates components of a computing device **1100** that may be utilized to execute embodiments and that includes a memory **1110**, program instructions **1112**, a processor or controller **1120** to execute program instructions **1112**, a network or communications interface **1130**, e.g., for communications with a network or interconnect **1140** between such components. The memory **1110** may be or include one or more of cache, RAM, ROM, SRAM, DRAM, RDRAM, EEPROM and other types of volatile or non-volatile memory capable of storing data. The processor unit **1120** may be or include multiple processors, a single threaded processor, a multi-threaded processor, a multi-core processor, or other type of processor capable of processing data. Depending on the particular system component (e.g., whether the component is a computer or a hand held mobile communications device), the interconnect **1140** may include a system bus, LDT, PCI, ISA, or other types of buses, and the communications or network interface may, for example, be an Ethernet interface, a Frame Relay interface, or other interface. The network interface **1130** may be configured to enable a system component to communicate with other system components across a network which may be a wireless or various other networks. It should be noted that one or more components of computing device **1100** may be located remotely and accessed via a network. Accordingly, the system configuration provided in FIG. **11** is provided to generally illustrate how embodiments may be configured and implemented.

[0077] Method embodiments or certain steps thereof, may be embodied in a computer program product such as an application that can be downloaded to an electronic payment device of the merchant, to a mobile communication device of the merchant, and to a mobile communication device of the consumer. Method embodiments or certain steps thereof may also be carried out by execution of software instructions that are embodied in, or readable from, a tangible medium or computer-readable medium or carrier or article of manufacture, e.g., one or more of the fixed and/or removable data storage data devices and/or data communications devices connected to a computer. Carriers may be, for example, magnetic storage medium, optical storage medium and magneto-optical storage medium. Examples of carriers include, but are not limited to, a floppy diskette, a memory stick or a flash

drive, CD-R, CD-RW, CD-ROM, DVD-R, DVD-RW, or other carrier now known or later developed capable of storing data. The processor **1120** performs steps or executes program instructions **1112** within memory **1110** and/or embodied on the carrier to implement method embodiments.

[0078] Although particular embodiments have been shown and described, it shonld be understood that the above discussion is not intended to limit the scope of these embodiments. While embodiments and variations of the many aspects of the invention have been disclosed and described herein, such disclosure is provided for purposes of explanation and illustration only. Thus, varions changes and modifications may be made without departing from the scope of the claims.

[0079] Further, certain embodiments are described with reference to GOPAYMENT as one example of a mobile payment application that may be used by a merchant to accept payment using a mobile communication device, but it should be understood that other mobile payment applications may be used, and that embodiments may be implemented by modifying mobile payment applications such as GOPAYMENT or by providing embodiment as an add-on or separate application for use with an existing mobile payment application.

[0080] Moreover, while embodiments are described with reference to a credit card transaction and providing credit card data to a payment processor depending on the authorization token presented, embodiments may involve varions types of electronic payment such as debit, ATM and gift cards, eCheck, PAYPAL, etc.

[0081] While multiple embodiments and variations of the many aspects of the invention have been disclosed and described hercin, such disclosure is provided for purposes of illustration only. Where methods and steps described above indicate certain events occurring in certain order, those of ordinary skill in the art having the benefit of this disclosure would recognize that the ordering of certain steps may be modified and that such modifications are in accordance with the variations of the invention. Additionally, certain of the steps may be performed concurrently in a parallel process when possible, as well as performed sequentially.

[0082] Accordingly, embodiments are intended to exemplify alternatives, modifications, and equivalents that may fall within the scope of the claims.

1. A computer-implemented method for processing data related to an electronic trausaction involving a consumer and a merchant, the method comprising:

establishing a near field communication connection between an electronic payment device of the merchant and a mobile communication of the consumer when the electronic payment device and the mobile communication device are in contact with or located in proximity to each other;

receiving authorization data that is shared between the mobile communication device and the electronic payment device utilizing the near field communication connection, wherein data of an electronic payment instrument utilized by the consumer is not transmitted to the merchant; and

trausmitting the authorization data from the mobile communication device through a first network to a first computer hosting respective data of respective electronic payment instruments of respective consumers, and from the electronic payment device throngh a second network to a second computer of an electronic payment processor,

wherein the authorization data is presented by the second computer to the first computer to request electronic payment data of the consumer associated with the authorization data.

2. The method of claim **1**, the electronic payment device comprising a mobile communication device including a mobile payment application executing thereon, the respective mobile communication devices of the consumer and the merchant being utilized to establish the near field communication connection and generate or receive the authorization data.

3. The method of claim **2**, the mobile communication device of the merchant comprising a Smartphone.

4. The method of claim **2**, the respective mobile communication devices of the consumer and the merchant being located within a store or office of the merchant when the near field communication connection is established.

5. The method of claim **2**, the respective mobile communication devices of the consumer and the merchant being at a location that is remote relative to a store or office of the merchant when the near field connection is established.

6. The method of claim **1**, the electronic payment instrument data being received at the second computer in response to presenting the authorization data to the first computer, the second computer hosting or accessing a merchant account on behalf of the merchant to process the electronic transaction using the received electronic payment instrument data.

7. The method of claim **1**, the electronic payment device and the mobile communication device being connected to each other in a peer to peer configuration.

8. The method of claim **7**, the authorization data being generated by the electronic payment device of the merchant and transmitted from the electronic payment device to the mobile communication device and from the electronic payment device to the second computer.

9. The method of claim **7**, the authorization data being generated by the mobile communication device and transmitted from the mobile communication device to the electronic payment device and from the mobile communication device to the first computer.

10. The method of claim **1**, the authorization data being generated by the first computer and received at the mobile communication device from the first computer, and trausmitted from the mobile communication device to the electronic payment device.

11. The method of claim **1**, the authorization data comprising a random number.

12. The method of claim **1**, the authorization data being dynamic such that first authorization data generated for a first purchase by the consumer is different than second authorization data generated for a second purchase by the consumer.

13. The method of claim **1**, the authorization data comprising an authorization token.

14. The method of claim **13**, the authorization token being usable for a single electronic transaction.

15. The method of claim **13**, the authorization token being valid to request electronic payment instrument data for a pre-determined limited time.

16. The method of claim **1**, the same authorization data shared between the mobile communication device and the electronic payment device being trausmitted from the electronic payment device to the second computer, from the mobile communication device to the first computer, aud from the second computer to the first computer when requesting electronic payment instrument data.

17. The method of claim **1**, the mobile communication device of the consumer comprising a mobile wallet, and the first computer comprising a cloud computing resource accessible by a plurality of consumers and payment processors.

18. The method of claim **17**, the electronic payment device of the merchant comprising a mobile payment application, wherein the transaction is completed based at least in part upon interaction between the mobile wallet and the mobile payment application.

19. The method of claim **1**, receiving from the electronic payment device at the mobile communication device through the near field communication connection, an incentive, offer or advertisement related to a form or type of electronic payment instrument available to be selected by the consumer using the mobile communication device.

20. The method of claim **19**, the incentive, offer or advertisement comprising a coupon or discount if the consumer utilizes an electronic payment instrument a pre-determined issuer bank.

21. The method of claim **1**, the electronic payment instrument comprising a credit card.

22. A computer-implemented method for processing data related to an electronic transaction involving a consumer and a merchant, the method comprising:

establishing a near field communication connection between an electronic payment device of the merchant and a mobile communication of the consumer when the electronic payment device and the mobile communication device are in contact with or located in proximity to each other;

generating authorization data embodying data of a transaction involving the consumer and the merchant, wherein data of an electronic payment instrument utilized by the consumer is not transmitted to the electronic payment device; and

transmitting the authorization data from the mobile communication device through a first network to a first computer hosting respective data of respective electronic payment instruments respective consumers, and from the electronic payment device through a second network to a second computer of an electronic payment processor,

wherein the authorization data is presented by the second computer to the first computer to request electronic payment data of the consumer associated with the authorization data.

23. The method of claim **22**, the authorization data being encoded with the transaction data.

24. The method of claim **23**, the authorization data being encoded with transaction data comprising at least one of a merchant identification, a transaction identification, a transaction amount, and accepted electronic payment instruments.

25. The method of claim **23**, wherein the authorization data is decoded by the first computer to determine electronic payment instrument data corresponding to the authorization data, the determined electronic payment instrument data being transmitted from the first computer to the second computer.

26. The method of claim **22**, the transaction data comprising at least one of a merchant identification, a transaction identification, a transaction amount, and accepted electronic payment instruments.

27. The method of claim **22**, the electronic payment device comprising a mobile communication device including a mobile payment application executing thereon, the respective mobile communication devices of the consumer and the merchant being utilized to establish the near field communication connection.

28. The method of claim **27**, the mobile communication device of the merchant comprising a Smartphone.

29. The method of claim **27**, the respective mobile communication devices of the consumer and the merchant being at a location that is remote relative to a store or office of the merchant when the near field connection is established.

30. The method of claim **22**, the electronic payment instrument data being received at the second computer in response to presenting the authorization data to the first computer, the second computer hosting or accessing a merchant account on behalf of the merchant to process the electronic transaction using the received electronic payment instrument data.

31. The method of claim **22**, the electronic payment device and the mobile communication device being connected to each other in a peer to peer configuration.

32. The method of claim **31**, the authorization data being generated by the electronic payment device of the merchant and transmitted from the electronic payment device to the mobile communication device and from the electronic payment device to the second computer.

33. The method of claim **31**, the transaction data being received by the mobile communication device, the authorization data being generated by the mobile communication device and transmitted from the mobile communication device to the electronic payment device and from the mobile communication device to the first computer.

34. The method of claim **22**, the transaction data being received by the first computer through the mobile communication device from the electronic payment device, the authorization data being generated by the first computer, transmitted from the first computer and received at the mobile communication device, and transmitted from the mobile communication device to the electronic payment device, and from the electronic payment device to the second computer.

35. The method of claim **22**, the authorization data being dynamic such that first authorization data generated for a first purchase by the consumer is different than second authorization data generated for a second purchase by the consumer.

36. The method of claim **22**, the authorization data comprising an authorization token.

37. The method of claim **36**, the authorization token being usable for a single electronic transaction.

38. The method of claim **36**, the authorization token being valid to request electronic payment instrument data for a limited time.

39. The method of claim **22**, the mobile communication device of the consumer comprising a mobile wallet, and the first computer comprising a cloud computing resource accessible by a plurality of consumers and payment processors.

40. The method of claim **22**, the electronic payment device of the merchant comprising a mobile payment application, wherein the transaction is completed based at least in part upon interaction between the mobile wallet and the mobile payment application.

41. The method of claim **22**, receiving from the electronic payment device at the mobile communication device through the near field communication connection, an incentive or advertisement related to an electronic payment instrument available to be selected by the consumer using the mobile communication device.

42. The method of claim **41**, the incentive or advertisement comprising a conpon or discount if the consumer utilizes a credit card of a pre-determined issuer bank.

43. The method of claim **22**, the electronic payment instrument utilized by the consumer comprising a credit card.

44. A computer-implemented method for processing data related to an electronic transaction involving a consumer and a merchant, the method comprising:

establishing a near field communication connection between an electronic payment device of the merchant and a mobile communication of the consumer when the electronic payment device and the mobile communication device are in contact with or located in proximity to each other;

generating authorization data, the authorization data being shared between the mobile communication device and the electronic payment device utilizing the near field communication connection, wherein data of an electronic payment instrument utilized by the consumer is not transmitted to the merchant; and

transmitting the authorization data from the mobile communication device through a first network to a first computer hosting respective data of respective electronic payment instruments of respective consumers;

storing the authorization data in a database of or accessed by the first computer to associate the authorization data and electronic payment instrument data of the consumer;

transmitting the authorization data from the electronic payment device through a second network to a second computer of an electronic payment processor;

transmitting the authorization data from the second computer through a third network to the first computer to request electronic payment data of the consumer;

searching the database to determine electronic payment data corresponding to the authorization data received at the first computer from the second computer;

transmitting the determined electronic payment data from the first computer to the second computer;

completing the transaction utilizing the second computer.

45. A computer-implemented method for processing data related to an electronic transaction involving a consumer and a merchant, the method comprising:

establishing a near field communication connection between an electronic payment device of the merchant and a mobile communication of the consumer when the electronic payment device and the mobile communication device are in contact with or located in proximity to each other;

generating authorization data, the authorization data being encoded with data of a transaction involving the consumer and the merchant, the authorization data being shared between the mobile communication device and the electronic payment device utilizing the near field communication connection, wherein data of an electronic payment instrument utilized by the consumer is not transmitted to the merchant; and

transmitting the authorization data from the mobile communication device through a first network to a first computer hosting respective data of respective electronic payment instruments of respective consumers;

decoding the authorization data at the first computer;

storing the authorization data and associated transaction data in a database of or accessed by the first computer to associate the authorization data, the transaction data and the electronic payment instrument data of the consumer;

transmitting the authorization data from the electronic payment device through a second network to a second computer of an electronic payment processor;

transmitting the authorization data and transaction data from the second computer through a third network to the first computer to request electronic payment data of the consumer;

decoding the authorization data at the first computer;

searching the database to determine electronic payment data and transaction data corresponding to the authorization data received at the first computer from the second computer;

comparing the transaction data stored in the database and the transaction data received from the second computer;

if the transaction data received from the second computer matches the transaction data stored in the database, transmitting the determined electronic payment data from the first computer to the second computer; and

completing the transaction utilizing the second computer.

46-63. (canceled)

* * * * *

US 20120296741A1

(19) **United States**

(12) **Patent Application Publication**

DYKES

(10) **Pub. No.: US 2012/0296741 A1**

(43) **Pub. Date: Nov. 22, 2012**

(54) **CLOUD BASED ELECTRONIC WALLET**

(75) Inventor: **Robert DYKES**, San Jose, CA (US)

(73) Assignee: **VERIFONE, INC.**, San Jose, CA (US)

(21) Appl. No.: **13/468,686**

(22) Filed: **May 10, 2012**

Related U.S. Application Data

(60) Provisional application No. 61/487,787, filed on May 19, 2011.

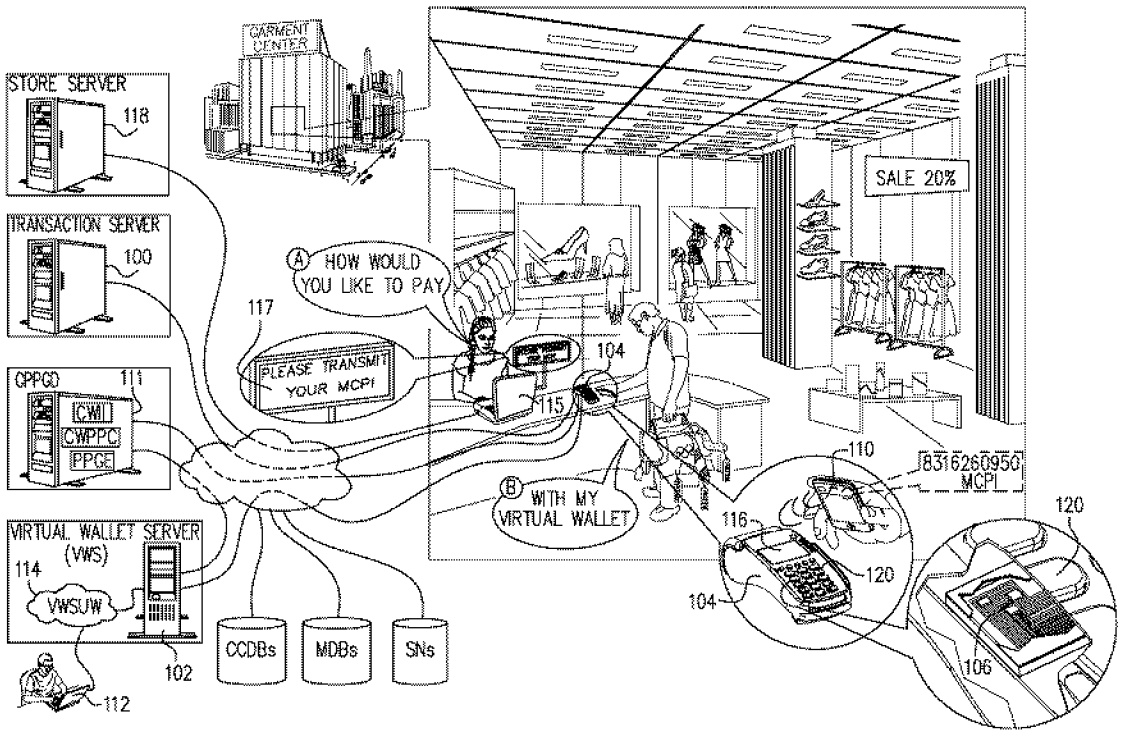
Publication Classification

(51) **Int. Cl.**
G06Q 20/20 (2012.01)
G06Q 30/02 (2012.01)

(52) **U.S. Cl.** **705/14.53**; 705/16

(57) **ABSTRACT**

A payment system including a transaction server, a virtual wallet server (VWS), at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN), but not purchaser payment particulars, to at least the VWS and at least one mobile communicator communicating a mobile communicator presence indicator (MCPI) but neither the purchaser WPIN nor the purchaser payment particulars to the at least one point of sale device.



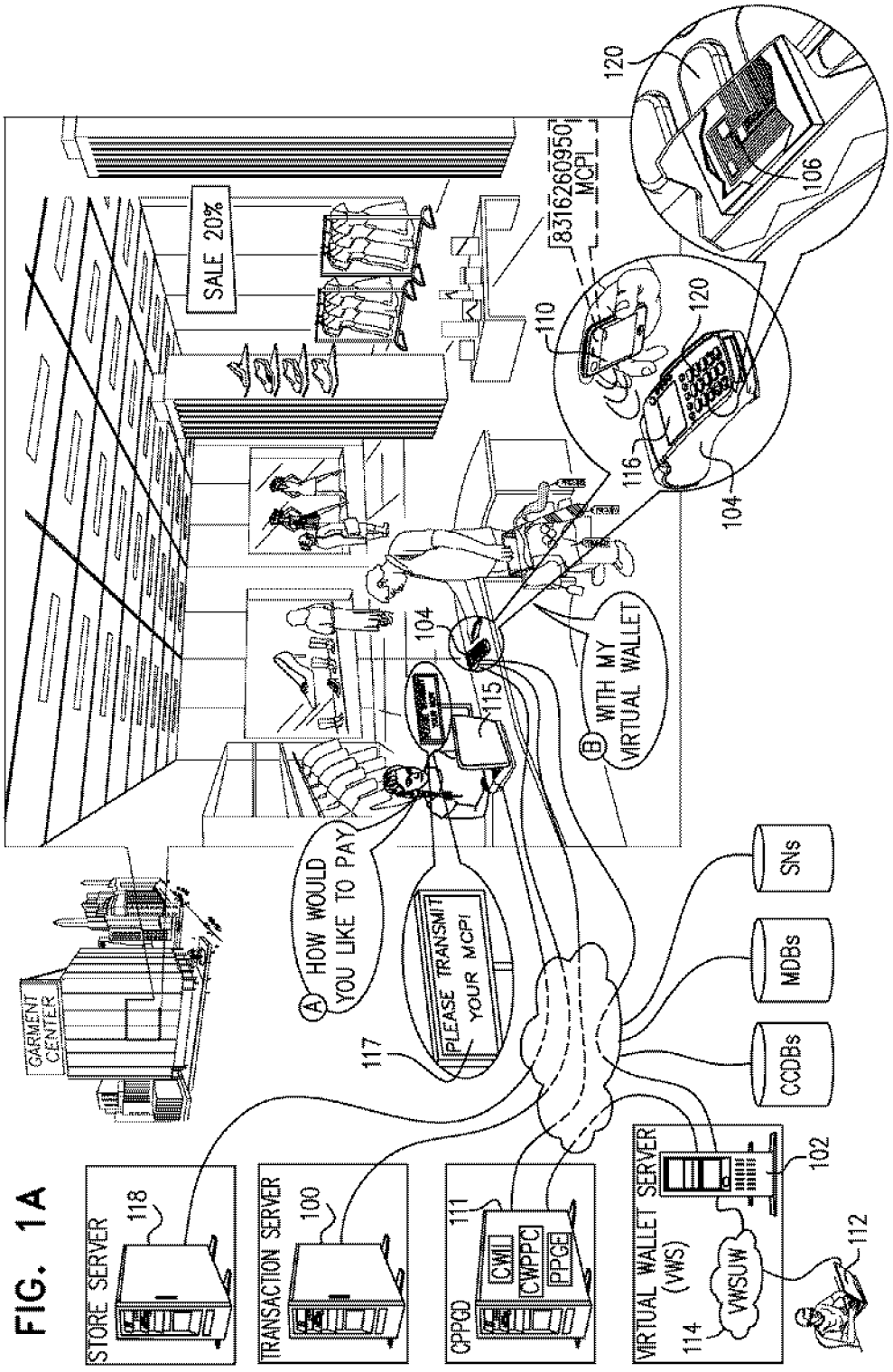

SALE 20%
8316260950
MCPI
120
106
110
120
116
104
104
115
HOW WOULD YOU LIKE TO PAY
WITH MY VIRTUAL WALLET
PLEASE TRANSMIT YOUR MCPI
117
GARMENT CENTER
STORE SERVER
118
TRANSACTION SERVER
100
CPPCD
111
CWLL
CWPPC
PPGE
VIRTUAL WALLET SERVER (VWS)
114
VWSUW
102
112
CCDBs
MDBs
SNs

FIG. 1A

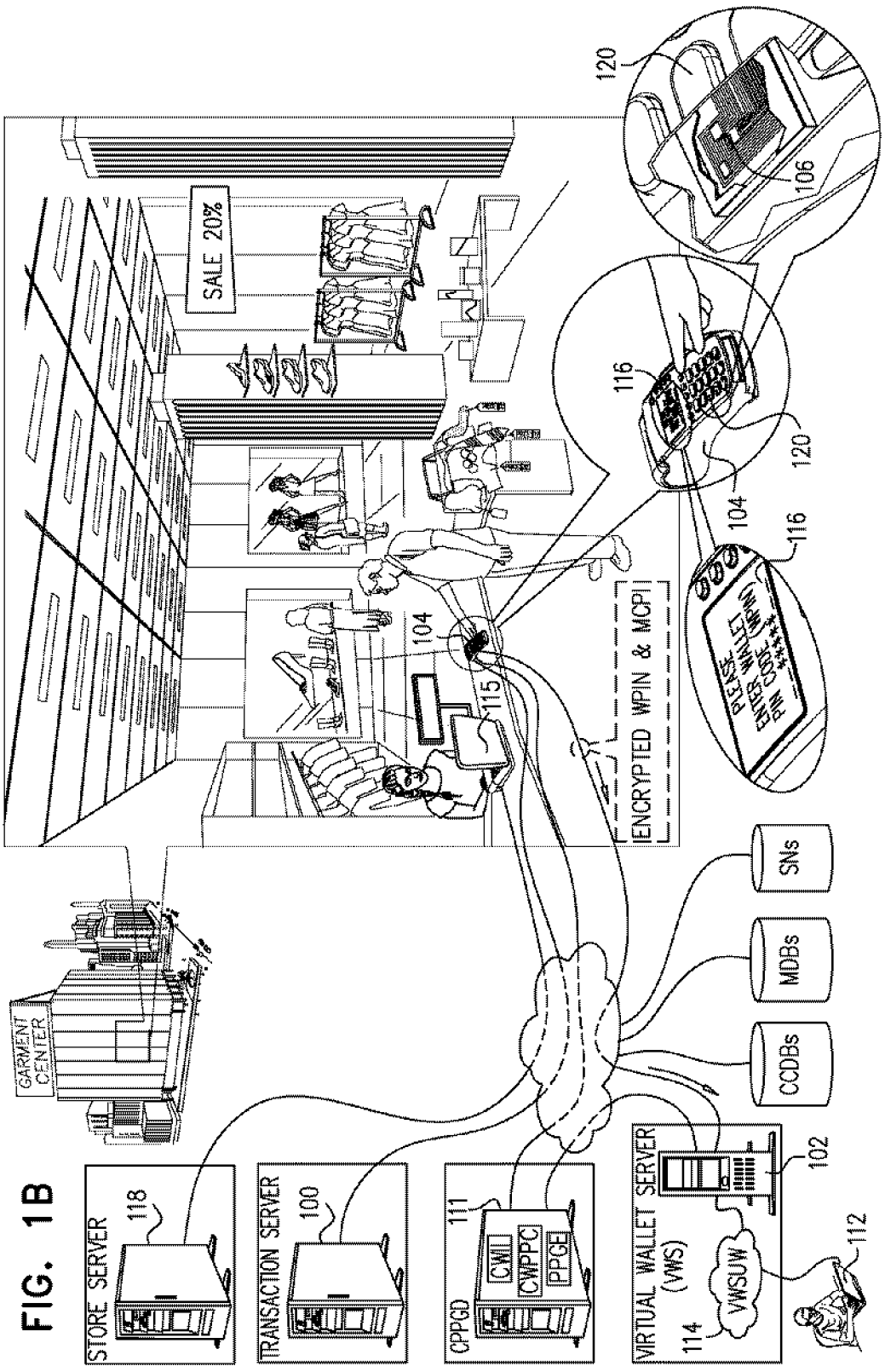

STORE SERVER
118
TRANSACTION SERVER
100
CPPGD
111
CWII
CWPPC
PPGE
VIRTUAL WALLET SERVER
(VWS)
114
VWSUW
102
112
CCDBs
MDBs
SNs
GARMENT CENTER
SALE 20%
104
115
ENCRYPTED WPIN & MCPI
116
120
106

FIG. 1B

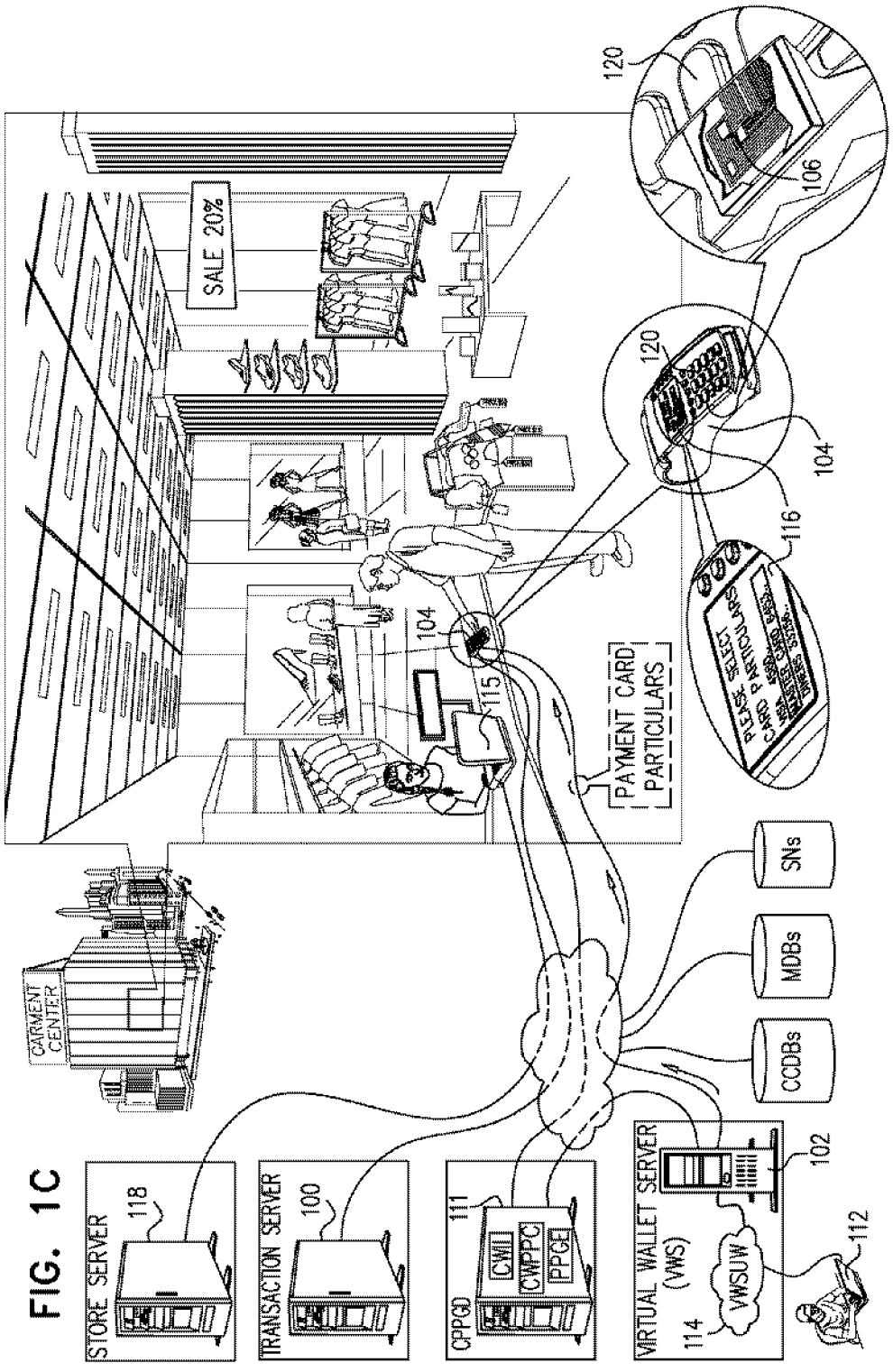

SALE 20%
120
106
120
104
116
104
115
PAYMENT CARD PARTICULARS
CARMENT CENTER
SNs
MDBs
CCDBs
VIRTUAL WALLET SERVER (VWS)
114
VWSUW
102
112
STORE SERVER
118
TRANSACTION SERVER
100
CPPGD
111
CWI
CWPPC
PPGE

FIG. 1C

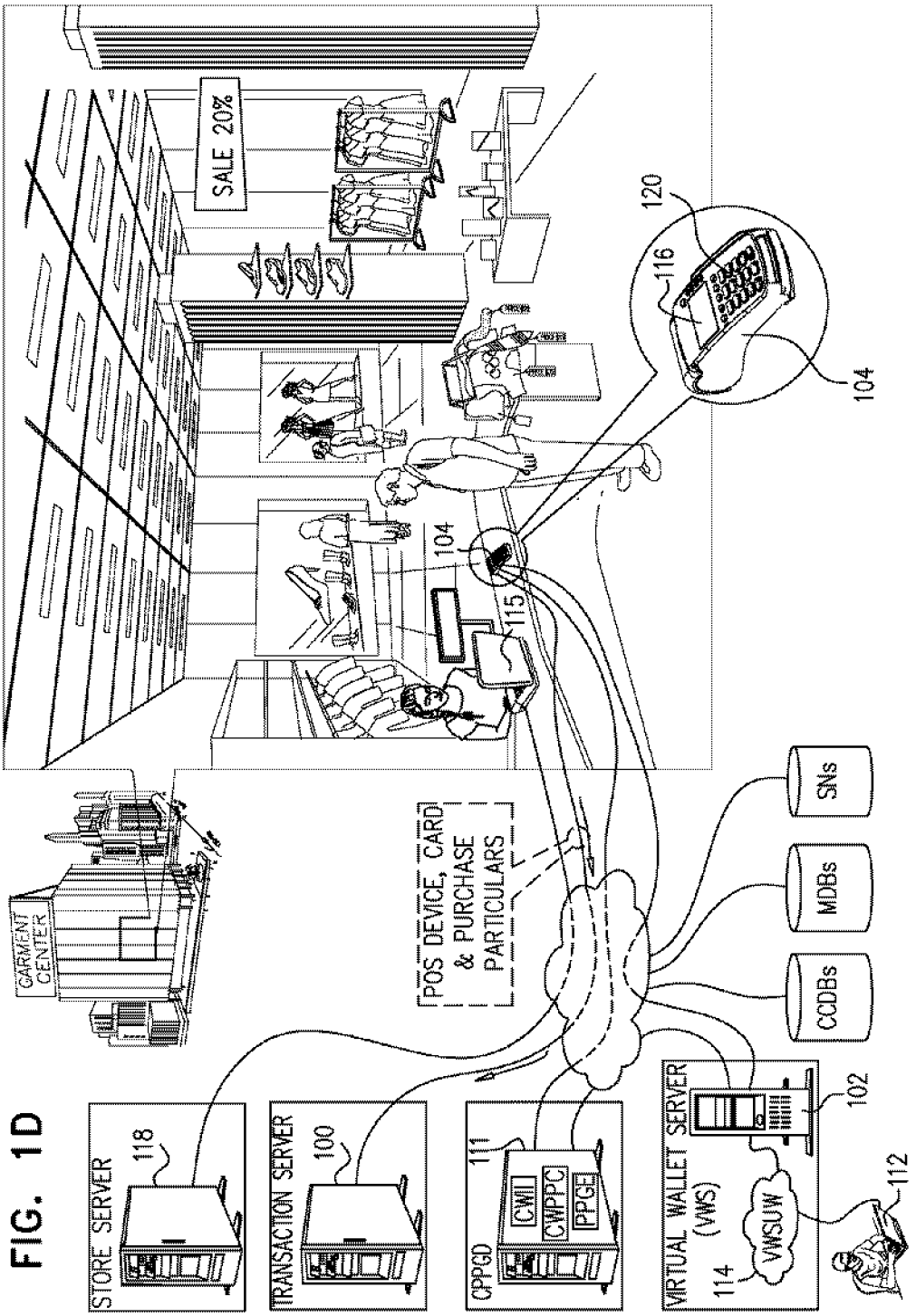

SALE 20%
104
115
120
116
104
GARMENT CENTER
[POS DEVICE, CARD] & PURCHASE PARTICULARS
SNs
MDBs
CCDBs
STORE SERVER
118
TRANSACTION SERVER
100
CPPGD
111
CWI
CWPPC
PPGE
VIRTUAL WALLET SERVER (VWS)
114
VWSUW
102
112

FIG. 1D

FIG. 2

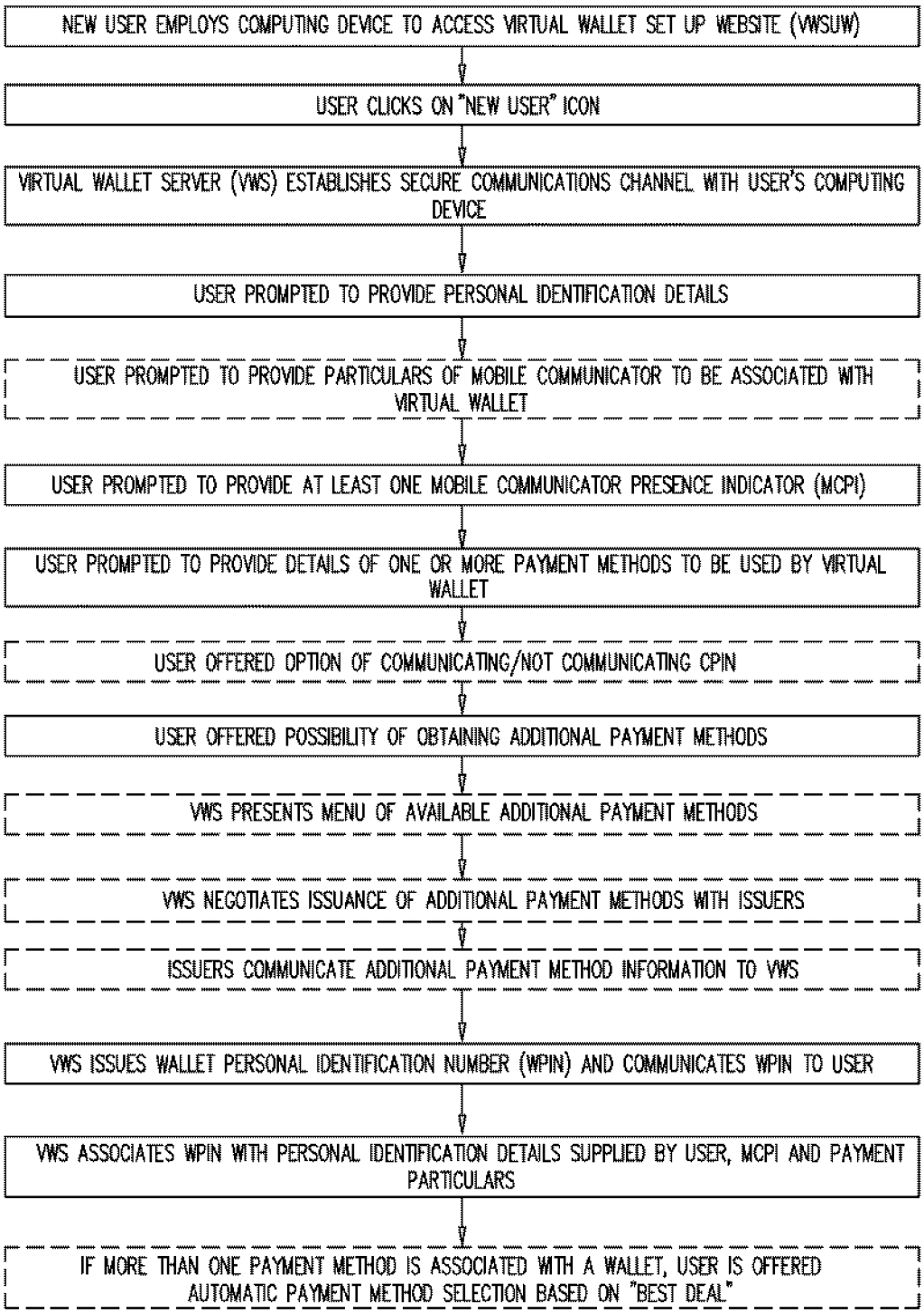

NEW USER EMPLOYS COMPUTING DEVICE TO ACCESS VIRTUAL WALLET SET UP WEBSITE (VWSUW)
USER CLICKS ON "NEW USER" ICON
VIRTUAL WALLET SERVER (VWS) ESTABLISHES SECURE COMMUNICATIONS CHANNEL WITH USER'S COMPUTING DEVICE
USER PROMPTED TO PROVIDE PERSONAL IDENTIFICATION DETAILS
USER PROMPTED TO PROVIDE PARTICULARS OF MOBILE COMMUNICATOR TO BE ASSOCIATED WITH VIRTUAL WALLET
USER PROMPTED TO PROVIDE AT LEAST ONE MOBILE COMMUNICATOR PRESENCE INDICATOR (MCPI)
USER PROMPTED TO PROVIDE DETAILS OF ONE OR MORE PAYMENT METHODS TO BE USED BY VIRTUAL WALLET
USER OFFERED OPTION OF COMMUNICATING/NOT COMMUNICATING CPIN
USER OFFERED POSSIBILITY OF OBTAINING ADDITIONAL PAYMENT METHODS
VWS PRESENTS MENU OF AVAILABLE ADDITIONAL PAYMENT METHODS
VWS NEGOTIATES ISSUANCE OF ADDITIONAL PAYMENT METHODS WITH ISSUERS
ISSUERS COMMUNICATE ADDITIONAL PAYMENT METHOD INFORMATION TO VWS
VWS ISSUES WALLET PERSONAL IDENTIFICATION NUMBER (WPIN) AND COMMUNICATES WPIN TO USER
VWS ASSOCIATES WPIN WITH PERSONAL IDENTIFICATION DETAILS SUPPLIED BY USER, MCPI AND PAYMENT PARTICULARS
IF MORE THAN ONE PAYMENT METHOD IS ASSOCIATED WITH A WALLET, USER IS OFFERED AUTOMATIC PAYMENT METHOD SELECTION BASED ON "BEST DEAL"

FIG. 3A

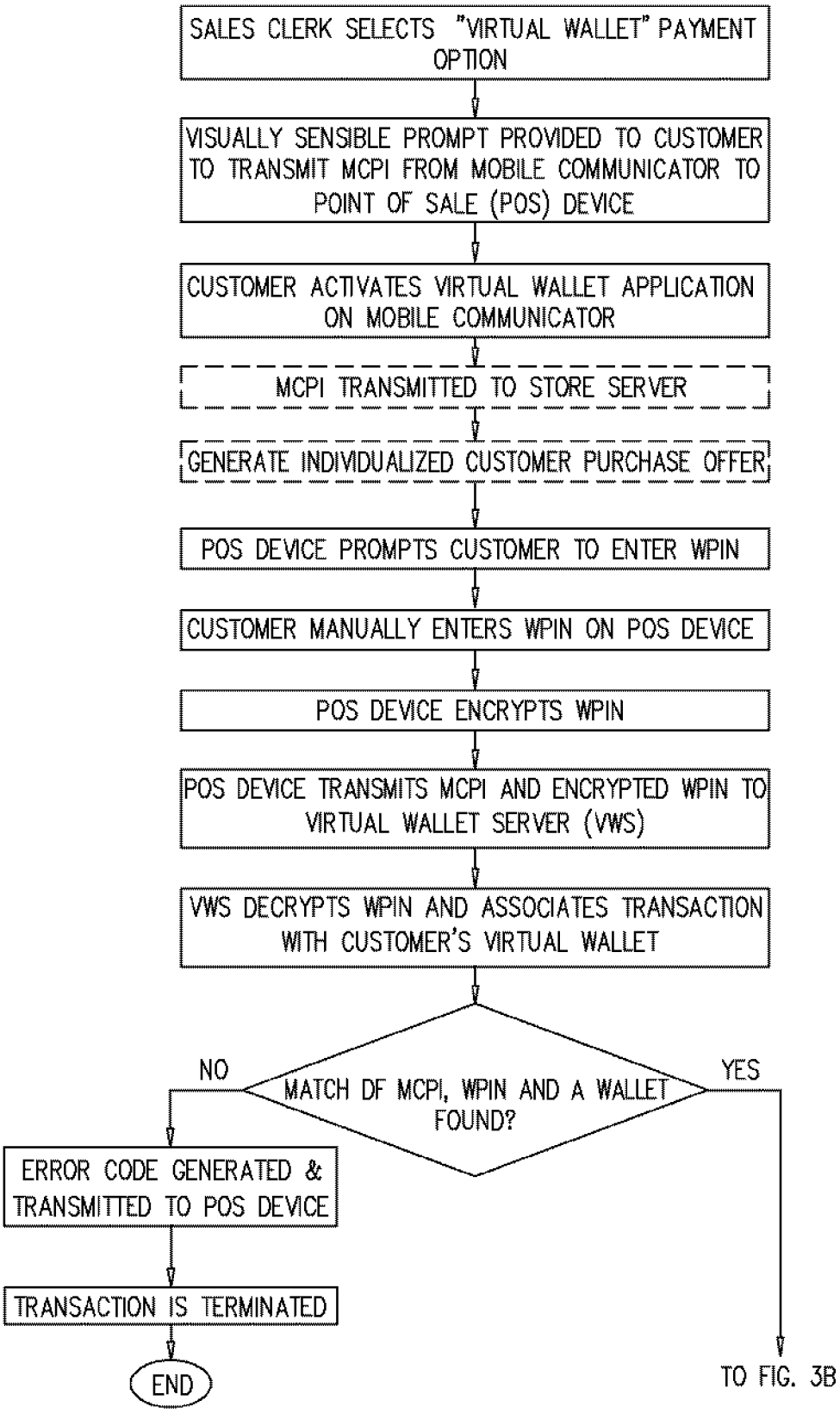

SALES CLERK SELECTS "VIRTUAL WALLET" PAYMENT OPTION
VISUALLY SENSIBLE PROMPT PROVIDED TO CUSTOMER TO TRANSMIT MCPI FROM MOBILE COMMUNICATOR TO POINT OF SALE (POS) DEVICE
CUSTOMER ACTIVATES VIRTUAL WALLET APPLICATION ON MOBILE COMMUNICATOR
MCPI TRANSMITTED TO STORE SERVER
GENERATE INDIVIDUALIZED CUSTOMER PURCHASE OFFER
POS DEVICE PROMPTS CUSTOMER TO ENTER WPIN
CUSTOMER MANUALLY ENTERS WPIN ON POS DEVICE
POS DEVICE ENCRYPTS WPIN
POS DEVICE TRANSMITS MCPI AND ENCRYPTED WPIN TO VIRTUAL WALLET SERVER (VWS)
VWS DECRYPTS WPIN AND ASSOCIATES TRANSACTION WITH CUSTOMER'S VIRTUAL WALLET
MATCH OF MCPI, WPIN AND A WALLET FOUND?
NO
YES
ERROR CODE GENERATED & TRANSMITTED TO POS DEVICE
TRANSACTION IS TERMINATED
END
TO FIG. 3B

FIG. 3B

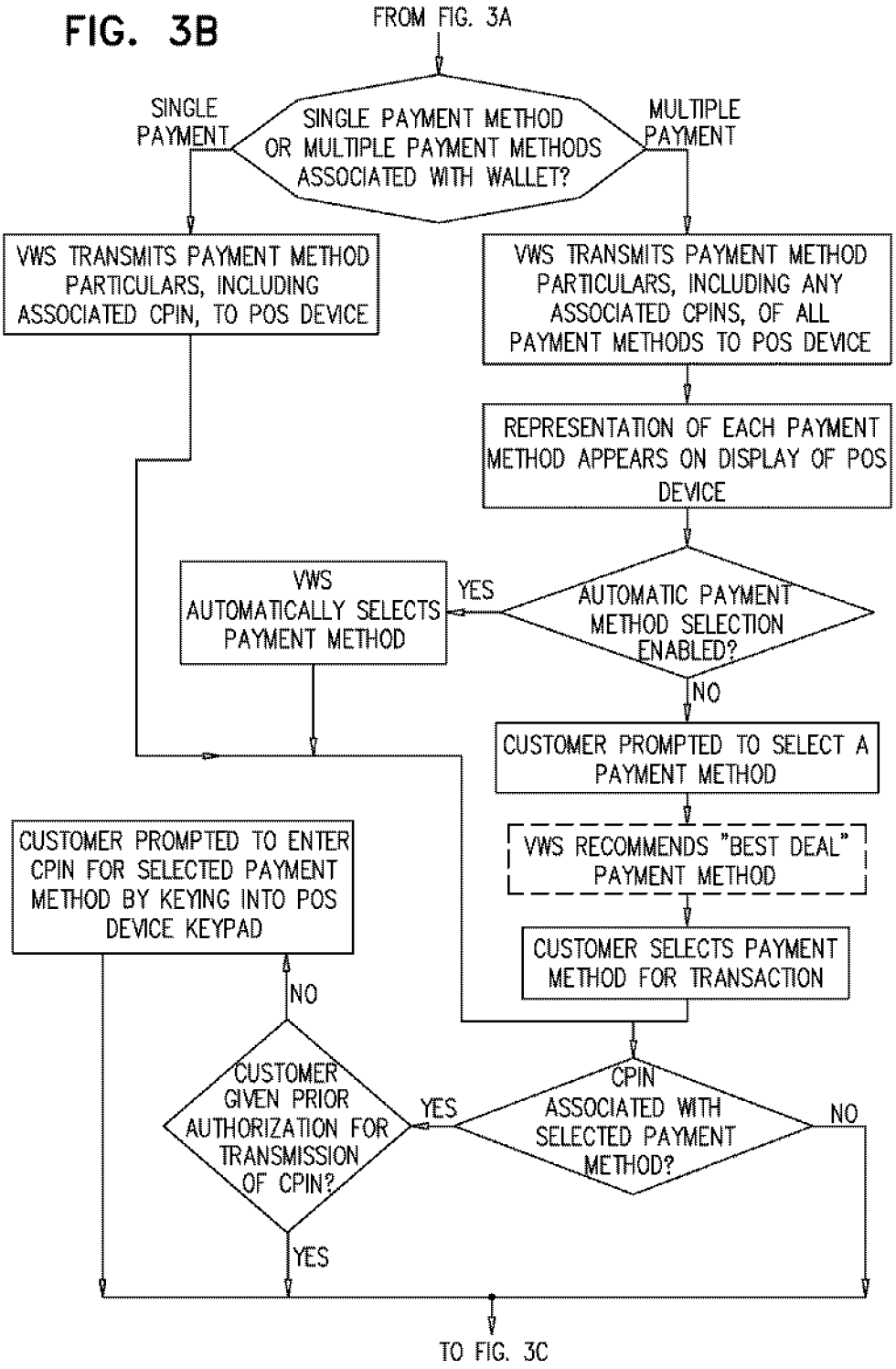

FROM FIG. 3A
SINGLE PAYMENT METHOD OR MULTIPLE PAYMENT METHODS ASSOCIATED WITH WALLET?
SINGLE PAYMENT
MULTIPLE PAYMENT
VWS TRANSMITS PAYMENT METHOD PARTICULARS, INCLUDING ASSOCIATED CPIN, TO POS DEVICE
VWS TRANSMITS PAYMENT METHOD PARTICULARS, INCLUDING ANY ASSOCIATED CPINS, OF ALL PAYMENT METHODS TO POS DEVICE
REPRESENTATION OF EACH PAYMENT METHOD APPEARS ON DISPLAY OF POS DEVICE
AUTOMATIC PAYMENT METHOD SELECTION ENABLED?
YES
VWS AUTOMATICALLY SELECTS PAYMENT METHOD
NO
CUSTOMER PROMPTED TO SELECT A PAYMENT METHOD
VWS RECOMMENDS "BEST DEAL" PAYMENT METHOD
CUSTOMER SELECTS PAYMENT METHOD FOR TRANSACTION
CPIN ASSOCIATED WITH SELECTED PAYMENT METHOD?
YES
NO
CUSTOMER GIVEN PRIOR AUTHORIZATION FOR TRANSMISSION OF CPIN?
NO
CUSTOMER PROMPTED TO ENTER CPIN FOR SELECTED PAYMENT METHOD BY KEYING INTO POS DEVICE KEYPAD
YES
TO FIG. 3C

FIG. 3C

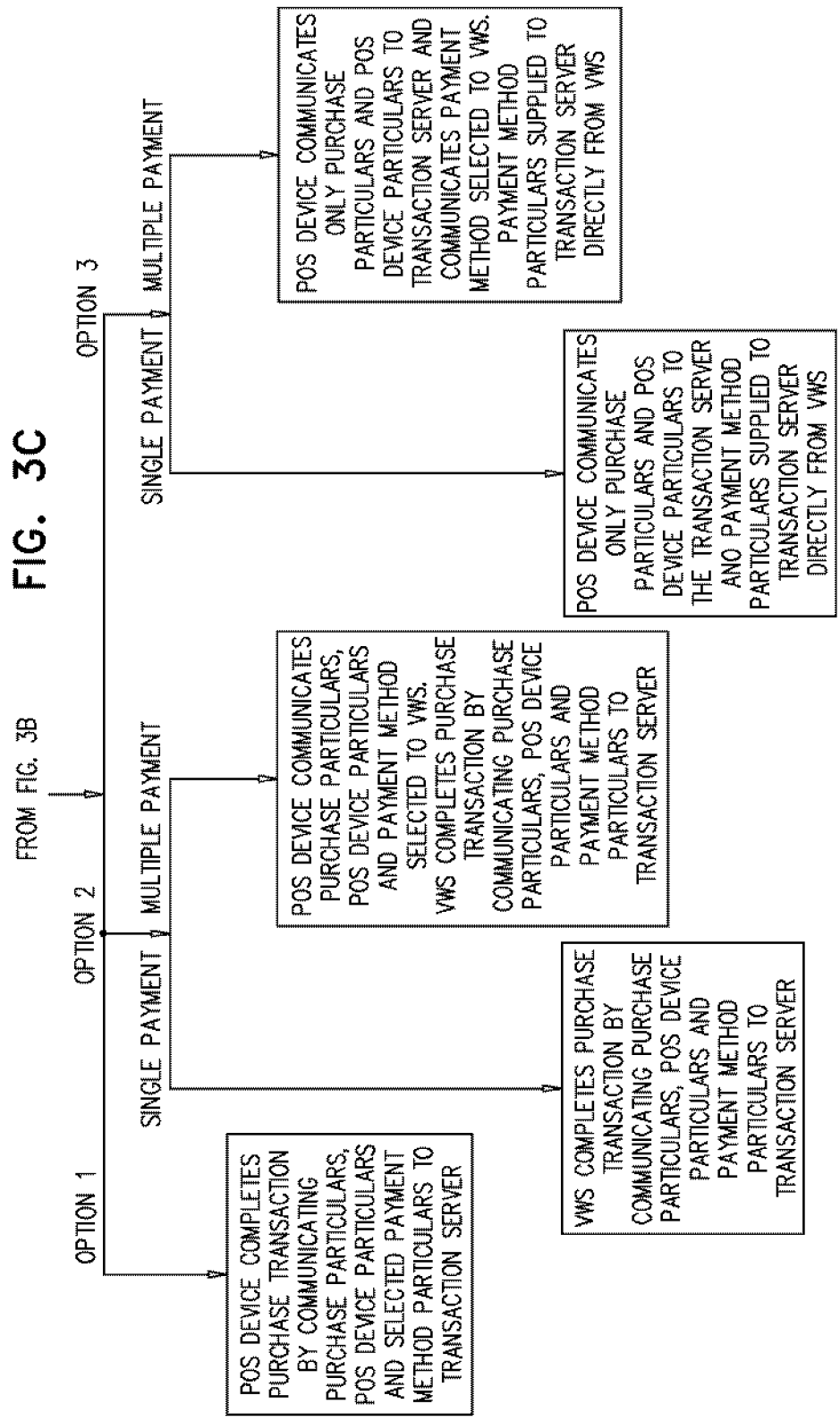
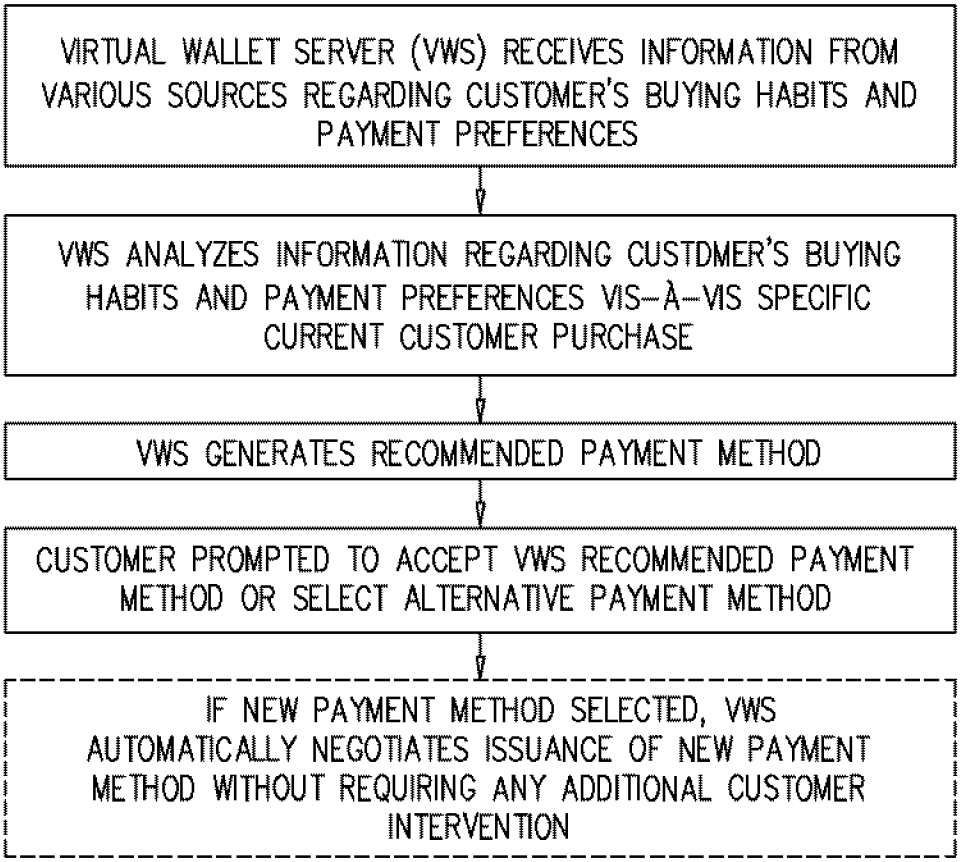

FROM FIG. 3B
OPTION 1
POS DEVICE COMPLETES PURCHASE TRANSACTION BY COMMUNICATING PURCHASE PARTICULARS, POS DEVICE PARTICULARS AND SELECTED PAYMENT METHOD PARTICULARS TO TRANSACTION SERVER
OPTION 2
SINGLE PAYMENT
VWS COMPLETES PURCHASE TRANSACTION BY COMMUNICATING PURCHASE PARTICULARS, POS DEVICE PARTICULARS AND PAYMENT METHOD PARTICULARS TO TRANSACTION SERVER
MULTIPLE PAYMENT
POS DEVICE COMMUNICATES PURCHASE PARTICULARS, POS DEVICE PARTICULARS AND PAYMENT METHOD SELECTED TO VWS. VWS COMPLETES PURCHASE TRANSACTION BY COMMUNICATING PURCHASE PARTICULARS, POS DEVICE PARTICULARS AND PAYMENT METHOD PARTICULARS TO TRANSACTION SERVER
OPTION 3
SINGLE PAYMENT
POS DEVICE COMMUNICATES ONLY PURCHASE PARTICULARS AND POS DEVICE PARTICULARS TO THE TRANSACTION SERVER AND PAYMENT METHOD PARTICULARS SUPPLIED TO TRANSACTION SERVER DIRECTLY FROM VWS
MULTIPLE PAYMENT
POS DEVICE COMMUNICATES ONLY PURCHASE PARTICULARS AND POS DEVICE PARTICULARS TO TRANSACTION SERVER AND COMMUNICATES PAYMENT METHOD SELECTED TO VWS. PAYMENT METHOD PARTICULARS SUPPLIED TO TRANSACTION SERVER DIRECTLY FROM VWS

FIG. 4


VIRTUAL WALLET SERVER (VWS) RECEIVES INFORMATION FROM VARIOUS SOURCES REGARDING CUSTOMER'S BUYING HABITS AND PAYMENT PREFERENCES
VWS ANALYZES INFORMATION REGARDING CUSTDMER'S BUYING HABITS AND PAYMENT PREFERENCES VIS-À-VIS SPECIFIC CURRENT CUSTOMER PURCHASE
VWS GENERATES RECOMMENDED PAYMENT METHOD
CUSTOMER PROMPTED TO ACCEPT VWS RECOMMENDED PAYMENT METHOD OR SELECT ALTERNATIVE PAYMENT METHOD
IF NEW PAYMENT METHOD SELECTED, VWS AUTOMATICALLY NEGOTIATES ISSUANCE OF NEW PAYMENT METHOD WITHOUT REQUIRING ANY ADDITIONAL CUSTOMER INTERVENTION

CLOUD BASED ELECTRONIC WALLET

REFERENCE TO RELATED APPLICATIONS

[0001] Reference is hereby made to U.S. Provisional Patent Application Ser. No. 61/487,787, filed May 19, 2011 and entitled CLOUD BASED ELECTRONIC WALLET, the disclosure of which is incorporated by reference in its entirety and priority of which is hereby claimed pursuant to 37 CFR 1.78(a) (4) and (5)(i).

FIELD OF THE INVENTION

[0002] The present invention relates to payment systems and methodologies generally and more particularly to electronic wallet payment systems.

BACKGROUND OF THE INVENTION

[0003] The following patent publications are believed to represent the current state of the art:

[0004] U.S. Patent Publication Nos. US2006/0253335; US2009/0104888; US2008/0048022; US2005/0071179 and US2002/0077993;

[0005] Published PCT Application No. WO08104704; and

[0006] Patent Publication Nos. TW200515229; CN101499190; KR20020004321 and TW200813871.

SUMMARY OF THE INVENTION

[0007] The present invention seeks to provide improved payment systems and methodologies.

[0008] There is thus provided in accordance with a preferred embodiment of the present invention a payment system including a transaction server, a virtual wallet server (VWS), at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN), but not purchaser payment particulars, to at least the VWS and at least one mobile communicator communicating a mobile communicator presence indicator (MCPI) but neither the purchaser WPIN nor the purchaser payment particulars to the at least one point of sale device.

[0009] Preferably, the at least one mobile communicator stores neither the purchaser WPIN nor the purchaser payment particulars. In accordance with a preferred embodiment of the present invention the at least one mobile communicator neither reads, writes, communicates nor stores either the purchaser WPIN or the purchaser payment particulars. Additionally or alternatively, the at least one point of sale device is capable of receiving the purchaser WPIN at the secure element and receiving the MCPI for card presence verification for carrying out a card present transaction with the VWS.

[0010] Preferably, the payment system also includes at least one customer purchases information (CPI) database containing customer-wise information regarding customer purchases and at least one customer-wise purchase proposal generation device (CPPGD) in data communication with the at least one CPI database, the at least one CPPGD including a customer-wise information interface (CWII) receiving from the at least one CPI database the customer-wise information regarding customer purchases, a customer-wise products not purchased calculator (CWPPC) operative to ascertain the identity of at least one product which is normally purchased by customers and which is not usually purchased by a specific customer from a given sales entity and a purchase proposal generation engine (PPGE) generating an individualized purchase proposal for the at least one product which is normally purchased by customers and which is not usually purchased by the specific customer from the given sales entity to the specific customer based on the customer-wise information regarding customer purchases.

[0011] In accordance with a preferred embodiment of the present invention the VWS is operative in conjunction with a plurality of payment modalities and is operative to automatically select one of the plurality of payment modalities for a given transaction, based on at least identity of a customer and identity of a merchant.

[0012] Preferably, the VWS is operative in conjunction with a plurality of payment modalities and the at least one point of sale device provides to the VWS at least data identifying a specific merchant and a specific purchase, the VWS being operative prior to completion of a specific transaction to recommend to a customer about to complete the transaction one of the plurality of payment modalities for the specific transaction between the specific merchant and a specific customer for the specific purchase at a specific time; based on at least one of identity of the specific customer, identity of the specific merchant, particulars of the specific purchase and the time.

[0013] There is also provided in accordance with another preferred embodiment of the present invention a payment system including a transaction server, a virtual wallet server (VWS), at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN) to at least the VWS and at least one mobile communicator communicating at least one mobile communicator presence indicator (MCPI) but storing neither the purchaser WPIN nor the purchaser payment card number.

[0014] There is further provided in accordance with yet another preferred embodiment of the present invention a payment system including a transaction server, a virtual wallet server (VWS), at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN) to at least the VWS and at least one mobile communicator communicating at least one mobile communicator presence indicator (MCPI) but neither reading, writing, communicating nor storing either the purchaser WPIN or the purchaser payment card number.

[0015] There is also provided in accordance with still another preferred embodiment of the present invention a payment system including a virtual wallet server (VWS), at least one point of sale device including a secure element enabling secure data communication with the VWS and at least one mobile communicator capable of communicating a mobile communicator presence indicator (MCPI) to the at least one point of sale device, the at least one point of sale device being capable of receiving a purchaser identifier at the secure element and receiving the MCPI for card presence verification for carrying out a card present transaction with the VWS.

[0016] Preferably, the at least one mobile communicator does not require a secure element for communicating the MCPI.

[0017] In accordance with a preferred embodiment of the present invention the at least one mobile communicator does not include a secure element for communicating the MCPI.

[0018] In accordance with a preferred embodiment of the present invention the MCPI includes at least one of a user selected identifier, a phone number of the at least one mobile

communicator, an international mobile subscriber identity (IMSI) of the at least one mobile communicator, an international mobile equipment identity (IMEI) of the at least one mobile communicator and a randomly generated temporary mobile subscriber identity (TMSI) of the at least one mobile communicator.

[0019] In accordance with a preferred embodiment of the present invention the TMSI is received by and stored in the mobile communicator. Additionally, the TMSI is received by the mobile communicator from the VWS via a wireless system.

[0020] There is even further provided in accordance with yet another preferred embodiment of the present invention a customer identity and product identity offer generation system including at least one enstomer purchases information (CPI) database containing customer-wisc information regarding customer purchases and at least one enstomer-wisc purchase proposal generation device (CPPGD) in data communication with the at least one CPI database, the at least one CPPGD including a customer-wise information interface (CWII) receiving from the at least one CPI database the customer-wise information regarding enstomer purchases, a customer-wise products not purchased calculator (CWPPC) operative to ascertain the identity of at least one product which is normally purchased by customers and which is not nsually purehased by a specific customer from a given sales entity and a purchase proposal generation engine (PPGE) generating an individualized purchase proposal for the at least one product which is normally purchased by customers and which is not usually purehased by the specific enstomer from the given sales entity to the specific enstomer based on the customer-wise information regarding enstomer purchases.

[0021] There is still further provided in accordance with still another preferred embodiment of the present invention a payment system including a virtual wallet server (VWS) operative in conjunction with a plurality of payment modalities and at least one point of sale device in data communication with the VWS and providing at least data identifying a specific merchant and a specific purchase, the VWS being operative prior to completion of a specific transaction to recommend to a customer abont to complete the transaction one of the plurality of payment modalitics for the specific transaction between the specific merchant and a specific customer for the specific purchase at a specific time; based on at least one of identity of the specific enstomer, identity of the specific merchant, particulars of the specific purchase and the time.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

[0023] FIGS. **1**A-**1**D are simplified pictorial illustrations of the operation of a payment system constructed and operative in accordance with a preferred embodiment of the present invention;

[0024] FIG. **2** is a simplified flowchart illustrating a virtual wallet set up procedure in the operation of the payment system of an embodiment of the present invention;

[0025] FIG. **3**A-**3**C are together a simplified flowchart illustrating operation of the payment system of an embodiment of the present invention; and

[0026] FIG. **4** is a simplified flowchart illustrating automatic generation of recommendations in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

[0027] Reference is now made to FIGS. **1**A-**1**D, which are pictorial illustrations of the operation of a virtual wallet payment system constructed and operative in accordance with a preferred embodiment of the present invention. The payment system preferably includes a transaction server **100**, which is operative for conducting conventional payment card transactions, such as credit card, debit card and prepaid card transactions, and a virtual wallet server (VWS) **102**, which stores at least payment card information of virtual wallet subscribers.

[0028] At least one point of sale device **104**, such as a VeriFone PINPad 1000SE, includes a secure element **106**, for storage therein of confidential data, and is operative to provide secure data communication of at least a purchaser wallet PIN (WPIN), such as an encrypted WPIN, to at least VWS **102** and possibly also to transaction server **100**. It is a particular feature of an embodiment of the present invention that the point of sale device **104** does not transmit a purchaser payment card number to the VWS **102**.

[0029] At least one mobile communicator **110**, such as a cellular telephone, which may or may not be Near Field Communications (NFC)-enabled, communicates a mobile communicator presence indicator (MCPI) to the point of sale device **104**. In a preferred embodiment of the present invention, the MCPI includes at least one of, or a combination of, a user selected identifier, the telephone number of mobile communicator **110**, an international mobile subscriber identity (IMSI) of mobile communicator **110**, an International Mobile Equipment Identity (IMEI) number of mobile communicator **110**, and a single-use key, such as a Temporary Mobile Subscriber Identity (TMSI) or another key that has been sent, for example, via a text message, to the mobile communicator **110** or to an application on the mobile communicator **110**.

[0030] In the illustrated embodiment of FIG. **1**A, both the mobile communicator **110** and the point of sale device **104** are shown to be NFC-enabled. It is a particular feature of the present invention that the mobile communicator **110** does not communicate either a purchaser WPIN or a purchaser payment card number to a point of sale device **104**. Accordingly, mobile communicators which do not have a secure element **106**, or where the secure element is not accessible, may be used for this purpose.

[0031] In a preferred embodiment of the present invention, the MCPI is transmitted to the point of sale device **104** and communicated from the point of sale device **104** to the VWS **102**. When the MCPI includes a single-use key, the single-use key is preferably generated using Rolling Code Encryption (RCE).

[0032] Reference is now made additionally to FIG. **2**, which is a simplified flowchart illustrating a virtual wallet set up procedure, which takes place prior to a purchase using the system depicted in FIGS. **1**A-**1**D.

[0033] Turning to FIG. **2**, it is seen that preferably a user employs his mobile communicator **110**, or another computing device, such as a home computer **112**, to access a virtual wallet set up website (VWSUW) **114**, which is hosted by, or

communicates with, VWS **102**. Alternatively, a suitably programmed point of sale device **104** may also be used to access virtual wallet set up website (VWSUW) **114**.

[0034] A new user typically starts a registration procedure by clicking on a 'NEW USER' icon. In response, VWS **102** establishes a secure communications channel with the user's mobile communicator **110** or another computing device employed by the user.

[0035] The user is then prompted to provide personal identification details, such as full name, mailing address, e-mail address and government issued identification, and, preferably, to provide particulars of the mobile communicator **110** which is intended to be used to operate the wallet. Alternatively, the wallet need not be associated with any given mobile communicator **110**.

[0036] The user is also prompted to provide at least one mobile communicator presence indicator (MCPI) to be transmitted by the user's mobile communicator **110** to a point of sale device **104** in order to operate the virtual wallet in a purchase transaction. Preferably, the MCPI includes one or more of a user selected identifier, a telephone number of the mobile communicator **110**, an international mobile subscriber identity (IMSI) of mobile communicator **110**, an international mobile equipment identity (IMEI) of mobile communicator **110** and a temporary mobile subscriber identity (TMSI) of mobile communicator **110**. Alternatively, the MCPI may be any other suitable identifier, which can be communicated from the user's mobile communicator **110** to the point of sale device **104**.

[0037] The user is then prompted to provide details of one or more modalities, typically payment cards, such as credit cards, debit cards and prepaid cards, or financial accounts, such as a bank account and an on-line payment account, to be used by the virtual wallet. Such details, hereinafter termed purchase payment particulars (PPP), preferably include the card number, expiration date and card specific PIN (CPIN), if such exists, or ID of the bank or financial institution and the bank account or financial account number. CPINs are typically required for using debit cards. It is appreciated that a user may be given the option not to communicate a CPIN to the VWS during set up. In such a case, the user may communicate the CPIN by entering it onto a PINpad of a point of sale device in the course of a future purchase transaction.

[0038] The user may then be offered the possibility of obtaining one or more additional payment cards or access to other payment methods. In such a case, the user may be presented with a menu showing the available payment cards and the conditions associated with each. Should a user express interest in obtaining one or more additional cards, the VWS **102**, using the personal identification details of the user, may negotiate issuance of such payment cards with the servers of the issuers via secure communication links. Upon issuance, the servers of the issuers communicate in a secure manner the card numbers and the CPINs, to the extent that they exist, to the VWS **102**. Preferably, at least the CPINs are communicated and stored in an encrypted form. It is a particular feature of this embodiment of the present invention that neither the full card numbers nor the CPINs are communicated to the user.

[0039] In accordance with a preferred embodiment of the present invention, the VWS **102** issues a wallet personal identification number (WPIN), which is communicated to the user in a conventional manner, suitable for communicating PIN numbers, such as by email or conventional mail.

[0040] At the VWS **102**, for each wallet an association is created between the WPIN, the personal identification details supplied by the user during set up, the MCPI and the particulars of one or more payment cards, such as card number and expiration date, as well as any CPIN or ID of the bank or financial institution and the bank account or financial account number. This associated data is preferably stored in an encrypted form at the VWS **102**. The CPINs are normally required to be stored in encrypted form.

[0041] When more than one card is associated with a given wallet, the customer is further offered the option to agree in advance to automatic card selection by VWS **102** in a purchase transaction, based on the "best deal" available for that specific customer for the given purchase, as ascertained at or near the time of the purchase by the VWS **102**.

[0042] It is appreciated that the customer may add, delete and change virtual wallet parameters via the VWSUW **114** at any time following the set up procedure. These parameters may include designation of the cards associated with his wallet, his MCPI and various other particulars of his wallet.

[0043] A registered user typically starts a virtual wallet parameter modification procedure by clicking on a 'REGISTERED USER' icon. In response, VWS **102** establishes a secure communications channel with the user's mobile communicator **110** or another computing device employed by the user.

[0044] The user downloads a "mobile wallet" application into his mobile communicator **110** and may initialize the "mobile wallet" application by inserting his MCPI. The user may be requested to indicate if his MCPI is his mobile phone number. The MCPI may be stored in the memory of mobile communicator **110**. If the MCPI is the telephone number or IMEI number of the mobile communicator **110** it may be retrieved directly from the SIM card or operating system of the mobile communicator operator.

[0045] Returning now to FIGS. **1A-1D**, a typical purchase transaction using the system and methodology of embodiments of the present invention is now described with additional reference to FIGS. **3A-3C**. It is seen that once a customer's purchases are rung up on a cash register **115**, a sales clerk asks the customer how he wishes to pay. If the customer answers "with my virtual wallet", the sales clerk or customer selects a payment option, here termed "virtual wallet," from a menu on the cash register **115** and/or the point of sale device **104**. Selection of the "virtual wallet" payment option causes a visually sensible prompt to the customer to appear on a display **116** on the point of sale device **104** and/or on a display **117** of the cash register **115**. The prompt requests that the customer transmit an MCPI from the mobile communicator **110** to the point of sale device **104** or, alternatively, to enter an MCPI, that may be provided by the mobile communicator **110**, on a keypad of the point of sale device **104**. The customer activates his virtual wallet application on his mobile communicator **110**, which preferably retrieves or has previously retrieved the MCPI. It is appreciated that when the MCPI includes a single-use key, the application, after using the single-use key, preferably retrieves a new single-use key for future use. The MCPI may be transmitted to a store server **118** to enable personalized generation of a personalized welcome message and/or other personalized messages or promotions to the customer at the point of sale device **104** or on mobile communicator **110**, on the basis of predefined associations between the MCPI and the customer.

[0046] As also seen in FIG. **1**A, in accordance with a preferred embodiment of the present invention, there is provided at least one customer-wise purchase proposal generation device (CPPGD) **111**, preferably in data communication with VWS **102**. Alternatively, the at least one customer-wise purchase proposal generation device may be embodied in VWS **102**. In another preferred embodiment of the present invention, at least one CPPGD **111** may be in data communication with POS device **104** independent of VWS **102** and VWS **102** may be obviated. CPPGD **111** is operative to generate at least one individualized purchase proposal for presentation to the customer at the time of completing a purchase.

[0047] The at least one CPPGD **111** preferably is in communication with at least one customer purchases information (CPI) database, such as a commercial credit database (CCDB), a merchant database (MDB) and a social network (SN), including information regarding the customer's buying habits, such as previous customer purchases history. The CPPGD **111** preferably provides offers to the customer via the point of sale device **104**. Such offers may include purchase offers based on the information regarding the customer's buying habits and specifically may include offers to purchase goods which the customer is known to purchase but does not currently purchase from the merchant at which the customer is currently making a purchase.

[0048] The CPPGD preferably includes a customer-wise information interface (CWII), a customer-wise products not purchased calculator (CWPPC) and a purchase proposal generation engine (PPGE). The CWII preferably receives information regarding customer buying habits, typically including at least information regarding previous product purchases by the customer, from the at least one CPI database. The CWPPC is preferably operative to ascertain the identity of at least one product which is normally purchased by other customers and which is not usually purchased by this customer from the sales entity the customer is currently purchasing from. The PPGE preferably generates an individualized purchase proposal to the customer for the at least one product identified by the CWPPC.

[0049] It is appreciated that communication of the MCPI to the point of sale device **104** may take place prior to, during or following tallying of a customer's purchases.

[0050] In a case where the MCPI is transmitted by the mobile communicator **110**, the transmission may be effected by the user placing his mobile communicator **110** on or in close proximity to an NFC (Near Field Communication) enabled point of sale device **104** or other NFC communication location associated with the point of sale device **104** and/or the cash register **115**.

[0051] It is a particular feature of the present invention that, for transactions not requiring a CPIN, receipt of the MCPI at the point of sale device **104**, together with the user entering the WPIN, may constitute an acceptable indication of customer presence which enables a transaction to be considered as being a "card-present" transaction.

[0052] It is a particular feature of the present invention that, for transactions requiring a CPIN, receipt of the MCPI at the point of sale device **104**, together with the user entering the CPIN and the WPIN, may constitute an acceptable indication of customer presence which enables a transaction to be considered as being a "card-present" transaction.

[0053] Communication of the MCPI to the point of sale device **104** may be via one of a number of communication links, such as BLUETOOTH®, WiFi, optical and cellular, or the MCPI may be entered manually. A preferred method of optical communication is described in assignee's U.S. patent application Ser. No. 13/006,137, entitled Light Based and Online Payment Systems and Methodologies, filed Jan. 13, 2011.

[0054] As seen in FIG. **1**B, upon receipt of the MCPI the point of sale device **104** prompts the customer to enter his WPIN by keying onto a secure keypad **120** of the point of sale device **104**. It is a particular feature of the present invention that the WPIN is entered manually by the customer onto the point of sale device **104**. This feature obviates the need for the mobile communicator **110** to have a secure element and to provide a secure communications link with the mobile communicator **110**.

[0055] The customer manually enters his WPIN on the point of sale device **104**. The point of sale device **104** preferably encrypts the WPIN. The point of sale device **104** preferably transmits, preferably in a single secure session, such as an SSL session, the MCPI and the encrypted WPIN to the VWS **102**.

[0056] The VWS **102** decrypts the WPIN and, using the MCPI, associates the proposed transaction with the virtual wallet of the customer. If the VWS **102** does not find a match of the MCPI and the WPIN with a specific wallet, an error code is generated and transmitted by the VWS **102** to the point of sale device **104**, and the transaction is terminated.

[0057] If a match of the MCPI and the WPIN and a specific wallet is found, the transaction proceeds.

[0058] If only a single payment modality is associated with the given wallet, such as a single payment card, the VWS **102** transmits the purchase payment particulars, such as payment card particulars, including the payment card number and its expiration date, to the point of sale device **104**. One or more, or all of, the purchase payment particulars may be transmitted in encrypted form. If a CPIN is associated with a given payment card and the customer has given prior authorization for the CPIN to be automatically provided, the CPIN is also transmitted, preferably in encrypted form, to the point of sale device **104**. Optionally, the transmission of purchase payment particulars takes place in a secure session.

[0059] As seen in FIG. **1**C, if multiple payment modalities, such as multiple payment cards, are associated with a given wallet, the VWS **102** transmits to the point of sale device **104** the purchase payment particulars of all such payment cards, including the payment card number and its expiration date. One or more, or all of, the payment card particulars may be transmitted in encrypted form. If a CPIN is associated with a given payment card, the CPIN is also transmitted, preferably in encrypted form, to the point of sale device **104**. Optionally, the transmission of purchase payment particulars, such as payment card particulars, takes place in a secure session.

[0060] As also seen in FIG. **1**C, when multiple payment cards are associated with a given wallet, a representation of each of the cards appears, preferably on a display **116** of the point of sale device **104**. The representation preferably includes the logo of the payment card company. Additionally, the logo or other details of the issuer and/or the last four digits of the card number may also be included in the representation. The customer is prompted to select one of the cards.

[0061] In accordance with an embodiment of the present invention, at the time of presentation to the customer of the various payment cards that can be used for the transaction, a recommendation may be automatically made to the customer as to which payment card or cards provides the "best deal".

The automatic provision of a recommendation normally requires prior authorization from the customer, which is normally given at the time of set up or in a subsequent modification session. The "best deal" may represent one or more of discounts, payment terms, coupons, points and other customer benefits. Antomatic generation of a recommendation is described hereinbelow with respect to FIG. **4**.

[0062] As seen in FIG. **1**C, the customer is prompted to select a payment card and selects a payment card with which to effect the purchase transaction or alternatively, based on a prior cnstomer agreement in the wallet setup procedure, the system may automatically select the payment card to be used in the transaction.

[0063] If a CPIN is associated with the selected payment card and the customer has not given prior authorization for transmission thereof, the customer is prompted to enter the CPIN for the selected payment card by keying it onto the secnre keypad **120** of the point of sale device **104**.

[0064] As seen in FIG. **1**D, the point of sale device **104** then completes the purchase transaction in a conventional manner by communicating purchase particulars, such as the amount and date of the transaction, particulars of the point of sale device **104**, such as the identification number of the point of sale device **104**, and the payment purchase particulars (PPP) of the selected payment card to the transaction server **100**.

[0065] Where a CPIN is associated with the selected payment card, the CPIN is decrypted at the point of sale device **104** and is re-encrypted for secure transmission to the transaction server **100**.

[0066] Alternatively, if a single payment card is associated with the virtual wallet, the virtual wallet server **102** may complete the purchase transaction in a conventional manner by communicating to the transaction server **100** purchase particulars, such as the amount and date of the transaction, particulars of the point of sale device **104**, such as the identification number of the point of sale device **104**, and the particulars of the selected payment card.

[0067] Alternatively, if a single payment card is associated with the virtnal wallet, the point of sale device **104** may communicate only the purchase particulars and the particulars of the point of sale device **104** to the transaction server **100** and the particulars of the single payment card are supplied to the transaction server **100** directly from the virtual wallet server **102**.

[0068] Alternatively, if multiple payment modalities, such as multiple payment cards and/or bank accounts, are associated with the virtual wallet, the point of sale device **104** may communicate to the virtual wallet server **102** the purchase particulars and the particulars of the point of sale device **104** and the customer's selection of payment modality, such as payment card. The virtual wallet server **102** may complete the purchase transaction in a conventional manner by communicating to the transaction server **100** purchase particulars, such as the amount and date of the transaction, particulars of the point of sale device **104**, such as the identification number of the point of sale device **104**, and the payment purchase particulars of the selected payment card.

[0069] Alternatively if multiple payment modalities, such as multiple payment cards and/or bank accounts, are associated with the virtual wallet, the point of sale device **104** may communicate only the purchase particulars and the particulars of the point of sale device **104** to the transaction server **100** and may communicate the customer's selection of payment card or bank account to the virtual wallet server **102**. The purchaser payment particulars are supplied to the transaction server **100** directly from the virtual wallet server **102**.

[0070] Reference is now made to FIG. **4**, which is a simplified flowchart illustrating automatic generation of a recommendation as to which of a plurality of payment cards or direct charge to a bank account is most advantageous for the customer in a given transaction, thereby providing the "best deal" for the customer. Based on prior authorization from the customer, the VWS **102** may employ information received from varions sources, including for example, commercial credit databases (CCDBs), merchants databases (MDBs) and social networks (SNs) regard the customer's buying habits and payment preferences.

[0071] The recommendation may be to use one of the payment cards or bank accounts that the customer currently holds. Alternatively, the recommendation may be to use a payment card that the customer does not currently hold, but which he is eligible to obtain.

[0072] The recommendation is preferably generated by utilizing at least one of the identity of the customer, the identity of the merchant, the information relating to the specific purchase and the time. Specifically, the recommendation may be based on at least one of information relating to the customer, such as the customer's payment history, information relating to the merchant, such as merchant or payment method discounts currently available using preferred payment options and the information relating to the specific purchase, such as currently available product promotional offers.

[0073] The customer is prompted to accept the recommendation or choose an alternative payment method. If the customer accepts a recommendation to obtain a new payment method, such as a new payment card or new financial account, the VWS **102** is preferably operative automatically to negotiate issuance of the new payment card or financial account, preferably without requiring any further intervention of the user. For this purpose, the VWS **102** may be required to divulge personal information of the customer and accordingly, the customer's agreement is solicited preferably at the set up stage of system operation.

[0074] It is a particular feature of the present invention that the purchaser's payment particulars, and specifically payment card number, are not communicated from the point of sale device **104** to the VWS **102** in a virtual wallet transaction. It is a particular feature of the present invention that the purchaser's payment particulars, and specifically payment card number, are also not communicated by the mobile communicator **110** to any of the point of sale device **104**, the VWS **102**, the transaction server **100** and the store server **118**. The purchaser's payment card particnlars, and specifically payment number, is stored in the VWS **102** and is communicated only from the VWS **102** to the transaction server **100** either directly or via the point of sale device **104** and optionally via both the point of sale device **104** and via the store server **118**.

[0075] It is appreciated that the terms 'user,' 'customer' and 'purchaser' are sometimes used interchangeably in the above description.

[0076] It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove as well as modifications thereof which are not in the prior art.

1. A payment system comprising:
a transaction server;
a virtual wallet server (VWS);
at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN), but not purchaser payment particulars, to at least said VWS; and
at least one mobile communicator communicating a mobile communicator presence indicator (MCPI) but neither said purchaser WPIN nor said purchaser payment particulars to said at least one point of sale device.

2. A payment system according to claim **1** and wherein said at least one mobile communicator stores neither said purchaser WPIN nor said purchaser payment particulars.

3. A payment system according to claim **1** and wherein said at least one mobile communicator neither reads, writes, communicates nor stores either said purchaser WPIN or said purchaser payment particulars.

4. A payment system according to claim **1** and wherein said at least one point of sale device is capable of receiving said purchaser WPIN at said secure element and receiving said MCPI for card presence verification for carrying out a card present transaction with said VWS.

5. A payment system according to claim **2** and wherein said at least one point of sale device is capable of receiving said purchaser WPIN at said secure element and receiving said MCPI for card presence verification for carrying out a card present transaction with said VWS.

6. A payment system according to claim **3** and wherein said at least one point of sale device is capable of receiving said purchaser WPIN at said secure element and receiving said MCPI for card presence verification for carrying out a card present transaction with said VWS.

7. A payment system according to claim **1** and also comprising:
at least one customer purchases information (CPI) database containing customer-wise information regarding customer purchases; and
at least one customer-wise purchase proposal generation device (CPPGD) in data communication with said at least one CPI database, said at least one CPPGD including:
a customer-wise information interface (CWII) receiving from said at least one CPI database said customer-wise information regarding customer purchases;
a customer-wise products not purchased calculator (CWPPC) operative to ascertain the identity of at least one product which is normally purchased by customers and which is not usually purchased by a specific customer from a given sales entity; and
a purchase proposal generation engine (PPGE) generating an individualized purchase proposal for said at least one product which is normally purchased by customers and which is not usually purchased by said specific customer from said given sales entity to said specific customer based on said customer-wise information regarding customer purchases.

8. A payment system according to claim **1** and wherein:
said VWS is operative in conjunction with a plurality of payment modalities and is operative to automatically select one of said plurality of payment modalities for a given transaction, based on at least identity of a customer and identity of a merchant.

9. A payment system according to claim **1** and wherein:
said VWS is operative in conjunction with a plurality of payment modalities; and
said at least one point of sale device provides to said VWS at least data identifying a specific merchant and a specific purchase,
said VWS being operative prior to completion of a specific transaction to recommend to a customer about to complete the transaction one of said plurality of payment modalities for said specific transaction between said specific merchant and a specific customer for said specific purchase at a specific time; based on at least one of:
identity of said specific customer;
identity of said specific merchant;
particulars of said specific purchase; and
the time.

10. A payment system comprising:
a transaction server;
a virtual wallet server (VWS);
at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN) to at least said VWS; and
at least one mobile communicator communicating at least one mobile communicator presence indicator (MCPI) but storing neither said purchaser WPIN nor said purchaser payment card number.

11. A payment system comprising:
a transaction server;
a virtual wallet server (VWS);
at least one point of sale device including a secure element and being operative to provide secure data communication of a purchaser wallet personal identification number (WPIN) to at least said VWS; and
at least one mobile communicator communicating at least one mobile communicator presence indicator (MCPI) but neither reading, writing, communicating nor storing either said purchaser WPIN or said purchaser payment card number.

12. A payment system comprising:
a virtual wallet server (VWS);
at least one point of sale device including a secure element enabling secure data communication with said VWS; and
at least one mobile communicator capable of communicating a mobile communicator presence indicator (MCPI) to said at least one point of sale device;
said at least one point of sale device being capable of receiving a purchaser identifier at said secure element and receiving said MCPI for card presence verification for carrying out a card present transaction with said VWS.

13. A payment system according to claim **12** and wherein said at least one mobile communicator does not require a secure element for communicating said MCPI.

14. A payment system according to claim **12** and wherein said at least one mobile communicator does not include a secure element for communicating said MCPI.

15. A payment system according to claim **12** and wherein said MCPI includes at least one of a user selected identifier, a phone number of said at least one mobile communicator, an international mobile subscriber identity (IMSI) of said at least one mobile communicator, an international mobile equipment identity (IMEI) of said at least one mobile communica-

tor and a randomly generated temporary mobile subscriber identity (TMSI) of said at least one mobile communicator.

16. A payment system according to claim **15** and wherein said TMSI is received by and stored in said at least one mobile communicator.

17. A payment system according to claim **15** and wherein said TMSI is received by said at least one mobile communicator from said VWS via a wireless system.

18. A customer identity and product identity offer generation system comprising:

at least one customer purchases information (CPI) database containing customer-wise information regarding customer purchases; and

at least one customer-wise purchase proposal generation device (CPPGD) in data communication with said at least one CPI database, said at least one CPPGD including:

a customer-wise information interface (CWII) receiving from said at least one CPI database said customer-wise information regarding customer purchases;

a customer-wise products not purchased calculator (CWPPC) operative to ascertain the identity of at least one product which is normally purchased by customers and which is not usually purchased by a specific customer from a given sales entity; and

a purchase proposal generation engine (PPGE) generating an individualized purchase proposal for said at least one product which is normally purchased by customers and which is not usually purchased by said specific customer from said given sales entity to said specific customer based on said customer-wise information regarding customer purchases.

19. A payment system comprising:

a virtual wallet server (VWS) operative in conjunction with a plurality of payment modalities; and

at least one point of sale device in data communication with said VWS and providing at least data identifying a specific merchant and a specific purchase,

said VWS being operative prior to completion of a specific transaction to recommend to a customer about to complete the transaction one of said plurality of payment modalities for said specific transaction between said specific merchant and a specific customer for said specific purchase at a specific time; based on at least one of:

identity of said specific customer;

identity of said specific merchant;

particulars of said specific purchase; and

the time.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Pasa et al.

(10) **Pub. No.: US 2013/0254115 A1**

(43) **Pub. Date: Sep. 26, 2013**

(54) **CONVERGED CROSS-PLATFORM ELECTRONIC WALLET**

(71) Applicant: **MasterCard International Incorporated**, Purchase, NY (US)

(72) Inventors: **Mehmet Pasa**, Westport, CT (US); **Michael J. Friedman**, Norwalk, CT (US); **Ngassam Ngnoumen**, Chesterfield, MO (US); **Celine Martig**, Greenwich, CT (US); **Shoshana C. Rosenfield**, Rye, NY (US); **Rupa Subramanian**, Norwalk, CT (US); **Zavida Mangaru**, Valley Stream, NY (US); **John F. Cacioppo**, Foristell, MO (US); **Scott Moser**, Kings Park, NY (US); **Amyn Dhala**, White Plains, NY (US)

(73) Assignee: **MasterCard International Incorporated**, Purchase, NY (US)

(21) Appl. No.: **13/888,112**

(22) Filed: **May 6, 2013**

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/746,904, filed on Jan. 22, 2013.

(60) Provisional application No. 61/588,505, filed on Jan. 19, 2012, provisional application No. 61/642,729, filed on May 4, 2012, provisional application No. 61/642,792, filed on May 4, 2012, provisional application No. 61/642,799, filed on May 4, 2012, provisional application No. 61/642,925, filed on May 4, 2012.

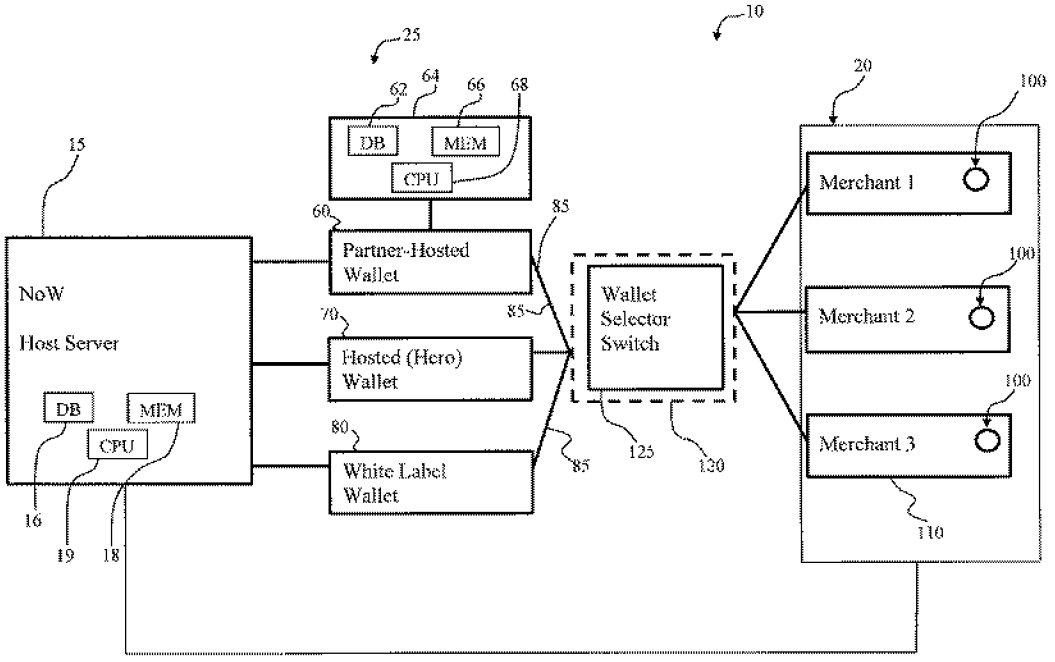
Publication Classification

(51) **Int. Cl.**
G06Q 20/36 (2012.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/3674*** (2013.01)
USPC **705/67**

(57) **ABSTRACT**

Various consumer interface platforms are converged to facilitate user access to an electronic network of wallets. The functions of both remote and NFC payment, among other interface platforms, give the purchaser access to a single electronic wallet for online E-commerce and a variety of mCommerce scenarios, some including brick and mortar, face-to-face (F2F), and/or point-of-sale (POS) transaction payments. The network of wallets has a network operator intermediating payment transactions between merchants and wallet providers. In this way, the parallel consumer interface platforms, such as remote platform enabling e-commerce payments, an NFC platform, and/or others, into a single converged payment platform that is usable in either or both transaction settings.



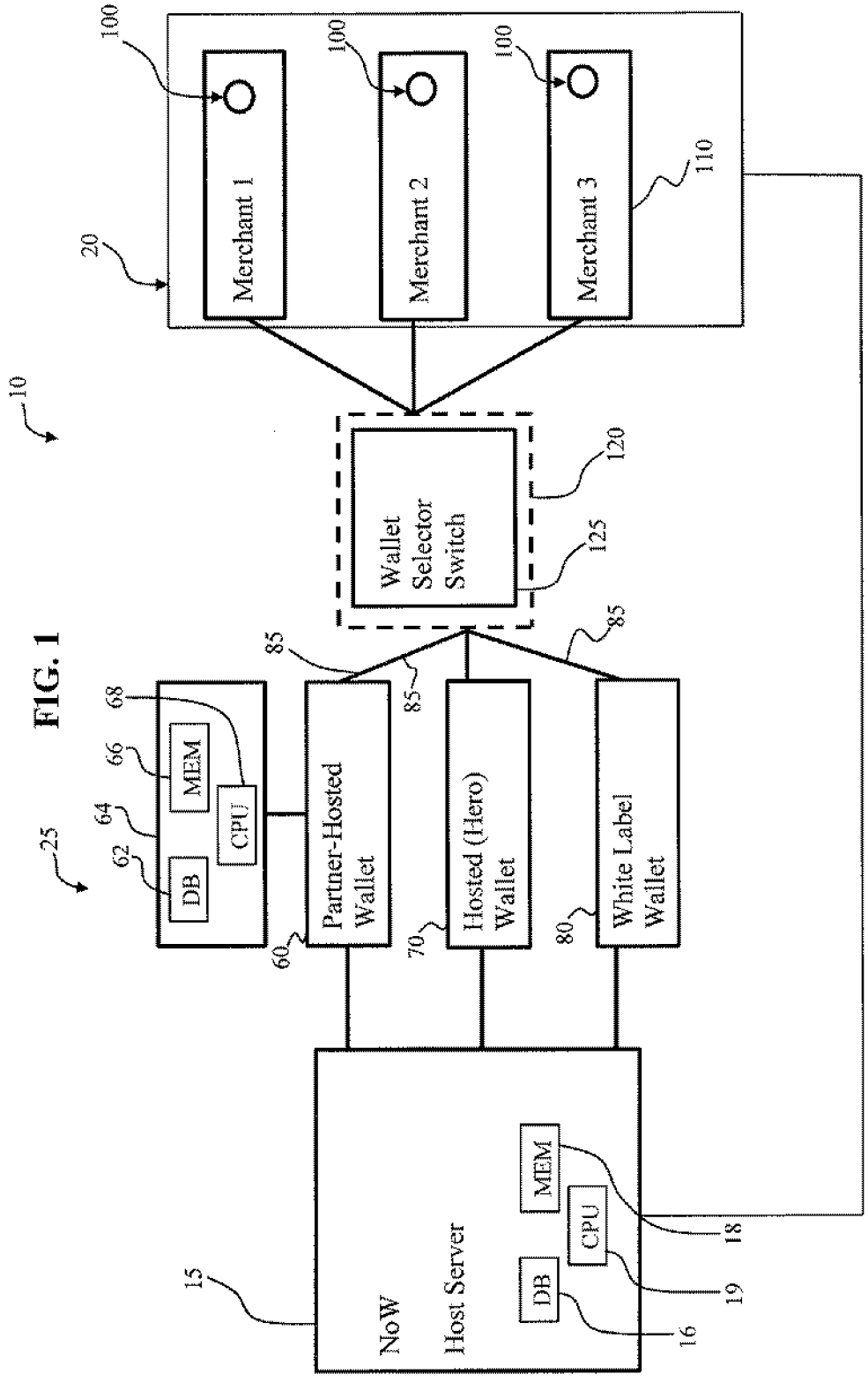

10
20
100
Merchant 1
100
Merchant 2
100
Merchant 3
110
120
Wallet Selector Switch
125
85
85
85
25
68
66
64
62
MEM
CPU
DB
60
Partner-Hosted Wallet
70
Hosted (Hero) Wallet
80
White Label Wallet
15
NoW Host Server
MEM
CPU
DB
18
19
16

FIG. 1

FIG. 2

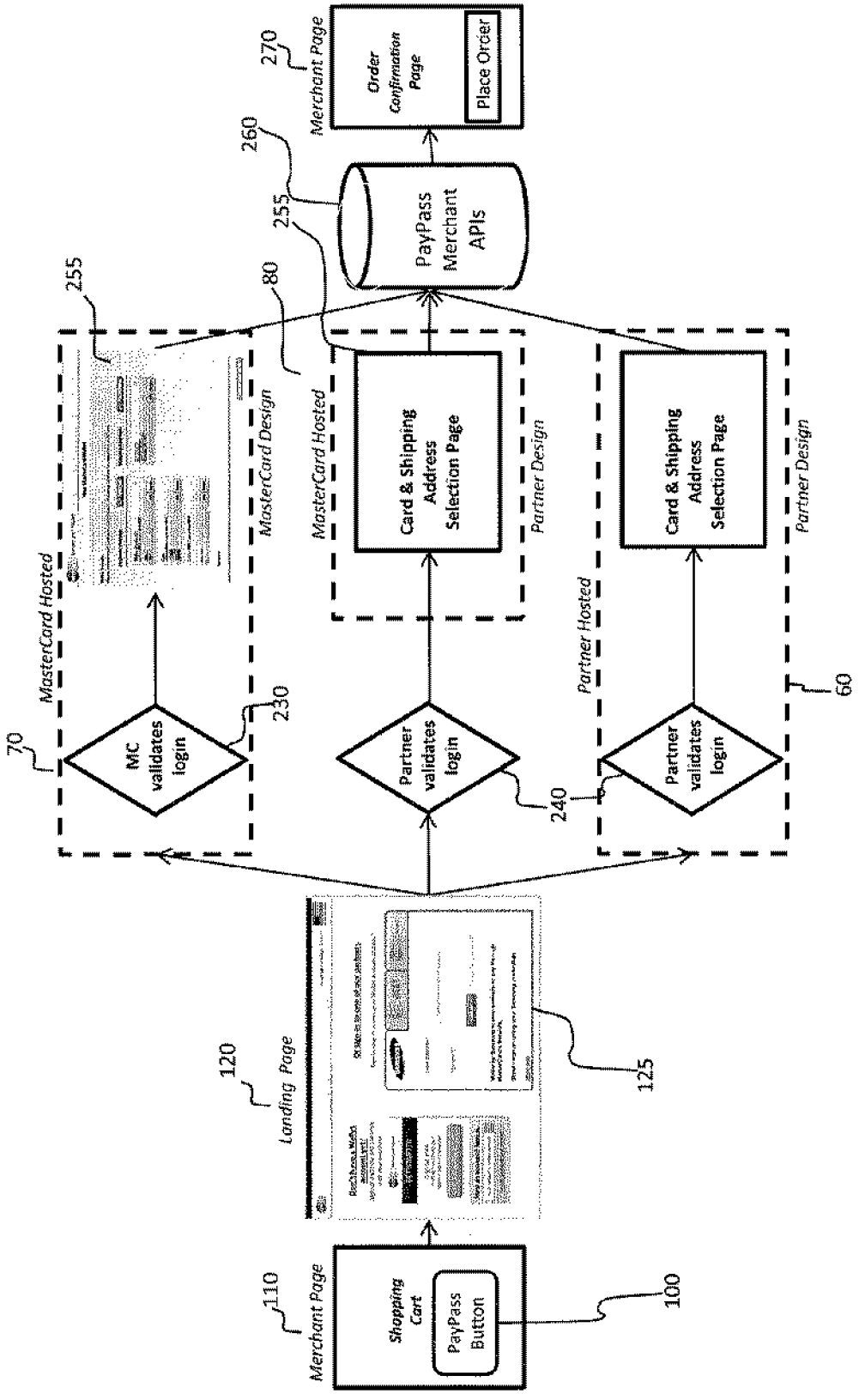
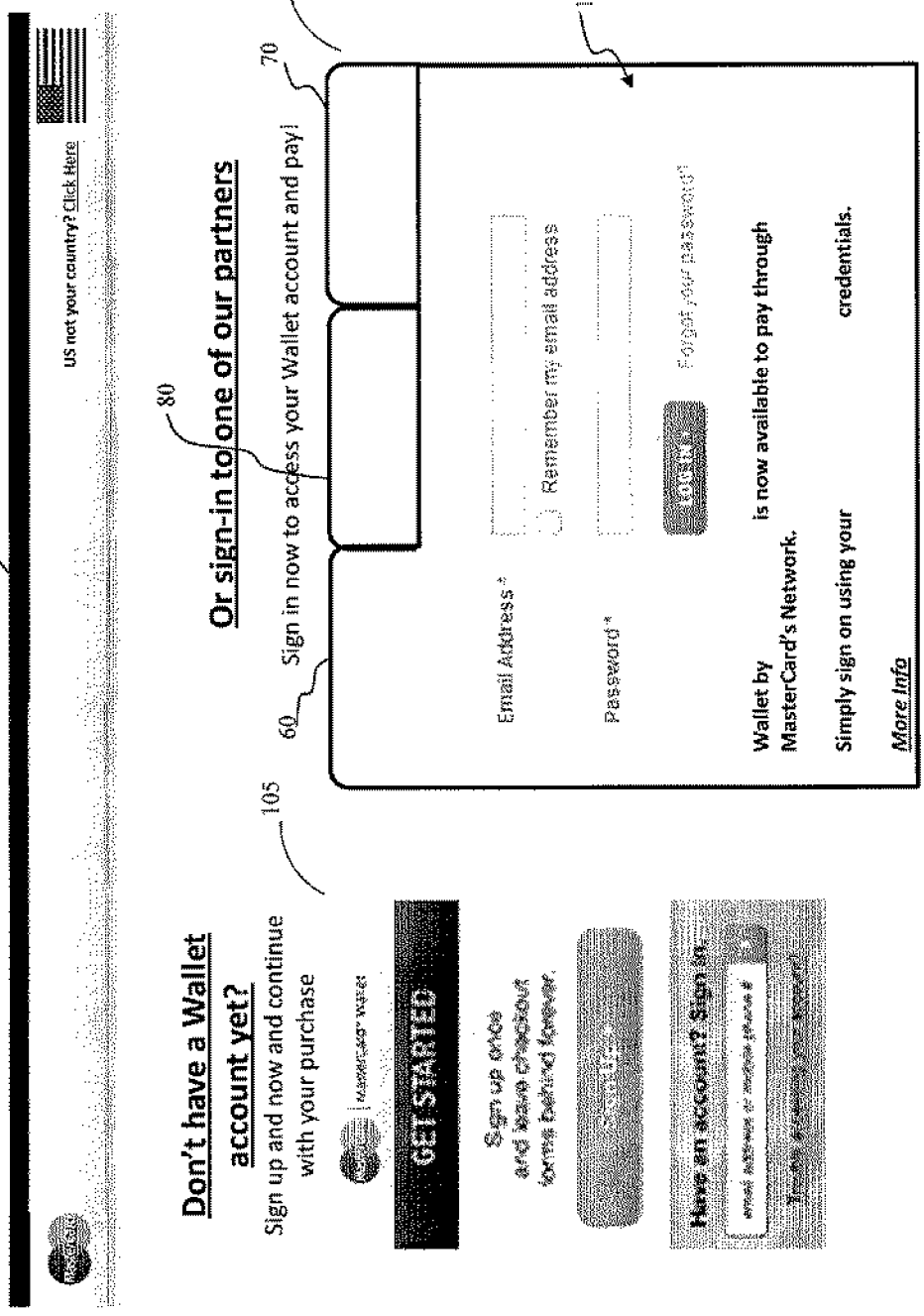

Merchant Page
110
Shopping Cart
PayPass Button
100
Landing Page
120
125
MasterCard Hosted
70
MC validates login
230
MasterCard Design
255
MasterCard Hosted
Card & Shipping Address Selection Page
Partner Design
80
Partner validates login
240
Partner Hosted
Card & Shipping Address Selection Page
Partner Design
60
PayPass Merchant APIs
255
260
Merchant Page
270
Order Confirmation Page
Place Order

Fig. 3A


120
US not your country? Click Here
80
Or sign-in to one of our partners
125
70
Sign in now to access your Wallet account and pay!
123
60
105
Don't have a Wallet account yet?
Sign up and now and continue with your purchase
GET STARTED
Email Address *
Remember my email address
Password *
Forgot your password?
Wallet by MasterCard's Network.
is now available to pay through
Simply sign on using your credentials.
More Info

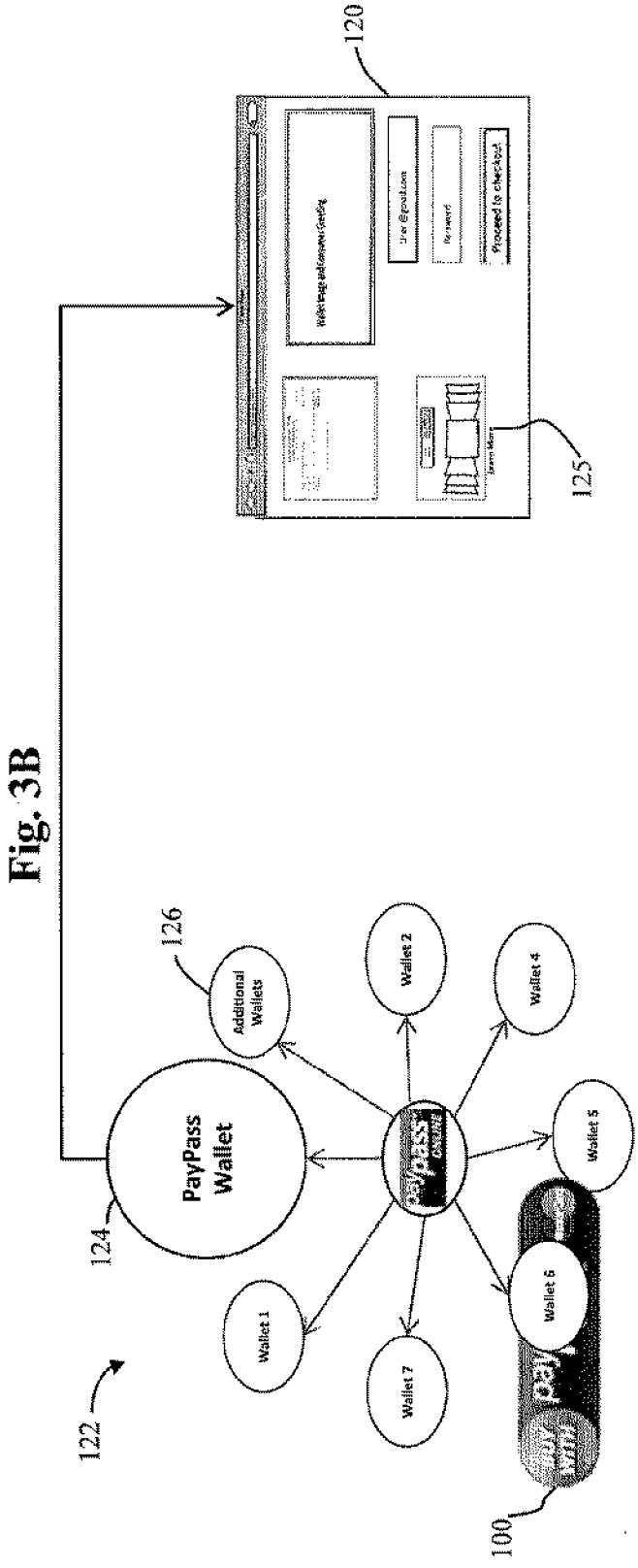

120
125
126
Additional Wallets
Wallet 2
Wallet 4
PayPass Wallet
Wallet 5
124
Wallet 1
Wallet 6
Wallet 7
122
100

Fig. 3B

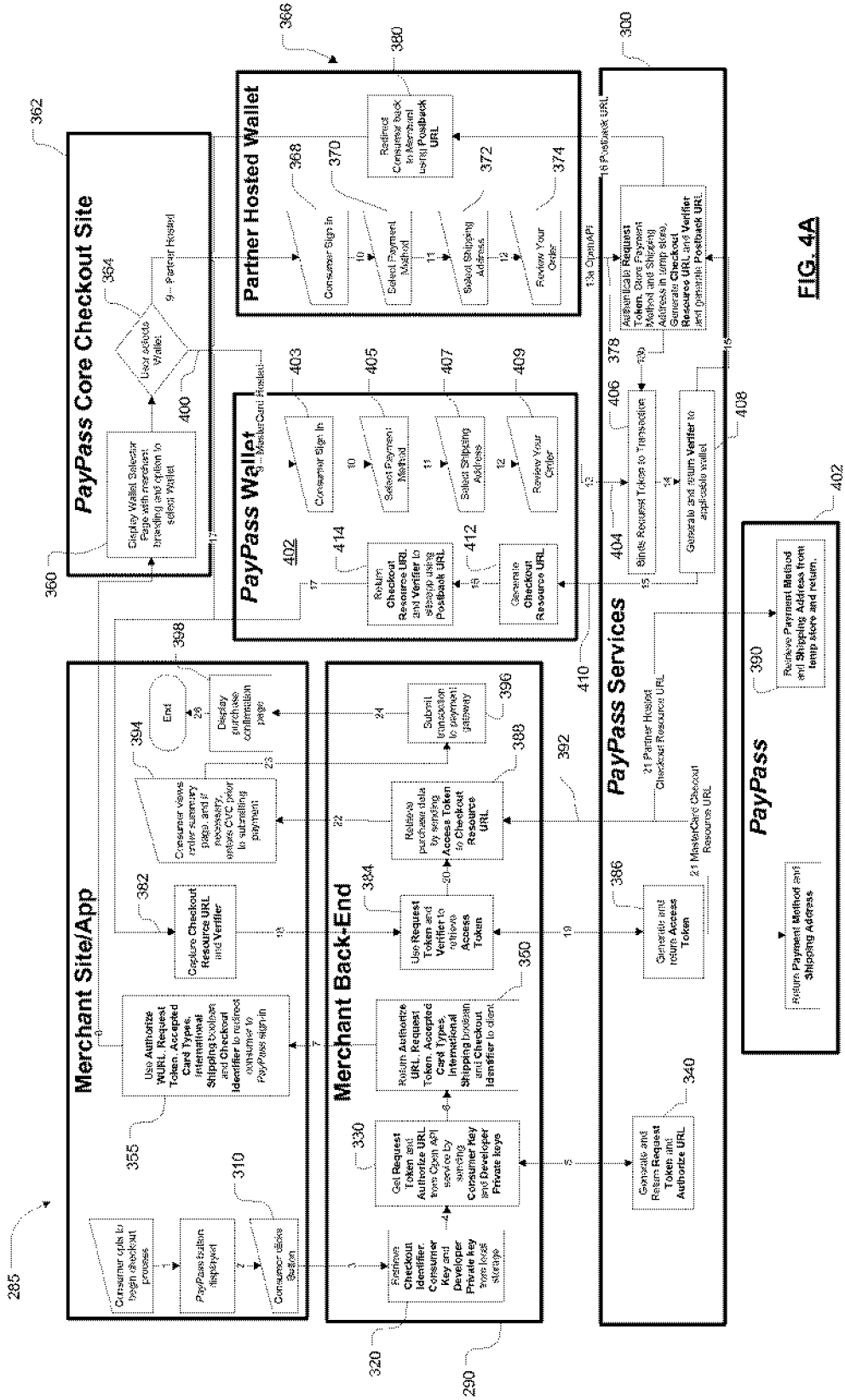

Merchant Site/App
Merchant Back-End
PayPass Services
PayPass
PayPass Core Checkout Site
PayPass Wallet
Partner Hosted Wallet
Consumer opts to begin checkout process
PayPass button displayed
Consumer clicks button
Use Authorize URL Request Token, Accepted Card Types, International Shipping boolean, and Checkout Identifier to redirect consumer to PayPass sign-in
Capture Checkout Resource URL and Verifier
Consumer views order summary page and if necessary enters CVC prior to submitting payment
Display purchase confirmation page
End
Retrieve Checkout Identifier, Consumer Key and Developer Private Key from local storage
Get Request Token and Authorize URL from Open API service by sending Consumer Key and Developer Private Keys
Return Authorize URL, Request Token, Accepted Card Types, International Shipping boolean and Checkout Identifier to client
Use Request Token and Verifier to retrieve Access Token
Retrieve purchase data by sending Access Token for Checkout Resource URL
Submit transaction to payment gateway
Generate and return Request Token and Authorize URL
Generate and return Access Token
Display Wallet Selector Page with merchant branding and option to select Wallet
User selects Wallet
Partner Hosted
Consumer Sign In
Select Payment Method
Select Shipping Address
Review Your Order
Redirect Consumer back to Merchant's Initial PostBack URL
Consumer Sign In
Select Payment Method
Select Shipping Address
Review Your Order
Return Checkout Resource URL and Verifier to Merchant using PostBack URL
Generate Checkout Resource URL
Authenticate Request Token, Store Payment Method and Shipping Address in temp store. Generate Checkout Resource URL and Verifier and generate PostBack URL
Store Request Token to Transaction
Generate and return Verifier to applicable wallet
Return Payment Method and Shipping Address
Retrieve Payment Method and Shipping Address from temp store and return.
285
290
310
320
330
340
350
355
360
362
364
366
368
370
372
374
378
380
382
384
386
388
389
390
392
394
396
400
402
403
404
405
406
407
408
409
410
412
414

FIG. 4A

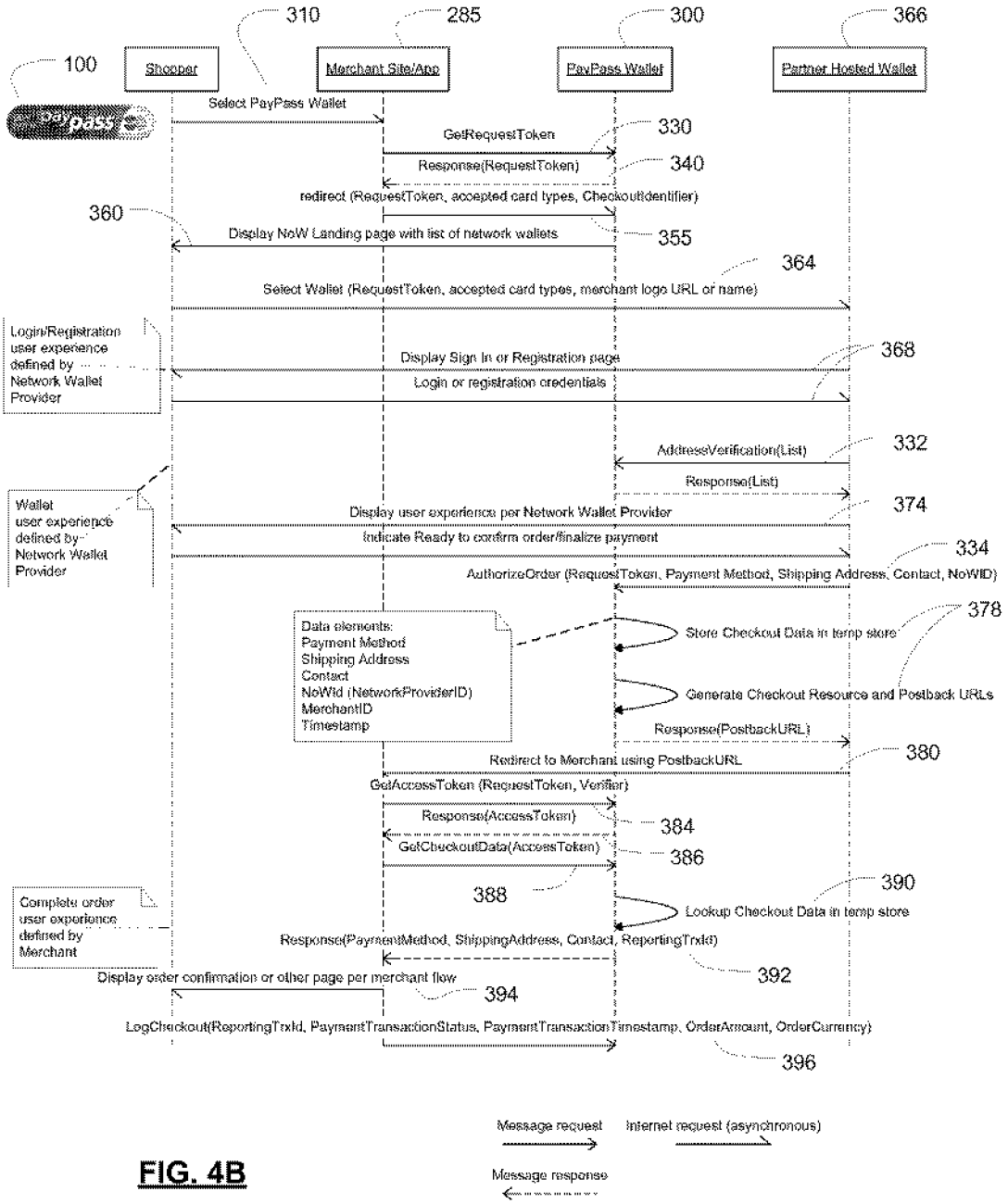
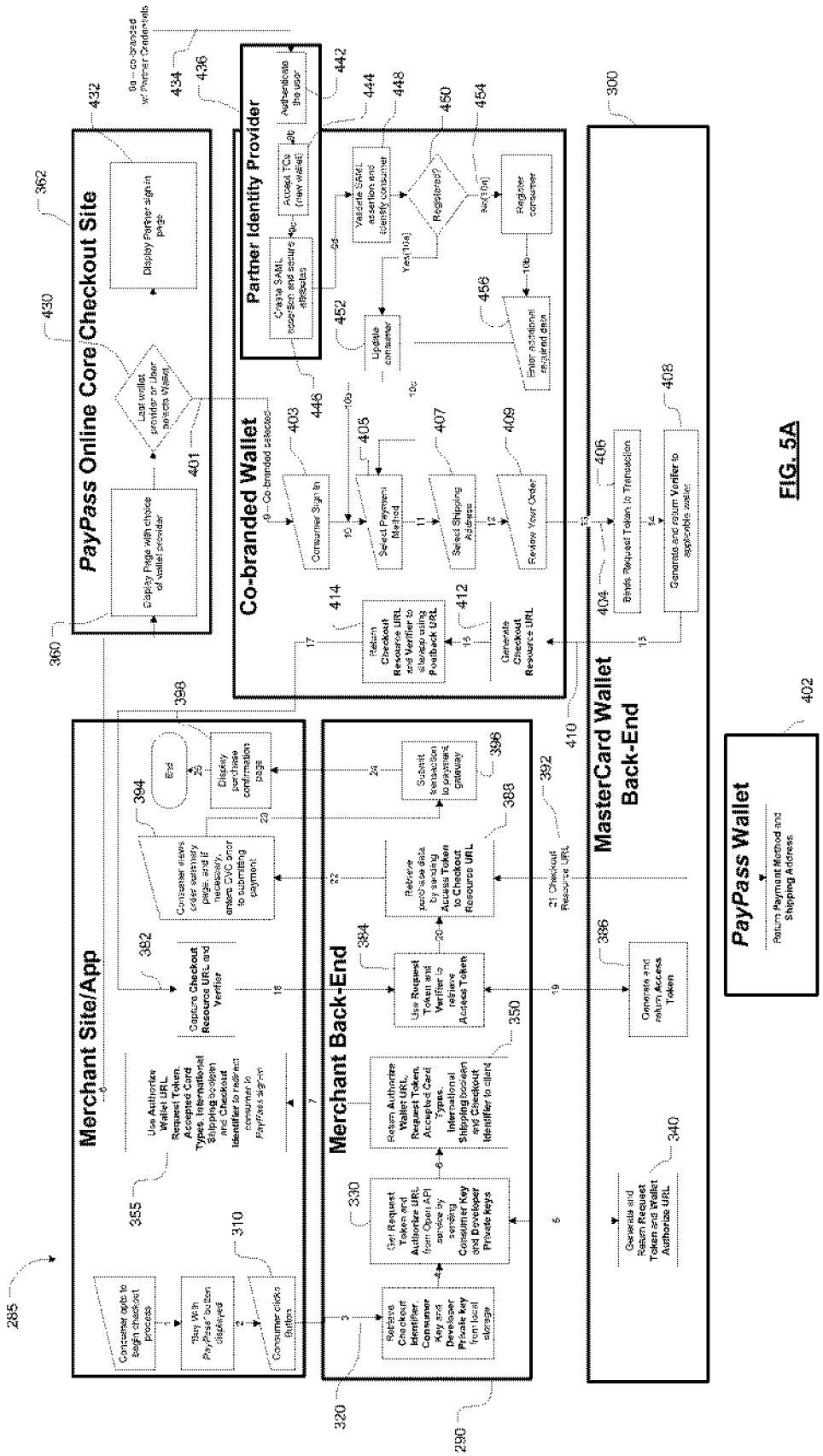

100
Shopper
310
Merchant Site/App
285
PayPass Wallet
300
Partner Hosted Wallet
366
Select PayPass Wallet
GetRequestToken
330
Response(RequestToken)
340
redirect (RequestToken, accepted card types, CheckoutIdentifier)
360
Display NoW Landing page with list of network wallets
355
364
Select Wallet (RequestToken, accepted card types, merchant logo URL or name)
Login/Registration user experience defined by Network Wallet Provider
Display Sign In or Registration page
368
Login or registration credentials
AddressVerification(List)
332
Response(List)
Wallet user experience defined by Network Wallet Provider
Display user experience per Network Wallet Provider
374
Indicate Ready to confirm order/finalize payment
334
AuthorizeOrder (RequestToken, Payment Method, Shipping Address, Contact, NoWID)
Data elements:
Payment Method
Shipping Address
Contact
NoWid (NetworkProviderID)
MerchantID
Timestamp
Store Checkout Data in temp store
378
Generate Checkout Resource and Postback URLs
Response(PostbackURL)
Redirect to Merchant using PostbackURL
380
GetAccessToken (RequestToken, Verifier)
Response(AccessToken)
384
GetCheckoutData(AccessToken)
386
388
390
Lookup Checkout Data in temp store
Complete order user experience defined by Merchant
Response(PaymentMethod, ShippingAddress, Contact, ReportingTrxId)
392
Display order confirmation or other page per merchant flow
394
LogCheckout(ReportingTrxId, PaymentTransactionStatus, PaymentTransactionTimestamp, OrderAmount, OrderCurrency)
396
Message request
Internet request (asynchronous)
Message response

FIG. 4B


PayPass Online Core Checkout Site
Co-branded Wallet
Partner Identity Provider
Merchant Site/App
Merchant Back-End
MasterCard Wallet Back-End
PayPass Wallet
Display Page with choice of wallet provider
Last wallet selected or User selects Wallet
Display Partner sign-in page
Authenticate the user
Consumer Sign In
Select Payment Method
Select Shipping Address
Review Your Order
Register consumer
Generate Checkout Resource URL
Return Checkout Resource URL and Verifier to site/app using Postback URL
Capture Checkout Resource URL and Verifier
Use Request Token and Verifier to retrieve Access Token
Retrieve payload data by providing Access Token to Checkout Resource URL
Submit transaction to payment gateway
Display confirmation page
Generate and return Access Token
Generate and Return Request Token and Wallet Authorize URL
Return Payment Method and Shipping Address
FIG. 5A

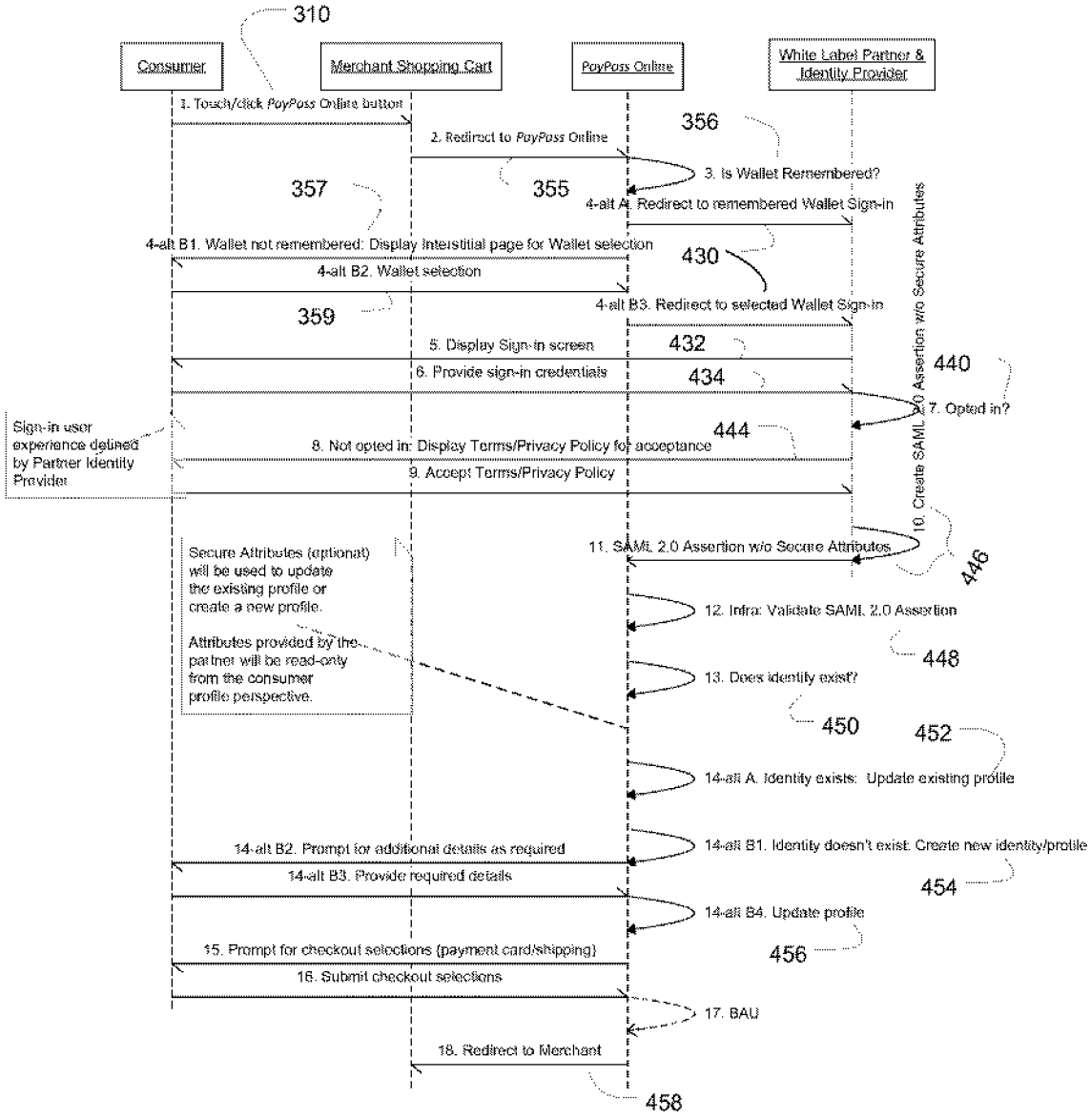
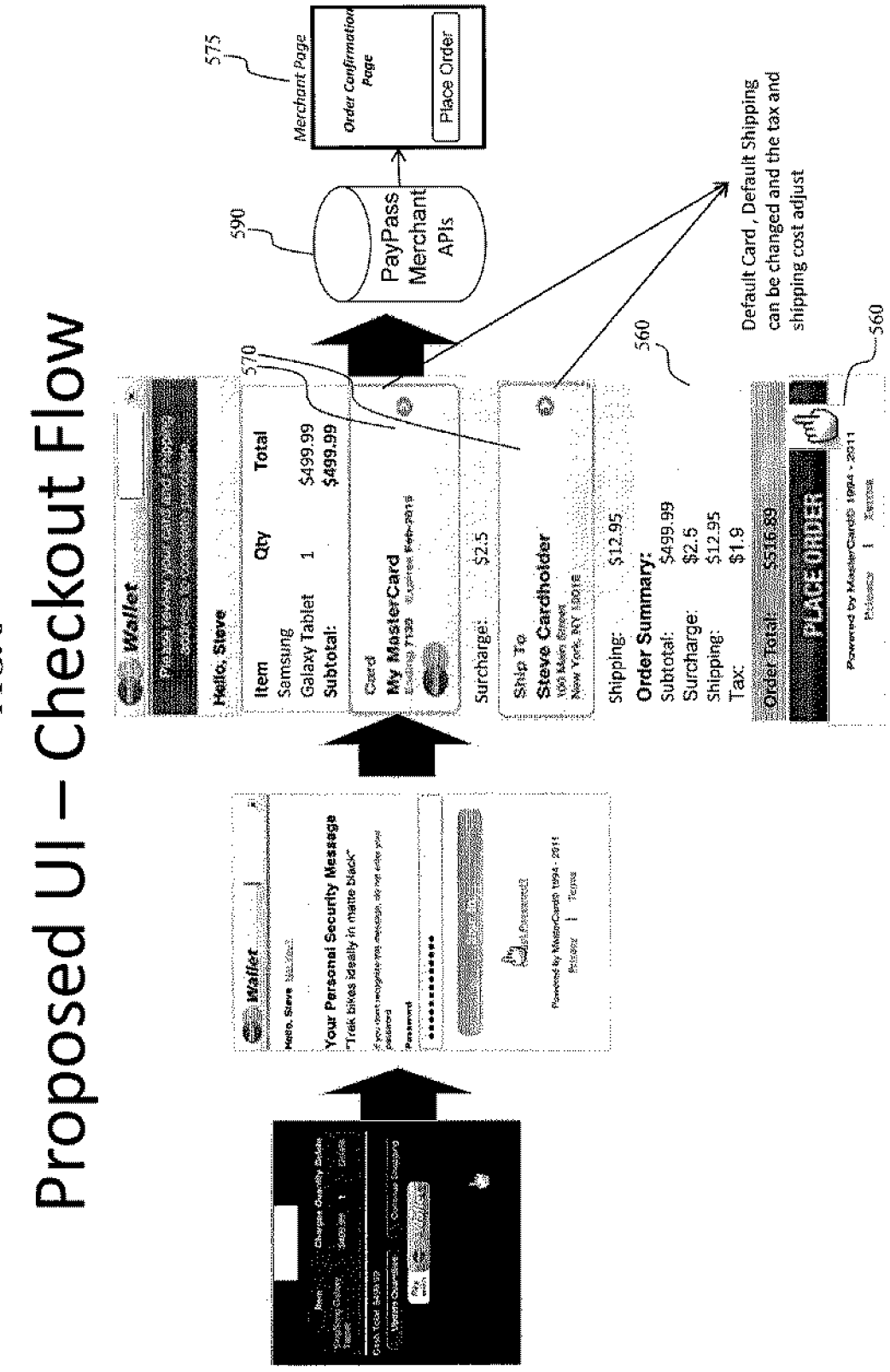

310
Consumer
Merchant Shopping Cart
PayPass Online
White Label Partner & Identity Provider
1. Touch/click PayPass Online button
2. Redirect to PayPass Online
356
3. Is Wallet Remembered?
355
357
4-alt A. Redirect to remembered Wallet Sign-in
4-alt B1. Wallet not remembered: Display interstitial page for Wallet selection
430
4-alt B2. Wallet selection
4-alt B3. Redirect to selected Wallet Sign-in
359
5. Display Sign-in screen
432
6. Provide sign-in credentials
434
440
10. Create SAML 2.0 Assertion w/o Secure Attributes
7. Opted in?
Sign-in user experience defined by Partner Identity Provider
444
8. Not opted in: Display Terms/Privacy Policy for acceptance
9. Accept Terms/Privacy Policy
11. SAML 2.0 Assertion w/o Secure Attributes
446
Secure Attributes (optional) will be used to update the existing profile or create a new profile.
Attributes provided by the partner will be read-only from the consumer profile perspective.
12. Infra: Validate SAML 2.0 Assertion
448
13. Does identity exist?
450
452
14-alt A. Identity exists: Update existing profile
14-alt B2. Prompt for additional details as required
14-alt B1. Identity doesn't exist. Create new identity/profile
14-alt B3. Provide required details
454
14-alt B4. Update profile
456
15. Prompt for checkout selections (payment card/shipping)
16. Submit checkout selections
17. BAU
18. Redirect to Merchant
458

FIG. 5B

FIG. 6

Proposed UI – Checkout Flow



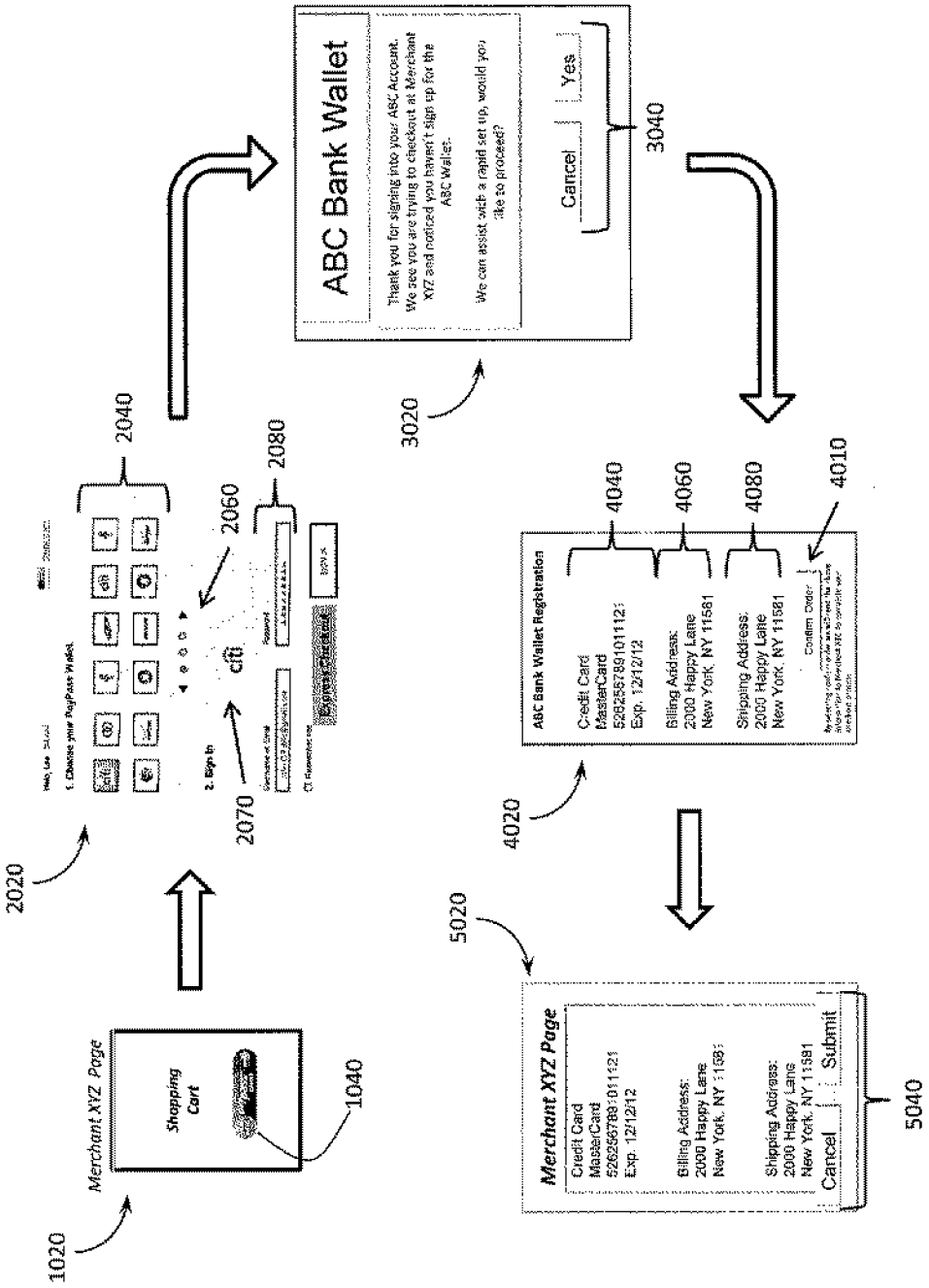
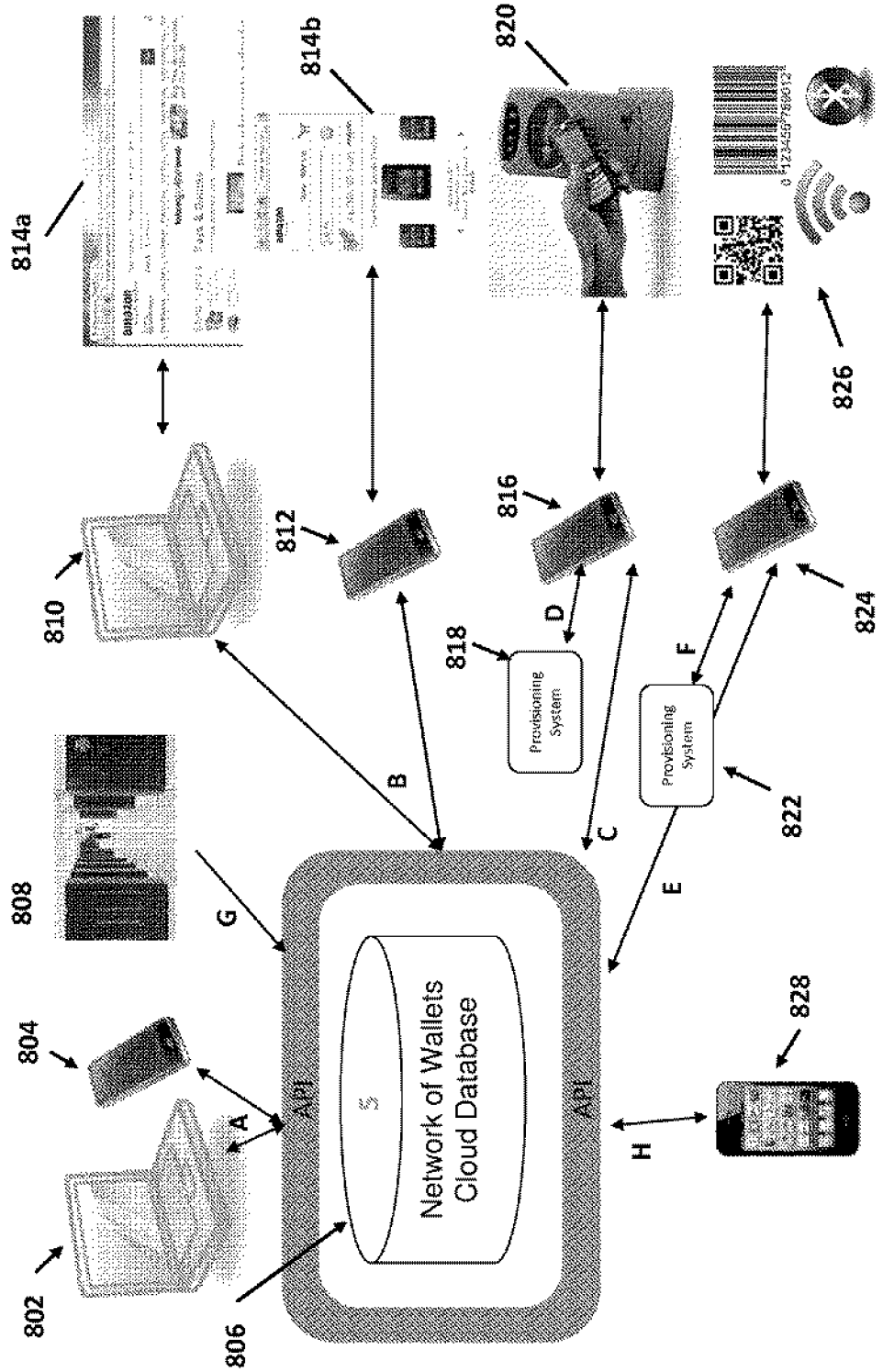

1020
Merchant XYZ Page
Shopping Cart
1040
2020
2040
2060
2080
2070
2. Sign In
3020
ABC Bank Wallet
Thank you for signing into your ABC Account. We see you are trying to checkout at Merchant XYZ and noticed you haven't sign up for the ABC Wallet.
We can assist with a rapid set up, would you like to proceed?
Cancel
Yes
3040
4020
ABC Bank Wallet Registration
Credit Card
MasterCard
Exp. 12/12/12
Billing Address:
2000 Happy Lane
New York, NY 11581
Shipping Address:
2000 Happy Lane
New York, NY 11581
Confirm Order
4040
4060
4080
4010
5020
Merchant XYZ Page
Credit Card
MasterCard
Exp. 12/12/12
Billing Address:
2000 Happy Lane
Shipping Address:
2000 Happy Lane
New York, NY 11581
Cancel
Submit
5040

FIG. 7

Fig. 8


814a
814b
820
826
810
812
816
824
818
Provisioning System
Provisioning System
822
808
804
802
806
828
Network of Wallets Cloud Database
API
API
A
B
C
D
E
F
G
H

CONVERGED CROSS-PLATFORM ELECTRONIC WALLET

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority under 35 U.S.C. §120 as a Continuation-In-Part of prior U.S. patent application Ser. No. 13/746,904, filed 22 Jan. 2013, entitled SYSTEM AND METHOD TO ENABLE A NETWORK OF DIGITAL WALLETS (Applicant Reference No. P00778-US-UTIL; Attorney Docket No. 1788-82), which in turn claims the benefit under 35 U.S.C. §119(e) of each of the following U.S. Provisional Patent Applications: Ser. No. 61/588,505, filed 19 Jan. 2012; Ser. No. 61/642,729, filed 4 May 2012; Ser. No. 61/642,792, filed 4 May 2012; and Ser. No. 61/642,799, filed 4 May 2012. The instant application further claims the benefit under 35 U.S.C. §119(e) of prior U.S. Provisional Patent Application Ser. No. 61/642,925, filed 4 May 2012.

[0002] The instant application is further related to prior U.S. patent application Ser. No. 13/209,312 (Applicant Reference No. P00655-US-UTIL; Attorney Docket No. 1788-65), and International PCT Application Serial No. PCT/US2011/047678 (Applicant Reference No. P00655-PCT-UTIL; Attorney Docket No. 1788-65 PCT), both filed 12 Aug. 2011, both entitled MULTI-COMMERCE CHANNEL WALLET FOR AUTHENTICATED TRANSACTIONS, and which prior applications in turn claim the priority benefit under 35 U.S.C. §119(e) and PCT Art. 8, respectively, of each of the following U.S. Provisional Patent Applications: Ser. No. 61/372,955 filed 12 Aug. 2010; and Ser. No. 61/468,847, filed 29 Mar. 2011.

[0003] The complete disclosure of each of the foregoing applications is hereby incorporated herein in their entireties by this reference for all purposes.

FIELD OF INVENTION

[0004] The present disclosure relates to electronic cashless transaction payments, and more particularly, to a system and method for enabling a consumer to have cross-platform access to a converged network of digital wallets.

BACKGROUND

[0005] The use of a digital wallet has quickly gained popularity, both for use in remote-based platforms and in "tap-to-pay" point-of-sale transactions using a cellular telephone, for example. Currently, there exist several different forms of digital wallets offered by different financial institutions, issuers and so on, and many more are in development. Such services are becoming available under many different brands including those of credit card suppliers and retailers, each of which may interface with different financing companies, and can be offered on different platforms, including point-of-sale technology (e.g., NFC), mobile applications, and remote online systems.

[0006] As consumers use digital wallets with more regularity, it is desirable to allow a diverse number of choices for competing brands of digital wallets according to a consumer preference. However, this can create a complicated system of overlapping functionality and interfacing menus for both the consumer, wishing to have more than one payment option, and merchants, who will need to process the different digital wallets through different channels. Accordingly, there is a need for a system to enable a network of digital wallets, which provides a link between multiple consumer interfaces provided on merchant web sites and an acceptance network for authorizing a purchase from any one of various digital wallet providers.

SUMMARY

[0007] The present invention provides a system for enabling a network of digital wallets which includes a common link to an acceptance network for authorizing a digital wallet purchase that allows multiple consumer interfaces via merchant landing pages and integration with various wallet providers. The acceptance network is preferably accessed through an acceptance mark button on a graphical interface provided to consumers on merchant landing pages. Selection of the acceptance mark provides access to various digital wallet services and providers for initiating a purchase. Accordingly, multiple merchant web sites can be linked through a single digital wallet acceptance mark, which provides access to a switch through which a wallet of choice is accessed by the consumer for payment at a remote location or at point-of-sale.

[0008] The system to enable a network of digital wallets also provides the features and functionality required to decouple the acceptance network from each digital wallet consumer interface.

[0009] The present invention also provides a method for authorizing a digital wallet transaction initiated by a consumer from a merchant web site. The method provides for payment using one of a plurality of digital wallets in the acceptance network.

[0010] A method for authorizing a digital wallet transaction initiated by a consumer from a merchant web site or app, in accordance with the present disclosure, includes providing an acceptance mark on a merchant landing page associated with the merchant web site or app for initiating the digital wallet transaction. The acceptance mark comprises a link to a host server for accessing an acceptance network for authorizing payment. The acceptance network comprises a plurality of digital wallets. A digital wallet is selected and purchase details including a payment card and a shipping address are selected for the transaction. An Access Token and a checkout resource URL associated with the digital wallet are generated by the host server, and the merchant web site or app sends the Access Token to the checkout URL to retrieve the purchase details for authorizing and completing the digital wallet transaction using the selected digital wallet.

[0011] In one aspect, a method for authorizing a digital wallet transaction initiated by a consumer from a merchant web site or app includes providing an acceptance mark on a merchant landing page associated with the merchant web site or app for initiating the digital wallet transaction, the acceptance mark comprising a link to a host server accessing an acceptance network for authorizing payment, the acceptance network comprising a plurality of digital wallets; routing the transaction to a digital wallet selected by the consumer from the plurality of digital wallets, the selected digital wallet capturing and validating the log-in credentials, the selected digital wallet capturing a payment card and a shipping address selected by the consumer for the digital wallet transaction; routing the transaction to the host server with purchase details including the payment card and the shipping address, the host server generating a postback merchant URL associated with the merchant web site or app, an Access Token and

a checkout resource URL associated with the selected digital wallet for retrieving the purchase details; and redirecting the transaction back to the merchant web site or app using the postback merchant URL, the merchant web site or app sending the Access Token to the checkout resource URL associated with the selected digital wallet to retrieve the purchase details for authorizing and completing the digital wallet transaction.

[0012] In another aspect, the method further includes displaying an interstitial page comprising a wallet selector switch in response to the consumer selecting the acceptance mark, the consumer selecting the digital wallet from the plurality of digital wallets for the transaction using the wallet selector switch.

[0013] In yet another aspect, the selected digital wallet is a default wallet, the default wallet being selected prior to the consumer selecting the acceptance mark. The method further comprises displaying an interstitial page associated with the default wallet in response to the consumer selecting the acceptance button.

[0014] Additional aspects of the method wherein the selected digital wallet is the default wallet can include the consumer establishing a default payment card and a default shipping address associated with the default digital wallet prior to selecting the acceptance mark, and providing an express checkout button associated with the default wallet, the default payment card and the default shipping address being captured for the transaction in response to the consumer selecting the express checkout button.

[0015] If the consumer is a recognized user of the acceptance network, in one aspect, the default wallet corresponds to one of the plurality of digital wallets most recently accessed by the consumer.

[0016] In an additional aspect, the selected digital wallet is a partner-hosted wallet, the method further comprising storing the purchase details including the selected payment card and shipping address in a temporary store associated with the checkout URL on the host server, and purging the temporary store in response to the merchant web site or app retrieving the purchase details for authorizing the digital wallet transaction.

[0017] In various aspects, the method can further comprise associating a coupon or offer with each of the plurality of digital wallets and displaying the coupon or offer associated with one of the plurality of digital wallets displayed on the wallet selector switch. The coupon or offer may be displayed, in one aspect, in response to the consumer hovering a pointer over the one of the plurality of digital wallets displayed.

[0018] Additional aspects of the method may include communicating the coupon or offer associated with the one of the plurality of digital wallets to the merchant web site or app prior to completing the digital wallet transaction, wherein the one of the plurality of digital wallets is the digital wallet selected from the plurality of digital wallets for the transaction.

[0019] Additional aspects of the method of the present disclosure can include associating a status with each of the plurality of digital wallets and displaying a graphical indicator of the status on the wallet selector switch.

[0020] The status can be associated with a capability to complete a pending transaction using the associated digital wallet, based on at least one of an amount of funds required for the transaction, a balance of available funds in the associated digital wallet, a class or merchant, a type of goods or service being transacted, an expiration of one or more card associated with the digital wallet, and whether a prior transaction using the digital wallet had failed.

[0021] In yet other aspects of the methods of the present disclosure, the host server displays a shopping order confirmation page prior to redirecting the transaction back to the merchant web site or app. The shopping order confirmation page includes the purchase details, the purchase details including shipping charges, taxes, and a surcharge rate and charge associated with the digital wallet selected. The methods include dynamically updating the shopping order confirmation page in response to the consumer selecting a different one of the plurality of digital wallets for the digital wallet.

[0022] In yet additional aspects, a history toggle can be provided on an interstitial page, the history toggle providing access to the historical purchase data of a recognized consumer of the network of wallets, the historical purchase data including data associated with each payment card registered to the consumer within the acceptance network.

[0023] In further aspects, the method includes returning a Request Token generated by the host server in response to the consumer selecting the acceptance mark, the host server generating a verifier associated with the Access Token, and the merchant web site or app capturing the checkout resource URL and the verifier after the transaction is redirected back to the merchant web site or app, the merchant web site or app using the Request Token and verifier to retrieve the Access Token from the host server for sending to the checkout resource URL and retrieving the purchase details.

[0024] In still further aspects, the method can include displaying an interstitial page comprising a wallet selector switch and a wallet log-in menu in response to the consumer selecting the acceptance mark, the consumer entering log-in credentials in the wallet log-in menu associated with a digital wallet selected from the plurality of digital wallets for the transaction.

[0025] In additional aspects, the selected digital wallet can be a federated co-branded wallet, the interstitial page being displayed and hosted by the host server, the interstitial page comprising a wallet log-in menu, wherein the log-in credentials entered by the consumer in the log-in menu are captured and validated by a partner server against a partner database, the method comprising framing the log-in menu in a widget for accessing the partner server.

[0026] These aspects can further include federating the captured log-in credentials to the selected wallet in response to the consumer being recognized by the partner server as an authorized user of another partner-hosted product.

[0027] Still further, aspects can include the partner server sending a SAML token and provisioning details of payment cards and shipping addresses associated with the consumer to the federated co-branded wallet displayed on the host server in response to validating the log-in credentials.

[0028] If the consumer is a recognized user of the acceptance network, additional aspects can include the partner server automatically updating the details of the payment cards in the federated co-branded wallet associated with the consumer in response to the consumer selecting the federated co-branded wallet for the transaction, the details including consumer contact information, payment cards, and shipping addresses.

[0029] If the consumer is recognized by the host server as an unregistered user of the acceptance network, in additional aspects, the method can include automatically creating a new

digital wallet account associated with the federated co-branded wallet for the consumer using the captured log-in credentials.

[0030] A method is also provided for authorizing a digital wallet transaction initiated by a consumer from a merchant web site or app, the method including: providing an acceptance mark on a merchant landing page associated with the merchant web site or app for initiating the digital wallet transaction, the acceptance mark comprising a link to a host server accessing an acceptance network for authorizing payment, the acceptance network comprising a plurality of digital wallets, the plurality of digital wallets including a federated co-branded wallet; displaying an interstitial page in response to a consumer selecting the acceptance mark, wherein the consumer is a registered user of the acceptance network, the interstitial page displaying a wallet interface to the federated co-branded wallet, the wallet interface being hosted on the host server, the wallet interface comprising a wallet log-in menu framed in a widget for accessing a partner server and a partner database associated with the federated co-branded wallet; capturing and validating the log-in credentials by the partner server against the partner database in response to the consumer entering the log-in credentials in the log-in menu, the partner server sending a SAML token to the federated co-branded wallet hosted by the host server and redirecting the transaction to the host server in response to validating the log-in credentials; provisioning, by the partner server, details of payment cards and shipping addresses associated with the consumer to the federated co-branded wallet on the host server in response to recognizing the consumer as the registered user; displaying a payment interface for capturing a payment card and a shipping address, the payment interface capturing the payment card and the shipping address selected by the consumer for the digital wallet transaction; and redirecting the transaction back to the merchant web site or app after capturing purchase details of the transaction, the purchase details including the payment card and the shipping address selected, the merchant web site retrieving the purchase details for authorizing and completing the digital wallet transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] FIG. **1** is a block diagram representation of an embodiment of a system of the present disclosure for enabling a network of digital wallets.

[0032] FIG. **2** is a block diagram representation of an embodiment of a method for enabling a network of digital wallets.

[0033] FIG. **3**A is a representation of an embodiment of a user log-in interface and switch for accessing the network of digital wallets in accordance with the present disclosure.

[0034] FIG. **3**B is a representation of another embodiment of a user interface and another embodiment of a switch for displaying and accessing the digital wallets in accordance with the present disclosure.

[0035] FIG. **4**A is a system flow representation of a checkout transaction with a partner-hosted wallet in accordance with an embodiment of a system and method of the present disclosure.

[0036] FIG. **4**B is a sequence diagram for the method of FIG. **4**A for completing a digital wallet transaction in accordance with the present disclosure.

[0037] FIG. **5**A is a system flow representation of a checkout transaction with partner login and direct provisioning in accordance with another embodiment of a method of the present disclosure.

[0038] FIG. **5**B is a sequence diagram for the method of FIG. **5**A for completing a digital wallet transaction in accordance with the present disclosure.

[0039] FIG. **6** is a representation of a flow sequence on checkout with in-wallet dynamic update of shopping order details in accordance with an embodiment of a method of the present disclosure.

[0040] FIG. **7** is a representation of a flow sequence for real-time wallet creation in accordance with an embodiment of a method of the present disclosure.

[0041] FIG. **8** is a representation of the multiple consumer interface pathways to a converged electronic wallet.

DETAILED DESCRIPTION OF EMBODIMENTS

[0042] The following sections describe exemplary embodiments of the present invention. It should be apparent to those skilled in the art that the described embodiments of the present invention provided herein are illustrative only and not limiting, having been presented by way of example only. All features disclosed in this description may be replaced by alternative features serving the same or similar purpose, unless expressly stated otherwise. Therefore, numerous other embodiments of the modifications thereof are contemplated as falling within the scope of the present invention as defined herein and equivalents thereto.

[0043] A "digital wallet" is known in the art and can be used by a consumer associated with the digital wallet for making an electronic transaction. Generally, the digital wallet has a data or information component associated with the consumer and transaction data, including payment methods, shipping addresses, billing address and other information. The information component is associated with a consumer interface for the consumer accessing the digital wallet to input necessary information for the transaction. The digital wallet is also associated with a software or services component for authorizing and completing the electronic transaction, including security and encryption for the customer's personal information and for the actual electronic transaction. The system and method of the present disclosure provide the functionality and services required to connect multiple consumer interfaces to a single acceptance network for payment which supports a plurality of digital wallets.

[0044] Examples of such consumer interface platforms are large and growing. Just a few of these are mentioned in the background above, namely point-of-sale technology, such as Near Field Communication (NFC), mobile applications for web-enabled smartphones, and remote on-line systems for traditional electronic commerce. For example, certain mobile electronic devices are provisioned with NFC capability, allowing them to function and substitute for existing IC based technology provided in certain payment card devices (e.g., EMV or the like).

[0045] Other consumer interface platforms include a mobile-device enabled system disclosed in the commonly assigned U.S. Provisional Patent Application Ser. No. 61/711,901 (Applicant Reference No. P00927-US-PROV; Attorney Docket No. M01.227P), filed 10 Oct. 2012, and entitled METHODS AND SYSTEMS FOR CONDUCTING REMOTE POINT OF SALE TRANSACTIONS, the entire disclosure of which is hereby incorporated herein by this

reference for all purposes. Generally speaking, the aforementioned application discloses a payment system styled as "PoW3", and concerns a method of mobile-device based e-commerce (or "m-commerce"). To consummate a transaction, the merchant will present a scanable code (e.g., bar code, QR code or the like) or otherwise interact with the user's mobile device (via e.g., WiFi, Bluetooth, SMS, without limitation). This transaction event (code scan, communication, etc.) will trigger the user's mobile device to establish a connection with a payment gateway. The payment gateway will synchronize the contents of the transaction with the user's mobile device, and provide access to the user's electronic wallet for payment. From their mobile device, the user may select a wallet and/or payment device to fund the transaction, or in some cases, a default wallet or payment device will have been previously selected.

[0046] The present disclosure converges the various consumer interface platforms, in this case merging the functions of both remote and NFC payment, among other interface platforms, giving the purchaser access to a single electronic wallet for online E-commerce and a variety of mCommerce scenarios, some including brick and mortar, face-to-face (F2F), and/or point-of-sale (POS) transaction payments. The network of wallets has a network operator intermediating payment transactions between merchants and wallet providers. Wallet providers represented generally reflect a co-branded or 'white label' wallet **80**, a hero wallet **70**, that is one operated by the same entity operating the network of wallets, or a partner-hosted wallet **60** operated by a partner participating in the federated network of wallets. In this way, the parallel consumer interface platforms, such as remote platform enabling e-commerce payments, an NFC platform, and/or others, into a single converged payment platform that is usable in either or both transaction settings.

[0047] The plurality of digital wallets can include any digital wallet suitable for remote or on-line purchases, including those digital wallets offered as a mobile app, particularly, a mobile phone app.

[0048] An "app" is used herein as that term is known, to refer to an application for a mobile device. An app, or mobile app, is a software application designed to run on, for example, smartphones, tablet computers, and other mobile devices.

[0049] A merchant page or merchant landing page is a consumer-facing graphical interface accessed from a merchant web site, or app. The acceptance network is preferably accessed by a consumer by selecting an acceptance mark provided on the merchant page.

[0050] A partner is a bank, retailer, or other third-party seeking to integrate its proprietary wallet solution into the acceptance network of digital wallets, providing its users with access to the network of wallets services.

[0051] A Request Token is used as that term is known in the art and is a request for authorized access to a service using, for example, an industry standard security OAuth, which allows third party web sites to share user data without requiring additional credentials. The network of digital wallets preferably uses this method for securing transactions to and from the host network of wallets' services. Additional tokens are used, such as an Access Token, to provide a location or URL (Uniform Resource Locator) from which data can be accessed, and a Verifier Token, to verify a party requesting access to data.

[0052] OpenAPI is an industry standard for enabling services to be easily shared across third party providers. The digital wallets preferably use this standard to interconnect the host network of wallets services with partner services.

[0053] The various services and applications referred to herein are executable programs running on a host (network of digital wallets or "NoW") server, and/or on a partner server, as indicated, according to the type of digital wallet. The flow of a method for completing a purchase initiated from a merchant page, from a merchant web site or app, is directed by the hosted program code to switch between wallets and to direct the flow between a merchant and a digital wallet for completing a purchase. A processing device associated with the merchant web site or app executes the back-end services required to interact with the host server and digital wallets to complete the purchase and authorize a transaction with the digital wallet.

[0054] The corresponding method steps for completing a purchase are preferably stored in memory associated with the host server and with the particular digital wallet, and executed by a processing device. Depending on the type of wallet selected by a purchaser, cardholder shipping and other details necessary to complete a transaction are stored in a database associated with a partner server hosting a partner wallet, or in a database associated with the host server.

[0055] Referring to FIG. **1**, an embodiment of a system to enable a network of digital wallets **10** includes a host ("Now") server **15** with secure databases **16** for storing cardholder, card and shipping data associated with various wallets offered within the network of digital wallets. The server **15** includes services for facilitating and monitoring connectivity between merchants **20** and an acceptance network **25** for authorizing a purchase. The acceptance network includes a plurality of digital wallets. Services and resources offered from the host server **15** to wallet providers and merchants participating in the network of wallets preferably include application programming interfaces (API's) for shared services for integrating wallet providers and merchants into the network of wallets, standards for consumer authentication, and the availability of, and ability to select from, multiple consumer interfaces, depending on the type of digital wallet a wallet provider (partner) chooses to offer. The services, applications, and executable programming steps for performing the methods of the present disclosure are preferably stored in memory **18** associated with the host server **15** and executed by a processing device **19**.

[0056] Referring still to FIG. **1**, digital wallet options include a partner-hosted ("partner") wallet **60**, which maintains all consumer details and purchase data and consumer log-in credentials in the partner's own secure database **62** and is hosted by a partner server **64** providing the partner wallet web site **60**. Additional options include a hero/retail wallet **70** hosted on the NoW server **15**, which maintains all consumer details, purchase data, and consumer login credentials in the host's databases **16**, and variations of a white-label wallet **80**, having a mix of control shared between the partner and host. The white-label wallets can include a federated and non-federated white-label wallet, embodiments of which are described further herein.

[0057] Referring to FIG. **2**, in one embodiment of a method of the present disclosure for enabling a network of digital wallets, and for authorizing a digital wallet transaction initiated by a consumer through the network of digital wallets, an icon or acceptance mark **100** is preferably provided as a link on a merchant landing page **110** to a switch **125** for routing the consumer to any digital wallet in the acceptance network **25**.

The purchaser selects the icon or acceptance mark **100** representing the network of wallets displayed on a merchant's shopping cart landing page **110**. The purchaser is brought to an interstitial landing page **120** to facilitate interaction with the network of wallets. The interstitial page **120** includes a wallet selector **125** for switching between the wallets available to the purchaser. In the embodiment of a switch selector shown in FIGS. **2** and **3**A, the switch capability is provided by selection of the appropriate tab displaying the desired wallet. Each tab of the wallet selector is associated with a hyperlink to a particular URL associated with the digital wallet, so that selection of a particular tab displays the associated digital wallet landing page.

[0058] The consumer selects one of the wallets and the payment process proceeds along one of the paths **85**, in accordance with the type of digital wallet selected. As shown schematically in the embodiment of FIG. **1**, the different types of digital wallets can include hero/retail NoW-hosted wallets **70**; federated or non-federated co-branded or white-label wallets **80**; and partner-hosted wallets **60**.

[0059] In the embodiment shown in FIG. **2**, the consumer is an unrecognized user. An unrecognized user includes a consumer who logs in for the first time, not yet registered with the network of wallets. An unrecognized user also includes a consumer who has cleared cookies previously stored on the user's device to allow identification. Referring to FIG. **3**A, upon selection of the acceptance button **100**, the unrecognized user is directed to an embodiment of the interstitial landing page **120** which allows the unrecognized user to create a wallet, and/or to select a wallet for payment. In this embodiment, the page is hosted by the network of wallets host server. It also includes a wallet selector **125** for selecting and signing in to different wallets. Preferably, an option for creating a hero wallet account **105** is also provided so that a new account can be created by a first time user of NoW directly through a menu **105** on the landing page **120**.

[0060] In additional embodiments, if the consumer is a recognized user of the network of wallets, selecting the acceptance mark **100** automatically routes the payment process through the switch to a default digital wallet web site, displaying the default digital wallet to the consumer. The default wallet can be, for example, the last wallet the consumer used, or one pre-selected as the default by the consumer.

[0061] A consumer is referred to as a recognized user of the network of wallets, if recognized, for example, by a cookie or a fingerprint or MAC address of the machine from which they are browsing, and is further recognized by the network of wallets as having login credentials associated with one of the digital wallets in the network of wallets.

[0062] In preferred embodiments, the interstitial landing page that is displayed with an open wallet, regardless of whether it is a default or user-selected wallet, will preferably still include the digital wallet selector **125**, along with the wallet branding and sign-in menu for the user's default or user-selected wallet. Accordingly, an option to access (or create) alternate (or additional) digital wallets remains available to the consumer until completion of the checkout and purchase process.

[0063] Referring to FIG. **3**A, in various embodiments, the interstitial landing page **120** can offer a consumer a selection of his or her country of residence. Depending on the country selected, a different menu of digital wallets available to the consumer can be displayed.

[0064] It should be appreciated that the tabulated menu shown in FIGS. **2** and **3**A is one non-limiting embodiment of a wallet selector of the present invention. One of ordinary skill in the art can appreciate that any number of variations of wallet selectors for accessing one of the digital wallets available in the network are within the scope of the invention, including a revolving pane design and a daisy wheel. The wallet selector can additionally include functionality to allow a consumer to compare different advantages of the various wallets prior to completing the purchase and checkout process. For example, various embodiments of the switch **125** can include displaying information such as specific offers or coupons associated with each wallet choice in the switch **125**. In one embodiment, a coupon or offer is displayed to the purchaser, for example, as a pop-up, when a pointer is hovered over the associated wallet. These offers or coupons can be communicated to the merchant upon selection of the wallet, and are applied during the checkout process.

[0065] Referring to FIG. **3**B, in one embodiment of the wallet selector **125**, a daisy wheel **122** is used to display all wallet options available to a particular user after selection of the acceptance mark **100**. A last-used wallet prong **124** of the daisy wheel (assuming a recognized purchaser), or other preferred wallet prong, can be highlighted, for example, by displaying the prong more prominently than the other available wallets. An "additional wallets" prong **126** can provide a link to an additional wallet selector showing more digital wallets. In various embodiments, hovering a pointer over any one of the prongs highlights that selection, and can simultaneously display the interstitial page **120** for a particular digital wallet, in addition to various coupons and offers associated with a purchaser's use of that wallet for the purchase. Incentives to create a digital wallet to unrecognized users of that particular digital wallet can likewise be displayed.

[0066] Referring again to FIG. **2**, the purchaser may choose from among the available digital wallets, which can include a Hero wallet **70**, a wallet operated and maintained by the provider or host **15** of the network of wallets, in this example, by assignee MasterCard®. The digital wallets can also include a white-label or co-branded wallet **80** that is maintained and operated by the provider or host **15** of the network of wallets, but which carries the branding of a partner entity in the network of wallets. In this embodiment, the purchaser may also choose a partner wallet **60**, one which is maintained and operated by a partner entity.

[0067] Referring to FIG. **3**A, the consumer enters login credentials on the selected wallet page, which can be hosted on the network-of-wallets host server or on the selected partner server. Preferably, the interstitial landing page **120** captures the log-in credentials for a consumer, for example, a User ID, such as an email address, along with an associated password. The payment process continues by validating the log-in credentials of the purchaser and encrypting the fields with a key issued by the wallet owner of the selected digital wallet to insure the login credential integrity. This process will differ depending on the type of wallet selected. For a hero wallet **70**, the host validates against its own database **230**, while for a partner-hosted wallet **60**, the partner validates **240** against its own database. As described further in reference to FIGS. **5**A and **5**B, for various embodiments of a co-branded **80** wallet, while the log-in page can be hosted on the NoW server, the login credentials can be validated against the partner's database **240**, or against the host database, where the host database maintains the partner's customer database.

[0068] Once the log-in credentials are validated, in various embodiments, a payment card and shipping address selection page **255** is displayed so that the consumer can choose a payment method. The choice of wallet will determine from which database the page **255** will be retrieved, e.g., from a partner database or from a host (NoW) database, and how this page is presented to the consumer. For example, in one embodiment, a co-branded wallet **80** is hosted by the network of wallets (MasterCard®) services, but the partner creates and controls the design of the page displayed to the consumer, which will follow the partner's brand. In this way, the network of wallets system enables partners to skin the MasterCard® host services.

[0069] Once the consumer selects and confirms the card selected for payment and the shipping address, the validation and shipping selection information is preferably aggregated and transmitted to the merchant through application programming interfaces (API's) **260** integrated on the merchant web site. The merchant retrieves the consumer data provided and displays an order confirmation page to the consumer **270**.

[0070] The system and method to enable a network of digital wallets of the present disclosure is a token mediation driven process connecting a merchant network **20** to a network of digital wallet providers **25**. A system flow diagram of a checkout transaction is provided in FIG. **4**A using a partner-hosted wallet **60** in a network of digital wallets hosted by MASTERCARD® under its PAYPASS™ trademark, and a hero ("PayPass") wallet **402** provided by the network of wallets host ("PayPass" services). A corresponding sequence diagram is provided in FIG. **4**B. For the partner-hosted wallet **366**, the partner maintains all control and responsibility for maintaining consumer login details and validation, storing consumer login and account management data and other consumer data in its own secure database. In addition, the partner designs and hosts the partner wallet web site landing pages.

[0071] As described further herein, there are a few points of partner integration into the checkout process, where partners must either accept or invoke transactions from a host wallet services layer **300**: a Checkout Initialization, Address Verification, and Checkout Authorization. The Checkout Initialization process defines what happens when the user chooses to make a payment with a particular wallet, in this case, one that is partner hosted. The Checkout Authorization process continues after the user selects the card and shipping options and is ready to complete the checkout. It is invoked, in this case, by the partner-hosted wallet to authorize the merchant to access consumer's checkout data, and is hosted by the network of wallets' host (PAYPASS™) server. The Address Verification Service can be used at various times to determine if a given merchant provides shipping to a given set of locations.

[0072] To begin a checkout process from a merchant web site or from an app provided on a mobile device **285**, a merchant landing page is displayed which includes an acceptance mark **100** (in this example, PAYPASS™). The consumer selects the acceptance button **310** to access the network of wallets service.

[0073] Programming applications running on a processing device in the back-end (server) **290** of the merchant web site or app retrieve a checkout identifier, consumer key and developer private key from local storage **320**. The consumer key and developer private key are sent to the host (PAYPASS™) server **300** hosting the network of wallets service to get a Request Token and Authorize Wallet URL **330** from an open API. The Request Token and Authorize Wallet URL are generated and returned **340** to the merchant **290** and forwarded to the merchant web site along with various merchant data, such as the merchant's accepted card types, International Shipping Boolean, and a Checkout Identifier **350**, for redirecting the consumer to an interstitial landing page **355** for sign-in to the network of wallets and wallet selection.

[0074] The interstitial landing page, which includes a sign-in menu for capturing login credentials and a wallet selector, is preferably displayed **360** with the merchant's branding from a network-of-wallets hosted (PAYPASS™) checkout site **362**. The fields on the login page for capturing credentials are preferably encrypted with a key issued by the wallet owner. The wallet selector includes those digital wallets that are available in the network of wallets and accepted by the merchant.

[0075] When the consumer selects a partner wallet **364** from the wallet selector, the consumer is directed to a partner site which hosts and maintains the partner digital wallet. The PayPass Wallet Services **300** executes a Checkout Initialization transaction with the partner hosted wallet selected **366** to start the sign in process. The partner wallet presents an interface to the user for logging in **368**, selecting a payment method **370** and a shipping address (if applicable) **372** and confirming the order **374**. An Address Verification Service (see FIG. **4**B) **332** is invoked during the Checkout Initialization, either before or after selecting the shipping address **372**, to confirm that the Merchant is willing to ship to each shipping address listed (or selected). The user wallet and payment credential experience is controlled by the partner for a partner-hosted wallet. The consumer can review the order **374** before selecting an "AuthorizeOrder" option **334**, for example, to initiate the Checkout Authorization process to continue with the checkout. When ready for checkout, the partner site sends the flow back to the PayPass Wallet Services **300** for executing the Checkout Authorization transaction through an open API, passing in the Request Token, payment method, shipping address and details, and preferably a transaction ID **334**.

[0076] In the Checkout Authorization process, the Request Token is authenticated, and the payment method selected and any details of the purchase including shipping address, consumer contact information, and merchantID from the consumer's digital wallet are passed from the partner site to the PayPass server **300**, where it is stored in a temporary store or database, referred to herein as "Temp Store," as a unique record in a relational database object. The Temp Store database preferably stores all checkout details from the partner wallet for that consumer required to complete the purchase, including a payment method, shipping address, contact, a network of wallets' provider ID, and a merchant ID, for example. The PayPass server **300** generates a network of wallets (PayPass) Checkout Resource URL and verifier for obtaining an Access Token in order to retrieve the information temporarily persisted or stored in the Temp Store, and a Merchant Postback URL **378**, the site to which the browser or app will redirect control back to the merchant and passes the URL and verifier back to the merchant using the Merchant Postback URL **380**.

[0077] After the checkout is authorized by the PayPass server, the process continues by directing flow back to the Merchant from the partner wallet using the Merchant Postback URL **380** provided by the PayPass server **300**. At this point, control is passed back to the merchant web site, which captures the Checkout Resource URL and verifier **382**, and

uses the Request Token and verifier together to obtain the Access Token from the PayPass server **384**. The PayPass server generates and returns the Access Token **386** to the merchant **290** (for the purpose of obtaining access to the payment details), which then sends the Access Token to the partner-hosted Checkout Resource URL to retrieve the payment method and details, including shipping address, from the Temp Store **388**. The data is retrieved from Temp Store **390** and a response with details from Temp Store is returned to the merchant **392** and used in the submission of a financial payment transaction from the merchant.

[0078] Temp Store is purged either when it expires (assuming it was not retrieved) within minutes, or immediately after the data is accessed by the merchant.

[0079] The merchant **285** can then display an order confirmation page **394**. At this point, control is back to the merchant and any desired additional checkout options can be presented to the consumer prior to submitting the transaction details to a payment gateway **396** for finalizing and confirming completion of the purchase **398**.

[0080] For comparison, FIG. **4**A also shows the flow of a transaction initiated after a purchaser selects **400** a wallet, which is a hero or host wallet (PayPass Wallet), from the wallet selector. In this case, once the login credentials are captured from the hero site **402** and forwarded to the server **404**, the Request Token is authenticated, as it was for the partner wallet, the authentication service binding the Request Token to the transaction **406** and generating and returning the Verifier to the applicable wallet **408**, in this case, to the hero wallet **402**. A Checkout Resource URL is generated **412** and the Checkout Resource URL and Verifier to the applicable (hero) wallet are returned to the merchant using a postback Merchant URL.

[0081] Other embodiments of partner wallets in the network of wallets are possible offering varying levels of control by the partner and various integration points into the acceptance network of wallets, referred to as co-branded wallets. For example, a non-federated co-branded "White Label" option allows the partner wallet to be hosted, controlled, and maintained by the host (MASTERCARD® or PAYPASS™) server. The consumer selects and logs into the partner wallet site, which is hyperlinked to the PayPass-hosted White Label partner wallet. All consumer data and login credentials are preferably bulk-uploaded and stored in secure containers maintained by the host for the partner or provisioned to the cloud. The partner provides a bulk upload of consumer and card data to the PayPass database, or provisions the cloud for use in the network of wallets.

[0082] As shown in FIG. **5**A, if the consumer selects a non-federated co-branded wallet **401**, the process flow, including the Checkout Initialization and Checkout Authorization, to complete a purchase order through the network of wallets acceptance button on a merchant page is essentially a clone of the hero wallet shown in FIG. **4**A. Control never leaves the host, except that the partner wallet's brand is displayed in the wallet selector landing page and subsequent landing pages after selection of the co-branded partner wallet. The partner creates the "skin" with its brand for the landing pages, including login and shipping pages, and provides the skins to the host which can be stored in a partner container in the host database. The co-branded landing page is displayed to the consumer after selection of the co-branded partner wallet, and while hosted on the PayPass server, appears to the consumer to be a partner hosted wallet. The login credentials and card are validated by the PayPass server and the partner is responsible for providing updates.

[0083] Referring to FIGS. **5**A and **5**B, another co-branded digital wallet option available to partners in the network of wallets is a federated, skinned White Label partner wallet that uses partner login credentials by framing the login and password prompts in a widget for accessing the wallet owner (partner) site, while the interstitial landing page **120** is a user interface hosted by the network of wallets host. The consumer's login credentials **123** are captured and validated by the partner and are federated to the network of wallets. No wallet creation and setup is required if the customer's login credentials already exist for one of the wallet owner cards. The consumer interacts with the White Label wallet without requiring an additional login sequence. The partner supplies the user experience and functionality to support authentication and password recovery within their own hosted web/mobile property. All other data and services are hosted by the network of wallets.

[0084] In one embodiment, when ready to initiate a purchase on a merchant site, a customer selects the acceptance button and is directed to the federated White Label wallet via the selector interstitial page. The consumer logs in to the partner wallet site from the landing page and login access and validation is handled at the partner site. The credentials are then passed to the host network of wallets service in a single login seamless to the customer. The federated single sign-on capability is preferably provided by SAML integration of the partner with the network of wallets host services. The partner controls access to their White Label Wallet and passes federated credentials via SAML 2.0, for example, to PayPass online hosting services for access. The partner sends a SAML token to the host network of wallets services, and a security assertion data logs the customer into the network of wallets. The token contains customer data attributes to setup the wallet and to insert cards into the wallet automatically.

[0085] This digital wallet option also allows direct partner provisioning. In other words, each time the recognized consumer of this type of federated skinned partner wallet logs in to the wallet, the partner feeds existing consumer data dynamically into a wallet. This data includes profile information, payment cards and addresses. The data is encrypted, supplied as an extension to the SAML token exchange and refreshed with each consumer login.

[0086] FIG. **5**A depicts the flow of the checkout process when the consumer is leveraging a federated White Label Partner wallet with partner login credentials. The browser will remember the last wallet selected, minimizing the number of steps in the consumer sign-in process. In the case where the last wallet is unknown, the consumer will be presented with a NoW (PayPass) hosted page listing of wallet providers allowing the consumer to select a wallet and sign-in. The partner provides and maintains the consumer experience and services to authenticate the consumer, in turn providing assertion of identity for the consumer to NoW. The partner also provides consumer cardholder and profile data for the purposes of registering and refreshing a consumer's data, and captures email addresses and mobile telephone numbers for cardholders, which are passed to the network of wallets server to create a wallet account for the user.

[0087] Referring to FIGS. **5**A and **5**B, for the recognized user of a federated White Label (co-branded) wallet, when the consumer clicks on the acceptance button **100** from a merchant page to initiate checkout, the process steps and flow for

retrieving a Request Token and Authorize Wallet URL and redirecting the consumer to the Network of Wallets checkout site **362** are the same as for the partner-hosted and hero wallets. Once flow is directed from the merchant site to the NoW site **355**, if the wallet is remembered **356**, flow is directed to the default wallet (co-branded) page **430**. If no wallet is remembered (unrecognized user) **357**, an interstitial page for wallet selection is displayed to the consumer **359**. Upon selection by the consumer, flow is directed to the wallet co-branded page **430**.

[0088] If the federated co-branded wallet is selected or defaulted to, the wallet is displayed for log-in **432** and the consumer enters sign-on credentials (login and password) **434** through the partner-hosted widget for capture of login credentials directly by a partner identity provider **436**. The partner authenticates the user **442** and if a new wallet is being created (the user has not yet opted in to the co-branded wallet **440**), requires the user to accept terms and conditions **444**, and creates SAML assertion and, optionally, secure attributes **446**, and passes the SAML assertion to the network of wallets' co-branded wallet services. The NoW validates the SAML assertion **448** and determines if the consumer identity exists in the NoW **450**. If the consumer is identified as a registered user of the NoW **452**, the consumer data is provisioned from the partner and updated to the NoW before proceeding. If a profile of the consumer does not exist (not a previously registered user), a new consumer profile and identity is created **454**, and additional details as required to complete a purchase, such as payment method and shipping address, are requested and entered by the consumer **456** before redirecting flow to the merchant **458** to complete the checkout process.

Additional Enhancements of the Consumer Experience During Checkout: Express Checkout

[0089] In various embodiments, an express checkout option is available to a consumer after opting to make a purchase through the network of wallets, which avoids the extra step of selecting a shipping address in addition to a payment card. This express checkout option is also applicable to other digital wallet options, not only those provided within a network of wallets. In one embodiment, a consumer registers for at least one of the digital wallets available in the network of wallets, and establishes a default card and shipping address. The consumer selects an acceptance mark **100** available from a merchant page (e.g., PAYPASS™) to access the network of wallets after a consumer places their items in a merchant's shopping cart. Because a consumer has previously established and accessed a wallet, the consumer is brought to the default wallet page. Recognition can be through cookies or device detection/finger printing, for example. As a recognized user, the username is pre-populated and the default wallet is highlighted and receives hero placement. If the consumer opts to use a different wallet, other wallet options can be chosen from a wallet selector provided on the wallet page.

[0090] Next, the consumer enters his/her password and selects an Express Checkout Button, so that the consumer is not brought to a card and shipping address page. Instead, the consumer's default card and address are automatically used and the consumer is not required to review them. The consumer is brought back to the merchant page, which displays the card and address details that were passed directly to the merchant via an API.

[0091] Optionally, prior to bringing the consumer back to the merchant page, an interstitial page is provided by the selected (default) wallet for confirming the details of the credit card, which is preferably referred to by a previously established nickname or by the last 4 digits of the card. The consumer clicks on a button to confirm the order and details and is then brought back to the merchant page.

Checkout Enhancements

[0092] Various additional embodiments of the system and method of the present disclosure are directed to in-wallet checkout enhancements available before control is redirected back to the merchant web page. In a current, known on-line checkout experience, a consumer logs in to a wallet or credit card from a merchant's checkout page. The wallet stores credit card and the associated billing address and shipping addresses, which can be used to populate address fields. During checkout, the consumer logs into the wallet, and selects a credit card and shipping address. A shipping option selection and order review, which includes shipping and tax charges, is only available to the consumer after leaving the wallet services pages, including shipping and card information, and arriving on the merchant site. No transaction history or spend tracking is available.

[0093] In various embodiments of the present system, improvements to the in-wallet checkout experience and added functionality for tracking wallet usage and expenditures are available. For example, in one embodiment, services are provided to enable a digital wallet to dynamically update the shopping order total with particular details, such as surcharge, shipping cost and tax. Such selections can be offered within the wallet interface, based on consumer selection of the credit card and shipping address. Additional details such as shipping options and costs associated therewith can also be provided. In particular embodiments, such details can be displayed dynamically when a consumer uses a mouse to hover over a particular wallet available in the network of wallets. Or, as shown in FIG. **6**, the details can be displayed and updated dynamically in a frame **560** with each combination of card and shipping details entered **570**. Accordingly, the consumer is made aware of the charges that apply to the purchase within a particular wallet and can exercise several choices before placing the order **580** and exiting the wallet services. Such choices include which card to use based on which has a lower surcharge, or which location to ship to, based on shipping charges, or which shipping option to choose based on need and cost.

[0094] This enhancement of the user's checkout experience provides a capability not currently available to consumers in choosing a particular credit card to use in a sales transaction. In particular, surcharge is a charge imposed by merchants for accepting credit cards which is then passed on to the consumers. Merchants have the ability to set these rates on credit cards, some of which carry higher rates. The proposed enhancement allows the wallet service to dynamically display the surcharge rate and charge associated with the card the consumer has selected, so that the consumer can make a choice within the wallet service of selecting a different card with a lower surcharge.

[0095] Upon placing the order, the information is aggregated and transmitted to the merchant through application programming interfaces (API's) **590**. The merchant retrieves the consumer data provided and displays an order confirmation page **575** to the consumer.

[0096] A history of a consumer's spending using a particular wallet can also be provided, so that the consumer does not have to look at multiple statements from multiple payment cards to track one's spending. The 'History' section of the wallet preferably includes stored details of purchases made with each payment card within the network of wallets, and tracks purchases made. Such details can include date, merchant, card used, and shipping address.

[0097] FIG. **7** is a schematic representation of a real-time interstitial electronic wallet creation process, depicted using a mobile phone-based payment/authentication system.

[0098] Referring now to FIG. **7**, illustrated is an exemplary process by which a credentialed user may create an electronic wallet in real time. The purchaser has selected certain goods or services to be purchased from a participating merchant, and arrives at either a checkout page or a shopping cart page, represented at **1020**. The purchaser is offered the option or opportunity to complete the purchase using the network of wallets which is represented by an icon **1040**. In the exemplary embodiment, the network of wallets is operated under the name "PayPass Online", PAYPASS™ being a trademark of MasterCard International Incorporated, the assignee of the instant application.

[0099] Having selected the network of wallets icon **1040** to process payment for the transaction, the purchaser is presented with an interstitial page **2020** which prompts the purchaser to select the provider of their chosen wallet from among the partners participating in the network of wallets and displayed at **2040**, including optional page select function **2060** or equivalent (rotating panes, daisy-wheel, etc., as described elsewhere herein). Having selected a partner wallet provider, for example ABC Bank. (The use of various symbols to represent partner wallet providers is by way of illustration only, and does not necessarily imply affiliation or endorsement by the respective symbol owners or any related entities, nor their agreement to participate in the network of wallets as described in this or any related application), selection may be highlighted among the display of partners **2040**, and/or optionally displayed again, as at **2070**. The purchaser is further prompted to enter a login username and password credentials **2080** associated with their selected partner wallet provider.

[0100] The case contemplated here, as depicted in FIG. **7** and described, is applicable to only a subset of all purchasers. Namely, the purchaser will have previously established identity credentials (e.g., login ID and password) with the partner provider they select at **2040**. The purchaser can therefore be verified by the respective partner, but does not have an established electronic wallet with a particular partner. It may be the case that a purchaser has established demand deposit account (DDA, e.g., checking or savings) with the banking institution that includes online banking service, and a login/password pair to access them, but does not have an established electronic wallet with that partner. That purchaser may simply be unaware of the wallet service offered by the banking partner, and may have clicked/selected the network of wallets checkout icon **1040** inadvertently, or out of curiosity. Alternately or additionally, the banking partner may selectively offer electronic wallet services to less than all of their customers, as an incentive or service enhancement. In the latter case, the subset of purchasers to whom the present method is applicable is still narrower, as determined by their eligibility to create an electronic wallet with the selected partner banking institution.

[0101] However, the presumed case is that the purchaser has not yet established a wallet with that partner. Therefore, the partner would authenticate the purchaser to the operator of the network of wallets. The purchaser is then presented with a further page **3020**, which confirms to the purchaser that their identity is recognized. In the case that the purchaser is eligible to open an electronic wallet with the partner, but has not yet done so, the purchaser is presented with the opportunity to establish a wallet with the partner immediately, which the purchaser may accept or decline at **3040**. A purchaser who is authenticated using their established credentials with the banking partner, but is ineligible to create an electronic wallet with that partner for whatever reason, and/or declines to create an electronic wallet, may be returned to either the network of wallets interstitial login screen **2020**, for example to select another wallet provider, or alternately to the merchant checkout page **1020**.

[0102] Where the purchaser accepts the invitation and chooses to create a wallet, the purchaser's wallet details are pre-populated based upon information known to the partner about the purchaser associated with the existing credentials and presented to the purchaser for verification **4020**. The wallet details include the relevant payment card numbers **4040**, a billing address associated with the payment card **4060**, and a shipping address **4080** where goods may be delivered. The purchaser must then confirm the pre-populated details **4100** to proceed with the transaction.

[0103] Upon confirming the wallet and payment details, the purchaser is returned to the merchant page. The operator of the network of wallets with have contemporaneously transmitted the necessary transaction details, e.g., card number details, billing and shipping addresses, etc. to the merchant, which are again presented to the purchaser from the merchant's page **5020**. The purchaser then has only to confirm the order by selecting the corresponding option at **5040**.

[0104] The purchaser will then have established a partner wallet in the federated network of wallets. Upon the purchaser's next transaction where the network of wallets is invoked, their existing wallet may be recognized. Furthermore, the purchaser may consent to a software cookie to be stored on the purchaser's system, which can be used to auto-identify the purchaser, at least in part. For example, upon the purchaser's next invocation of the network of wallets, their existing wallet may be recognized, and that wallet provider pre-selected. The purchaser then has only to enter the appropriate username and password, thereby streamlining the checkout process. Moreover, as will be apparent, on subsequent logins by the same purchaser the need to create a new wallet with respect to that same partner, as described herein is obviated.

Converged Platform

[0105] With reference now to FIG. **8**, illustrated is a representation of the multiple consumer interface pathways to a converged electronic wallet. A consumer may use an internet pathway via, as example only personal computer **802** or mobile device **804** to establish and manage their one or more consumer wallet accounts. Interaction between personal computer **802** or mobile device **804** on the one hand and a NoW cloud database **806** is via proprietary web services interface. The consumer securely enters and verifies payment data via this web-based user interface A. A registration user interface displayed on the consumer's mobile device **804** can be optimized for mobile screen form factor.

[0106] Optionally, a third party wallet provider **808** can automate creation of consumer wallet account, for example via systematic provisioning of consumer payment data via secure, proprietary web services interface (G).

[0107] eCommerce purchases are those that occur via consumer personal computer **810** or web-enabled mobile device **812**. The computer **810** and mobile device **812** interact with the cloud database **806** via proprietary web services interface (B). Interface (B) enables secure provision of consumer payment data to a merchant **814***a*, **814***b*, with whom the consumer is transacting. The NoW checkout user interface as displayed on consumer mobile device **812** may be optimized for mobile screen form factor.

[0108] NoW cloud database **806** maintains consumer wallet profile centrally for hosted wallets (i.e., **70**, **80**), and/or serves as the gateway to partner-hosted wallets **60**. Each connected device has access to central consumer wallet profile and the same group of electronic wallets regardless of the interface platform, ensuring consistent access to payment data across all enabled consumer devices.

[0109] In the case where the consumer makes use of a mobile device **816** that is NFC-enabled or having some other secure element for face-to-face transaction using their NoW electronic wallet, a provisioning system **818** securely stores payment device data into local storage on consumer mobile phone **818** via a secure provisioning interface (D). Provisioning occurs either "over the air" or via direct connect to consumer (or other) computer.

[0110] The consumer initiates "tap-to-pay" mobile NFC transaction by bringing their mobile device **818** in proximity with an NFC-enabled POS terminal **820**. The consumer uses their mobile device **818** to choose payment details, or will have previously selected a default setting. In certain cases, including without limitation certain high-value transactions, the consumer may be asked to verify their identity, e.g., by PIN or the like. The mobile device **818** securely transmits payment details to POS terminal **820** via contactless payment protocol. If other data is required to complete the purchase transaction (e.g., shipping address, loyalty account, promotional offer, etc.), the consumer mobile phone **820** acquires this data from cloud database **806** via proprietary web services interface (C), prior to transmission to POS **820** via contactless payment protocol.

[0111] Still another consumer interface pathway enables remote or F2F transactions via NoW. Therein, a provisioning system **822** securely stores payment device data into local storage on consumer mobile phone **824** via secure provisioning interface (F). Provisioning occurs either "over the air", or via direct connect to consumer (or other) device.

[0112] A consumer initiates payment in this case by engaging in a "trigger event" **826**. A Trigger event may include, without limitation, QR read via phone camera, barcode read via phone camera, display QR/bar code on phone screen, Wi-Fi, Bluetooth, among others. An app provided on a consumer mobile device **824** may be used to initiate payment interface with merchant, authenticates the consumer identity, and transmit payment data to merchant. The consumer mobile device **824** acquires data required to complete the purchase (e.g., shipping address, loyalty account, promotional offer, etc. from the NoW cloud database **806** via proprietary web services interface (E) prior to transmission to the merchant via secure, proprietary interface.

[0113] Still another consumer interface platform can be implemented by the merchant choosing to provide a native, "in app" checkout experience for mCommerce transactions. In this interface platform, the entire payment user experience is controlled by a merchant app on the user mobile device **828**. In this case, the merchant app acquires consumer payment data from the NoW server **806** securely via secure, proprietary web services interface (H).

Health Check Option

[0114] An optional additional feature of the user interface for access to the Network of Wallets and/or the wallet selector page is what can be referred to as a "health check" of available wallets. Consider that an electronic wallet may be provided with one or more debit or credit accounts, and/or one or more pre-paid cards or accounts. A debit or credit account may be limited in balance by the available account balance in a demand deposit account associated with a given debit card, the available credit limit of a credit account associated with a given credit card. Additionally, the balance on a given pre-paid card or account may be limited or exhausted.

[0115] In order to improve the customer experience, information about the state of one or more wallets may be conveyed early in the checkout process. This would be preferred over an alternative scenario wherein the user would select a wallet without regard to available balance, for example, then continue to nearly complete the checkout process to the point where the merchant authorizes the charges, only to have those charges declined, for example because of insufficient available balance.

[0116] Therefore, in one embodiment, once the user is logged into the network of wallets, whether directly or via a partner login, a listing or other graphic or textural device indicating a choice of wallets may include information regarding the state of health for a given wallet. For example, reference may be made to the amount of the merchant transaction that precipitated the network of wallets login, as compared to available balance in the wallet. Other limiting factors besides available balance that would prevent a transaction from being completed may be the class of merchant with regard to restriction placed upon one or more payment sources stored in a given electronic wallet, effective reducing the available balance for that transaction. In other cases, the card or cards associated with a given wallet may be expired. In still others, a prior attempt to transact on a particular wallet may have failed for unknown reasons. Most preferably, any foreseeable reason why the instant transaction may be declined with reference to a particular wallet and transaction should be considered as part of the health check.

[0117] The health check information may be conveyed, for example, by selecting an order of listing available wallets. More specifically, any that do not have the capacity to complete a transaction may be ordered lower in the selection listing than another available wallet having ability to complete the transaction. With regard to a graphical representation such as the switch, flip (rotating pane) or daisy wheel described herein elsewhere (and without limitation to those graphical devices), an 'unhealthy' wallet with reference to the instant transaction may be positioned less conveniently than others, may be showing in a different shade or color (e.g., gray tone), or may simply be hidden altogether. Some combination of indications may be used as well.

[0118] Alternately, the user may identified by cookies placed on the user's access device from a prior use of an electronic wallet associated with the network of wallets. In this case, the state of health of a wallet may be indicated even

before the user logs into the network, and may aid the user in selecting a wallet partner via which they choose to login.

[0119] In additional embodiments, it is further contemplated that the user experience be enhanced by including an identifiable link or graphic icon which the user may associate with the network of wallets, even or especially while interacting with one of the federated partners in the network of wallets. The link or graphic icon, which we will refer to as a "pin" is preferably small and unobtrusive, yet visible and identifiable. The pin may, for example, expand when hovered upon by a user-selection device (e.g., mouse pointer). Such hovering over and/or selection of the pin by a user will transfer the user from the partner site to the network of wallets site, for example to select a different wallet or wallet provider. Alternately or additionally, the user may be presented with a selection of partner wallets to transfer directly to.

[0120] An additional feature which may be integrated into the network of wallets checkout experience is a shopping cart. The network of wallets as described herein can be entered from the merchant's checkout page, for example, via a clickable icon. Data concerning the pending transaction (seller, description, quantity, price, terms, etc.) are passed to network operator in the course of processing the checkout transaction. Optionally, in certain embodiments, this information may be made available to the user during the course of their interactions with the network of wallets (e.g., login, wallet selection, etc.).

[0121] In one particular embodiment, the shopping cart is integrated with the pin described above. Hovering over the pin initiates an expansion of the pin graphic into a selection of data or alternate destinations for the user. Among these may include the shopping cart, showing a précis of pertinent data to the pending transaction (e.g., seller, description, quantity, price, terms, etc.). Furthermore, it may be convenient to permit the user to select the shopping cart, or items in it, and be returned to the merchant site to append or change the transaction.

[0122] Although the invention has been described with reference to certain preferred embodiments, it will be appreciated by those skilled in the art that modifications and variations may be made without departing from the spirit and scope of the invention. It should be understood that applicant does not intend to be limited to the particular details described above and illustrated in the accompanying drawings.

What is claimed is:

1. A method for authorizing a digital wallet transaction, the method comprising:

providing a host server having one or more secure databases for storing cardholder and card data associated with a plurality of electronic wallets offered within a network of digital wallets, the host server including services for facilitating and monitoring connectivity between one or more merchants and an acceptance network for authorizing a purchase transaction;

responsive to a user initiation of the purchase transaction, routing the purchase transaction to a digital wallet selected by the user from the plurality of digital wallets, the selected digital wallet capturing a payment card selected by the consumer for the digital wallet transaction; and

redirecting the transaction back to the merchant web site or app using the postback merchant URL, the merchant web site or app sending the Access Token to the checkout resource URL associated with the selected digital wallet to retrieve the purchase details for authorizing and completing the digital wallet transaction.

2. The method of claim **1**, further comprising storing in the host server shipping address data associated with the cardholder, and providing the shipping address data selected by the cardholder to the merchant for facilitating shipment or delivery of goods or services.

3. The method of claim **1**, wherein the selected digital wallet is a default wallet, the default wallet being selected prior to the consumer authorizing the purchase transaction.

4. The method of claim **3**, wherein the consumer is a recognized user of the acceptance network, the default wallet corresponding to one of the plurality of digital wallets most recently accessed by the consumer.

5. The method of claim **3**, further comprising displaying an interstitial page associated with the default wallet in response to the consumer selecting the acceptance button

6. The method of claim **1**, further comprising associating a coupon or offer with each of the plurality of digital wallets, and displaying the coupon or offer associated with one of the plurality of digital wallets displayed on the wallet selector switch.

7. The method of claim **6**, the displaying step comprising displaying the coupon or offer in response to the consumer hovering a pointer over the one of the plurality of digital wallets displayed.

8. The method of claim **7**, further comprising communicating the coupon or offer associated with the one of the plurality of digital wallets to the merchant web site or app prior to completing the digital wallet transaction, wherein the one of the plurality of digital wallets is the digital wallet selected from the plurality of digital wallets for the transaction.

9. The method of claim **1**, wherein the user initiates the payment transaction by engaging in a trigger event with respect to a mobile device, the trigger event comprising at least one of a QR read, barcode read, display of QR or bar code on a mobile device, SMS communication, Wi-Fi communication, and Bluetooth communication.

10. The method of claim **1**, wherein the user is given access to the contents of the selected digital wallet without regard to the user interface platform.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Nwokolo et al.

(10) **Pub. No.: US 2013/0297504 A1**

(43) **Pub. Date: Nov. 7, 2013**

(54) **TRANSACTION DATA TOKENIZATION**

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATE**, Purchase, NY (US)

(72) Inventors: **Obinna Nwokolo**, New York, NY (US); **Daniel Goodman**, White Plains, NY (US)

(73) Assignee: **MASTERCARD INTERNATIONAL INCORPORATED**, Purchase, NY (US)

(21) Appl. No.: **13/835,088**

(22) Filed: **Mar. 15, 2013**

Related U.S. Application Data

(60) Provisional application No. 61/642,872, filed on May 4, 2012.

Publication Classification

(51) **Int. Cl.**
G06Q 20/36 (2012.01)

(52) **U.S. Cl.**
CPC *G06Q 20/363* (2013.01)
USPC **705/41**

(57) **ABSTRACT**

A system and method of tokenizing sensitive cardholder payment information for use in cashless transactions includes receiving a request to process a cashless transaction between a merchant and a purchaser using first payment data stored with an electronic wallet provider on behalf of the purchaser. First payment data is retrieved from the electronic wallet provider. The first payment data is tokenized into a payment token, and provided to the merchant for use in completing the cashless transaction. The merchant issues a request to process payment for the cashless transaction using the payment token. The payment token is detokenized into second payment data, with correspondence between the first and second payment data being indicative of payment token authenticity. Payment for the cashless transaction is processed using the second payment data, and the merchant is provided with a response indicating either the success or failure of the payment processing.

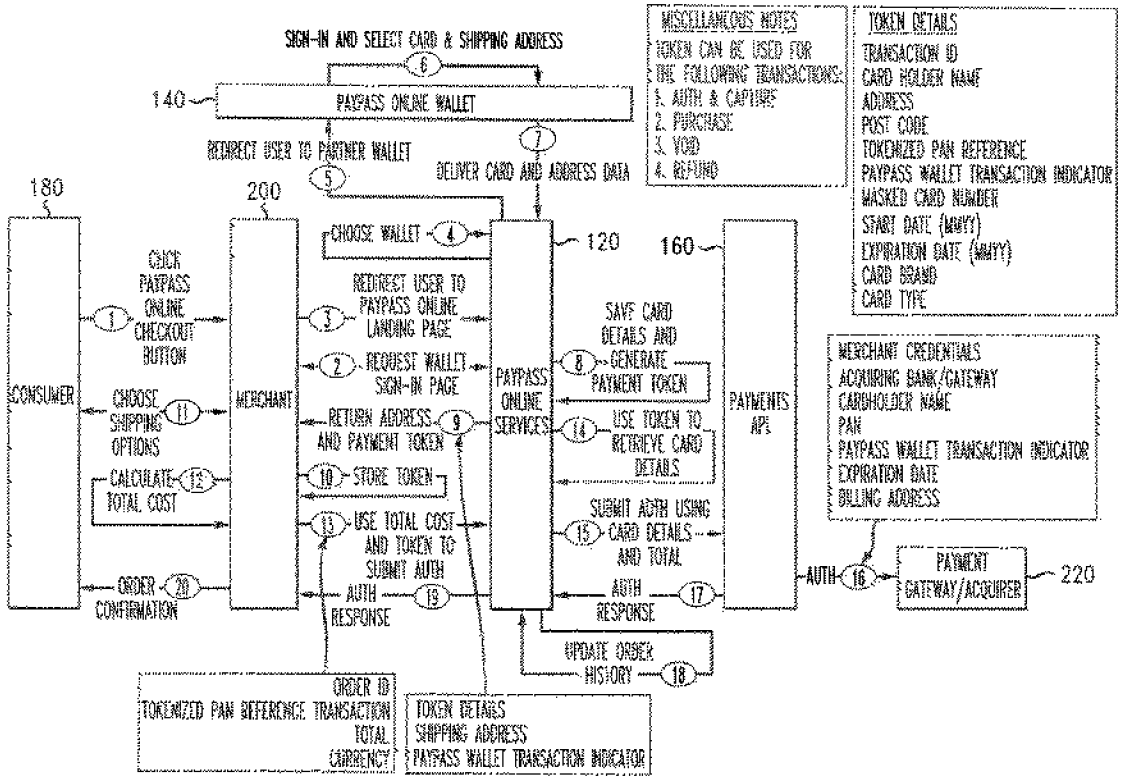


FIG. 1

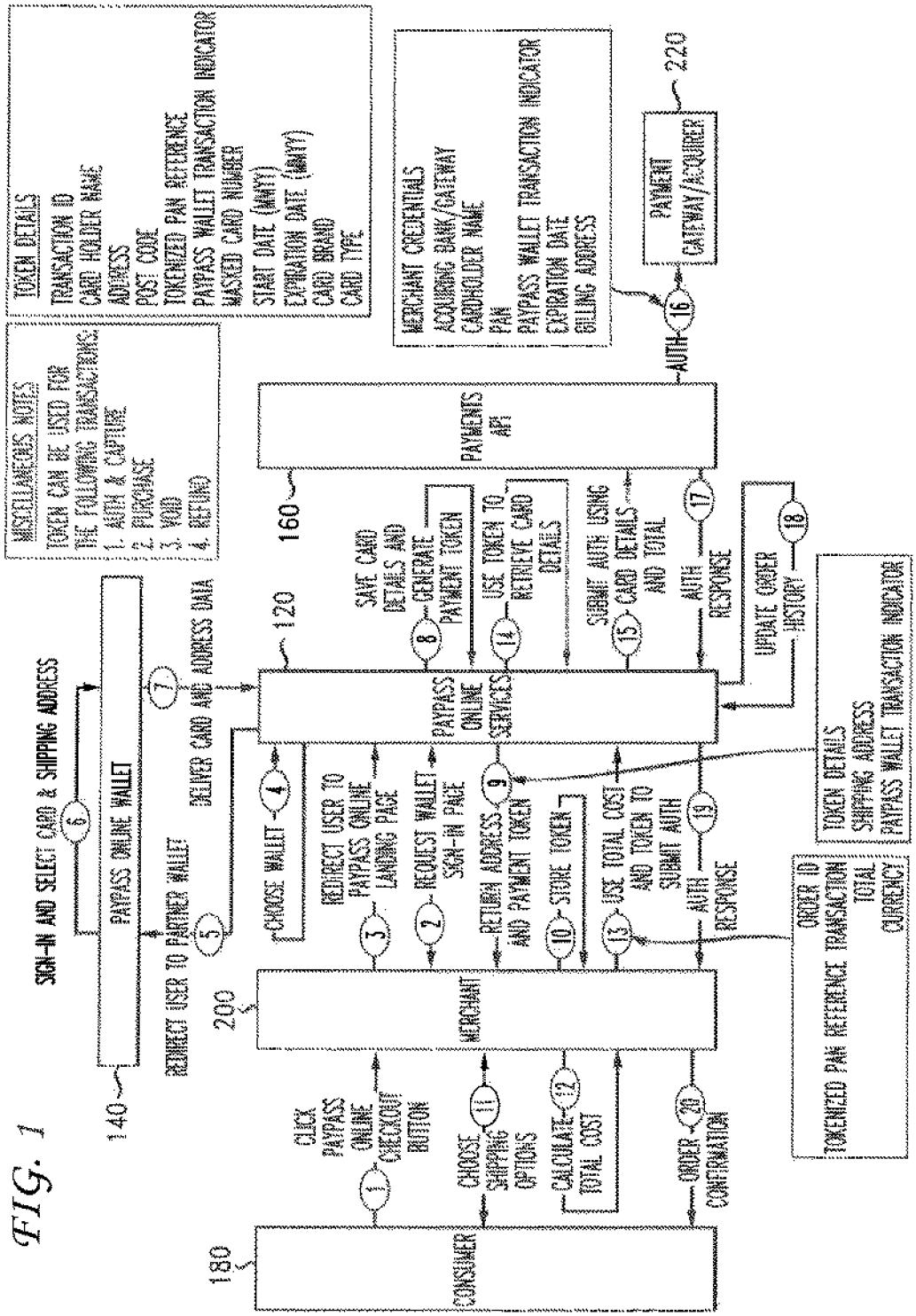
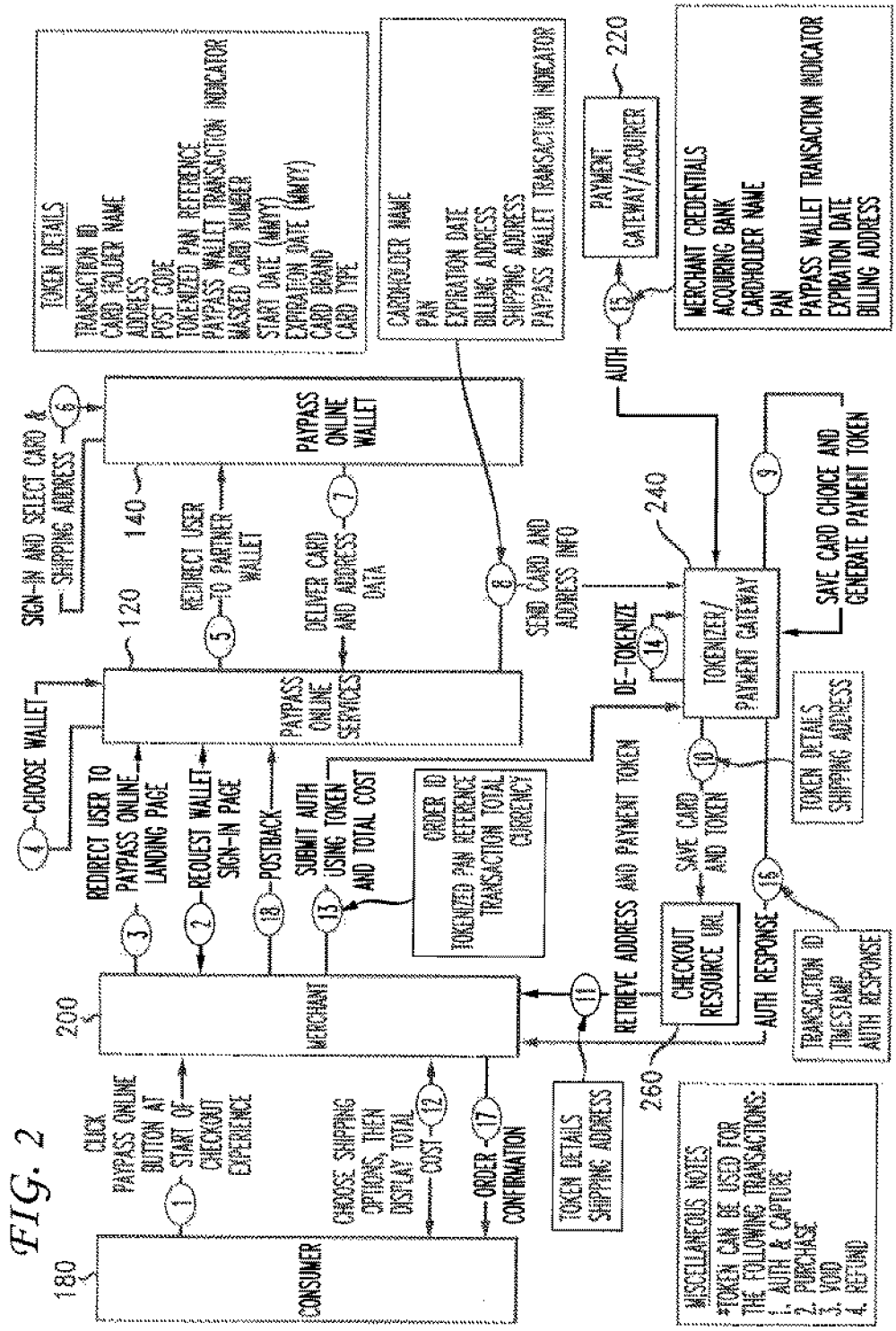

SIGN-IN AND SELECT CARD & SHIPPING ADDRESS
PAYPASS ONLINE WALLET
REDIRECT USER TO PARTNER WALLET
DELIVER CARD AND ADDRESS DATA
CHOOSE WALLET
REDIRECT USER TO PAYPASS ONLINE LANDING PAGE
REQUEST WALLET SIGN-IN PAGE
RETURN ADDRESS AND PAYMENT TOKEN
STORE TOKEN
USE TOTAL COST AND TOKEN TO SUBMIT AUTH
AUTH RESPONSE
ORDER CONFIRMATION
CALCULATE TOTAL COST
CHOOSE SHIPPING OPTIONS
CLICK PAYPASS ONLINE CHECKOUT BUTTON
CONSUMER
MERCHANT
PAYPASS ONLINE SERVICES
SAVE CARD DETAILS AND GENERATE PAYMENT TOKEN
USE TOKEN TO RETRIEVE CARD DETAILS
SUBMIT AUTH USING CARD DETAILS AND TOTAL
AUTH RESPONSE
UPDATE ORDER HISTORY
PAYMENTS API
AUTH
PAYMENT GATEWAY/ACQUIRER
MISCELLANEOUS NOTES
TOKEN CAN BE USED FOR THE FOLLOWING TRANSACTIONS:
1. AUTH & CAPTURE
2. PURCHASE
3. VOID
4. REFUND
TOKEN DETAILS
TRANSACTION ID
CARD HOLDER NAME
ADDRESS
POST CODE
TOKENIZED PAN REFERENCE
PAYPASS WALLET TRANSACTION INDICATOR
MASKED CARD NUMBER
START DATE (MMYY)
EXPIRATION DATE (MMYY)
CARD BRAND
CARD TYPE
MERCHANT CREDENTIALS
ACQUIRING BANK/GATEWAY
CARDHOLDER NAME
PAN
PAYPASS WALLET TRANSACTION INDICATOR
EXPIRATION DATE
BILLING ADDRESS
ORDER ID
TOKENIZED PAN REFERENCE TRANSACTION TOTAL CURRENCY
TOKEN DETAILS
SHIPPING ADDRESS
PAYPASS WALLET TRANSACTION INDICATOR
140
200
120
160
220
180

FIG. 2


180
CONSUMER
200
MERCHANT
120
PAYPASS ONLINE SERVICES
140
PAYPASS ONLINE WALLET
220
PAYMENT GATEWAY/ACQUIRER
240
TOKENIZER/ PAYMENT GATEWAY
260
CHECKOUT RESOURCE URL
1 CLICK PAYPASS ONLINE BUTTON AT START OF CHECKOUT EXPERIENCE
2 REQUEST WALLET SIGN-IN PAGE
3 REDIRECT USER TO PAYPASS ONLINE LANDING PAGE
4 CHOOSE WALLET
5 REDIRECT USER TO PARTNER WALLET
6 SIGN-IN AND SELECT CARD & SHIPPING ADDRESS
7 DELIVER CARD AND ADDRESS DATA
8 SEND CARD AND ADDRESS INFO
9 SAVE CARD CHOICE AND GENERATE PAYMENT TOKEN
10 SAVE CARD AND TOKEN
11 RETRIEVE ADDRESS AND PAYMENT TOKEN
12 CHOOSE SHIPPING OPTIONS, THEN DISPLAY TOTAL COST
13 SUBMIT AUTH USING TOKEN AND TOTAL COST
14 DE-TOKENIZE
15 AUTH
16 AUTH RESPONSE
17 ORDER CONFIRMATION
18 POSTBACK
TOKEN DETAILS
TRANSACTION ID
CARD HOLDER NAME
ADDRESS
POST CODE
TOKENIZED PAN REFERENCE
PAYPASS WALLET TRANSACTION INDICATOR
MASKED CARD NUMBER
START DATE (MMYY)
EXPIRATION DATE (MMYY)
CARD BRAND
CARD TYPE
CARDHOLDER NAME
PAN
EXPIRATION DATE
BILLING ADDRESS
SHIPPING ADDRESS
PAYPASS WALLET TRANSACTION INDICATOR
MERCHANT CREDENTIALS
ACQUIRING BANK
CARDHOLDER NAME
PAN
PAYPASS WALLET TRANSACTION INDICATOR
EXPIRATION DATE
BILLING ADDRESS
ORDER ID
TOKENIZED PAN REFERENCE
TRANSACTION TOTAL
CURRENCY
TOKEN DETAILS
SHIPPING ADDRESS
TRANSACTION ID
TIMESTAMP
AUTH RESPONSE
MISCELLANEOUS NOTES
*TOKEN CAN BE USED FOR THE FOLLOWING TRANSACTIONS:
1. AUTH & CAPTURE
2. PURCHASE
3. VOID
4. REFUND

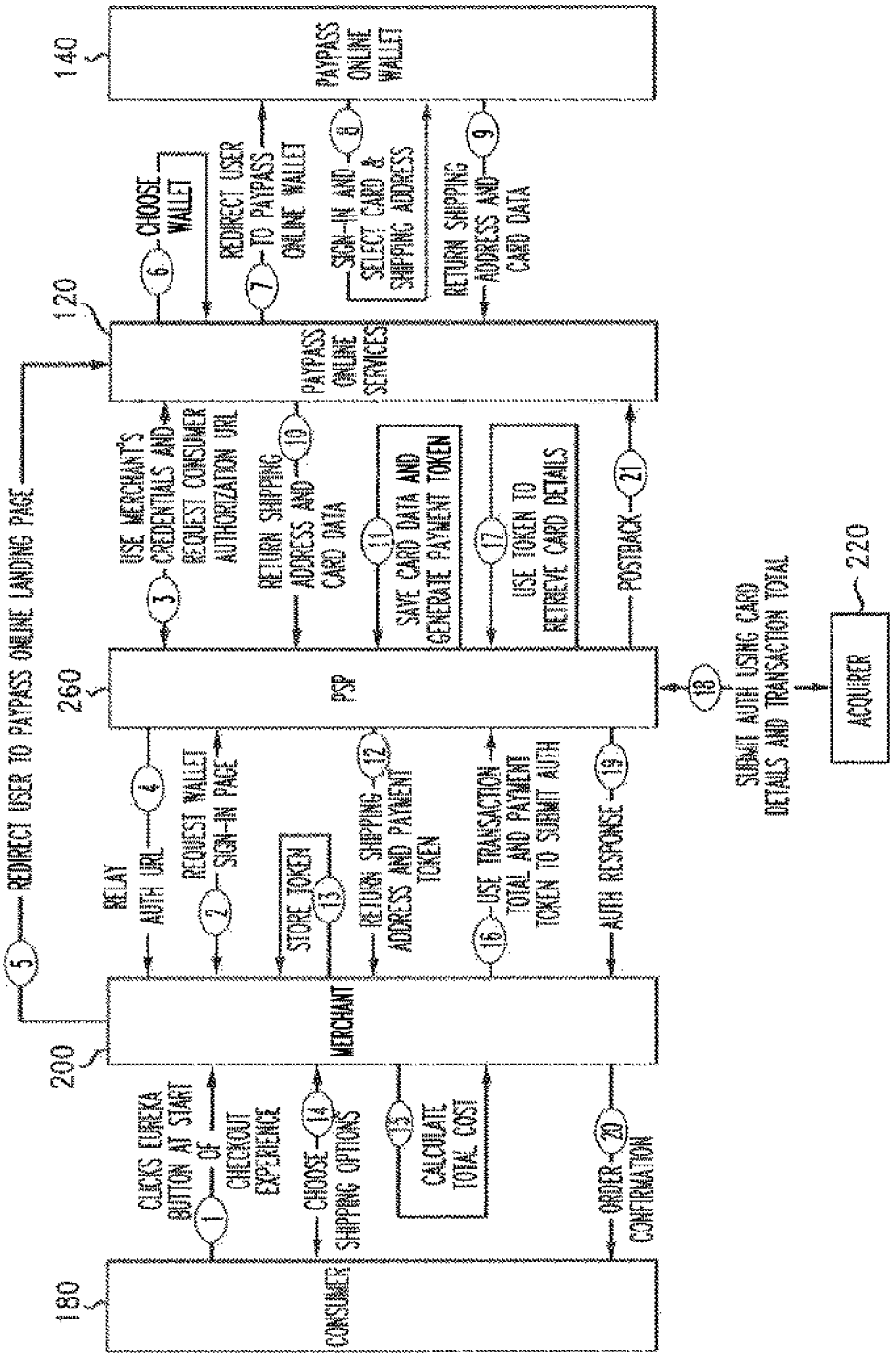

180
CONSUMER
200
MERCHANT
260
PSP
120
PAYPASS ONLINE SERVICES
140
PAYPASS ONLINE WALLET
220
ACQUIRER
1 CLICKS EUROPA BUTTON AT START OF CHECKOUT EXPERIENCE
2 REQUEST WALLET SIGN-IN PAGE
3 USE MERCHANT'S CREDENTIALS AND REQUEST CONSUMER AUTHORIZATION URL
4 RELAY AUTH URL
5 REDIRECT USER TO PAYPASS ONLINE LANDING PAGE
6 CHOOSE WALLET
7 REDIRECT USER TO PAYPASS ONLINE WALLET
8 SIGN-IN AND SELECT CARD & SHIPPING ADDRESS
9 RETURN SHIPPING ADDRESS AND CARD DATA
10 RETURN SHIPPING ADDRESS AND CARD DATA
11 SAVE CARD DATA AND GENERATE PAYMENT TOKEN
12 RETURN SHIPPING ADDRESS AND PAYMENT TOKEN
13 STORE TOKEN
14 CHOOSE SHIPPING OPTIONS
15 CALCULATE TOTAL COST
16 USE TRANSACTION TOTAL AND PAYMENT TOKEN TO SUBMIT AUTH
17 USE TOKEN TO RETRIEVE CARD DETAILS
18 SUBMIT AUTH USING CARD DETAILS AND TRANSACTION TOTAL
19 AUTH RESPONSE
20 ORDER CONFIRMATION
21 POSTBACK

FIG. 3

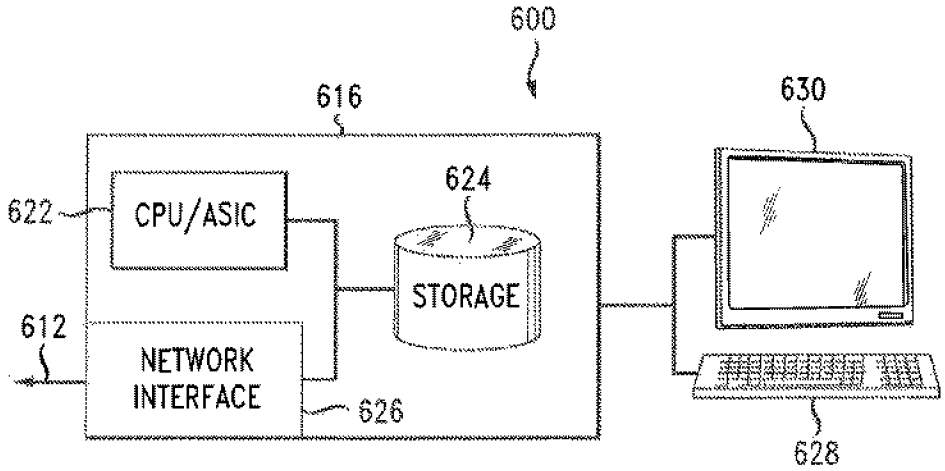

600
616
630
624
622
CPU/ASIC
STORAGE
612
NETWORK
INTERFACE
626
628

FIG. 4

TRANSACTION DATA TOKENIZATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the priority benefit under 35 U.S.C. §119(e) of prior U.S. Provisional Patent Application Ser. No. 61/642,872 (Attorney Docket No. 1788-96P), entitled "TRANSACTION DATA TOKENIZATION", filed 4 May 2012 by the present inventive entity.

[0002] This application is related to non-provisional U.S. Utility patent application Ser. No. 13/209,312 entitled "MULTI-COMMERCE CHANNEL WALLETS FOR AUTHENTICATED TRANSACTIONS", and also International PCT Application Serial No. PCT/US2011/047678 having the same title, both filed 12 Aug. 2011, both of which in turn claim the priority benefit of U.S. Provisional Application Ser. No. 61/372,955 filed 12 Aug. 2010 and also of U.S. Provisional Application Ser. No. 61/468,847 filed 29 Mar. 2011.

[0003] This application is further related to U.S. Utility patent application Ser. No. 13/746,904 entitled "SYSTEM TO ENABLE A NETWORK OF WALLETS", filed 22 Jan. 2013 (Attorney Docket No. 1788-82), which in turn claims the priority benefit of U.S. Provisional Application Ser. No. 61/588,505 (Attorney Docket No. 1788-82P) entitled "SYSTEM TO ENABLE A NETWORK OF WALLETS", filed 19 Jan. 2012; of U.S. Provisional Application Ser. No. 61/642,729 (Attorney Docket No. 1788-82P2), entitled "SYSTEM AND METHOD TO ENABLE A NETWORK OF DIGITAL WALLETS", filed on 4 May 2012; of U.S. Provisional Application Ser. No. 61/642,792 (Attorney Docket No. 1788-91P), entitled "REAL-TIME INTERSTITIAL ELECTRONIC WALLET CREATION", filed on 4 May 2012; and of U.S. Provisional Application Ser. No. 61/642,799 (Attorney Docket No. 1788-97P), entitled "INTEGRATION OF A PARTNER HOSTED WALLET WITH A NETWORK OF WALLETS", filed on 4 May 2012.

[0004] This application is further related to U.S. Provisional Application Ser. No. 61/642,925 (Attorney Docket No. 1788-95P), entitled "EUREKA CONVERGED", and filed on 4 May 2012.

[0005] The complete disclosures of all related applications cited above and any of their corresponding priority applications are hereby incorporated in their entirety for all purposes by this reference.

BACKGROUND

[0006] 1. Field of the Disclosure

[0007] The present invention relates to transactions for payment of goods/services and, more particularly, to a system and method for tokenization for sensitive or confidential transaction payment data.

[0008] 2. Brief Discussion of Related Art

[0009] Cashless electronic payment for transaction of goods and services is become ubiquitous in modern society. In connection with this, electronic wallets are becoming a more prevalent counterpart to electronic forms of payment for a wide variety of transactions. Generally speaking, an electronic wallet is a system by which a credit card, debit card, pre-paid card, etc., is stored where a single electronic application which provides access to them, analogous to the way in which one might store corresponding physical payment cards in a tangible wallet.

[0010] The disclosure in the application entitled "MULTI-COMMERCE CHANNEL WALLETS FOR AUTHENTICATED TRANSACTIONS", and also the related application entitled "SYSTEM AND METHOD TO ENABLE A NETWORK OF DIGITAL WALLETS", includes a federated network of electronic wallets. The purchaser may select this network of wallets which includes partners who are members of the federation, each of whom provide electronic wallet services. One option presented to the purchaser may be the option to use an electronic wallet maintained and provided by the payment processing entity, e.g., MasterCard International Incorporated (assignee of the instant application), which is also operating the network of wallets.

[0011] Given the overwhelming volume of transactions consummated per second, and the necessity that transactions be authorized expeditiously in order to be an acceptable form of payment for all parties involved in the transaction, the circumstances naturally lend themselves to automation of the approval process. However, without adequate oversight on an individual or per-transaction basis, and/or without the parties to the transaction being known to others involved, including the intermediary, the opportunity for malicious abuse of the payment system require adequate safeguards.

[0012] A problem presented is where the transaction details required to consummate a purchaser's transaction may be used thereafter for malicious purposes, for example if the security of such data is compromised by a third party, or by another bad actor with access to cardholder data used during the transaction. A solution to this problem is required.

SUMMARY OF THE DISCLOSURE

[0013] In order to overcome these and other problems, weaknesses and/or drawbacks in the present state of the art, provided according to the instant disclosure is a system and method for tokenization of sensitive data use in connection with cashless and electronic transactions.

[0014] More specifically, a method of tokenizing sensitive cardholder payment information for use in cashless transactions includes receiving a request to process a cashless transaction between a merchant and a purchaser using first payment data stored with an electronic wallet provider on behalf of the purchaser. First payment data is retrieved from the electronic wallet provider. The first payment data is tokenized into a payment token, and provided to the merchant for use in completing the cashless transaction. The merchant issues a request to process payment for the cashless transaction using the payment token.

[0015] The payment token is detokenized into second payment data, where correspondence between the first and second payment data is indicative of the authenticity of the payment token received from the merchant. Payment for the cashless transaction is processed using the second payment data, and the merchant is provided with a response indicating either the success or failure of the payment processing.

[0016] In a further embodiment of the present disclosure, the payment data is passed to one of a third party tokenizer and a payment service provider, wherein the third party tokenizer or payment service provider tokenizes the payment data into a payment token, provides the payment token to the merchant for use in completing the cashless transaction, receives, from the merchant, the request to process payment for the cashless transaction using the payment token, detokenizes the payment token, processes payment for the cashless transaction using the payment data, and provides the

response to the merchant indicating either the success or failure of the payment processing. In this embodiment, the third party tokenizer, or the payment service provider, provides an indication of the success or failure of the payment processing.

[0017] In a more particular embodiment of the present disclosure, the payment token further comprises one or more of the following data: a transaction identifier; a name of the cardholder; an address of the cardholder; a postal code related to the address of the cardholder; an indicator that the transaction is related to an electronic wallet; a masked payment card number; a start date related to the payment card; an expiration date related to the payment card; a brand of the payment card; and a type of payment card. Optionally or additionally, the tokenized payment data may include a virtual card number.

[0018] In still a further embodiment of the present disclosure, the payment token is bound to the received transaction request, whereby the payment token is valid only under predetermined conditions including one or more of having been submitted by a predetermined merchant, requesting payment of a predetermined dollar amount or range of dollar amounts, and submitted for payment within a predetermined timeframe.

[0019] In still a further embodiment of the present disclosure, the method is performed by an operator of a network of wallets, and further the electronic wallet provider is one of the operator of the network of wallets on its own behalf, the operator of the network of wallets on behalf of a third party, and a third party provider of electronic wallet services.

[0020] Further provided according to the present disclosure is an electronic system for carrying out the foregoing method including a processor and a non-transitory machine readable recording medium which embodies thereon a program of instruction. The program of instruction, when executed by the processor, cause the machine to carry out the foregoing method in one or more of its embodiments. Also provided according to the present disclosure is such a non-transitory machine readable medium.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] Some embodiments are illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like reference numerals refer to like structures across the several views, and wherein:

[0022] FIG. **1** is a schematic representation of a payment/authentication system and method according to a first embodiment of the present disclosure;

[0023] FIG. **2** is a schematic representation of a payment/authentication system and method according to a second embodiment of the present disclosure, including a third-party tokenization entity;

[0024] FIG. **3** is a schematic representation of a payment/authentication system and method according to a third embodiment of the present disclosure, including a third-party payment service provider performing tokenization; and

[0025] FIG. **4** illustrates schematically a representative computer according to the present disclosure, operative to implement the disclosed methods.

DETAILED DESCRIPTION OF THE DISCLOSURE

[0026] Referring now to FIG. **1**, illustrated is a sequence of operations for the tokenization of payment transaction data within the context of a federated network of wallets, for example as described according to related application attorney docket nos. 1788-65, 1788-82P, and/or 1788-82P2. In such a scenario, the operator of the network of wallets is embodied according to reference **120** of FIG. **1**, in this case under the name of PayPass Online Services (PPOS). Furthermore, represented as entity **140**, PayPass Online Wallet (PPOW), the operator of the network of wallets is further acting as one of the electronic wallet service providers within the federation of network wallets.

[0027] Furthermore, in the present embodiment the operator of the network of wallets is also functioning as payment API provider, reference **160**. Other parties to the transaction are represented as consumer **180**, merchants **200**, and payment gateway or acquirer **220**. At the point illustrated in the payments process, it is presumed that consumer **180** has selected the group of services to be involved in the transaction with merchant **200**. As this process is typically embodied, for example in an online e-commerce transaction, consumer **180** has placed certain goods or services in an electronic shopping cart, and has arrived at a checkout page. The consumer will be presented with options for payment which will include an on-line checkout button invoking the network of wallets operated by PayPass online services **120**, which the consumer **180** selects at step **1**.

[0028] At step **2**, the merchant communicates the wallet sign-in request to PPOS **120** and receives a URL to a wallet sign-in page. Merchant **200** then redirects the user to the network of wallets landing page, step **3**. The user is given the opportunity to choose an electronic wallet from among those available, including the opportunity to create a new wallet. The wallets may include one operated by PPOW **140** apart from their capacity as the network of wallets operator, alternately wallets operated by PPOW **140** partners with partner-branding or skinning, having the partner's look and feel but operated by wallet provider PPOW **140**. Finally, the partner may provide their own wallet services and substitution for PPOW **140**. The purchaser chooses their wallet in step **4**, and PPOS **120** redirects the user to their selected wallet in step **5**.

[0029] The consumer signs in to their selected wallet in step **6**. They also select from among the payment sources, for example card accounts, associated with their selected wallet. The purchaser further selects a shipping address associated with the wallet. The online wallet provider/PPOW **140** delivers selected card and address data to the operator of the network of wallets, PPOS **120**, in step **7**.

[0030] Network operator **120** then saves the selected card details and uses the card details to generate a payment token which will be shared with the merchant in order to consummate the transaction in step **8**. The card details delivered from PPOW **140** would generally include a primary account number (PAN). This sensitive information is better protected, and further the merchant **200** can be enabled to complete the transaction without this specific information. Therefore, the generation of a payment token step **8** would include the payment token as a programming object or file. The token generally includes a transaction identifier; a cardholder name; billing address; postal code; a tokenized PAN reference in substitution for the PAN; a wallet transaction indicator; a masked card number representing the selected card from the wallet; a start date associated with the selected card; an expiration date associated with the card; the card brand and/or

type. At step **9**, PPOS **120** returns a return address and the payment token together to the merchant **200** in order to finalize the transaction.

[0031] In certain embodiments, the tokenized card reference may include a virtual card number (VCN). The virtual card number in substitution for the PAN may provide additional security features. For example, the VCN may be limited to one or a fixed number of uses. A one-time use VCN would being applicable for an isolated transaction. A VCN enabled for repeated use would allowing the merchant **200** to use of the same payment token and/or VCN. On such example where this might be beneficial is with recnrring fixed transactions or variable transactions within a predetermined amount range.

[0032] Moreover, at the point in the transaction where the token is generated, the full final amount of the transaction may not yet be known. Options such as shipping address or shipping services may affect the final cost through surcharges and/or applicable sales tax. Capping the dollar amount of associated with the payment token consistent with the legitimate completion of the transaction for which it is generated provides an additional layer of security. In addition to capping a dollar amount on the payment token, the payment token may be bound to the merchant involved in initiating the corresponding transaction for which it is generated. That is to say, the particular payment token would not be honored if presented by some other merchant for anthentication. In this way, shonld the payment token be compromised or intercepted by a malicions third party or other bad actor, the payment token would not be useful with any other merchant.

[0033] Having received the payment token in step **9**, the merchant **200** stores the token as step **10**, then presents the consumer **180** with any final options (for example shipping services) to complete the transaction, that being step **11**. At step **12**, merchant **200** calcnlates the token total cost in light of the options selected by the consumer **180**, and proceeds to step **13** by submitting the total cost of the transaction and the payment token for authentication and payment. The data included at step **13** may include an order ID reference, the tokenized PAN reference provided with the payment token from the network operator **120** at step **9**, a total transaction amount, and a currency of the transaction.

[0034] PPOS **120** receives the token and authentication request, and uses the token to retrieve the card details to process the payment in step **14**. PPOS **120** then submits the authentication using the card details, including PAN, and a total transaction amount in step **15**. The payment API **160** provided by the network operator takes the authentication request and passes it to a payment gateway or acquirer **220** and receives back an authentication response in step **16**. The authentication request provided by the payment API **160** will generally include merchant credentials; the name of the acquiring bank/payment gateway provider; cardholder name; PAN; wallet transaction indicator; expiration date of the applicable card; and billing address associated with the account upon which the card is drawn.

[0035] Payments API **160** then receives and passes an authentication response which in turn is passed to PPOS **120** at step **17**. PPOS **120**, now with knowledge of the authentication outcome, updates the order history in step **18**, and in tnrn passes the authentication response to the merchant **200** in step **19**. Presuming the authentication is affirmative, the merchant **200** confirms the order to the consumer **180**, step **20**.

[0036] Referring now to FIG. **2**, illustrated is an alternative payment transaction. The steps, featnres, and parties in common with FIG. **1** will not be described in great detail where they do not substantially differ. In the embodiment of FIG. **2** the process and parties proceeds generally in accordance with the above description of FIG. **1**, up to step **8**. As compared with step **8** of FIG. **1**, according to FIG. **2**, PPOS **120** effectively ontsources the tokenization and gateway authorization. A third party tokenizer and/or payment gateway entity **240** performs these functions.

[0037] Tokenizer entity **240** saves the consumer's card choice and generates a payment token associated with the transaction in step **9**. At step **10**, thc tokenizer entity **240** transmits the payment token details and shipping address to the merchant **200**, providing a Checkout Resource URL **260**. Merchant **200** retrieves the payment token and shipping address from the Checkont Resonrce URL **260** in step **11**. The consumer **180** chooses shipping options, upon which the total cost is computed, at step **12**. The merchant **200** then submits the payment token with total transaction cost information in step **13**. An order ID, the tokenized PAN reference, a transaction total and cnrrently of transaction may be communicated together. Tokenizer entity **240** detokenizes the authentication request in step **14** and submits the authentication request to the payment gateway/acquirer **220** in step **15**. The response to tokenizer entity **240** from the payment gateway/acquirer **220** is transmitted to the merchant **200** in step **16**, then on to the consumer **180** with an order confirmation in step **17**. A post-back message to PPOS **120** is generated at step **18** to record the outcome of the transaction. In this way, PPOS **120** can log the transaction outcome as part of a value-added service to consumer **180**, an acquirer and/or issuer, despite being removed from the authentication process.

[0038] FIG. **3** illustrates still another scenario in which the merchant **200** contracts with a third party payment service provider (PSP) **260**. The third party PSP **260** stands between the merchant **200** on one side and the PPOS **120** and PPOW **140** on the other. Moreover, the PSP **260** has agree, accepted and/or audited security processes, and is a trusted collaborator for handling confidential transaction information, such as PAN associated with the transactions it processes.

[0039] In the embodiment of FIG. **3**, PSP **260** stands between POS **120** and merchant **200**. PSP **260** performs the tokenization at step **11**, and processes the authentication with acquirer **220** in step **18**. Additionally, PSP **260** will provide a postback message in step **21** to PPOS **120**, confirming the ontcome of the transaction.

[0040] It will be appreciated by those skilled in the art that the methods as described above may be operated by a machine operator having a suitable interface mechanism, and/or more typically in an automated manner, for example by operation of a network-enabled computer system including a processor executing a system of instructions stored on a machine-readable medium, RAM, hard disk drive, or the like. The instructions will cause the processor to operate in accordance with the present disclosure.

[0041] Turning then to FIG. **4**, illustrated schematically is a representative computer **616** of the system **600**. The computer **616** includes at least a processor or CPU **622** which is operative to act on a program of instructions stored on a computer-readable medium **624**. Execution of the program of instruction causes the processor **622** to carry out, for example, the methods described above according to the various embodiments. It may further or alternately be the case that the pro-

cessor **622** comprises application-specific circuitry including the operative capability to execute the prescribed operations integrated therein. The computer **616** will in many cases includes a network interface **626** for communication with an external network **612**. Optionally or additionally, a data entry device **628** (e.g., keyboard, mouse, trackball, pointer, etc.) facilitates human interaction with the server, as does an optional display **630**. In other embodiments, the display **630** and data entry device **628** are integrated, for example a touch-screen display having a GUI.

[0042] Variants of the above-disclosed and other features and functions, or alternatives thereof, may be desirably combined into many other different systems or applications. Various presently unforeseen or unanticipated alternatives, modifications, variations, or improvements therein may be subsequently made by those skilled in the art which are also intended to be encompassed by the following claims.

What is claimed is:

1. A method of tokenizing sensitive cardholder payment information for use in cashless transactions, the method comprising:

receiving a request to process a cashless transaction between a merchant and a purchaser using first payment data stored with an electronic wallet provider on behalf of the purchaser;

retrieving first payment data from the electronic wallet provider;

tokenizing the first payment data into a payment token;

providing the payment token to the merchant for use in completing the cashless transaction;

receiving, from the merchant, a request to process payment for the cashless transaction using the payment token;

detokenizing the payment token into second payment data, wherein correspondence between the first and second payment data is indicative of the authenticity of the payment token received from the merchant;

processing payment for the cashless transaction using the second payment data; and

providing an response to the merchant indicating either the success or failure of the payment processing.

2. The method according to claim **1**, further comprising:

passing the payment data to one of a third party tokenizer and a payment service provider, wherein the third party tokenizer or payment service provider

tokenizes the payment data into a payment token;

provides the payment token to the merchant for use in completing the cashless transaction;

receives, from the merchant, the request to process payment for the cashless transaction using the payment token;

detokenizes the payment token;

processes payment for the cashless transaction using the payment data; and

provides the response to the merchant indicating either the success or failure of the payment processing; and

receiving from the merchant, the third party tokenizer, or the payment service provider an indication of the success or failure of the payment processing.

3. The method according to claim **1**, wherein the payment token further comprises one or more of the following data

a transaction identifier, a name of the cardholder, an address of the cardholder, a postal code related to the address of the cardholder, an indicator that the transaction is related to an electronic wallet, a masked payment card number, a start date related to the payment card, an expiration date related to the payment card, a brand of the payment card, and a type of payment card.

4. The method according to claim **1**, wherein the payment token is bound to the received transaction request, whereby the payment token is valid only under predetermined conditions including one or more of having been submitted by a predetermined merchant, requesting payment of a predetermined dollar amount or range of dollar amounts, and submitted for payment within a predetermined timeframe.

5. The method according to claim **1**, wherein the tokenized payment data includes a virtual card number.

6. The method according to claim **1**, wherein the method is performed by an operator of a network of wallets, and further the electronic wallet provider is one of the operator of the network of wallets on its own behalf, the operator of the network of wallets on behalf of a third party, and a third party provider of electronic wallet services.

7. A non-transitory computer readable storage medium embodying thereon a program of instruction which, when executed by a processor, cause the processor to carry out a method of tokenizing sensitive cardholder payment information for use in cashless transactions, the method comprising:

receiving a request to process a cashless transaction between a merchant and a purchaser nsing first payment data stored with an electronic wallet provider on behalf of the purchaser;

retrieving first payment data from the electronic wallet provider;

tokenizing the first payment data into a payment token;

providing the payment token to the merchant for use in completing the cashless transaction;

receiving, from the merchant, a request to process payment for the cashless transaction using the payment token;

detokenizing the payment token into second payment data, wherein correspondence between the first and second payment data is indicative of the authenticity of the payment token received from the merchant;

processing payment for the cashless transaction using the second payment data; and

providing an response to the merchant indicating either the success or failure of the payment processing.

8. The medium according to claim **7**, wherein the method embodied in the program of instruction further comprises:

passing the payment data to one of a third party tokenizer and a payment service provider, wherein the third party tokenizer or payment service provider

tokenizes the payment data into a payment token;

provides the payment token to the merchant for use in completing the cashless transaction;

receives, from the merchant, the request to process payment for the cashless transaction using the payment token;

detokenizes the payment token;

processes payment for the cashless transaction using the payment data; and

provides the response to the merchant indicating either the success or failure of the payment processing; and

receiving from the merchant, the third party tokenizer, or the payment service provider an indication of the success or failure of the payment processing.

9. The medium according to claim **7**, wherein according to the method embodied in the program of instruction, the payment token further comprises one or more of the following data

a transaction identifier, a name of the cardholder, an address of the cardholder, a postal code related to the address of the cardholder, an indicator that the transaction is related to an electronic wallet, a masked payment card number, a start date related to the payment card, an expiration date related to the payment card, a brand of the payment card, and a type of payment card.

10. The medium according to claim **7**, wherein according to the method embodied in the program of instruction, the payment token is bound to the received transaction request, whereby the payment token is valid only under predetermined conditions including one or more of having been submitted by a predetermined merchant, requesting payment of a predetermined dollar amount or range of dollar amounts, and submitted for payment within a predetermined timeframe.

11. The medium according to claim **7**, wherein according to the method embodied in the program of instruction, the tokenized payment data includes a virtual card number.

12. A system for tokenizing sensitive cardholder payment information for use in cashless transactions, the system comprising:

a processor;

a non-transitory computer readable storage medium embodying thereon a program of instruction which, when executed by a processor, cause the processor to carry ont a method of tokenizing sensitive cardholder payment information for use in cashless transactions, the method comprising

receiving a request to process a cashless transaction between a merchant and a purchaser using first payment data stored with an electronic wallet provider on behalf of the purchaser;

retrieving first payment data from the electronic wallet provider;

tokenizing the first payment data into a payment token;

providing the payment token to the merchant for use in completing the cashless transaction;

receiving, from the merchant, a request to process payment for the cashless transaction using the payment token;

detokenizing the payment token into second payment data, wherein correspondence between the first and second payment data is indicative of the authenticity of the payment token received from the merchant;

processing payment for the cashless transaction using the second payment data; and

providing an response to the merchant indicating either the success or failure of the payment processing.

13. The system according to claim **12**, wherein the method embodied in the program of instruction further comprises:

passing the payment data to one of a third party tokenizer and a payment service provider, wherein the third party tokenizer or payment service provider

tokenizes the payment data into a payment token;

provides the payment token to the merchant for use in completing the cashless transaction;

receives, from the merchant, the request to process payment for the cashless transaction using the payment token;

detokenizes the payment token;

processes payment for the cashless transaction using the payment data; and

provides the response to the merchant indicating either the success or failure of the payment processing; and

receiving from the merchant, the third party tokenizer, or the payment service provider an indication of the success or failure of the payment processing.

14. The system according to claim **12**, wherein according to the method embodied in the program of instruction the payment token further comprises one or more of the following data

a transaction identifier, a name of the cardholder, an address of the cardholder, a postal code related to the address of the cardholder, an indicator that the transaction is related to an electronic wallet, a masked payment card number, a start date related to the payment card, an expiration date related to the payment card, a brand of the payment card, and a type of payment card.

15. The system according to claim **12**, wherein according to the method embodied in the program of instruction the payment token is bound to the received transaction request, whereby the payment token is valid only under predetermined conditions including one or more of having been submitted by a predetermined merchant, requesting payment of a predetermined dollar amount or range of dollar amonnts, and submitted for payment within a predetermined timeframe.

16. The system according to claim **12**, wherein according to the method embodied in the program of instruction the tokenized payment data includes a virtual card number.

17. The system according to claim **12**, operated by an operator of a network of wallets, and further the electronic wallet provider is one of the operator of the network of wallets on its own behalf, the operator of the network of wallets on behalf of a third party, and a third party provider of electronic wallet services.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

CHOI et al.

(10) **Pub. No.: US 2013/0299596 A1**

(43) **Pub. Date: Nov. 14, 2013**

(54) **APPARATUS AND METHOD FOR SELECTING SECURE ELEMENT IN NEAR FIELD COMMUNICATION DEVICE**

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.**, Gyeonggi-do (KR)

(72) Inventors: **Bong-Sik CHOI**, Gyeongsangbuk-do (KR); **Dae-Haeng CHO**, Gyeongsangbuk-do (KR)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Gyeonggi-do (KR)

(21) Appl. No.: **13/888,619**

(22) Filed: **May 7, 2013**

(30) **Foreign Application Priority Data**

May 8, 2012 (KR) 10-2012-0048667

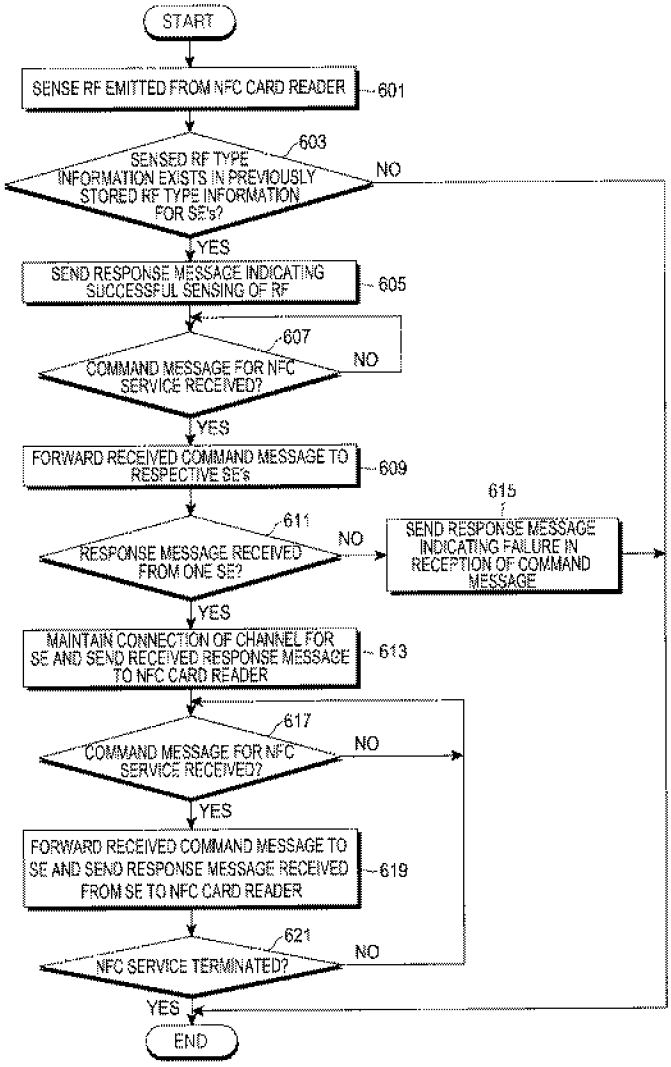
Publication Classification

(51) **Int. Cl.**
G06K 19/07 (2006.01)

(52) **U.S. Cl.**
CPC *G06K 19/0725* (2013.01)
USPC **235/492**

(57) **ABSTRACT**

An apparatus and method for selecting a Secure Element (SE) in a Near Field Communication (NFC) device are provided. Identifiers (IDs) are displayed to indicate which application programs correspond to a plurality of SEs. Upon selection of one of the IDs, an SE corresponding to the selected application-program ID from among the plurality of SEs is activated. An NFC controller is configured to select an SE from one of at least three schemes including a User Selection Scheme, Automatic Selection Scheme, and a Hybrid Scheme.



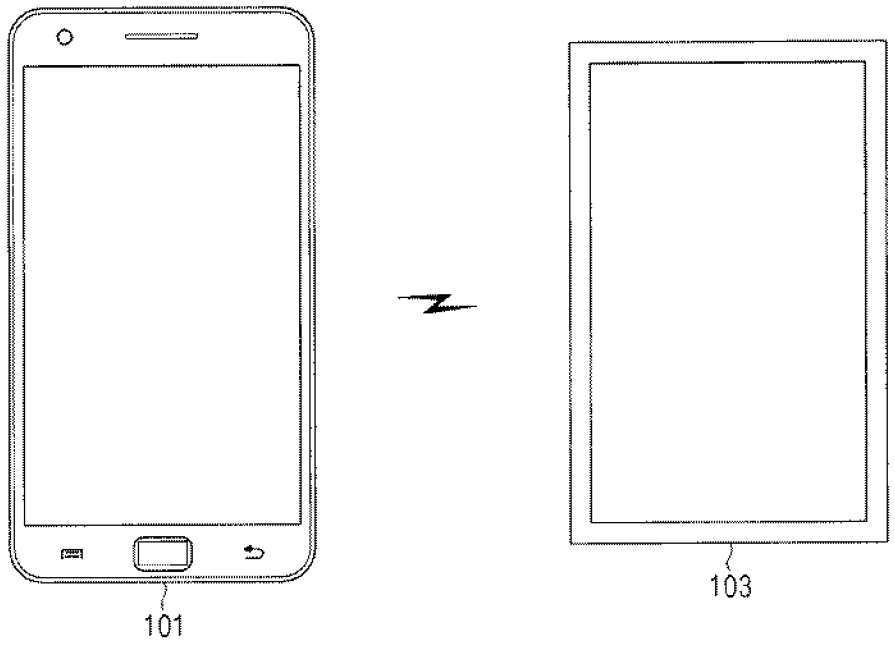


FIG.1

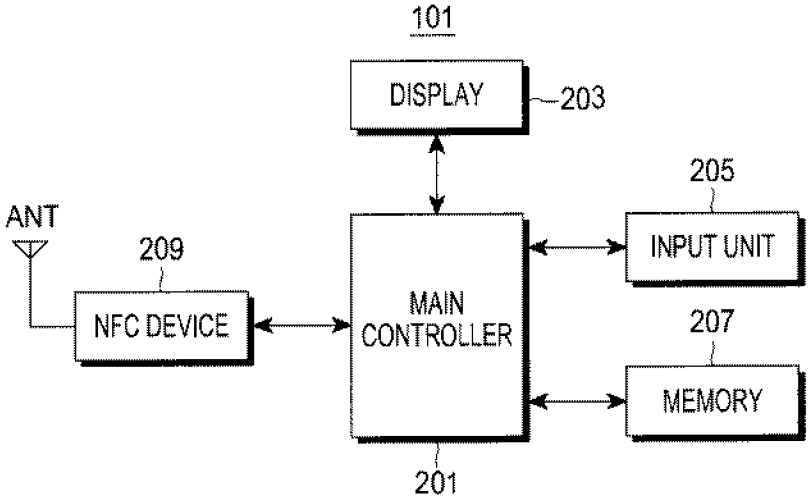

101
DISPLAY
203
205
ANT
209
INPUT UNIT
MAIN CONTROLLER
NFC DEVICE
207
MEMORY
201

FIG.2

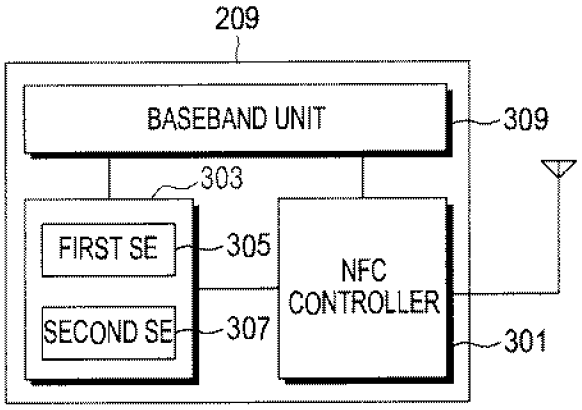

209
BASEBAND UNIT
309
303
FIRST SE
305
NFC CONTROLLER
SECOND SE
307
301

FIG.3

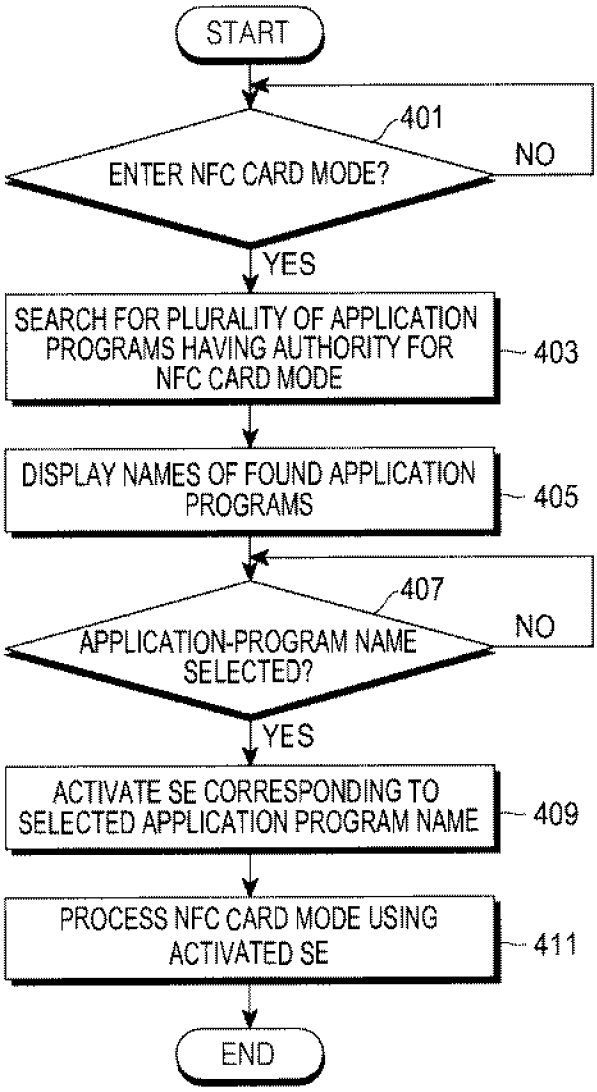

START
401
ENTER NFC CARD MODE?
NO
YES
SEARCH FOR PLURALITY OF APPLICATION PROGRAMS HAVING AUTHORITY FOR NFC CARD MODE
403
DISPLAY NAMES OF FOUND APPLICATION PROGRAMS
405
407
APPLICATION-PROGRAM NAME SELECTED?
NO
YES
ACTIVATE SE CORRESPONDING TO SELECTED APPLICATION PROGRAM NAME
409
PROCESS NFC CARD MODE USING ACTIVATED SE
411
END

FIG.4

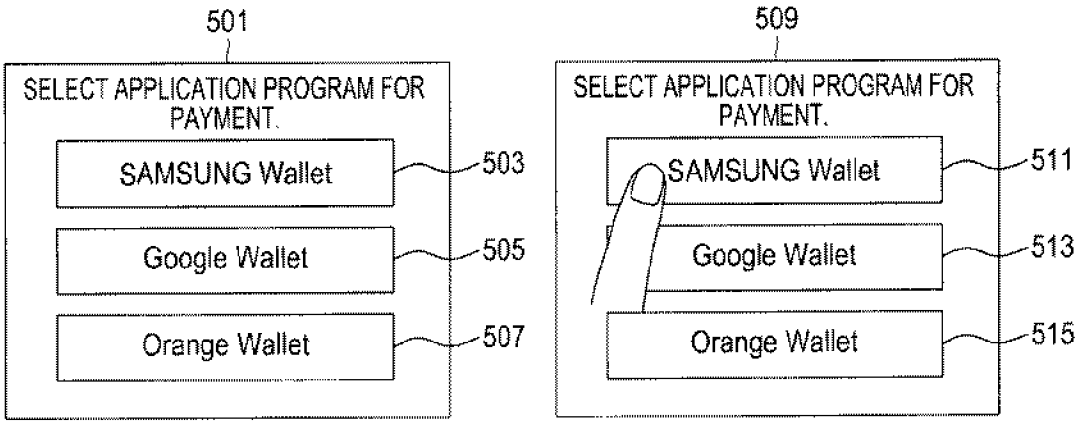

501
SELECT APPLICATION PROGRAM FOR PAYMENT.
SAMSUNG Wallet
503
Google Wallet
505
Orange Wallet
507
509
SELECT APPLICATION PROGRAM FOR PAYMENT.
SAMSUNG Wallet
511
Google Wallet
513
Orange Wallet
515

FIG.5

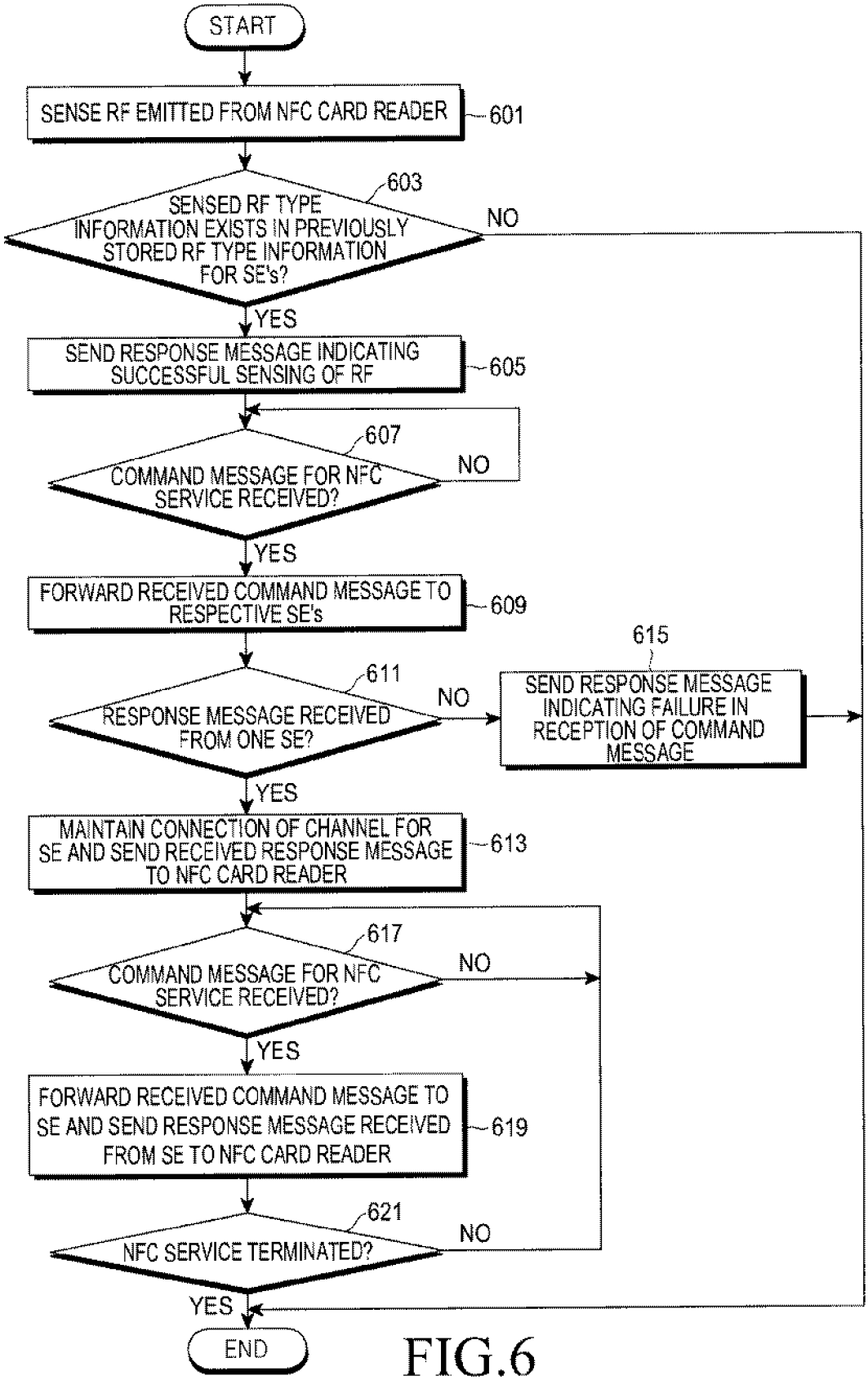

START
SENSE RF EMITTED FROM NFC CARD READER
601
603
SENSED RF TYPE INFORMATION EXISTS IN PREVIOUSLY STORED RF TYPE INFORMATION FOR SE's?
NO
YES
SEND RESPONSE MESSAGE INDICATING SUCCESSFUL SENSING OF RF
605
607
COMMAND MESSAGE FOR NFC SERVICE RECEIVED?
NO
YES
FORWARD RECEIVED COMMAND MESSAGE TO RESPECTIVE SE's
609
615
611
RESPONSE MESSAGE RECEIVED FROM ONE SE?
NO
SEND RESPONSE MESSAGE INDICATING FAILURE IN RECEPTION OF COMMAND MESSAGE
YES
MAINTAIN CONNECTION OF CHANNEL FOR SE AND SEND RECEIVED RESPONSE MESSAGE TO NFC CARD READER
613
617
COMMAND MESSAGE FOR NFC SERVICE RECEIVED?
NO
YES
FORWARD RECEIVED COMMAND MESSAGE TO SE AND SEND RESPONSE MESSAGE RECEIVED FROM SE TO NFC CARD READER
619
621
NFC SERVICE TERMINATED?
NO
YES
END

FIG.6

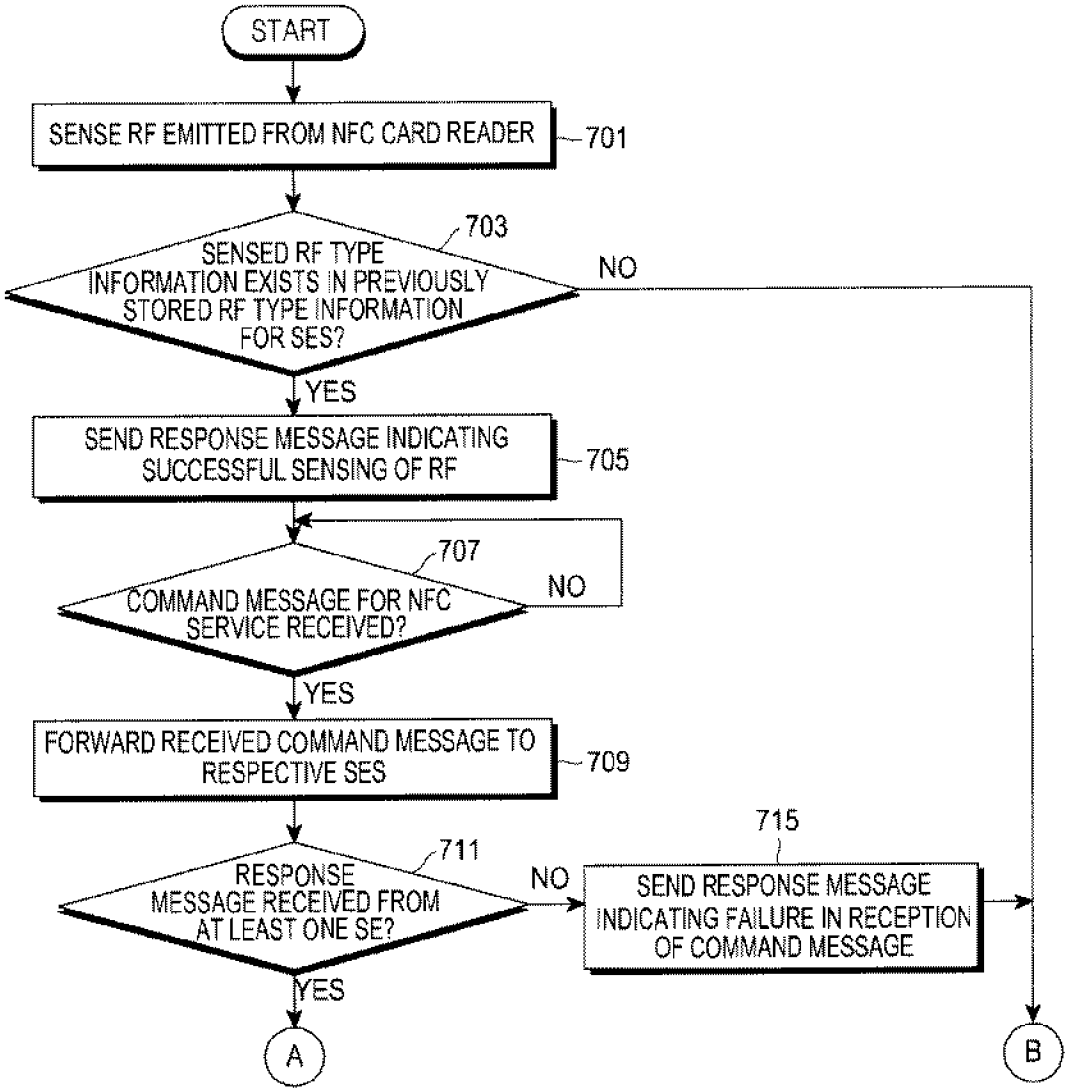

START
SENSE RF EMITTED FROM NFC CARD READER
701
703
SENSED RF TYPE INFORMATION EXISTS IN PREVIOUSLY STORED RF TYPE INFORMATION FOR SES?
NO
YES
SEND RESPONSE MESSAGE INDICATING SUCCESSFUL SENSING OF RF
705
707
COMMAND MESSAGE FOR NFC SERVICE RECEIVED?
NO
YES
FORWARD RECEIVED COMMAND MESSAGE TO RESPECTIVE SES
709
711
RESPONSE MESSAGE RECEIVED FROM AT LEAST ONE SE?
NO
715
SEND RESPONSE MESSAGE INDICATING FAILURE IN RECEPTION OF COMMAND MESSAGE
YES
A
B

FIG.7A

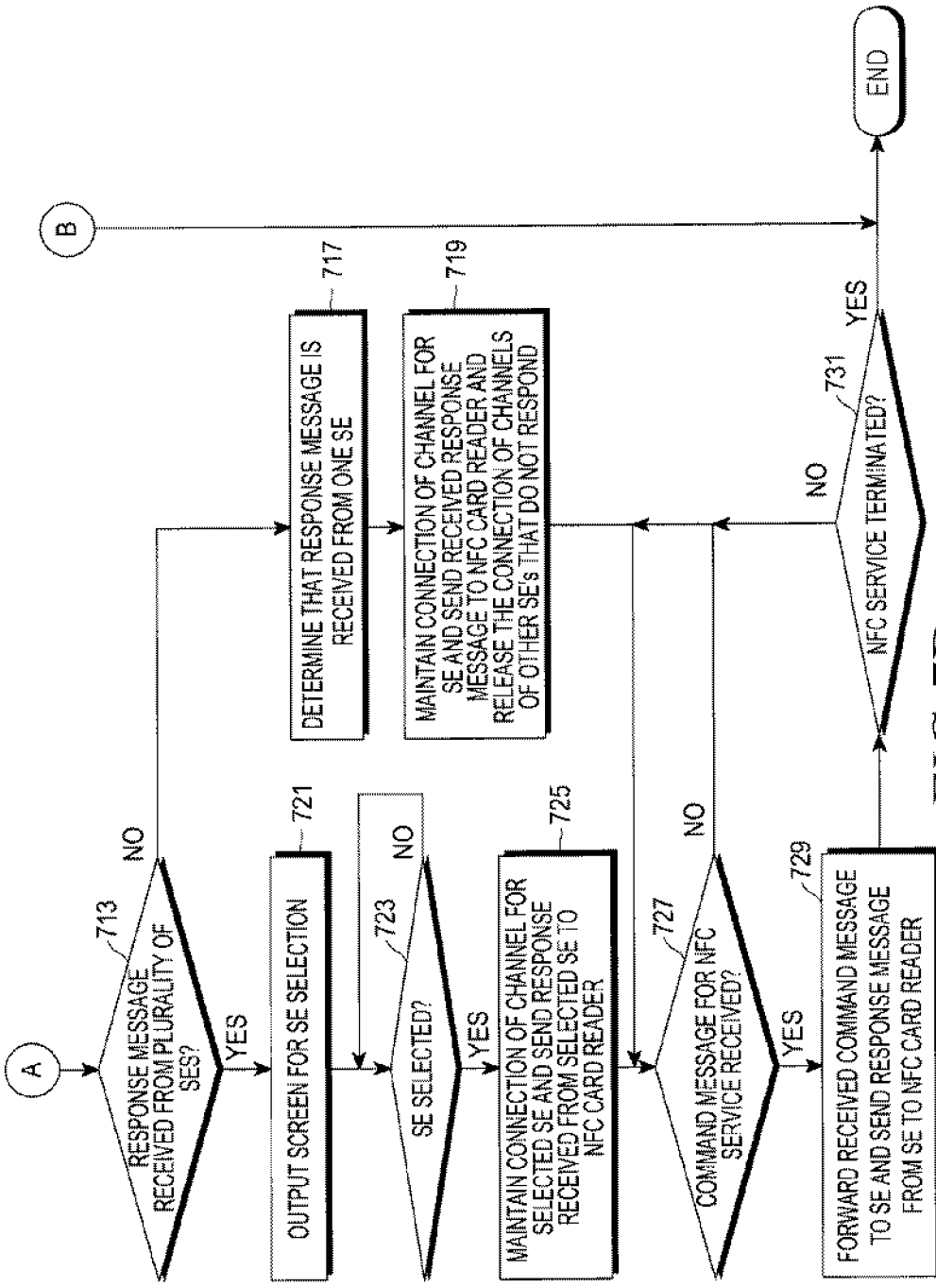

A
B
713
RESPONSE MESSAGE RECEIVED FROM PLURALITY OF SES?
NO
YES
717
DETERMINE THAT RESPONSE MESSAGE IS RECEIVED FROM ONE SE
719
MAINTAIN CONNECTION OF CHANNEL FOR SE AND SEND RECEIVED RESPONSE MESSAGE TO NFC CARD READER AND RELEASE THE CONNECTION OF CHANNELS OF OTHER SE's THAT DO NOT RESPOND
721
OUTPUT SCREEN FOR SE SELECTION
723
SE SELECTED?
NO
YES
725
MAINTAIN CONNECTION OF CHANNEL FOR SELECTED SE AND SEND RESPONSE RECEIVED FROM SELECTED SE TO NFC CARD READER
727
COMMAND MESSAGE FOR NFC SERVICE RECEIVED?
NO
YES
729
FORWARD RECEIVED COMMAND MESSAGE TO SE AND SEND RESPONSE MESSAGE FROM SE TO NFC CARD READER
731
NFC SERVICE TERMINATED?
NO
YES
END

FIG.7B

APPARATUS AND METHOD FOR SELECTING SECURE ELEMENT IN NEAR FIELD COMMUNICATION DEVICE

CLAIM OF PRIORITY

[0001] This application claims the benefit under 35 U.S.C. §119(a) from a Korean Patent Application filed in the Korean Intellectual Property Office on May 8, 2012 and assigned Serial No. 10-2012-0048667, the entire disclosure of which is hereby incorporated by reference in its entirety.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to a Near Field Communication (NFC) device. More particularly, the present invention relates to an apparatus and method for selecting a Secure Element (SE) in a NFC device, particularly when there may be more than one SE provided.

[0004] 2. Description of the Related Art

[0005] With the development of Near Field Communication (NFC) techniques, NFC devices now can provide various services. In particular, the services provided in the NFC devices may include a card mode for executing functions such as a credit card function, a transportation card function, and so forth. To execute the card mode, a Secure Element (SE) for encrypting and storing user related information is required.

[0006] When a plurality of SEs are provided, since it is not pre-defined which SE among them is to be used for an NFC controller to forward data, a NFC device cannot efficiently support the plurality of SEs. Therefore, there is a need for a scheme for solving this problem.

SUMMARY OF THE INVENTION

[0007] Accordingly, the present invention proposes a method and apparatus for selecting one of a plurality of Secure Elements (SEs) to be used for an NFC controller to forward data.

[0008] The present invention also proposes a method and apparatus for selecting one of a plurality of SEs by using one or more application programs associated with the plurality of SEs.

[0009] The present invention also proposes a method and apparatus for selecting one of a plurality of SEs, taking account of whether a command message received from a Near Field Communication (NFC) card reader has responded.

[0010] According to an exemplary aspect of the present invention, there is provided an apparatus for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the apparatus preferably including an SE unit including a plurality of SEs and a main controller for displaying identifiers (IDs) indicating application programs respectively corresponding to one more of the plurality of SEs, and upon selection of one of the IDs, activating an SE corresponding to the selected application-program ID among the plurality of SEs.

[0011] According to another exemplary aspect of the present invention, there is provided an apparatus for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the apparatus including an SE unit including a plurality of SEs and a main controller for, upon receiving a command message for an NFC service from an NFC card reader, checking whether a response message with respect to the command message is received from at least one of the plurality of SEs, when receiving the response message from one of the plurality of SEs, then maintaining connection of a channel for the SE which sends the response message and releasing connection of channels for the other SEs, and processing the NFC service through the SE for which channel connection is maintained.

[0012] According to another exemplary aspect of the present invention, there is provided a method for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the method preferably including determining and/or displaying identifiers (IDs) indicating application programs corresponding to a plurality of SEs and upon selection of one of the IDs, activating an SE corresponding to the selected application-program ID among the plurality of SEs.

[0013] According to another exemplary aspect of the present invention, there is provided a method for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the method preferably including upon receiving a command message for an NFC service from an NFC card reader, checking whether a response message with respect to the command message is received from at least one of a plurality of SEs, if receiving the response message from one of the plurality of SEs, then maintaining connection of a channel for the SE which sends the response message and releasing connection of channels for the other SEs, and processing the NFC service through the SE for which channel connection is maintained.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The above and other descriptions and advantages of exemplary embodiments of the present invention will become more apparent to a person of ordinary skill in the art from the following detailed description taken in conjunction with the accompanying drawings, in which:

[0015] FIG. **1** is a structural diagram of a Near Field Communication (NFC) system according to an exemplary embodiment of the present invention;

[0016] FIG. **2** is a block diagram of a portable terminal according to an exemplary embodiment of the present invention;

[0017] FIG. **3** is a block diagram of an NFC device according to an exemplary embodiment of the present invention;

[0018] FIG. **4** is a flowchart providing an overview of exemplary operation of a method for selecting a Security Element (SE) in a portable terminal according to a first exemplary embodiment of the present invention;

[0019] FIG. **5** is a diagram showing screens which are output for selecting an SE in a portable terminal according to the first exemplary embodiment of the present invention;

[0020] FIG. **6** is a flowchart operation of a method for selecting an SE in an NFC device according to a second exemplary embodiment of the present invention; and

[0021] FIGS. **7**A and **7**B are flowcharts providing an overview of exemplary operation of a method for selecting an SE in an NFC device according to a third exemplary embodiment of the present invention.

DETAILED DESCRIPTION

[0022] Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to the accompanying drawings. In addition, a detailed description of well-known functions and constructions may not be provided if they unnecessarily obscure appreciation of the sub-

EWS-004286

ject matter of the present invention by a person of ordinary skill in the art with the description of what is already known.

[0023] A Near Field Communication (NFC) device according to an exemplary embodiment of the present invention may be included in a portable terminal. Herein, the term "portable terminal" is to be construed broadly and may constitute a mobile electronic device which can be easily carried such as a video phone, a cellular phone, a smart phone, an International Mobile Telecommunication (IMT)-2000 terminal, a Wideband Code Division Multiple Access (WCDMA) terminal, a Universal Mobile Telecommunication Service (UMTS) terminal, a Personal Digital Assistant (PDA), a Portable Multimedia Player (PMP), a Digital Multimedia Broadcasting (DMB) terminal, an Electronic(E) book, a portable computer (e.g., a notebook, a tablet, etc.), a digital camera, portable television, or the like, just to name some non-limiting possibilities.

[0024] FIG. **1** is a structural diagram of an NFC system according to an exemplary embodiment of the present invention.

[0025] Referring now to FIG. **1**, the NFC system may preferably include a portable terminal **101** and an NFC card reader **103**. The NFC card reader **103** can wirelessly read, for example, smart cards, for micro-payment transactions.

[0026] The NFC card reader **103** emits a predetermined Radio Frequency (RF) within a predetermined region, and upon receiving a response message with respect to the emitted RF from the portable terminal **101**, performs an NFC service by using the portable terminal **101**. For example, the predetermined region may be within a radius of about 10 cm from the NFC card reader **103**.

[0027] Herein, the NFC service refers to a service executed using the NFC device included in the portable terminal **101**. The NFC service may include, for example, a terminal mode, a card mode (or NFC card mode), and a Peer-To-Peer (P2P) mode. The terminal mode executes a function of reading a tag and inputting information to the tag; the card mode executes a transportation card or credit card function; and the P2P mode executes a function of sharing data. For example, the data may include business card or multimedia data.

[0028] The portable terminal **101** preferably includes the NFC device which includes a plurality of Secure Elements (SEs). The portable terminal **101** selects one of the plurality of SEs according to user's selection or automatically.

[0029] More specifically, in a first exemplary embodiment of the present invention, the portable terminal **101** checks if it enters the NFC card mode. If so, the portable terminal **101** searches for one or more application programs having authority for the NFC card mode from among all application programs.

[0030] The portable terminal **101** may check whether an application program has authority for the NFC card mode based on program specifications of that application program.

[0031] Herein, program specifications of an application program may include authority for accessing the NFC card mode, an identifier (ID) of the application program, and an SE type associated with the application program. For example, if the application program is a Java Platform-based program, a file name of the program specifications may be "jad". Another example may be an Android-based program and a file name of the program specifications may be "mainfest".

[0032] The ID of the application program may comprise at least one of a name and an icon of the application program. For example, the program specifications may include a name of the application program. Herein, the name of the application program refers to a name to be displayed on a display **203**, and for example, the name may comprise a Google Wallet, an Orange Wallet, a SAMSUNG Wallet, or the like. The SE type may comprise an eSE, UICC, an ASSD, or the like.

[0033] The portable terminal **101** identifies SE types corresponding to respective application programs having authority for the NFC card mode based on program specifications of the respective application programs, and stores the identified SE types for the respective application programs.

[0034] Thereafter, the portable terminal **101** can display IDs of the found application programs, and checks whether one of the displayed IDs is selected. If an ID of a particular application program is selected from the displayed IDs, the portable terminal **101** activates an SE corresponding to the selected application-program ID among the plurality of SEs, and processes the NFC card mode by using the activated SE.

[0035] In a second exemplary embodiment of the present invention, the portable terminal **101** senses a Radio Frequency (RF) emitted from the NFC card reader **103**, and generates RF type information regarding the sensed RF. Herein, the RF type information regarding the sensed RF may include band information of the sensed RF. For example, if the sensed RF is 13.56 MHz, the RF type information regarding the sensed RF may include 13.56 MHz which is a band of the sensed RF.

[0036] The portable terminal **101** checks whether the generated RF type information exists in previously stored RF type information of the plurality of SEs. Herein, RF type information of the plurality of SEs may include RF frequency band information associated with each of the plurality of SEs. For example, if, among the plurality of SEs, a first SE operates in 13.55 MHz through 13.60 MHz, and a second SE operates in 13.20 MHz through 13.50 MHz, then RF type information of the plurality of SEs may include a band of 13.20 MHz through 13.50 MHz and a band of 13.55 MHz through 13.60 MHz which are the operating RF bands for the plurality of SEs.

[0037] In this example, if the generated RF type information does not exist in the previously stored RF type information, the NFC service is then terminated. On the other hand, if the generated RF type information exists, the portable terminal **101** sends to the NFC card reader **103** a response message indicating that the RF is successfully sensed. The portable terminal **101** checks as to whether a command message for the NFC service is received from the NFC card reader **103**.

[0038] If the command message is received, the portable terminal **101** forwards the received command message to each of the plurality of SEs and checks as to whether a response message with respect to the command message is received from one of the plurality of SEs. If no response message is received in response to the command message, the portable terminal **101** generates a response message indicating a processing failure with respect to the command message, sends the generated response message to the NFC card reader **103**, and terminates the NFC service. On the other hand, if the response message with respect to the command message is received, the portable terminal **101** maintains connection of a channel for only the SE which sends the response message, and releases connection of channels for the SEs which does not send the response message. The portable terminal **101** then sends the response message received from the SE to the NFC card reader **103**.

[0039] The portable terminal **101** checks whether a command message for the NFC service is received from the NFC card reader **103**. If so, the portable terminal **101** forwards the received command message to the SE, receives a response message with respect to the command message from the SE, and then sends the received response message to the NFC card reader **103**.

[0040] The portable terminal **101** checks as to whether the NFC service is terminated. If the NFC service is not terminated, the portable terminal **101** repeats an operation of receiving a command message from the NFC card reader **103**, forwarding the command message to the SE, and sending a response message with respect to the command message to the NFC card reader **103**, until termination of the NFC service.

[0041] In a third exemplary embodiment of the present invention, the portable terminal **101** senses an RF emitted from the NFC card reader **103** and generates RF type information regarding the sensed RE. The portable terminal **101** checks whether the generated RF type information exists in previously stored RF type information of the plurality of SEs. If not, then the NFC service is terminated. On the other hand, when the generated RF type information exists in the previously stored RF type information, the portable terminal **101** sends to the NFC card reader **103** a response message indicating that the RF has been successfully sensed.

[0042] The portable terminal **101** checks whether a command message for the NFC service is received from the NFC card reader **103**. If so, the portable terminal **101** forwards the received command message to each of the plurality of SEs, and checks if a response message with respect to the command message is received from at least one of the plurality of SEs.

[0043] If no response message is received in response to the command message, the portable terminal **101** generates a response message indicating a processing failure with respect to the command message, sends the generated response message to the NFC card reader **103**, and then terminates the NFC service.

[0044] On the other hand, when a response message with respect to the command message is received, the portable terminal **101** checks whether the response message is received from each of the plurality of SEs. If the response message is received from one of the plurality of SEs, the portable terminal **101** maintains connection of a channel for only the SE which sends the response message, and releases connection of channels for the other SEs which does not send the response message. The portable terminal **101** sends the response message received from that SE to the NFC card reader **103**.

[0045] If the response message is received from each of the plurality of SEs, the portable terminal **101** outputs icons indicating the plurality of SEs or IDs of application programs associated with the plurality of SEs for SE selection. For example, the portable terminal **101** may output names of the application programs associated with the plurality of SEs. The portable terminal **101** checks to determine if one of the pluralities of SEs is selected. If a name of an application program is selected from among the names of the application programs associated with the plurality of SEs, the portable terminal **101** may determine that a corresponding SE is selected from among the plurality of SEs.

[0046] Once the particular SE is selected, the portable terminal **101** then maintains connection of a channel for only the selected SE among the plurality of SEs, releases connection of channels for the other SEs, and sends a response message received from the selected SE to the NFC card reader **103**.

[0047] The portable terminal **101** checks if a command message for the NFC service is received from the NFC card reader **103**. If the command message is received, the portable terminal **101** forwards the received command message to the SE for which channel connection is maintained, receives a response message with respect to the command message from that SE, and sends the received response message to the NFC card reader **103**. The portable terminal **101** checks if the NFC is terminated. If the NFC service is not terminated, the portable terminal **101** repeats an operation of receiving a command message from the NFC card reader **103**, forwarding the received command message to a corresponding SE, and sending a response message with respect to the command message to the NFC card reader **103**, until termination of the NFC service.

[0048] FIG. **2** is a block diagram of the portable terminal **101** according to an exemplary embodiment of the present invention. Now referring to FIG. **2**, operations of the portable terminal **101** will be described.

[0049] Referring to FIG. **2**, the portable terminal **101** may preferably include a main controller **201**, a display **203**, an input unit **205**, a memory **207**, and an NFC device **209**.

[0050] The display **203** displays an image signal on a screen, and displays data requested to be output from the main controller **201**. If the display **203** is implemented is as a touch display screen, for example, of a capacitive type or a resistive type, the input unit **105** may include only preset minimum keys and the display **203** may replace a part of a key input function of the input unit **205**.

[0051] The memory **207**, which comprises a non-transitory machine readable medium may include program and data memories. Herein, the program memory stores booting and Operating System (OS) for controlling a general operation of the portable terminal **101**, and the data memory stores various data generated in operation of the portable terminal **101**.

[0052] In particular, the memory **207** stores IDs of application programs corresponding to a plurality of SEs. Herein, each of the application programs is associated with one of the plurality of SEs, and processes the card mode by using the associated SE.

[0053] For example, the memory **207** may store application program IDs corresponding to a plurality of SEs as shown in Table 1.

TABLE 1

SE	Application Program ID
First SE	aaa
Second SE	bbb

[0054] Herein, "aaa" represents an ID of a first application program associated with the first SE, and "bbb" represents an ID of a second application program associated with the second SE. The ID of the first or second application program represents a unique ID assigned to the application program.

[0055] The main controller **201** performs an overall operation of the portable terminal **101**. In particular, the main controller **201**, which comprises hardware including a processor or microprocessor, upon receiving an SE selection request from the NFC device **209**, displays names of a plurality of application programs corresponding to a plurality of

EWS-004288

SEs based on IDs of the plurality of application programs for the plurality of SEs stored in the memory **207**, and checks if one of the displayed names of the application programs is selected by a user. If the is a selection by a user, the main controller **201** sends an ID of an SE corresponding to the selected application-program name to the NFC device **209**.

[0056] The NFC device **209** receives selection of one of the plurality of SEs from the user or automatically selects one of them, and processes the NFC service by using the selected SE.

[0057] FIG. **3** is a block diagram of the NFC device **209** according to an exemplary embodiment of the present invention. Now referring to FIG. **3**, operations of the NFC device **209** will now be described. Referring to FIG. **3**, the NFC device **209** may include an NFC controller **301**, an SE unit **303**, and a baseband unit **309**.

[0058] The baseband unit **309** performs radio frequency (RF) communication between the portable terminal **101** and the NFC card reader **103**. More specifically, the baseband unit **309** may include an RF transmitter for up-converting a frequency of a transmission signal and amplifying the transmitted signal and an RF receiver for low-noise amplifying a received signal and down-converting the frequency of the received signal.

[0059] The SE unit **303** is in charge of security, and stores user related information for payment. The SE unit **303**, for example, may include a first SE **305** and a second SE **307**. Typically, the first SE **305** may comprise any one of an Embedded SE (eSE), a Universal Integrated Circuit Card (UICC), and Advanced Security Secure Digital (ASSD), and the second SE **307** may comprise any one of the other SEs. For example, if the first SE **305** is eSE, the second SE **307** may be an UICC or ASSD.

[0060] Herein, eSE is a type of an SE configured with one chipset in portable terminals. The ownership of eSE is owned by a manufacturer. The UICC is a type of an SE configured in a USIM chip of a portable terminal, and the ownership thereof is owned by a common carrier. The ASSD is a type of an SE configured in a micro SD card of a portable terminal, and the ownership thereof is owned by a manufacturer or a common carrier.

[0061] The NFC controller **301** controls an overall operation of the NFC device **209**. More specifically, the NFC controller **301** is configured to select an SE in the following three schemes comprising, a User Selection Scheme, Automatic Selection Scheme, and a Hybrid Scheme to be discussed herein below.

[0062] 1) User Selection Scheme The NFC controller **301** checks if the NFC device **209** enters the card mode. If the NFC device entered card mode, the NFC controller **301** sends an SE selection request to the main controller **201** and receives an ID indicating an SE selected by a user from among a plurality of SEs in response to the sent SE selection request. The NFC controller **301** activates the SE corresponding to the received ID from among the plurality of SEs, and executes the card mode by using the activated SE.

[0063] 2) Automatic Selection Scheme

[0064] The NFC controller **301** senses an RF emitted from the NFC card reader **103**, generates RF type information regarding the sensed RF, and checks whether the generated RF type information exists in previously stored RF type information for a plurality of SEs. If the generated RF type information does not exist in the previously stored RF type information, the NFC controller **301** performs no operation with respect to the sensed RF. On the other hand, if the generated RF type information exists, the NFC controller **301** sends to the NFC card reader **103** a response message indicating that the RF has been successfully sensed.

[0065] The NFC controller **301** checks to determine whether a command message for an NFC service is received from the NFC card reader **103**. If the command message is received, the NFC controller **301** forwards the received command message to each of the plurality of SEs, and checks whether a response message with respect to the command message is received from one of the plurality of SEs.

[0066] If no response message is received in response to the command message, the NFC controller **301** generates a response message indicating a processing failure with respect to the command message and sends the generated response message to the NFC card reader **103**. On the other hand, if a response message with respect to the command message is received, the NFC controller **301** maintains connection of a channel for only the SE which sends the response message and releases connection of channels for the other SEs which does not send the response message. The NFC controller **301** sends the response message received from the SE to the NFC card reader **103**, and checks to determine whether a command message for the NFC service is received from the NFC card reader **103**.

[0067] If the command message is received, the NFC controller **301** forwards the received command message to the SE, receives a response message with respect to the command message from the SE, and sends the received response message to the NFC card reader **103**. The NFC controller **301** checks to determine whether the NFC service is terminated. If the NFC service is not terminated, the NFC controller **301** repeats an operation of receiving a command message from the NFC card reader **103**, forwarding the command message to the SE, and sending a response message with respect to the command message to the NFC card reader **103**, until termination of the NFC service.

[0068] 3) Hybrid Scheme

[0069] Herein, the hybrid scheme is a combination of the user selection scheme and the automatic selection scheme.

[0070] More specifically, the NFC controller **301** senses an RF signal emitted from the NFC card reader **103**, generates RF type information regarding the sensed RF, and checks to determine whether the generated RF type information exists in previously-stored RF type information for a plurality of SEs. If the generated RF type information does not exist in the previously-stored RF type information, the NFC controller **301** does not perform any operation with respect to the sensed RF. On the other hand, if the generated RF type information exists, the NFC controller **301** sends to the NFC card reader **103** a response message indicating that the RF has been successfully sensed.

[0071] The NFC controller **301** checks to determine whether a command message for the NFC service is received from the NFC card reader **103**. If the command message is received, the NFC controller **301** forwards the received command message to each of the plurality of SEs, and checks whether a response message with respect to the command message has been received from each of the plurality of SEs.

[0072] In the case where no response message is received in response to the command message, the NFC controller **301** generates a response message indicating a processing failure with respect to the command message and sends the generated response message to the NFC card reader **103**.

[0073] On the other hand, if a response message with respect to the command message is received from each of the plurality of SEs, the NFC controller **301** sends an SE selection request to the main controller **201** and receives an ID indicating an SE selected by the user from among the plurality of SEs in response to the sent SE selection request. The NFC controller **301** maintains connection of a channel only for the SE corresponding to the received ID among the plurality of SEs, and releases connection of channels for the other SEs. On the other hand, if a response message with respect to the command message is received from an SE, the NFC controller **301** maintains connection of a channel only for the SE from which the response message is received, and releases connection of channels for the other SEs.

[0074] The NFC controller **301** sends the response message received from the SE to the NFC card reader **103**, and checks to determine whether a command message for the NFC service is received from the NFC card reader **103**.

[0075] If the command message is received, the NFC controller **301** forwards the received command message to the SE, receives the response message with respect to the command message to the SE, and forwards the received response message to the NFC card reader **103**. The NFC controller **301** checks whether or not the NFC service is terminated. If not, the NFC controller **301** repeats an operation of receiving a command message from the NFC card reader **103**, forwarding the command message to the SE, and sending a response message with respect to the command message to the NFC card reader **103**, until there is termination of the NFC service.

[0076] FIG. **4** is a flowchart of a method for selecting an SE in the portable terminal **101** according to the first exemplary embodiment of the present invention.

[0077] Referring now to FIG. **4**, in step **401**, the portable terminal **101** checks whether card mode has been entered. If card mode (in an embodiment NFC card mode) has been entered, the portable terminal **101** then performs step **403**. However, in the event that the portable terminal **101** enters the card mode, then it repeats step **401**.

[0078] In step **403**, the portable terminal **101** searches for at least one application programs having authority for the NFC card mode from among all application programs and can then perform step **405**.

[0079] With regard to step **403**, more specifically, the portable terminal **101** may determine whether each application program has authority for the NFC card mode based on program specifications of the application program.

[0080] Herein, program specifications of an application program may include, for example, authority for the NFC card mode, a name of the application program, and an SE type associated with the application program. For example, if the application program is a Java Platform-based program, a file name of the program specifications may be "jad". Another example may be an Android-based program and a file name of the program specifications may be "mainfest". The name of the application program refers to a name to be displayed on a display **203**, and for example, the name may be a Google Wallet, an Orange Wallet, a Samsung Wallet, or the like. The SE type may be eSE, UICC, an ASSD, or the like.

[0081] The portable terminal **101** identifies an SE type corresponding to each of the application programs having authority for the NFC card mode based on the program specifications of the application program, and stores the identified SE type for each application program, as shown in Table 1.

[0082] In step **405**, the portable terminal **101** displays names of the found application programs and performs step **407**. In step **407**, the portable terminal **101** checks whether one of the displayed names of the application programs is selected. If so, the portable terminal **101** then performs step **409**. However, unless one of the displayed names is selected, the portable terminal **101** repeats performance of step **407**.

[0083] At step **409**, the portable terminal **101** activates an SE corresponding to the selected application-program name among the plurality of SEs, and then at step **411** processes the NFC card mode by nsing the activated SE in step **411**.

[0084] FIG. **5** is a diagram showing screens ontput for selecting an SE in the portable terminal **101** according to the first exemplary embodiment of the present invention.

[0085] Referring now to FIG. **5**, a screen **501** is a screen on which the portable terminal **101** displays names of application programs having authority for the NFC card mode. For example, the portable terminal **101** may display a SAMSUNG Wallet **503**, a Google Wallet **505**, and an Orange Wallet **507**.

[0086] A screen **503** is a screen on which the user selects one of the displayed names of the application programs. For example, the portable terminal **101** may determine which one of the displayed SAMSUNG Wallet **503**, Google Wallet **505**, and Orange Wallet **507** is selected as shown on the screen **509**. If the SAMSUNG Wallet **503** is selected, the portable terminal **101** may activate an SE associated with the SAMSUNG Wallet **503** among the plurality of SEs.

[0087] FIG. **6** is a flowchart showing exemplary operation of a method for selecting an SE in the NFC device **209** according to the second exemplary embodiment of the present invention.

[0088] Referring now to FIG. **6**, at Step **601** the portable terminal **101** senses an RF emitted from the NFC card reader **103** and generates RF type information regarding the sensed RF.

[0089] At step **603**, the portable terminal **101** checks whether the generated RF type information exists in previously-stored RF type information for a plurality of SEs. If the generated RF type information does not exist in the previonsly stored RF type information, the portable terminal **101** terminates the NFC service. On the other hand, if the generated RF type information exists, the portable terminal **101** performs step **605**.

[0090] At step **605**, the portable terminal **101** sends to the NFC card reader **103** a response message indicating that the RF has been successfully sensed.

[0091] At step **607**, the portable terminal **101** checks as to whether a command message for the NFC service is received from the NFC card reader **103**. If so, the portable terminal **101** then performs step **609**; if no command message is received, the portable terminal **101** repeats performance of step **607**.

[0092] At step **609**, the portable terminal **101** forwards the received command message to each of the plurality of SEs, and at step **611** checks to determine whether a response message with respect to the command message is received from one of the plurality of SEs. If no response message is received in response to the command message, the portable terminal **101** then performs step **615**; otherwise, the portable terminal **101** performs step **613**.

[0093] At step **615**, the portable terminal **101** generates a response message indicating a processing failure with respect to the command message, sends the generated response message to the NFC card reader **103**, and terminates the NFC

service. At step **613**, the portable terminal **101** maintains connection of a channel for only the SE which sends the response message, and releases connection of channels for the other SEs which does not send the response message. The portable terminal **101** sends the response message received from the SE to the NFC card reader **103**, and performs step **617**.

[0094] At step **617**, the portable terminal **101** checks to determine whether a command message for the NFC service is received from the NFC card reader **103**. If a command message has been received, the portable terminal **101** then performs step **619**; if no command message is received, the portable terminal **101** then repeats step **617**.

[0095] At step **619**, the portable terminal **101** forwards the received command message to the SE, receives a response message with respect to the command message from the SE, sends the received response message to the NFC card reader **103**, and then performs step **621**.

[0096] At step **621**, the portable terminal **101** checks whether the NFC service is terminated. If not, the portable terminal **101** performs step **617**, otherwise, the process is terminated.

[0097] FIGS. **7**A and **7**B are flowcharts describing exemplary operation of a method for selecting an SE in the NFC device **209** according to a third exemplary embodiment of the present invention.

[0098] Referring now to FIGS. **7**A and **7**B, it is shown in FIG. **7**A at step **701** the portable terminal **101** senses an RF emitted from the NFC card reader **103** and generates RF type information regarding the sensed RF in step **701**, and then performs step **703**.

[0099] At step **703**, the portable terminal **101** checks to determine whether the generated RF type information exists in previously-stored RF type information for a plurality of SEs. If the generated RF type information does not exist in the previously-stored RF type information, the portable terminal **101** terminates the NFC service. On the other hand, if the generated RF type information exists, the portable terminal **101** then performs step **705**.

[0100] At step **705**, the portable terminal **101** sends to the NFC card reader **103** a response message indicating that the RF has been successfully sensed, and then performs step **707**.

[0101] At step **707**, the portable terminal **101** checks whether a command message for the NFC service is received from the NFC card reader **103**. If the command message is received, the portable terminal **101** then performs step **709**; otherwise, the portable terminal **101** repeats performance of step **707**.

[0102] At step **709**, the portable terminal **101** forwards the received command message to each of the plurality of SEs, and at step **711** checks whether or not a response message with respect to the command message is received from at least one of the plurality of SEs. If no response message is received in response to the command message, the portable terminal **101** then performs step **715**; otherwise, the portable terminal **101** performs step **713** (FIG. **7**B).

[0103] At step **715**, the portable terminal **101** generates a response message indicating a processing failure with respect to the command message, sends the generated response message to the NFC card reader **103**, and terminates the NFC service.

[0104] At step **713**, the portable terminal **101** checks whether a response message is received from each of the plurality of SEs. If the response message is received from each of the plurality of SEs, the portable terminal **101** performs step **721**; if the response message is received from one of the plurality of SEs, the portable terminal **101** performs step **717**.

[0105] At step **719**, the portable terminal **101** maintains connection of a channel for only the SE which sends the response message and releases connection of channels for the other SEs which does not send the response message, and then preforms step **719**. In step **719**, the portable terminal **101** sends the response message received from the SE to the NFC card reader **103** and performs step **727**.

[0106] In step **721**, the portable terminal **101** outputs icons indicating the plurality of SEs or IDs of application programs associated with the plurality of SEs for SE selection, and performs step **723**. Herein, the IDs of the application programs may be at least one of the icons and names indicating the application programs. For example, the portable terminal **101** may output the names of the application programs associated with the plurality of SEs, as shown on the screen **501**.

[0107] In step **732**, the portable terminal **101** checks to determine whether one of the pluralities of SEs is selected. If a particular SE is selected out of the plurality of SEs, the portable terminal **101** performs step **725**; otherwise, the portable terminal **101** repeats performance of step **723**. If a name of an application program is selected from among names of application programs associated with the plurality of SEs as shown on the screen **503**, the portable terminal **101** may determine that an associated particular SE is selected from among the plurality of SEs.

[0108] At step **725**, the portable terminal **101** maintains connection of a channel for only the selected SE, releases connection of channels for the other SEs, sends a response message received from the selected SE to the NFC card reader **103**, and then performs step **727**.

[0109] At step **727**, the portable terminal **101** checks if a command message for the NFC service is received from the NFC card reader **103**. If the command message is received, the portable terminal **101** performs step **729**; otherwise, the portable terminal **101** repeats performance of step **727**.

[0110] At step **729**, the portable terminal **101** forwards the received command message to the SE for which channel connection is maintained, receives a response message with respect to the command message from the SE, sends the received response message to the NFC card reader **103**, and the performs step **731**.

[0111] At step **731**, the portable terminal **101** checks to determine whether the NFC service is terminated. If the NFC service is not terminated, the portable terminal **101** performs step **727**, otherwise, the process is terminated.

[0112] In this way, the present invention can effectively select one of a plurality of SEs by using application programs associated with the plurality of SEs. The present invention also effectively selects one of the pluralities of SEs, taking account of whether a command message received from an NFC card reader is responded.

[0113] While the present invention has been described with reference to detailed embodiments thereof such as a mobile communication terminal, various modifications may be made therein without departing from the scope of the present invention as defined by the following claims. Accordingly, the scope of the present invention should be defined by the claims and equivalents thereof rather than by the described embodiments.

[0114] In particular, while the NFC controller **301** is described as controlling the NFC device **29**, the main controller **201** may control the NFC device **209**. For example, the main controller **201** may select one of the pluralities of SEs by using one of the user selection scheme, the automatic selection scheme, and the hybrid scheme.

[0115] In addition, the main controller **201** displays names of application programs having authority for the NFC card mode, and upon user's selection of one of the displayed names, generates an ID indicating an SE associated with the selected application-program name, but this operation may be performed by the NFC controller **301**.

[0116] As is apparent from the foregoing description, the present invention can efficiently select one of the pluralities of SEs by nsing application programs associated with the plurality of SEs.

[0117] Moreover, the present invention can effectively select one of the pluralities of SEs, taking account of whether the command received from the NFC card reader is responded.

[0118] The above-described methods according to the present invention can be implemented in hardware, firmware or as software or computer code that is stored in a recording medium such as a CD ROM, flash, EPROM, EEPROM, RAM, a floppy disk, thumbnail drive, a hard disk, or a magneto-optical disk or computer code downloaded over a network originally stored on a remote recording medium and then stored on a non-transitory medium and loaded into hardware such as a processor or microprocessor. The machine executable code stored on the non-transitory machine readable medium can be stored on a local recording medium, and loaded into hardware such as a general purpose computer, or a special processor or in programmable or dedicated hardware, such as an ASIC or FPGA. As would be understood in the art, the computer, the processor, microprocessor controller or the programmable hardware include memory components, e.g., RAM, ROM, Flash, etc. that may store or receive software or computer code that when accessed and executed by the computer, processor or hardware implement the processing methods described herein. In addition, it would be recognized that when a general purpose computer accesses code for implementing the processing shown herein, the execntion of the code transforms the general purpose computer into a special purpose computer for executing the processing shown herein. In addition, an artisan understands and appreciates that a "processor" or "microprocessor" constitntes hardware in the claimed invention. Finally, the claimed invention can include the nse of a location information server comprising more than one server, such as a proxy server.

[0119] While the present invention has been particularly shown and described with reference to exemplary embodiments thereof, it will be understood by those of ordinary skill in the art that various embodimeuts or modifications may be made therein without departing from the spirit and scope of the present invention as defined by the following claims. Accordingly, the scope of the present invention should be defined by the claims and equivalents thereof rather than by the described embodiments.

What is claimed is:

1. An apparatus for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the apparatus comprising:

an SE unit comprising a plurality of SEs;

an NFC controller configured to activate an SE from the plurality of SE's to forward data thereto;

a display unit; and

a main controller for controlling the display unit to display identifiers (IDs) indicating one or more application programs corresponding to the plurality of SEs, and upon selection of one of the IDs, provides the NFC controller with the selected application-program ID corresponding to the SE to be activated from among the plurality of SEs corresponding to the selected application-program ID.

2. The apparatus of claim **1**, wherein the IDs comprise at least one of names and icons of the one or more application programs.

3. The apparatus of claim **1**, wherein the main controller controls display of the IDs upon entering a card mode.

4. The apparatus of claim **1**, wherein the main controller, upon entering a card mode, searches for a plurality of application programs which have authority for the card mode based on program specifications of all of the plurality application programs, identifies SEs corresponding to the application programs found in the search, and displays IDs of the found application programs.

5. The apparatus of claim **4**, wherein the program specifications of all of the plurality of application programs comprise indicating authority for the card mode for each individual application programs, names of individual application programs, and IDs indicating SEs associated with the application programs.

6. An apparatus for selecting a Secnre Element (SE) in a Near Field Communication (NFC) device, the apparatus comprising:

an SE unit comprising a plurality of SEs; and

a main controller configured for, upon receiving a command message for an NFC service from an NFC card reader, checking whether a response message with respect to the command message is received from at least one of the plurality of SEs, and upon receiving the response message from one of the plurality of SEs, maintains a channel connection for the one SE which sends the response message and releases channel connections for a remainder of the plurality of SEs, and processes the NFC service through the SE for which channel connection is maintained.

7. The apparatns of claim **6**, wherein when the main controller receives the response message from each of the plurality of SEs, controls a display of the IDs indicating the plurality of SEs, and upon selection of one of the displayed IDs, the main controller maintains the channel connection for an SE corresponding to the selected ID from among the plurality of SEs and releases channel connections for the remainder of the plurality of SEs, and processes the NFC service through the SE for the selected ID in which chaunel connection is maintained.

8. The apparatus of claim **7**, wherein the IDs comprise at least one of names and icons of one or more application programs corresponding to the plurality of SEs.

9. The apparatus of claim **7**, wherein the main controller, upon entering the card mode, searches for a plurality of application programs having authority for the card mode based on program specifications from among all application programs, identifies SEs of the plurality of SEs corresponding to application programs found in the search, and displays IDs of the found application programs.

10. The apparatns of claim **9**, wherein the program specifications comprise authority for the card mode, names of the application programs, and IDs indicating SEs from the plurality of associated with the application programs.

11. A method for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the method comprising:

displaying identifiers (IDs) by a display unit indicating application programs corresponding to a plurality of SEs; and

upon selection of one of the IDs, activating by an NFC controller an SE corresponding to the selected application-program ID from among the plurality of SEs.

12. The method of claim **11**, wherein the IDs comprise at least one of names and icons of the application programs.

13. The method of claim **11**, wherein the displaying of the IDs comprises displaying the IDs upon entering a card mode.

14. The method of claim **11**, wherein the displaying of the IDs comprises:

upon entering a card mode, searching by a main controller for a plurality of application programs having authority for the card mode from among all application programs based on program specifications; and

identifying SEs corresponding to the application programs found in the search and displaying IDs of the found application programs.

15. The method of claim **14**, wherein the program specifications comprise authority for the card mode, names of the application programs, and IDs indicating respective SEs associated with the application programs.

16. A method for selecting a Secure Element (SE) in a Near Field Communication (NFC) device, the method comprising:

upon receiving a command message for an NFC service from an NFC card reader, checking by a main controller whether a response message with respect to the command message is received from at least one of a plurality of SEs;

upon receiving the response message from one of the plurality of SEs, maintaining a channel connection of the SE which sends the response message and releasing channel connections for the other SEs; and

processing the NFC service through the SE for which channel connection is maintained.

17. The method of claim **16**, further comprising:

upon receiving the response message from each of the plurality of SEs, displaying the IDs indicating each one of the plurality of SEs;

when one of the displayed IDs is selected, maintaining a channel connection for an SE corresponding to the selected ID from among the plurality of SEs and releasing channel connections for the other SEs; and

processing the NFC service throngh the SE for the selected ID in which the channel connection is maintained.

18. The method of claim **17**, wherein the IDs comprise at least one of names and icons of one or more application programs.

19. The method of claim **17**, wherein the displaying of the IDs comprises:

upon entering the card mode, searching for a plurality of application programs having authority for the card mode from among all application programs based on program specifications of all of the application programs; and

identifying respective SEs corresponding to the found application programs and displaying IDs of the found application programs.

20. The method of claim **19**, wherein the program specifications comprise authority for the card mode, names of the application programs, and IDs indicating SEs associated with the application programs.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Ran

(10) **Pub. No.: US 2013/0332293 A1**

(43) **Pub. Date: Dec. 12, 2013**

(54) **MOBILE PAYMENT VIA A VIRTUAL PERIPHERAL DEVICE**

(75) Inventor: **Alexander S. Ran**, Palo Alto, CA (US)

(73) Assignee: **INTUIT INC.**, Mountain View, CA (US)

(21) Appl. No.: **13/489,600**

(22) Filed: **Jun. 6, 2012**

Publication Classification

(51) **Int. Cl.**

G06Q 20/40 (2012.01)

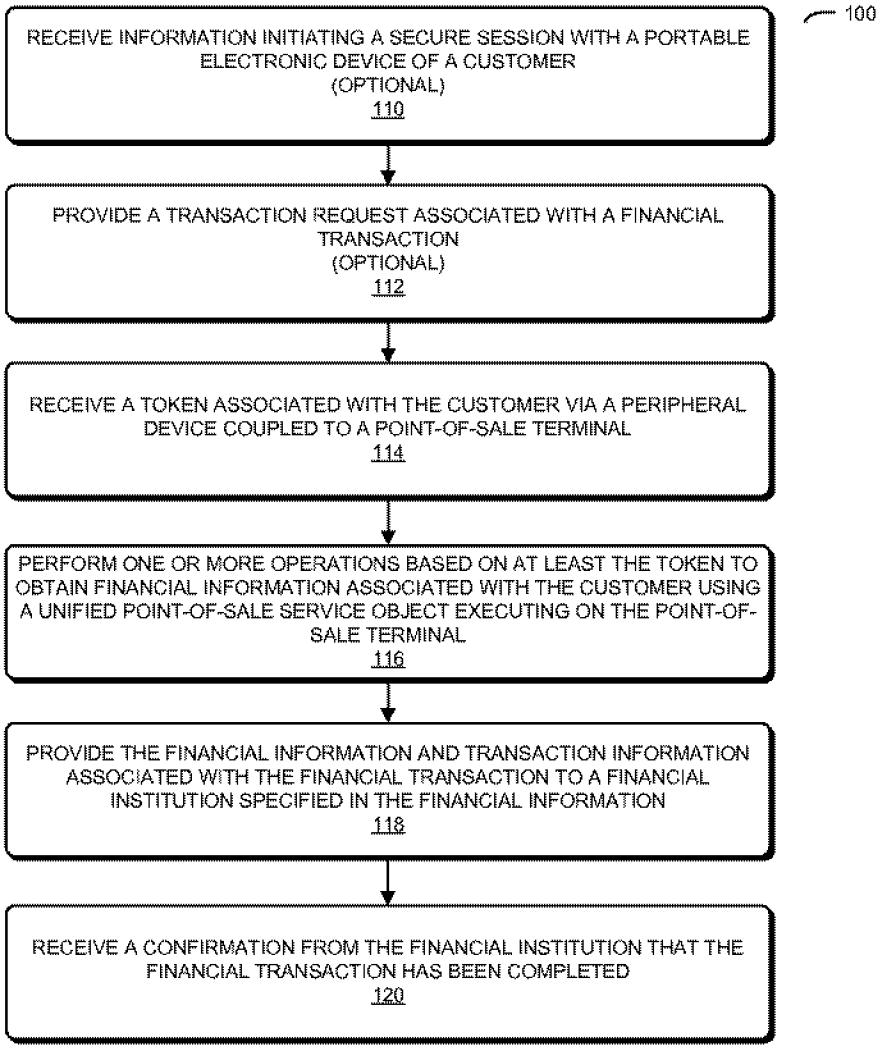
G06Q 20/20 (2012.01)

(52) **U.S. Cl.**

USPC **705/17**

(57) **ABSTRACT**

During a financial transaction, a customer provides a token that identifies the customer to a peripheral device (which is other than a credit-authorization terminal or a magnetic-stripe reader) coupled to the point-of-sale terminal. Then, a unified point-of-sale service object executing on the point-of-sale terminal, which is a driver for a virtual peripheral device, performs one or more operations based on at least the token to obtain financial information associated with the customer. After providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information, the point-of-sale terminal receives a confirmation from the financial institution that the financial transaction has been completed. For example, the confirmation may be received via a credit-authorization-terminal service object that is a driver for the credit-authorization terminal.



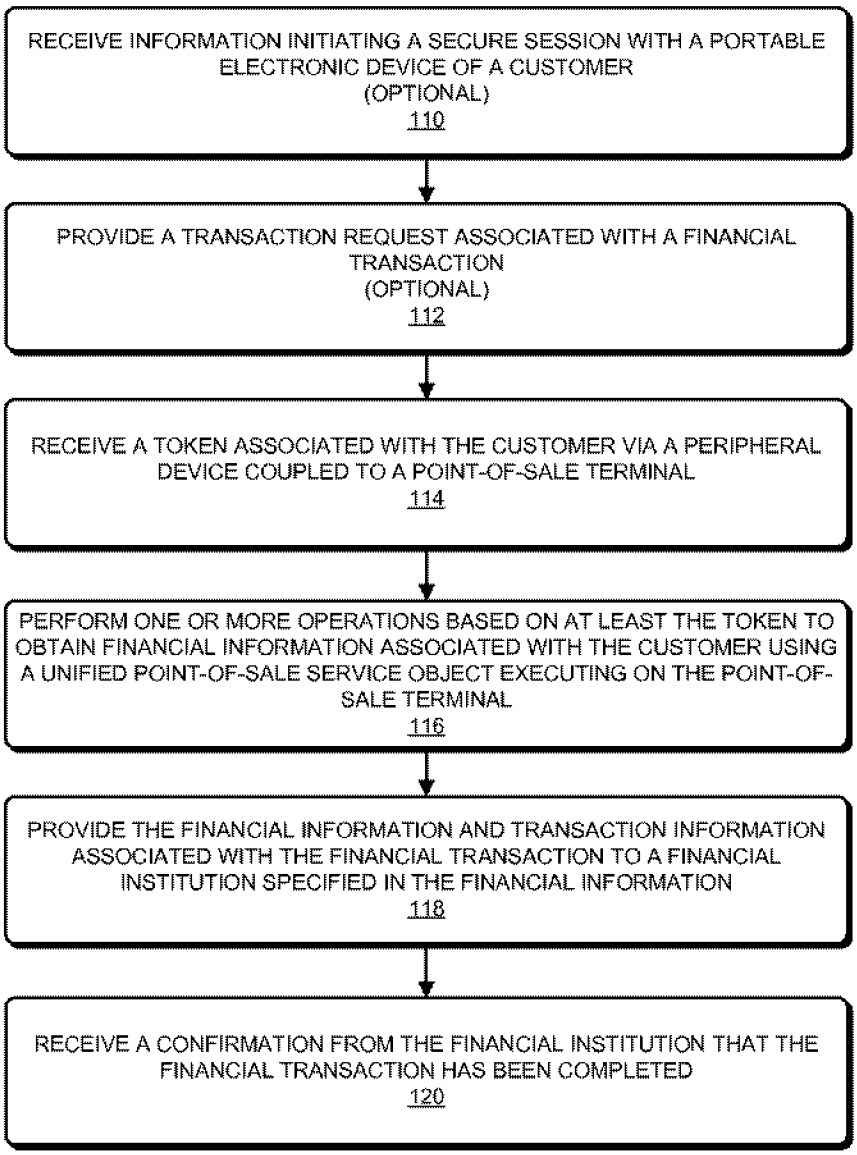

100
RECEIVE INFORMATION INITIATING A SECURE SESSION WITH A PORTABLE ELECTRONIC DEVICE OF A CUSTOMER
(OPTIONAL)
110
PROVIDE A TRANSACTION REQUEST ASSOCIATED WITH A FINANCIAL TRANSACTION
(OPTIONAL)
112
RECEIVE A TOKEN ASSOCIATED WITH THE CUSTOMER VIA A PERIPHERAL DEVICE COUPLED TO A POINT-OF-SALE TERMINAL
114
PERFORM ONE OR MORE OPERATIONS BASED ON AT LEAST THE TOKEN TO OBTAIN FINANCIAL INFORMATION ASSOCIATED WITH THE CUSTOMER USING A UNIFIED POINT-OF-SALE SERVICE OBJECT EXECUTING ON THE POINT-OF-SALE TERMINAL
116
PROVIDE THE FINANCIAL INFORMATION AND TRANSACTION INFORMATION ASSOCIATED WITH THE FINANCIAL TRANSACTION TO A FINANCIAL INSTITUTION SPECIFIED IN THE FINANCIAL INFORMATION
118
RECEIVE A CONFIRMATION FROM THE FINANCIAL INSTITUTION THAT THE FINANCIAL TRANSACTION HAS BEEN COMPLETED
120

FIG. 1

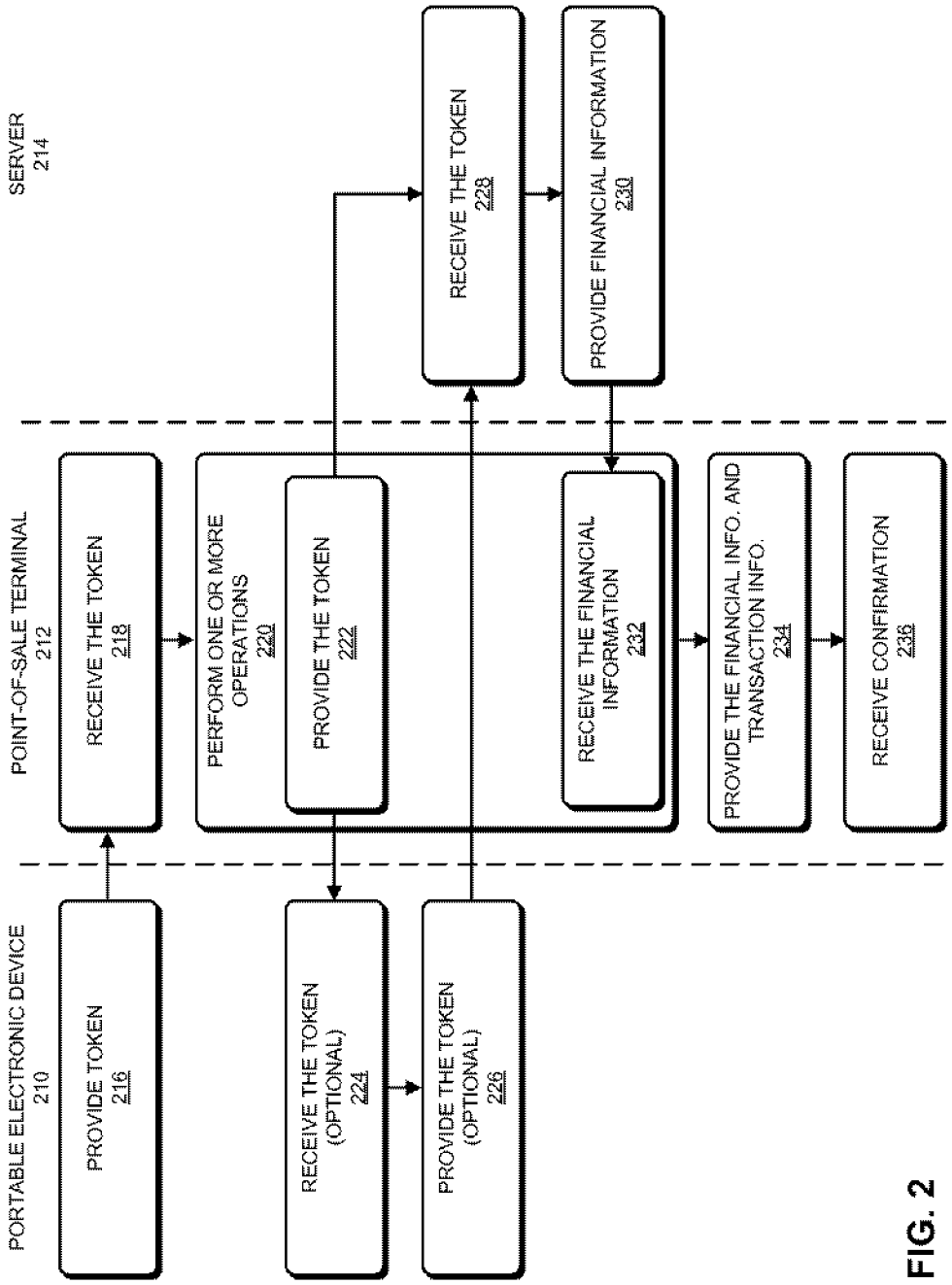

PORTABLE ELECTRONIC DEVICE
210
PROVIDE TOKEN
216
RECEIVE THE TOKEN
(OPTIONAL)
224
PROVIDE THE TOKEN
(OPTIONAL)
226
POINT-OF-SALE TERMINAL
212
RECEIVE THE TOKEN
218
PERFORM ONE OR MORE
OPERATIONS
220
PROVIDE THE TOKEN
222
RECEIVE THE FINANCIAL
INFORMATION
232
PROVIDE THE FINANCIAL INFO. AND
TRANSACTION INFO.
234
RECEIVE CONFIRMATION
236
SERVER
214
RECEIVE THE TOKEN
228
PROVIDE FINANCIAL INFORMATION
230

FIG. 2

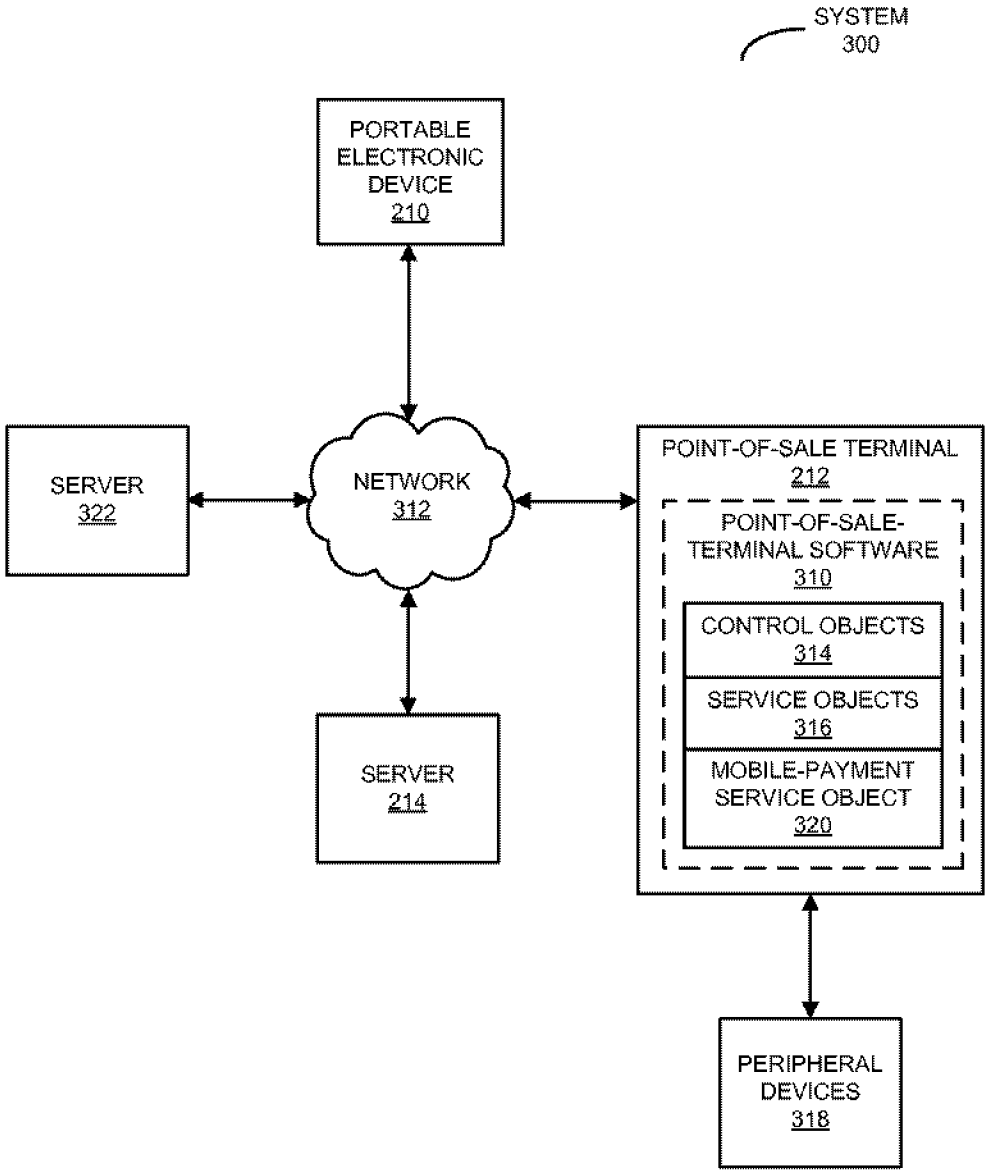

SYSTEM
300
PORTABLE ELECTRONIC DEVICE
210
SERVER
322
NETWORK
312
SERVER
214
POINT-OF-SALE TERMINAL
212
POINT-OF-SALE-TERMINAL SOFTWARE
310
CONTROL OBJECTS
314
SERVICE OBJECTS
316
MOBILE-PAYMENT SERVICE OBJECT
320
PERIPHERAL DEVICES
318

FIG. 3

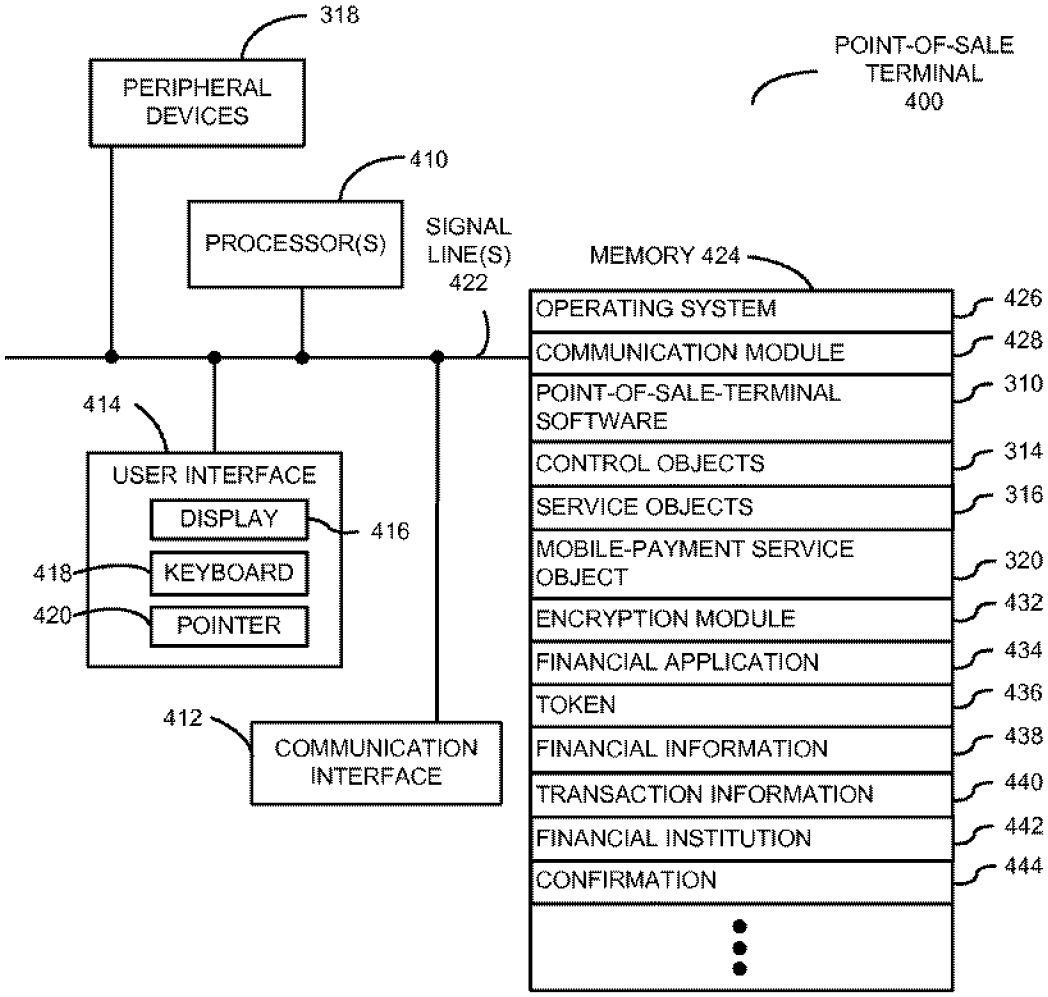

318
PERIPHERAL DEVICES
POINT-OF-SALE TERMINAL 400
410
PROCESSOR(S)
SIGNAL LINE(S) 422
MEMORY 424
OPERATING SYSTEM
426
COMMUNICATION MODULE
428
POINT-OF-SALE-TERMINAL SOFTWARE
310
CONTROL OBJECTS
314
SERVICE OBJECTS
316
MOBILE-PAYMENT SERVICE OBJECT
320
ENCRYPTION MODULE
432
FINANCIAL APPLICATION
434
TOKEN
436
FINANCIAL INFORMATION
438
TRANSACTION INFORMATION
440
FINANCIAL INSTITUTION
442
CONFIRMATION
444
414
USER INTERFACE
DISPLAY
416
418
KEYBOARD
420
POINTER
412
COMMUNICATION INTERFACE

FIG. 4

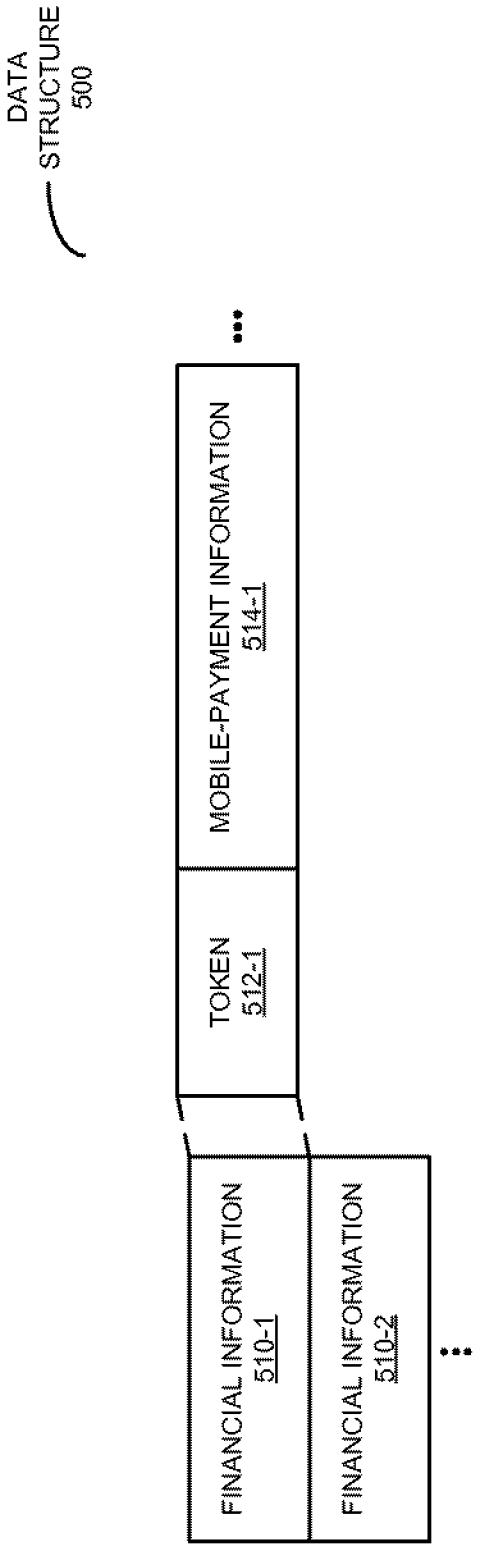

DATA STRUCTURE 500
FINANCIAL INFORMATION 510-1
FINANCIAL INFORMATION 510-2
TOKEN 512-1
MOBILE-PAYMENT INFORMATION 514-1

FIG. 5

MOBILE PAYMENT VIA A VIRTUAL PERIPHERAL DEVICE

BACKGROUND

[0001] The present disclosure relates to a technique for conducting a financial transaction at a point-of-sale terminal.

[0002] The popularity and functionality of portable electronic devices has resulted in their use in an increasing variety of applications. For example, developers are investigating the use of cellular telephones to conduct financial transactions at point-of-sale terminals, such as cash registers.

[0003] Some proposals for these financial transactions (which are sometimes referred to as 'mobile payments') involve using a cellular telephone to provide financial information (such as financial information that is usually contained in a barcode or a magnetic stripe of a debit or credit card) directly to a point-of-sale terminal via an existing peripheral device that is coupled to the point-of-sale terminal, such as a barcode scanner or a magnetic-stripe reader. However, these approaches can significantly constrain the interaction with the customer during the mobile-payment process, which may hinder adoption of mobile payments.

[0004] Alternatively, in other proposals mobile-payments are implemented by changing existing point-of-sale-terminal hardware and/or software. However, these changes will significantly increase the cost and complexity of implementing mobile payments, and therefore may also restrict adoption of mobile payments.

SUMMARY

[0005] The disclosed embodiments relate to a point-of-sale terminal that conducts a financial transaction. During operation, the point-of-sale terminal receives a token associated with a customer via a peripheral device coupled to the point-of-sale terminal. This token identifies the customer, and the peripheral device is other than a credit-authorization terminal or a magnetic-stripe reader. Then, a unified point-of-sale service object executing on the point-of-sale terminal performs one or more operations based on at least the token to obtain financial information associated with the customer, where the unified point-of-sale service object is a driver for a virtual peripheral device. Moreover, the point-of-sale terminal provides the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information. Next, the point-of-sale terminal receives a confirmation from the financial institution that the financial transaction has been completed.

[0006] Note that the one or more operations may include: providing the token to a third party that is other than the financial institution; and receiving the financial information from the third party. For example, the token may be provided to the third party via a portable electronic device of the customer. Alternatively or additionally, the token may be provided to the third party via a network coupled to the point-of-sale terminal.

[0007] In some embodiments, prior to receiving the token, the point-of-sale terminal receives information initiating a secure session with the portable electronic device of the customer. This information may be conveyed using: wireless communication, near-field communication, an audio channel, and/or a video channel.

[0008] Furthermore, in some embodiments, prior to receiving the token the point-of-sale terminal provides a transaction request associated with the financial transaction from point-of-sale-terminal software executing on the point-of-sale terminal to the unified point-of-sale service object.

[0009] Additionally, note that providing the financial information and the transaction information associated with the financial transaction, and receiving the confirmation may occur via a credit-authorization-terminal service object which is a driver for the credit-authorization terminal. This credit-authorization-terminal service object may be compatible with a unified point-of-sale standard.

[0010] Another embodiment provides a method that includes at least some of the operations performed by the point-of-sale terminal.

[0011] Another embodiment provides a computer-program product for use with the point-of-sale terminal. This computer-program product includes instructions for at least some of the operations performed by the point-of-sale terminal.

BRIEF DESCRIPTION OF THE FIGURES

[0012] FIG. **1** is a flow chart illustrating a method for conducting a financial transaction in accordance with an embodiment of the present disclosure.

[0013] FIG. **2** is a drawing illustrating the method of FIG. **1** in accordance with an embodiment of the present disclosure.

[0014] FIG. **3** is a block diagram illustrating a system that performs the method of FIGS. **1** and **2** in accordance with an embodiment of the present disclosure.

[0015] FIG. **4** is a block diagram illustrating a point-of-sale terminal that performs the method of FIGS. **1** and **2** in accordance with an embodiment of the present disclosure.

[0016] FIG. **5** is a block diagram illustrating a data structure for use in the point-of-sale terminal of FIG. **4** in accordance with an embodiment of the present disclosure.

[0017] Note that like reference numerals refer to corresponding parts throughout the drawings. Moreover, multiple instances of the same part are designated by a common prefix separated from an instance number by a dash.

DETAILED DESCRIPTION

[0018] Embodiments of a point-of-sale terminal, a technique for conducting a financial transaction, and a computer-program product (e.g., software) for use with the point-of-sale terminal are described. During the financial transaction, a customer provides a token that identifies the customer to a peripheral device (which is other than a credit-authorization terminal or a magnetic-stripe reader) coupled to the point-of-sale terminal. For example, the customer may provide the token using a portable electronic device, such as a cellular telephone. Then, a unified point-of-sale service object executing on the point-of-sale terminal, which is a driver for a virtual peripheral device, performs one or more operations based on at least the token to obtain financial information associated with the customer. After providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information, the point-of-sale terminal receives a confirmation from the financial institution that the financial transaction has been completed. For example, the confirmation may be received via a credit-authorization-terminal service object that is a driver for the credit-authorization terminal.

[0019] By allowing the customer to conduct the financial transaction in a manner compatible with a unified point-of-sale standard, but without using a credit-authorization termi-

nal or a magnetic-stripe reader, this financial technique may facilitate commercial activity. In particular, the financial technique may facilitate mobile payments via a portable electronic device (such as a cellular telephone) without requiring changes to point-of-sale-terminal hardware or software (i.e., in a way that is compatible with existing point-of-sale-terminal hardware and software), and without constraining the interaction with the customer during the mobile payments. In this way, the financial technique provides a software solution that can be broadly adopted with little or no expense or inconvenience for merchants or customers.

[0020] In the discussion that follows, a user or a customer may include: an individual (for example, an existing customer, a new customer, a service provider, a vendor, a contractor, etc.), an organization, a business and/or a government agency. Furthermore, a 'business' should be understood to include: for-profit corporations, non-profit corporations, organizations, groups of individuals, sole proprietorships, government agencies, partnerships, etc.

[0021] We now describe embodiments of the financial technique, which may be performed by a point-of-sale terminal (such as point-of-sale terminal **400** in FIG. **4**). FIG. **1** presents a flow chart illustrating a method **100** for conducting a financial transaction. During operation, the point-of-sale terminal (such as a cash register) receives a token associated with a customer via a peripheral device coupled to the point-of-sale terminal (operation **114**). This token identifies the customer, and the peripheral device is other than a credit-authorization terminal or a magnetic-stripe reader.

[0022] Then, a unified point-of-sale service object executing on the point-of-sale terminal performs one or more operations based on at least the token to obtain financial information associated with the customer (operation **116**), where the unified point-of-sale service object is a driver for a virtual peripheral device. (The unified point-of-sale service object is sometimes referred to as a 'virtual mobile payment peripheral.') As described below with reference to FIG. **2**, the one or more operations may include: providing the token to a third party that is other than the financial institution; and receiving the financial information from the third party. For example, the token may be provided to the third party via a portable electronic device of the customer. Alternatively or additionally, the token may be provided to the third party via a network coupled to the point-of-sale terminal.

[0023] Moreover, the point-of-sale terminal provides the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information (operation **118**). Next, the point-of-sale terminal receives a confirmation from the financial institution that the financial transaction has been completed (operation **120**). For example, providing the financial information and the transaction information associated with the financial transaction (operation **118**), and receiving the confirmation (operation **120**) may occur via a credit-authorization-terminal service object which is a driver for the credit-authorization terminal. This credit-authorization-terminal service object, as well as the virtual mobile payment peripheral, may be compatible with a unified point-of-sale standard, such as the UnifiedPOS or UPOS standard (from the National Retail Federation of Washington, D.C.).

[0024] In some embodiments, prior to receiving the token (operation **114**), the point-of-sale terminal optionally receives information initiating a secure session with the portable electronic device of the customer (operation **110**) at the start of the financial transaction. This information may be conveyed using: wireless communication, near-field communication, an audio channel, and/or a video channel.

[0025] Furthermore, in some embodiments, prior to receiving the token (operation **114**) the point-of-sale terminal optionally provides a transaction request associated with the financial transaction (operation **112**) from point-of-sale-terminal software executing on the point-of-sale terminal to the unified point-of-sale service object. In response to this transaction request, the unified point-of-sale service object may await the token from the peripheral device.

[0026] In an exemplary embodiment, the financial technique is implemented using the portable electronic device, the point-of-sale terminal and at least one server, which communicate through a network, such as a cellular-telephone network and/or the Internet (e.g., using a client-server architecture). This is illustrated in FIG. **2**, which presents a flow chart illustrating method **100** (FIG. **1**). During this method, a user of portable electronic device **210** provides the token (operation **216**) that identifies the user. For example, the user may be a customer, and portable electronic device **210** may be a cellular telephone. In these embodiments, the token may be conveyed using: wireless communication, near-field communication, an audio channel, and/or a video channel. Alternatively, the user may enter the token into a keypad or portable electronic device **210** may display or provide an image of a barcode that includes a spatial pattern corresponding to the token.

[0027] After receiving the token (operation **218**) via the peripheral device (such as a wireless receiver, a barcode scanner or the keypad), the unified point-of-sale service object executing on point-of-sale terminal **212** performs the one or more operations (operation **220**) based on at least the token to obtain financial information associated with the customer. (As described further below with reference to FIG. **3**, the unified point-of-sale service object may be the driver for the virtual peripheral device.) For example, the token may be provided to server **214** associated with the third party (which may be other than the financial institution that will make payment for the customer in the financial transaction), such as a provider of the financial technique. In particular, point-of-sale terminal **212** may provide the token (operation **222**) to server **214** via a network. Alternatively, the token may be optionally provided (operation **222**) to server **214** via portable electronic device **210** (operations **224** and **226**).

[0028] Moreover, after receiving the token (operation **228**), server **214** may access and provide the financial information (operation **230**) to point-of-sale terminal **212**. For example, the financial information may include mobile-payment information for the customer, such as: an account identifier, an available amount that can be spent, a financial institution (such as a bank), etc.

[0029] Furthermore, after receiving the financial information (operation **232**), point-of-sale terminal **212** provides the financial information and the transaction information (operation **234**) associated with the financial transaction to the financial institution specified in the financial information. For example, the transaction information may include: a transaction day/time, a merchant identifier, a product code and a transaction amount.

[0030] Note that the financial information and the transaction information may be received by a server associated with the financial institution (not shown), which then completes the financial transaction (for example, by making payment on

behalf of the consumer to the merchant associated with point-of-sale terminal **212**). After the financial transaction is complete (not shown), this server may provide the confirmation that the financial transaction has been completed (not shown). Alternatively, the financial information and the transaction information may be received by server **214** (not shown), which then completes the financial transaction (not shown) and provides the confirmation (not shown).

[0031] Then, point-of-sale terminal **212** receives the confirmation (operation **236**). For example, the confirmation may be received via a credit-authorization-terminal service object which is a driver for the credit-authorization terminal coupled to point-of-sale terminal **212**.

[0032] In some embodiments of method **100** (FIGS. **1** and **2**), there may be additional or fewer operations. Moreover, the order of the operations may be changed, and/or two or more operations may be combined into a single operation.

[0033] In an exemplary embodiment, the financial technique leverages the UPOS standard to integrate mobile payments with point-of-sale-terminal software. Most commercially available point-of-sale-terminal software (such as point-of-sale operating systems) supports the UPOS standard, which covers integration of peripheral devices, such as: a credit-authorization terminal, a magnetic-stripe reader, etc. The UPOS architecture is based on the concept of control objects and service objects. During operation of a point-of-sale terminal, the point-of-sale-terminal software interacts with one or more control objects for tasks such as credit-payment authorization. A control object connects to the appropriate service object that serves the role of a driver for an external or peripheral device that performs the task(s) and returns the result. For example, in the case of the credit-payment authorization, the credit-authorization-terminal service object is the driver for the credit-authorization terminal.

[0034] In the financial technique, mobile payments are integrated with the point-of-sale-terminal software by using a service object to drive a virtual peripheral device. Thus, instead of using a service object to drive an actual peripheral device, a service object becomes a virtual peripheral device itself while implementing the logic necessary to complete a task (in this case, the financial transaction). This logic may include interacting directly with the user's portable electronic device and/or with a server associated with the third party that facilitates or provides the financial technique (including providing the financial information in response to receiving the token from the point-of-sale terminal). In this way, the standard point-of-sale peripheral integration interface may be used to enable a software-only solution that facilitates mobile payments that work with a majority of existing point-of-sale-terminal software and hardware.

[0035] In an exemplary embodiment, a customer wants to purchase a product or a service from a merchant. A cashier at a point-of-sale terminal may ring up the purchased item(s). The cashier may also optionally invoke a barcode-scanner operation, such as that normally used for a store loyalty card. In response, the point-of-sale-terminal software may submit a transaction request to a virtual barcode scanner (i.e., the unified point-of-sale service object) that is provided by a provider of the financial technique. In response to this transaction request, the virtual barcode scanner may await the token from the peripheral device (such as a barcode scanner).

[0036] Then, the customer may optionally perform an operation for session creation (i.e., an operation that initiates a session). For example, session creation may involve: a near-field-communication 'tap,' or audio or video signal transmission or reception that initiates a proximity connection with the unified point-of-sale service object on the point-of-sale terminal. This communication between the portable electronic device and the point-of-sale terminal may use BlueTooth® (from the BlueTooth Special Interest Group of Kirkland, Wash.) and/or WiFi™ (from the WiFi Alliance of Austin, Tex.).

[0037] Next, a mobile-payment application executing on the portable electronic device (which may also be provided by the provider of the financial technique) provides a token (such as a numerical identifier) to the barcode-scanner service object on the point-of-sale terminal. This token identifies the user either to the merchant and/or to the provider of the financial technique (who may be accessible to all service objects executing on the point-of-sale terminal via a secure data connection). After receiving the financial information from the merchant and/or the provider, the barcode-scanner service object returns the financial information associated with the user to the point-of-sale-terminal software.

[0038] In some embodiments, the cashier optionally performs additional operations for awarding loyalty points, redeeming coupons and offers, etc.

[0039] Furthermore, after receiving the financial information, the cashier may perform a credit-authorization operation for the amount due using the credit-authorization-terminal service object. In response, the point-of-sale-terminal software makes a corresponding request to the credit-authorization-terminal service object.

[0040] Additionally, the credit-authorization-terminal service object interacts with the mobile-payment application on the user's portable electronic device and/or with server **214** (FIG. **2**) to obtain payment authorization from both the consumer and the payment processor (such as the financial institution). This authorization is passed back to the point-of-sale-terminal software. In some embodiments, the point-of-sale-terminal software optionally prints a receipt using a UPOS printer service object that passes receipt information to the mobile-payment application and/or to server **214** (FIG. **2**).

[0041] By using a substitute unified point-of-sale service object, such as the virtual barcode scanner (as opposed to the credit-authorization terminal or the magnetic-stripe reader, and, more generally, hardware that scans a credit or a debit card and receives authorization), which can connect to server **214** (FIG. **2**) associated with the provider of the financial technique, the financial technique may facilitate mobile payments.

[0042] Note that a variety of communication techniques may be used to provide a connection between the mobile-payment application and the unified point-of-sale service object, including: proximity communication (such as BlueTooth® and/or WiFi™), audio communication, video communication, near-field communication, and/or a wireless area network (for example, in embodiments where the portable electronic device and the point-of-sale terminal have access to a wireless area network or Internet protocol).

[0043] We now describe embodiments of the system and the point-of-sale terminal, and their use. FIG. **3** presents a block diagram illustrating a system **300** that performs method **100** (FIGS. **1** and **2**). In this system, a user of portable electronic device **210** may use a software product (for example, the mobile-payment application), such as a software application that is resident on and that executes on portable electronic device **210**. (Alternatively, the user may interact with a web

page that is provided by server **214** via network **312**, and which is rendered by a web browser on portable electronic device **210**. For example, at least a portion of the software application may be an application tool that is embedded in the web page, and which executes in a virtual environment of the web browser. Thus, the application tool may be provided to the user via a client-server architecture.) This software application may be a standalone application or a portion of another application that is resident on and which executes on portable electronic device **210** (such as a software application that is provided by server **214** or that is installed and which executes on portable electronic device **210**).

[0044] As discussed previously, during a financial transaction (such as purchasing a product from a merchant), the user (who is the customer in the preceding discussion) may use the software application to provide a token (which identifies the user) from portable electronic device **210** to point-of-sale terminal **212** via network **312**. As shown in FIG. **3**, point-of-sale-terminal software **310** may include control objects **314** (such as a credit-authorization-terminal control object, a magnetic-stripe-reader control object, an electronic-money-transfer control object, etc.) that interface via a UPOS standard peripheral interface with drivers or service objects **316** (such as a credit-authorization-terminal service object, a magnetic-stripe-reader service object, an electronic-money-transfer service object, etc.) for peripheral devices **318** (such as a credit-authorization terminal, a magnetic-stripe reader, etc.). The token may be received by a UPOS service object such as mobile-payment service object **320** (for example, the virtual barcode scanner), which is a driver for a virtual peripheral device.

[0045] After receiving the token, mobile-payment service object **320** performs one or more operations based on at least the token to obtain financial information associated with the user. For example, mobile-payment service object **320** may provide the token to server **214** via network **312** either directly or via portable electronic device **210**, and server **214** may use the customer specified by the token to access and return the financial information to mobile-payment service object **320** and, thus, point-of-sale terminal **212**.

[0046] Then, point-of-sale terminal **212** may provide the financial information and the transaction information associated with the financial transaction to a financial institution specified in the financial information. For example, the credit-authorization-terminal control object may provide the financial information and the transaction information to the credit-authorization-terminal service object, which in turn drives the credit-authorization terminal that provides the financial information and the transaction information via network **312** to server **214** or server **322** (which is associated with the financial institution). Thus, the financial information and the transaction information may be directly provided to the financial institution that completes the financial transaction or it may be provided first to the provider of the financial technique (via server **214**), which interacts with server **322** via network **312** to complete the financial transaction.

[0047] Next, point-of-sale terminal **212** receives a confirmation from the financial institution that the financial transaction has been completed. This confirmation may be received directly from server **322** via network **312** or indirectly from server **214** via network **312**.

[0048] Note that information in system **300** may be stored at one or more locations in system **300** (i.e., locally or remotely). Moreover, because this data may be sensitive in nature, it may be encrypted. For example, stored data and/or data communicated via network **312** may be encrypted.

[0049] FIG. **4** presents a block diagram illustrating a point-of-sale terminal **400** that performs method **100** (FIGS. **1** and **2**), such as point-of-sale terminal **212** (FIGS. **2** and **3**). Point-of-sale terminal **400** includes one or more processing units or processors **410**, a communication interface **412**, a user interface **414**, and one or more signal lines **422** coupling these components together. Note that the one or more processors **410** may support parallel processing and/or multi-threaded operation, the communication interface **412** may have a persistent communication connection, and the one or more signal lines **422** may constitute a communication bus. Moreover, the user interface **414** may include: a display **416**, a keyboard **418**, and/or a pointer **420**, such as a mouse.

[0050] Memory **424** in point-of-sale terminal **400** may include volatile memory and/or non-volatile memory. More specifically, memory **424** may include: ROM, RAM, EPROM, EEPROM, flash memory, one or more smart cards, one or more magnetic disc storage devices, and/or one or more optical storage devices. Memory **424** may store an operating system **426** that includes procedures (or a set of instructions) for handling various basic system services for performing hardware-dependent tasks. Memory **424** may also store procedures (or a set of instructions) in a communication module **428**. These communication procedures may be used for communicating with one or more computers and/or servers, including computers and/or servers that are remotely located with respect to point-of-sale terminal **400**.

[0051] Memory **424** may also include multiple program modules (or sets of instructions), including: point-of-sale-terminal software **310** (or a set of instructions), control objects **314** (or a set of instructions), service objects **316** (or a set of instructions), mobile-payment service object **320** (or a set of instructions), encryption module **432** (or a set of instructions) and/or financial application **434** (or a set of instructions). Note that one or more of these program modules (or sets of instructions) may constitute a computer-program mechanism.

[0052] During the financial transaction in method **100** (FIGS. **1** and **2**), mobile-payment service object **320** receives a token **436** from a customer. Then, mobile-payment service object **320** performs one or more operations based on at least token **436** to obtain financial information **438** associated with the customer. For example, mobile-payment service object **320** may directly or indirectly provide token **436** to server **214** (FIGS. **2** and **3**) using communication module **428** and communication interface **412**, and in response mobile-payment service object **320** may receive financial information **438** from server **214** (FIGS. **2** and **3**).

[0053] Alternatively, financial information **438** may be stored on point-of-sale terminal **400** and may be accessed using token **436**. For example, token **436** may be associated with a loyalty program, and financial information **438** may have been previously provided by the customer when their loyalty account was set up. In some embodiments, this look-up operation uses a data structure that stores financial information associated with customers. This is shown in FIG. **5**, which presents a data structure **500** that includes financial information **510**. In particular, financial information **510-1** may include: token **512-1** and mobile-payment information **514-1** (such as an account identifier, an available amount that can be spent, a financial institution, etc.).

[0054] Referring back to FIG. **4**, point-of-sale terminal **400** may directly or indirectly provide financial information **438** and transaction information **440** associated with the financial transaction to a financial institution **442** specified in financial information **438**. Next, point-of-sale terminal **400** directly or indirectly receives a confirmation **444** from financial institution **442** that the financial transaction has been completed.

[0055] Because information in point-of-sale terminal **400** may be sensitive in nature, in some embodiments at least some of the data stored in memory **424** and/or at least some of the data communicated using communication module **428** is encrypted using encryption module **432**.

[0056] Instructions in the varions modules in memory **424** may be implemented in: a high-level procedural language, an object-oriented programming language, and/or in an assembly or machine language. Note that the programming language may be compiled or interpreted, e.g., configurable or confignred, to be executed by the one or more processors **410**.

[0057] Although point-of-sale terminal **400** is illustrated as having a number of discrete items, FIG. **4** is intended to be a functional description of the various features that may be present in point-of-sale terminal **400** rather than a structnral schematic of the embodiments described herein. In practice, and as recognized by those of ordinary skill in the art, the functions of point-of-sale terminal **400** may be distributed over a large number of servers or computers, with various gronps of the servers or computers performing particular subsets of the functions. In some embodiments, some or all of the functionality of point-of-sale terminal **400** may be implemented in one or more application-specific integrated circuits (ASICs) and/or one or more digital signal processors (DSPs).

[0058] Point-of-sale terminals (such as point-of-sale terminal **400**), as well as computers and servers in system **300** (FIG. **3**) may include one of a variety of devices capable of manipulating computer-readable data or communicating such data between two or more computing systems over a network, including: a personal computer, a laptop computer, a tablet computer, a mainframe computer, a portable electronic device (such as a cellular phone or PDA), a server and/or a client computer (in a client-server architecture). Moreover, network **312** (FIG. **3**) may include: the Internet, World Wide Web (WWW), an intranet, a cellular-telephone network, LAN, WAN, MAN, or a combination of networks, or other technology enabling communication between computing systems.

[0059] In some embodiments one or more of the modules in memory **424** may be associated with and/or included in a financial application **434**. This financial application may include: Quicken™ and/or TurboTax™ (from Intuit, Inc., of Mountain View, Calif.), Microsoft Money™ (from Microsoft Corporation, of Redmond, Wash.), SplashMoney™ (from SplashData, Inc., of Los Gatos, Calif.), Mvelopes™ (from In2M, Inc., of Draper, Utah), and/or open-source applications such as Gnucash™, PLCash™, Budget™ (from Snowmint Creative Solutions, LLC, of St. Paul, Minn.), and/or other planning software capable of processing financial information.

[0060] Moreover, financial application **434** may be associated with and/or include software such as: QuickBooks™ (from Intnit, Inc., of Mountain View, Calif.), Peachtree™ (from The Sage Group PLC, of Newcastle Upon Tyne, the United Kingdom), Peachtree Complete™ (from The Sage Group PLC, of Newcastle Upon Tyne, the United Kingdom), MYOB Business Essentials™ (from MYOB US, Inc., of Rockaway, N.J.), NetSuite Small Business Accounting™ (from NetSuite, Inc., of San Mateo, Calif.), Cougar Mountain™ (from Cougar Mountain Software, of Boise, Id.), Microsoft Office Accounting™ (from Microsoft Corporation, of Redmond, Wash.), Simply Accounting™ (from The Sage Group PLC, of Newcastle Upon Tyne, the United Kingdom), CYMA IV Accounting™ (from CYMA Systems, Inc., of Tempe, Ariz.), DacEasy™ (from Sage Software SB, Inc., of Lawrenceville, Ga.), Microsoft Money™ (from Microsoft Corporation, of Redmond, Wash.), Tally.ERP (from Tally Solutions, Ltd., of Bangalore, India) and/or other payroll or accounting software capable of processing payroll information.

[0061] System **300** (FIG. **3**), point-of-sale terminal **400** (FIG. **4**) and/or data structure **500** may include fewer components or additional components. Moreover, two or more components may be combined into a single component, and/or a position of one or more components may be changed. In some embodiments, the functionality of system **300** (FIG. **3**) and/or point-of-sale terminal **400** may be implemented more in hardware and less in software, or less in hardware and more in software, as is known in the art.

[0062] The foregoing description is intended to enable any person skilled in the art to make and use the disclosure, and is provided in the context of a parti-cular application and its requirements. Moreover, the foregoing descriptions of embodiments of the present disclosure have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the present disclosure to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present disclosure. Additionally, the discussion of the preceding embodiments is not intended to limit the present disclosure. Thus, the present disclosure is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

1. A point-of-sale-terminal-implemented method for conducting a financial transaction, the method comprising:

initiating, at a point-of-sale terminal, a secnre session with a portable electronic device of a customer;

receiving, at the point-of-sale terminal, a token from the portable electronic device, wherein the token identifies the cnstomer and the token is received using a unified point-of-sale service object executing on the point-of-sale terminal, and wherein the unified point-of-sale service object acts as a virtual peripheral device driver for a virtual peripheral device;

using the unified point-of-sale service object executing on the point-of-sale terminal, performing one or more operations based on at least the token to obtain financial information associated with the customer;

providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information; and

receiving a confirmation from the financial institution that the financial transaction has been completed.

2. The method of claim **1**, wherein the one or more operations include:

providing the token to a third party, wherein the third party is other than the financial institution; and

receiving the financial information from the third party.

3. The method of claim **2**, wherein the token is provided to the third party via a portable electronic device of the customer.

4. The method of claim **2**, wherein the token is provided to the third party via a network coupled to the point-of-sale terminal.

5. (canceled)

6. The method of claim **1**, wherein the information is conveyed using one of: wireless communication, near-field communication, an audio channel, and a video channel.

7. The method of claim **1**, wherein, prior to receiving the token, the method further comprises providing a transaction request associated with the financial transaction from point-of-sale-terminal software executing on the point-of-sale terminal to the unified point-of-sale service object.

8. The method of claim **1**, wherein providing the financial information and the transaction information associated with the financial transaction, and receiving the confirmation occur via a credit-authorization-terminal service object which is a driver for the credit-authorization terminal; and

wherein the credit-authorization-terminal service object is compatible with a unified point-of-sale standard.

9. A computer-program product for use in conjunction with a point-of-sale terminal, the computer-program product comprising a non-transitory computer-readable storage medium and a computer-program mechanism embedded therein, to conduct a financial transaction, the computer-program mechanism including:

instructions for initiating, at a point-of-sale terminal, a secure session with a portable electronic device of a customer;

instructions for receiving, at the point-of-sale terminal, a token from the portable electronic device, wherein the token identifies the customer and the token is received using a unified point-of-sale service object executing on the point-of-sale terminal, and wherein the unified point-of-sale service object acts as a virtual peripheral device driver for a virtual peripheral device;

instructions for using the unified point-of-sale service object executing on the point-of-sale terminal to perform one or more operations based on at least the token to obtain financial information associated with the customer;

instructions for providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information; and

instructions for receiving a confirmation from the financial institution that the financial transaction has been completed.

10. The computer-program product of claim **9**, wherein the one or more operations include:

providing the token to a third party, wherein the third party is other than the financial institution; and

receiving the financial information from the third party.

11. The computer-program product of claim **10**, wherein the token is provided to the third party via a portable electronic device of the customer.

12. The computer-program product of claim **10**, wherein the token is provided to the third party via a network coupled to the point-of-sale terminal.

13. (canceled)

14. The computer-program product of claim **9**, wherein the information is conveyed using one of: wireless communication, near-field communication, an audio channel, and a video channel.

15. The computer-program product of claim **9**, wherein, prior to the instructions for receiving the token, the computer-program mechanism further includes instructions for providing a transaction request associated with the financial transaction from point-of-sale-terminal software executing on the point-of-sale terminal to the unified point-of-sale service object.

16. The computer-program product of claim **9**, wherein providing the financial information and the transaction information associated with the financial transaction, and receiving the confirmation occur via a credit-authorization-terminal service object which is a driver for the credit-authorization terminal; and

wherein the credit-authorization-terminal service object is compatible with a unified point-of-sale standard.

17. A point-of-sale terminal, comprising:

a processor;

memory; and

a program module, wherein the program module is stored in the memory and configurable to be executed by the processor to conduct a financial transaction, the program module including:

instructions for initiating, at a point-of-sale terminal, a secure session with a portable electronic device of a customer;

instructions for receiving at the point-of-sale terminal, a token from the portable electronic device, wherein the token identifies the customer and the token is received using a unified point-of-sale service object executing on the point-of-sale terminal, and wherein the unified point-of-sale service object acts as a virtual peripheral device driver for a virtual peripheral device;

instructions for using the unified point-of-sale service object executing on the point-of-sale terminal to perform one or more operations based on at least the token to obtain financial information associated with the customer;

instructions for providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information; and

instructions for receiving a confirmation from the financial institution that the financial transaction has been completed.

18. The point-of-sale terminal of claim **17**, wherein the one or more operations include:

providing the token to a third party, wherein the third party is other than the financial institution; and

receiving the financial information from the third party.

19. The point-of-sale terminal of claim **18**, wherein the token is provided to the third party via a portable electronic device of the customer.

20. The point-of-sale terminal of claim **18**, wherein the token is provided to the third party via a network coupled to the point-of-sale terminal.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Ran

(10) **Pub. No.: US 2013/0346222 A1**

(43) **Pub. Date: Dec. 26, 2013**

(54) **MOBILE PAYMENT SYSTEM**

(75) Inventor: **Alexander S. Ran**, Palo Alto, CA (US)

(73) Assignee: **INTUIT INC.**, Mountain View, CA (US)

(21) Appl. No.: **13/528,109**

(22) Filed: **Jun. 20, 2012**

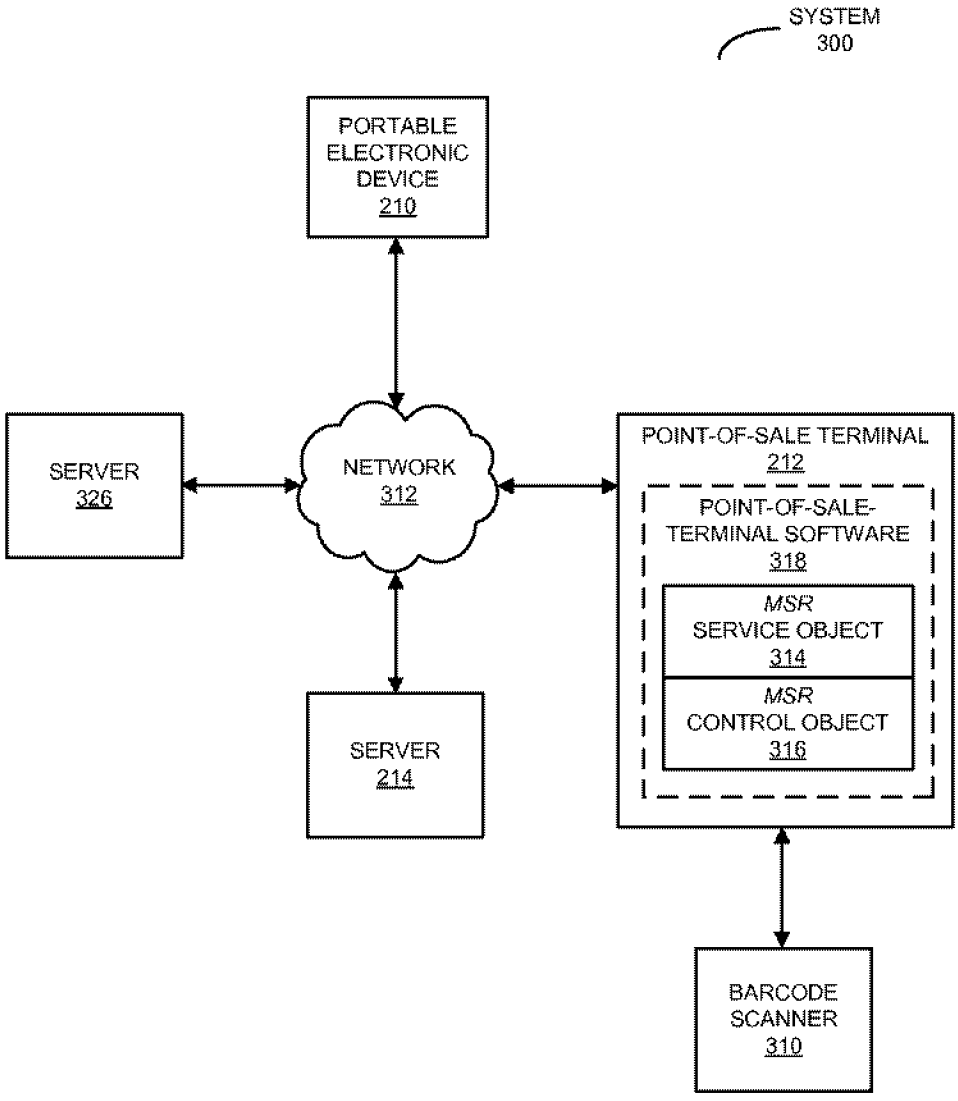
Publication Classification

(51) **Int. Cl.**
G06Q 20/20 (2012.01)

(52) **U.S. Cl.**
USPC **705/17**; 705/16

(57) **ABSTRACT**

During a financial transaction, a customer provides an identifier to a peripheral device (which may be a barcode scanner, a wireless receiver or a keyboard) coupled to the point-of-sale terminal. This identifier corresponds to a one-time payment credential token that includes financial information of the customer. Then, a service object executing on the point-of-sale terminal, which acts as a driver for the peripheral device, performs one or more operations based on at least the identifier to obtain the financial information. After providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information, the point-of-sale terminal receives a confirmation from the financial institution that the financial transaction has been completed.



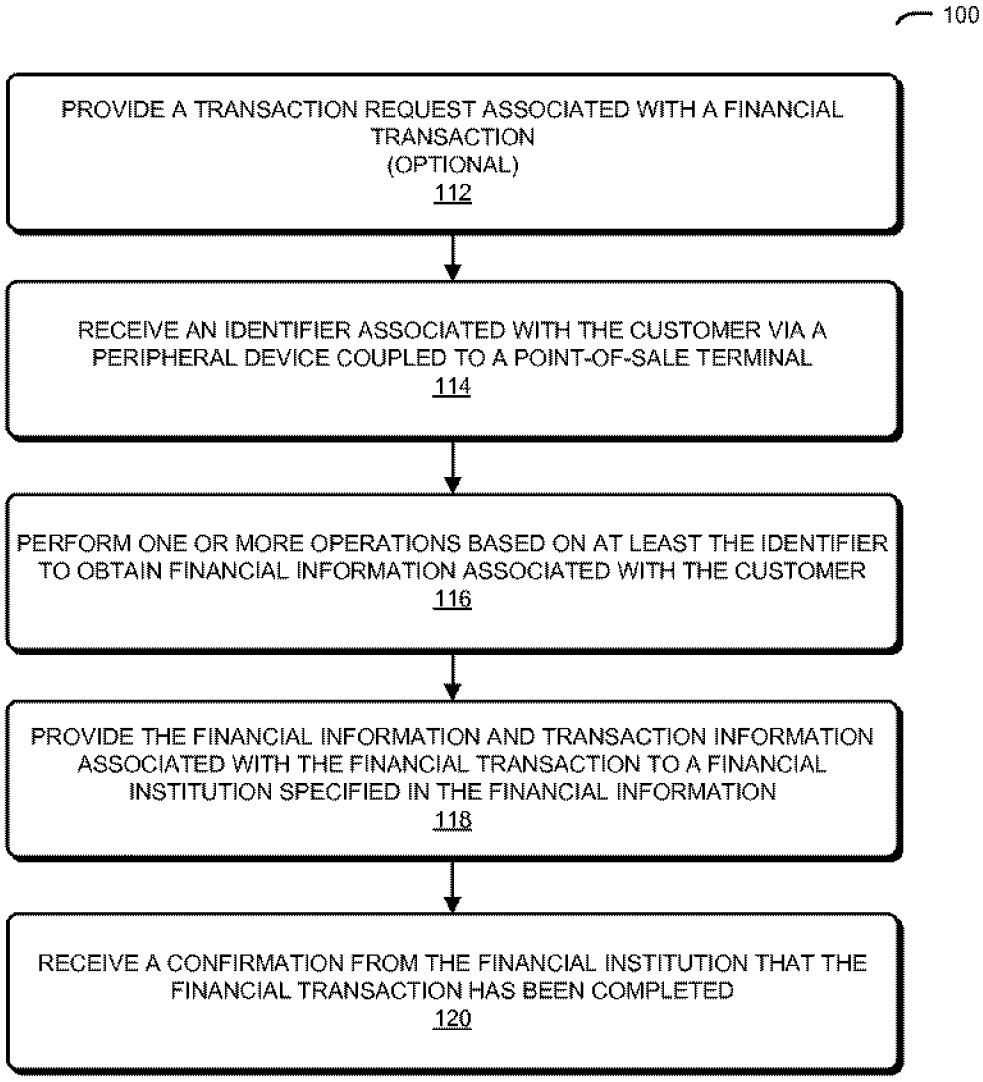

100
PROVIDE A TRANSACTION REQUEST ASSOCIATED WITH A FINANCIAL TRANSACTION
(OPTIONAL)
112
RECEIVE AN IDENTIFIER ASSOCIATED WITH THE CUSTOMER VIA A PERIPHERAL DEVICE COUPLED TO A POINT-OF-SALE TERMINAL
114
PERFORM ONE OR MORE OPERATIONS BASED ON AT LEAST THE IDENTIFIER TO OBTAIN FINANCIAL INFORMATION ASSOCIATED WITH THE CUSTOMER
116
PROVIDE THE FINANCIAL INFORMATION AND TRANSACTION INFORMATION ASSOCIATED WITH THE FINANCIAL TRANSACTION TO A FINANCIAL INSTITUTION SPECIFIED IN THE FINANCIAL INFORMATION
118
RECEIVE A CONFIRMATION FROM THE FINANCIAL INSTITUTION THAT THE FINANCIAL TRANSACTION HAS BEEN COMPLETED
120

FIG. 1

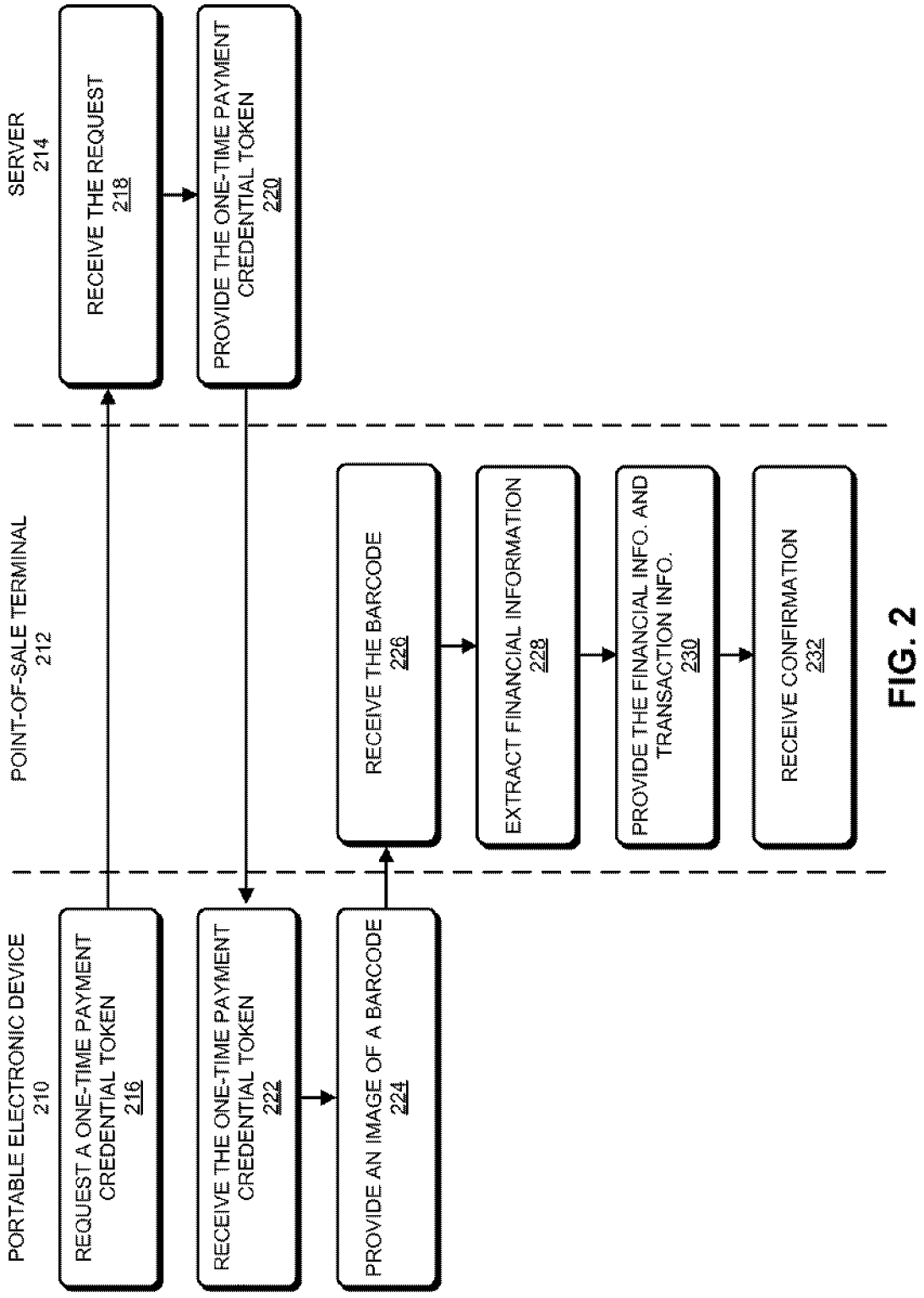

PORTABLE ELECTRONIC DEVICE
210
REQUEST A ONE-TIME PAYMENT CREDENTIAL TOKEN
216
RECEIVE THE ONE-TIME PAYMENT CREDENTIAL TOKEN
222
PROVIDE AN IMAGE OF A BARCODE
224
POINT-OF-SALE TERMINAL
212
RECEIVE THE BARCODE
226
EXTRACT FINANCIAL INFORMATION
228
PROVIDE THE FINANCIAL INFO. AND TRANSACTION INFO.
230
RECEIVE CONFIRMATION
232
SERVER
214
RECEIVE THE REQUEST
218
PROVIDE THE ONE-TIME PAYMENT CREDENTIAL TOKEN
220

FIG. 2

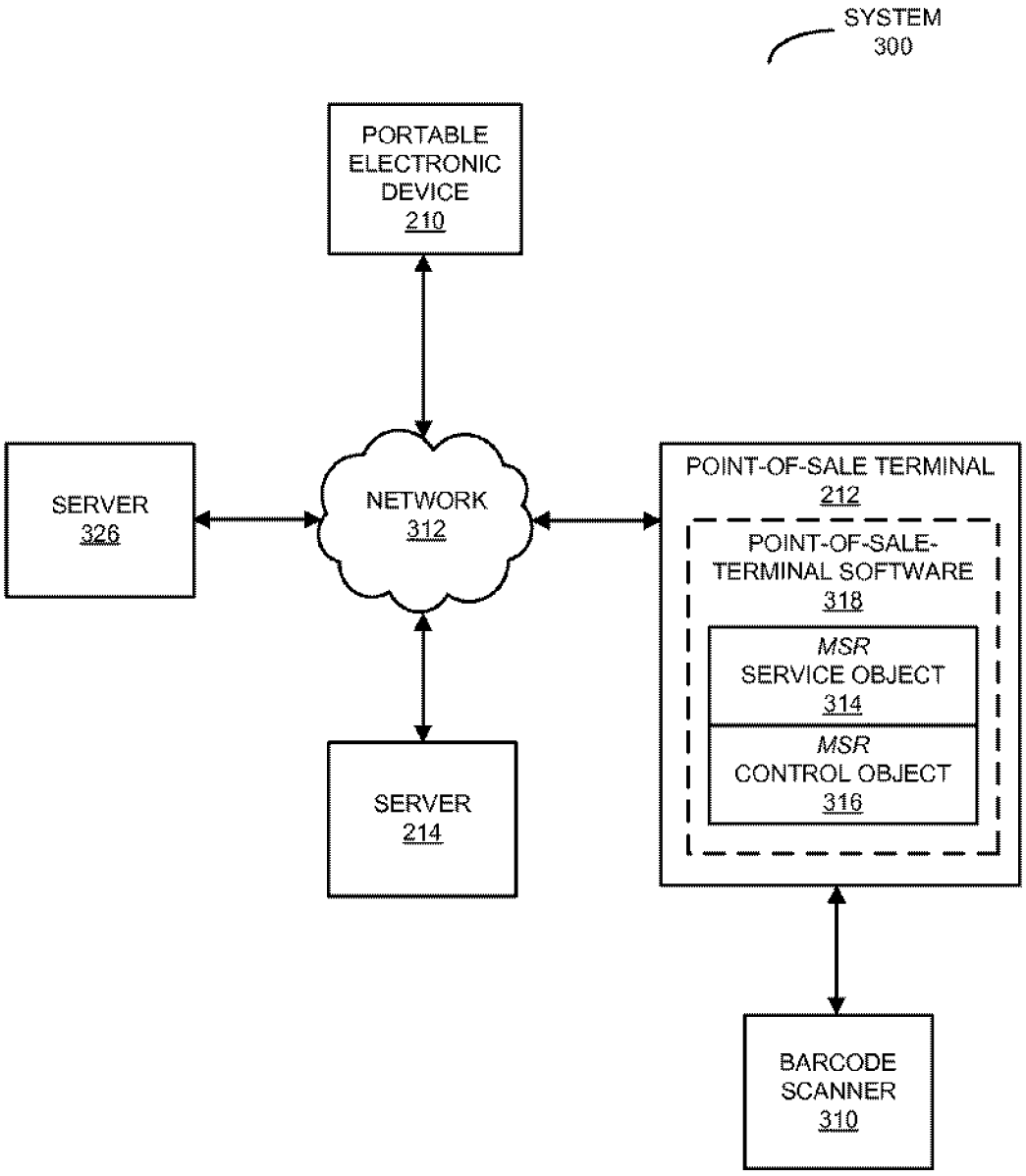

SYSTEM
300
PORTABLE ELECTRONIC DEVICE
210
SERVER
326
NETWORK
312
SERVER
214
POINT-OF-SALE TERMINAL
212
POINT-OF-SALE-TERMINAL SOFTWARE
318
MSR SERVICE OBJECT
314
MSR CONTROL OBJECT
316
BARCODE SCANNER
310

FIG. 3

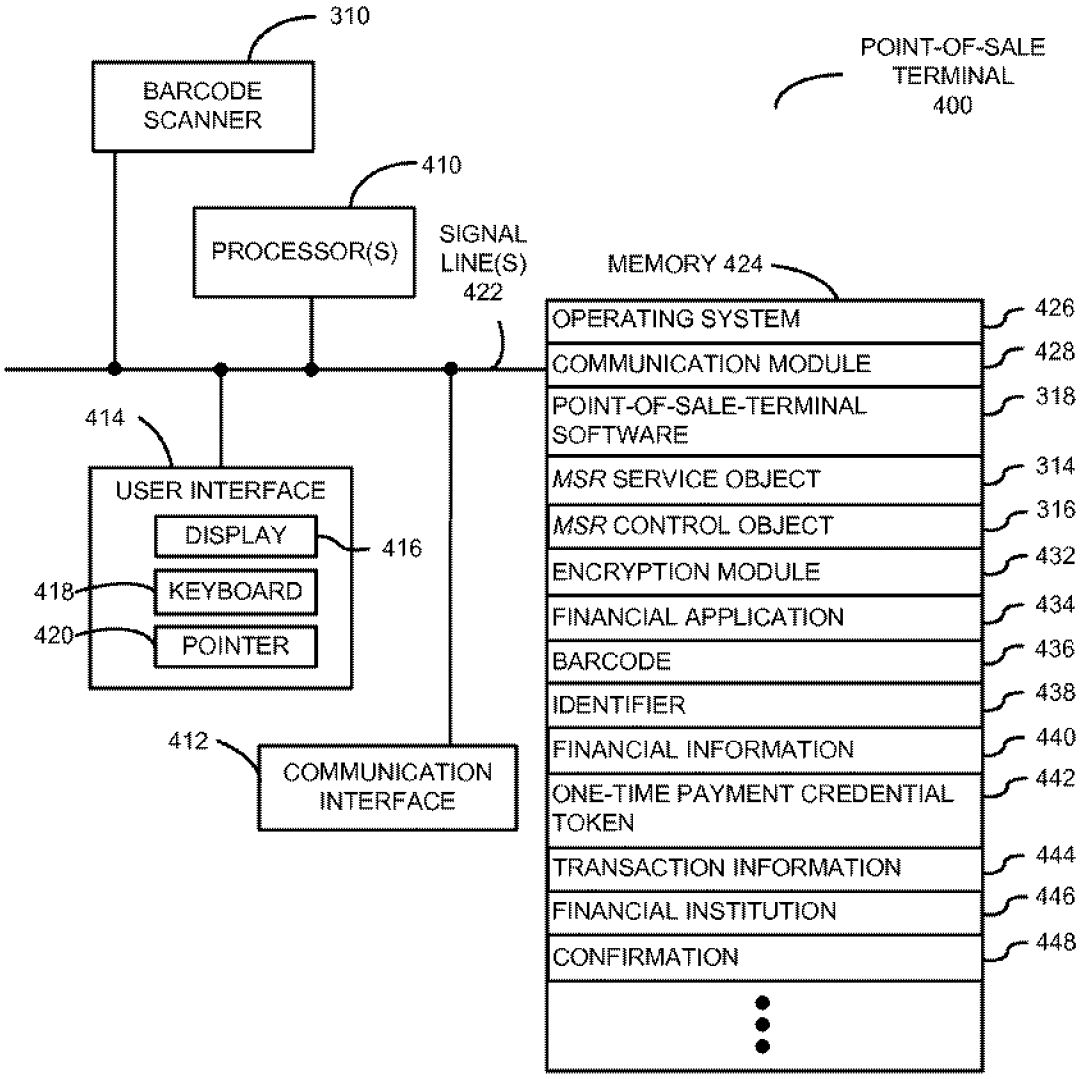

310
BARCODE SCANNER
POINT-OF-SALE TERMINAL 400
410
PROCESSOR(S)
SIGNAL LINE(S) 422
MEMORY 424
OPERATING SYSTEM
426
COMMUNICATION MODULE
428
POINT-OF-SALE-TERMINAL SOFTWARE
318
414
USER INTERFACE
DISPLAY
416
MSR SERVICE OBJECT
314
MSR CONTROL OBJECT
316
ENCRYPTION MODULE
432
418
KEYBOARD
FINANCIAL APPLICATION
434
420
POINTER
BARCODE
436
IDENTIFIER
438
412
COMMUNICATION INTERFACE
FINANCIAL INFORMATION
440
ONE-TIME PAYMENT CREDENTIAL TOKEN
442
TRANSACTION INFORMATION
444
FINANCIAL INSTITUTION
446
CONFIRMATION
448

FIG. 4

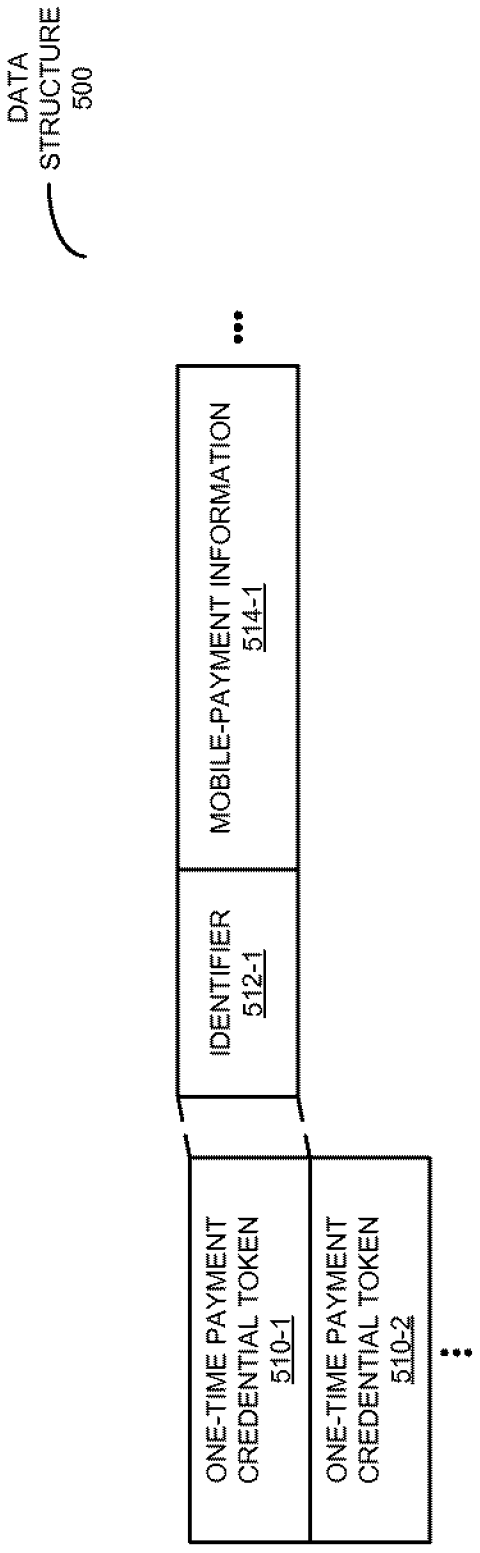

DATA STRUCTURE 500
ONE-TIME PAYMENT CREDENTIAL TOKEN 510-1
ONE-TIME PAYMENT CREDENTIAL TOKEN 510-2
IDENTIFIER 512-1
MOBILE-PAYMENT INFORMATION 514-1

FIG. 5

MOBILE PAYMENT SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application is related to U.S. patent application Ser. No. 13/489,600, Attorney Docket No. INTU-126471, entitled "Mobile Payment Via a Virtual Peripheral Device," by Alexander S. Ran, which was filed on Jun. 6, 2012, the contents of which are herein incorporated by reference in its entirety.

FIELD

[0002] The present disclosure relates to a technique for conducting a financial transaction at a point-of-sale terminal.

SUMMARY

[0003] The disclosed embodiments relate to a point-of-sale terminal that conducts a financial transaction. During operation, the point-of-sale terminal receives an identifier associated with a customer via a peripheral device coupled to the point-of-sale terminal and a service object executing on the point-of-sale terminal. For example, the identifier may be received by from a portable electronic device. This identifier corresponds to a one-time payment credential token that includes financial information of the customer, and the service object acts as a driver for the peripheral device. Then, the point-of-sale terminal performs one or more operations based on at least the identifier to obtain the financial information. Moreover, the point-of-sale terminal provides the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information. Next, the point-of-sale terminal receives a confirmation (for example, from the financial institution) that the financial transaction has been completed.

[0004] Note that the one or more operations may include: providing the identifier to a third party, where the third party is other than the financial institution; receiving the one-time payment credential token from the third party; and extracting the financial information from the one-time payment credential token. Alternatively, the one or more operations may include: generating the one-time payment credential token from the identifier; and/or extracting the financial information from the one-time payment credential token.

[0005] In some embodiments, the service object includes a magnetic-stripe-reader service object.

[0006] Furthermore, the identifier may be included in the one-time payment credential token, and the peripheral device may include a barcode scanner that captures an image of a barcode that includes the one-time payment credential token, which may be provided by the portable electronic device.

[0007] Note that the service object executing on the point-of-sale terminal may present the barcode scanner to the point-of-sale terminal as a keyboard. For example, the service object executing on the point-of-sale terminal may accept the token from the keyboard because the input from a barcode scanner is often seen by the point-of-sale terminal as a keyboard input.

[0008] In some embodiments, the peripheral device includes: a barcode scanner, a wireless receiver and/or a keyboard.

[0009] Additionally, the one-time payment credential token may only be valid for the financial transaction.

[0010] Another embodiment provides a method that includes at least some of the operations performed by the point-of-sale terminal.

[0011] Another embodiment provides a computer-program product for use with the point-of-sale terminal. This computer-program product includes instructions for at least some of the operations performed by the point-of-sale terminal.

BRIEF DESCRIPTION OF THE FIGURES

[0012] FIG. **1** is a flow chart illustrating a method for conducting a financial transaction in accordance with an embodiment of the present disclosure.

[0013] FIG. **2** is a drawing illustrating the method of FIG. **1** in accordance with an embodiment of the present disclosure.

[0014] FIG. **3** is a block diagram illustrating a system that performs the method of FIGS. **1** and **2** in accordance with an embodiment of the present disclosure.

[0015] FIG. **4** is a block diagram illustrating a point-of-sale terminal that performs the method of FIGS. **1** and **2** in accordance with an embodiment of the present disclosure.

[0016] FIG. **5** is a block diagram illustrating a data structure for use in the point-of-sale terminal of FIG. **4** in accordance with an embodiment of the present disclosure.

[0017] Note that like reference numerals refer to corresponding parts throughout the drawings. Moreover, multiple instances of the same part are designated by a common prefix separated from an instance number by a dash.

DETAILED DESCRIPTION

[0018] Embodiments of a point-of-sale terminal, a technique for conducting a financial transaction, and a computer-program product (e.g., software) for use with the point-of-sale terminal are described. During the financial transaction, point-of-sale-terminal software executes a software module that obtains customer financial information for payment authorization by a payment processing service. In particular, a customer may use a portable electronic device (such as a cellular telephone) to provide an identifier to a peripheral device (which may be a barcode scanner, a wireless receiver or a keyboard) conpled to the point-of-sale terminal. This identifier corresponds to a one-time payment credential token that includes financial information of the customer. Then, a service object executing on the point-of-sale terminal, which acts as a driver for a peripheral device coupled to the point-of-sale terminal, performs one or more operations based on at least the identifier to obtain the financial information. After providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information, the point-of-sale terminal receives a confirmation from the financial institution that the financial transaction has been completed.

[0019] By allowing the customer to conduct the financial transaction without requiring changes to the point-of-sale terminal, the merchant-acquirer payment-processor service, or existing portable electronic devices, this financial technique may facilitate commercial activity. In particnlar, the financial technique may facilitate low-cost and simple mobile payments via a cellular telephone. In this way, the financial teehnique provides a software solution that can be broadly adopted with little or no expense or inconvenience for merchants or customers.

[0020] In the discussion that follows, a user or a customer may include: an individual (for example, an existing cus-

tomer, a new customer, a service provider, a vendor, a contractor, etc.), an organization, a business and/or a government agency. Furthermore, a 'business' should be understood to include: for-profit corporations, non-profit corporations, organizations, groups of individuals, sole proprietorships, government agencies, partnerships, etc.

[0021] We now describe embodiments of the financial technique, which may be performed by a point-of-sale terminal (such as point-of-sale terminal **400** in FIG. **4**). FIG. **1** presents a flow chart illustrating a method **100** for conducting a financial transaction. During operation, the point-of-sale terminal (such as a cash register) receives an identifier associated with a customer via a peripheral device coupled to the point-of-sale terminal (operation **114**). This identifier corresponds to a one-time payment credential token (e.g., the one-time payment credential token may only be valid for the financial transaction) that includes financial information of the customer.

[0022] Then, the point-of-sale terminal performs one or more operations based on at least the identifier to obtain the financial information (operation **116**). As described further below with reference to FIG. **2**, the identifier may be included in the one-time payment credential token (which is sometimes referred to as a 'transient payment credential token'), and the peripheral device includes a barcode scanner that captures an image of a barcode that includes the one-time payment credential token, which is provided by the portable electronic device. This barcode may be generated on the portable electronic device or it may be received by the portable electronic device from a third party, where the third party may or may not be other than a financial institution specified in the financial information (such as a provider of the financial technique).

[0023] Alternatively, the one or more operations may include: providing the identifier to the third party; receiving the one-time payment credential token from the third party; and extracting the financial information from the one-time payment credential token. For example, the identifier may be provided to the third party: via the portable electronic device of the customer (i.e., indirectly) and/or via a network coupled to the point-of-sale terminal (i.e., directly). Alternatively, the one or more operations may include: generating the one-time payment credential token from the identifier; and/or extracting the financial information from the one-time payment credential token (if the one-time payment credential token is received from the portable electronic device).

[0024] In some embodiments, at least one of the operations is performed by a unified point-of-sale service object executing on the point-of-sale terminal. This unified point-of-sale service object may be or may acts as a driver for the peripheral device.

[0025] Thus, in different embodiments the one-time payment credential token may be: dynamically generated and provided by the portable electronic device, received by the portable electronic device from the third party and then provided to the point-of-sale terminal, dynamically generated on the point-of-sale terminal, and/or received by the point-of-sale terminal from the third party.

[0026] Because barcode scanners at the point-of-sale terminal are used to read Universal product codes, and a Universal Product Code typically only includes 11 digits, the unified point-of-sale service object executing on the point-of-sale terminal may overcome this limitation by extending the information obtained from the barcode scanner to constitute a well-formed payment credential expected by, for example, a magnetic-stripe-reader control object. Alternatively or additionally, the unified point-of-sale service object executing on the point-of-sale terminal may accept the token from the keyboard because the input from a barcode scanner is often seen by the point-of-sale terminal as a keyboard input.

[0027] Moreover, the point-of-sale terminal provides the financial information and transaction information (operation **118**) associated with the financial transaction to the financial institution specified in the financial information. For example, the financial institution may include a merchant-acquirer processor in a payment card network (such as a credit- or a debit-card network). In some embodiments, the one-time payment credential token is also provided to the financial institution.

[0028] Next, the point-of-sale terminal receives a confirmation (operation **120**) from the financial institution that the financial transaction has been completed. For example, providing the financial information and the transaction information (operation **118**) associated with the financial transaction, and receiving the confirmation (operation **120**) may occur via a magnetic-stripe-reader service object. This magnetic-stripe-reader service object, as well as the other-mentioned unified point-of-sale service object, may be compatible with a unified point-of-sale standard, such as the UnifiedPOS or UPOS standard (from the National Retail Federation of Washington, D.C.).

[0029] In some embodiments, prior to receiving the identifier (operation **114**) the point-of-sale terminal optionally provides a transaction request associated with the financial transaction (operation **112**) from point-of-sale-terminal software executing on the point-of-sale terminal to the unified point-of-sale service object. In response to this transaction request, the unified point-of-sale service object may await the identifier from the peripheral device.

[0030] In an exemplary embodiment, the financial technique is implemented using the portable electronic device, the point-of-sale terminal and at least one server, which communicate through a network, such as a cellular-telephone network and/or the Internet (e.g., using a client-server architecture). This is illustrated in FIG. **2**, which presents a flow chart illustrating method **100** (FIG. **1**). During this method, a user of portable electronic device **210** provides the identifier that identifies the user. For example, the user may be a customer, and portable electronic device **210** may be a cellular telephone. As shown in FIG. **2**, portable electronic device **210** requests a one-time payment credential token (operation **216**) from server **214**, which may be associated with a third party that is other than the financial institution that will process the financial transaction and/or will make payment for the customer in the financial transaction, such as a provider of the financial technique.

[0031] In response to receiving the request (operation **218**), server **214** provides the one-time payment credential token (operation **220**). For example, when providing the one-time payment credential token, server **214** may access the pre-existing one-time payment credential token or may generate the one-time payment credential token.

[0032] Moreover, after receiving the one-time payment credential token (operation **222**), portable electronic device **210** provides the one-time payment credential token (which includes or is the identifier) to point-of-sale terminal **212** in the form of an image of a barcode (operation **224**), and more generally an image of a spatial pattern. Furthermore, the

peripheral device (such as a barcode scanner) coupled to point-of-sale terminal **212** receives the barcode (operation **226**).

[0033] Then, the unified point-of-sale service object executing on point-of-sale terminal **212** performs the one or more operations based on at least the identifier to obtain financial information associated with the customer. (As described further below with reference to FIG. **3**, the unified point-of-sale service object may be or may act as the driver for the peripheral device.) For example, as shown in FIG. **2** the unified point-of-sale service object may extract the financial information (operation **228**) from the one-time payment credential token. The financial information may include mobile-payment information for the customer, such as: an account identifier, an available amount that can be spent, a financial institution (such as a bank), a bank identification number (which defines transaction routing information), etc. Note that the financial information may be similar to that provided by a financial vehicle (such as a credit card), but has a different context because a physical credit card is not used in the described financial transaction.

[0034] Furthermore, point-of-sale terminal **212** may provide the financial information and the transaction information (operation **230**) associated with the financial transaction to the financial institution specified in the financial information. For example, the transaction information may include: a transaction day/time, a merchant identifier, a product code and a transaction amount.

[0035] Note that the financial information and the transaction information may be received by a server associated with the financial institution (not shown), which then completes the financial transaction (for example, by authorizing or making payment on behalf of the consumer to the merchant associated with point-of-sale terminal **212**). After the financial transaction is complete (not shown), this server may provide the confirmation that the financial transaction has been completed (not shown). Alternatively, the financial information and the transaction information may be received by server **214**, which then completes the financial transaction (not shown) and provides the confirmation (not shown).

[0036] Additionally, point-of-sale terminal **212** receives the confirmation (operation **232**). For example, the confirmation may be received via a magnetic-stripe-reader service object from a merchant acquirer payment processing service.

[0037] In some embodiments of method **100** (FIGS. **1** and **2**), there may be additional or fewer operations. For example, instead of providing an image of a barcode (operation **224**), portable electronic device **210** may convey the identifier and/or the one-time payment credential token using: wireless communication, near-field communication, an audio channel, and/or a video channel. Alternatively, the user may enter the identifier and/or the one-time payment credential token into a keypad. Therefore, instead of the barcode scanner, the peripheral device may include a wireless receiver or the keypad.

[0038] Moreover, instead of receiving the one-time payment credential token from portable electronic device **210**, in some embodiments the one-time payment credential token may be generated by portable electronic device **210** based on the identifier received from portable electronic device **210**, or a pre-existing one-time payment credential token that is stored on the point-of-sale terminal **212** may be accessed or looked-up based on the identifier received from portable electronic device **210**.

[0039] Alternatively, instead of receiving the one-time payment credential token from portable electronic device **210**, in some embodiments point-of-sale terminal **212** provides the identifier to server **214** via a network or via portable electronic device **210**. In response, server **214** may provide the one-time payment credential token to point-of-sale terminal **212**.

[0040] In method **100** (FIGS. **1** and **2**), note that the order of the operations may be changed, and/or two or more operations may be combined into a single operation.

[0041] In an exemplary embodiment, the financial technique leverages the UPOS standard to integrate mobile payments with point-of-sale-terminal software. Most commercially available point-of-sale-terminal software (such as point-of-sale operating systems) supports the UPOS standard, which covers integration of peripheral devices, such as: a credit-authorization terminal, a magnetic-stripe reader, etc. The UPOS architecture is based on the concept of control objects and service objects. During operation of a point-of-sale terminal, the point-of-sale-terminal software interacts with one or more control objects for tasks such as credit-payment authorization. A control object connects to the appropriate service object that serves the role of a driver for an external or peripheral device that performs the task(s) and returns the result. For example, in the case of the credit-payment authorization, a credit-authorization-terminal service object is or acts as the driver for a credit-authorization terminal.

[0042] In the financial technique, mobile payments are integrated with the point-of-sale-terminal software by using a service object to drive the peripheral device. Thus, while driving an actual peripheral device, the service object implements the logic necessary to complete a task (in this case, the financial transaction). This logic may include interacting directly with the user's portable electronic device and/or with a server associated with the third party that facilitates or provides the financial technique (including optionally receiving the one-time payment credential token from the third party after the point-of-sale terminal optionally provided the identifier to the third party). In this way, the standard point-of-sale peripheral integration interface may be used to enable a software-only solution that facilitates mobile payments that work with a majority of existing point-of-sale-terminal software and hardware.

[0043] In an exemplary embodiment, a customer wants to purchase a product or a service from a merchant. A cashier at a point-of-sale terminal may ring up the purchased item(s). The cashier may also optionally invoke a barcode-scanner operation, such as that normally used for a store loyalty card. In response, the point-of-sale-terminal software may submit a transaction request to a barcode-scanner driver (i.e., the unified point-of-sale service object) that is provided by a provider of the financial technique. In response to this transaction request, the barcode-scanner driver may await the identifier and/or the one-time payment credential token from the peripheral device (such as a barcode scanner or a keyboard).

[0044] Next, a mobile-payment application executing on the portable electronic device (which may also be provided by the provider of the financial technique) provides the identifier and/or the one-time payment credential token (which may have been provided to the portable electronic device by the third party in response to a previous request by the mobile-payment application) to the barcode scanner and, thus, the barcode-scanner service object on the point-of-sale terminal.

For example, the portable electronic device may display the barcode that includes the one-time payment credential token (and, thus, the identifier, which may be the same as the one-time payment credential token).

[0045] After receiving the one-time payment credential token, the barcode-scanner service object may return the one-time payment credential token (and, thus, the financial information associated with the user) to the point-of-sale-terminal software. Then, the point-of-sale terminal may extract the financial information (such as the mobile-payment information for the customer) from the one-time payment credential token.

[0046] In some embodiments, the cashier then optionally performs additional operations for awarding loyalty points, redeeming coupons and offers, etc.

[0047] Furthermore, after receiving the financial information, the cashier may perform a credit-authorization operation for the amount due using a merchant acquirer payment processing service. As described below with reference to FIG. **3**, the merchant-acquirer processor may interact with server **214** to confirm that the one-time payment credential token is valid prior to authorizing payment and providing the confirmation to point-of-sale terminal **212**.

[0048] In some embodiments, the point-of-sale-terminal software optionally prints a receipt using a UPOS printer service object that passes receipt information to the mobile-payment application and/or to server **214** (FIG. **2**).

[0049] By using the peripheral device and a substitute unified point-of-sale service object, the financial technique may facilitate mobile payments using standard open-loop payment-card-network transactions at point-of-sale terminals with portable electronic devices (such as cellular telephones) as payment instruments that (directly or indirectly) convey the necessary financial information.

[0050] Note that there are several challenges associated with using an image of a barcode to provide the identifier and/or the one-time payment credential token to the point-of-sale terminal. Notably, if a portable electronic device displayed a barcode that includes payment-card-account information (such as a credit-card number), there would be a significant risk of fraud (a copy of the image could be used to conduct financial transactions). In addition, standard point-of-sale-terminal software typically does not use barcode scanners to obtain payment card credentials. Instead, point-of-sale-terminal software usually uses credit-authorization terminals or magnetic-stripe readers to obtain such financial information.

[0051] The first challenge can be addressed by generating transient payment credentials (such as the one-time payment credential token) for each financial transaction. However, the issuer of the mobile payment instrument (such as the financial institution) typically needs to be able to authorize financial transactions against a real user account. Therefore, during a given financial transaction, the issuer may need the ability to map the one-time payment credential token received in the payment processing flow to an actual user account. To do so, the issuer or the third party may generate the one-time payment credential token in response to a request from the mobile-payment application executing on the portable electronic device prior to the financial transaction while storing the association to the user's account until the financial-transaction processing is complete. Alternatively, the mobile-payment application can generate the one-time payment credential token and push it to the issuer or the third party prior to the financial transaction. Furthermore, if a trusted execution environment is available on the portable electronic device (either in the form of a secure element or a trusted execution mode of the main processor), a one-time payment-credential-token technique known to the issuer or the third party can be executed on the portable electronic device without the need to connect to the issuer or the third party prior to the financial transaction.

[0052] As described previously, a general approach to address the second challenge may use the UPOS standard for integrating point-of-sale-terminal software with third-party peripheral devices. In this approach, the third party can publish a UPOS driver or service object for credit-authorization terminals or magnetic-stripe readers. This UPOS driver can be loaded on UPOS compliant point-of-sale terminals (which include the majority of existing point-of-sale terminals). When invoked by the point-of-sale-terminal software in a payment-credential-reading flow, the UPOS driver may use the barcode scanner to acquire the barcode from the display of the portable electronic device, and may convert it into well-formed payment credentials. This financial information may be passed to the point-of-sale-terminal software to be processed in the same way as any other payment-card financial transaction.

[0053] Note that a variety of conversion techniques may be used to convert the barcode to the financial information. In general, this conversion does not need to be secure or complicated. In addition, this approach can also deal with the possible limitations associated with barcode scanners or the resolution of displays on portable electronic devices which may restrict the length and symbols represented by the barcode. For example, the standard Universal Product Code includes 11 digits. This may not be sufficient to represent payment-card track data. However, because the UPOS driver can process this Universal Product Code prior to delivering it to the point-of-sale-terminal software, it can be appropriately transformed (thus, the UPOS driver may map the barcode, which includes the identifier, to a one-time payment credential token and, thus, the financial information). For example, the financial information conveyed in a one-time payment credential token may include: a 6-digit bank identification number stored in the configuration of the UPOS driver that guarantees proper routing of the financial transaction by the payment-card network to the financial institution; a virtual (transient) account number defined by 10 digits in the barcode data; an expiration date generated based on the financial-transaction date and other input if desirable; and a card verification value (CVV) or card verification code (CVC) generated based on one or more of these or other inputs, such as the last digit from the barcode (alternatively the last digit can be used to correct barcode-scanning errors).

[0054] We now describe embodiments of the system and the point-of-sale terminal, and their use. FIG. **3** presents a block diagram illustrating a system **300** that performs method **100** (FIGS. **1** and **2**). In this system, a user of portable electronic device **210** may use a software product (for example, the mobile-payment application), such as a software application that is resident on and that executes on portable electronic device **210**. (Alternatively, the user may interact with a web page that is provided by server **214** via network **312**, and which is rendered by a web browser on portable electronic device **210**. For example, at least a portion of the software application may be an application tool that is embedded in the web page, and which executes in a virtual environment of the

web browser. Thus, the application tool may be provided to the user via a client-server architecture.) This software application may be a standalone application or a portion of another application that is resident on and which executes on portable electronic device **210** (such as a software application that is provided by server **214** or that is installed and which executes on portable electronic device **210**).

[0055] As discussed previously, during a financial transaction (such as purchasing a product from a merchant) the user (who is the customer in the preceding discussion) may use the software application to request and receive a one-time payment credential token from server **214** via network **312**.

[0056] Then, the software application displays the one-time payment credential token (or an identifier corresponding to the one-time payment credential token) in a barcode on a display on portable electronic device **210**. This barcode is scanned by barcode scanner **310** and processed by a UPOS driver or service object, such as a magnetic-stripe-reader (MSR) service object **314**, to extract the financial information. Note that magnetic-stripe-reader service object **314** may present barcode scanner **310** to point-of-sale terminal **212** as a keyboard to overcome limitations associated with Universal Product Codes, such as the number of digits. Alternatively or additionally, magnetic-stripe-reader service object **314** may accept the token from the keyboard because the input from a barcode scanner is often seen by the point-of-sale terminal as a keyboard input.

[0057] Moreover, magnetic-stripe-reader service object **314** provides the financial information to the UPOS control object, such as magnetic-stripe-reader control object **316** (and, thus, point-of-sale-terminal software **318**) via a UPOS standard peripheral interface.

[0058] Next, magnetic-stripe-reader control object **316** passes the financial information to point-of-sale-terminal software that communicates the financial information and the transaction information to server **326** associated with the financial institution specified in the financial information using network **312**. In order to authorize the financial transaction, server **326** may contact server **214** via network **312** to confirm that the one-time payment credential token used to obtain the financial information is the same as that provided by server **214** to portable electronic device **210**.

[0059] If the one-time payment credential token is the same, server **326** may authorize the financial transaction and provide a confirmation to point-of-sale terminal **212** via network **312**. Magnetic-stripe-reader control object **316** may receive the confirmation, which is then passed to point-of-sale-terminal software **318**.

[0060] Note that information in system **300** may be stored at one or more locations in system **300** (i.e., locally or remotely). Moreover, because this data may be sensitive in nature, it may be encrypted. For example, stored data and/or data communicated via network **312** may be encrypted.

[0061] FIG. **4** presents a block diagram illustrating a point-of-sale terminal **400** that performs method **100** (FIGS. **1** and **2**), such as point-of-sale terminal **212** (FIGS. **2** and **3**). Point-of-sale terminal **400** includes one or more processing units or processors **410**, a communication interface **412**, a user interface **414**, and one or more signal lines **422** coupling these components together. Note that the one or more processors **410** may support parallel processing and/or multi-threaded operation, the communication interface **412** may have a persistent communication connection, and the one or more signal lines **422** may constitute a communication bus. Moreover, the user interface **414** may include: a display **416**, a keyboard **418**, and/or a pointer **420**, such as a mouse.

[0062] Memory **424** in point-of-sale terminal **400** may include volatile memory and/or non-volatile memory. More specifically, memory **424** may include: ROM, RAM, EPROM, EEPROM, flash memory, one or more smart cards, one or more magnetic disc storage devices, and/or one or more optical storage devices. Memory **424** may store an operating system **426** that includes procedures (or a set of instructions) for handling various basic system services for performing hardware-dependent tasks. Memory **424** may also store procedures (or a set of instructions) in a communication module **428**. These communication procedures may be used for communicating with one or more computers and/or servers, including computers and/or servers that are remotely located with respect to point-of-sale terminal **400**.

[0063] Memory **424** may also include multiple program modules (or sets of instructions), including: point-of-sale-terminal software **318** (or a set of instructions), magnetic-stripe-reader service object **314** (or a set of instructions), magnetic-stripe-reader control object **316** (or a set of instructions), encryption module **432** (or a set of instructions) and/or financial application **434** (or a set of instructions). Note that one or more of these program modules (or sets of instructions) may constitute a computer-program mechanism.

[0064] During the financial transaction in method **100** (FIGS. **1** and **2**), barcode scanner **310** and magnetic-stripe-reader service object **314** receive an image of a barcode **436** from a portable electronic device of a customer. Then, magnetic-stripe-reader service object **314** performs one or more operations based on at least identifier **438** in barcode **436** to obtain financial information **440** of the customer. For example, barcode **436** may include one-time payment credential token **442**, which may include or may correspond to identifier **438** (e.g., one-time payment credential token **442** may be computed from identifier **438**). Magnetic-stripe-reader service object **314** may extract financial information **440** (such as mobile-payment information) from one-time payment credential token **442**. Note that one-time payment credential token **442** and financial information **440** may be stored in a data structure. This is shown in FIG. **5**, which presents a data structure **500** that includes one-time payment credential tokens **510**. In particular, one-time payment credential token **442** may include: identifier **512-1** and mobile-payment information **514-1** (such as an account identifier, an available amount that can be spent, a financial institution, transaction routing information, etc.).

[0065] Referring back to FIG. **4**, magnetic-stripe-reader service object **314** may provide financial information **440** to magnetic-stripe-reader control object **316** and, thus, point-of-sale-terminal software **318**. Next, point-of-sale terminal **400** may directly or indirectly provide financial information **440** and transaction information **444** associated with the financial transaction to a financial institution **446** specified in financial information **440**. For example, magnetic-stripe-reader control object **316** may provide financial information **440** and transaction information **444** using communication module **428** and network interface **412**.

[0066] Furthermore, point-of-sale terminal **400** directly or indirectly receives a confirmation **448** from financial institution **446** that the financial transaction has been completed. For example, magnetic-stripe-reader control object **316** may receive confirmation **448** via communication interface **412** and communication module **428**.

[0067] Because information in point-of-sale terminal **400** may be sensitive in nature, in some embodiments at least some of the data stored in memory **424** and/or at least some of the data communicated using communication module **428** is encrypted using encryption module **432**.

[0068] Instructions in the various modules in memory **424** may be implemented in: a high-level procedural langnage, an object-oriented programming language, and/or in an assembly or machine language. Note that the programming language may be compiled or interpreted, e.g., configurable or configured, to be executed by the one or more processors **410**.

[0069] Although point-of-sale terminal **400** is illustrated as having a number of discrete items, FIG. **4** is intended to be a functional description of the various features that may be present in point-of-sale terminal **400** rather than a structural schematic of the embodiments described herein. In some embodiments, some or all of the functionality of point-of-sale terminal **400** may be implemented in one or more application-specific integrated circuits (ASICs) and/or one or more digital signal processors (DSPs).

[0070] Point-of-sale terminals (such as point-of-sale terminal **400**), as well as computers and servers in system **300** (FIG. **3**) may include one of a variety of devices capable of manipulating computer-readable data or communicating such data between two or more computing systems over a network, including: a personal computer, a laptop computer, a tablet computer, a mainframe computer, a portable electronic device (such as a cellular phone or PDA), a server and/or a client computer (in a client-server architecture). Moreover, network **312** (FIG. **3**) may include: the Internet, World Wide Web (WWW), an intranet, a cellular-telephone network, LAN, WAN, MAN, or a combination of networks, or other technology enabling communication between computing systems.

[0071] In some embodiments one or more of the modules in memory **424** may be associated with and/or included in a financial application **434**. This financial application may include planning software capable of processing financial information. Moreover, financial application **434** may be associated with and/or include payroll or accounting software capable of processing payroll information.

[0072] System **300** (FIG. **3**), point-of-sale terminal **400** (FIG. **4**) and/or data structure **500** may include fewer components or additional components. Moreover, two or more components may be combined into a single component, and/or a position of one or more components may be changed. In some embodiments, the functionality of system **300** (FIG. **3**) and/or point-of-sale terminal **400** may be implemented more in hardware and less in software, or less in hardware and more in software, as is known in the art.

[0073] The foregoing description is intended to enable any person skilled in the art to make and use the disclosure, and is provided in the context of a particular application and its requirements. Moreover, the foregoing descriptions of embodiments of the present disclosure have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the present disclosure to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present disclosure. Additionally, the discussion of the preceding embodiments is not intended to limit the present disclosure. Thus, the present disclosure is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

1. A point-of-sale-terminal-implemented method for conducting a financial transaction, the method comprising:

receiving a one-time payment credential token associated with a customer from a portable electronic device via a peripheral device coupled to the point-of-sale terminal and a service object executing on the point-of-sale terminal, wherein the service object acts as a driver for the peripheral device, wherein the peripheral device includes a barcode scanner that scans a 11-digit barcode that includes the one-time payment credential token,

wherein the one-time payment credential token is generated by a trusted execution environment executing a technique known to a third party on the portable electronic device, and wherein said technique does not need to connect to the third party prior to the financial transaction, and

wherein the one-time payment credential token includes financial information of the customer, wherein the financial information includes a 6-digit bank identification number, a virtual account number, an expiration date, and a card verification code;

performing one or more operations based on at least the one-time payment credential token to obtain the financial information;

using the point-of-sale terminal, providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information; and

receiving a confirmation that the financial transaction has been completed.

2. The method of claim **1**, wherein the one or more operations include:

extracting the financial information from the one-time payment credential token.

3. (canceled)

4. The method of claim **1**, wherein the service object includes a magnetic-stripe-reader service object.

5. (canceled)

6. The method of claim **1**, wherein the service object executing on the point-of-sale terminal presents the barcode scanner to the point-of-sale terminal as a keyboard.

7. The method of claim **1**, wherein the one or more operations include extracting the financial information from the one-time payment credential token.

8. The method of claim **1**, wherein the one-time payment credential token is only valid for the financial transaction.

9. The method of claim **1**, wherein the peripheral device is selected from the group consisting of: a barcode scanner, a wireless receiver, and a keyboard.

10. A computer-program product for use in conjunction with a point-of-sale terminal, the computer-program product comprising a non-transitory computer-readable storage medium and a computer-program mechanism embedded therein, to conduct a financial transaction, the computer-program mechanism including:

instructions for receiving a one-time payment credential token associated with a customer from a portable electronic device via a peripheral device coupled to the point-of-sale terminal and a service object executing on the point-of-sale terminal, wherein the service object acts as a driver for the peripheral device, wherein the

peripheral device includes a barcode scanner that scans a 11-digit barcode that includes the one-time payment credential token,

wherein the one-time payment credential token is generated by a trusted execution environment executing a technique known to a third party on the portable electronic device, and wherein said technique does not need to connect to the third party prior to the financial transaction, and

wherein the one-time payment credential token includes financial information of the customer, wherein the financial information includes a 6-digit bank identification number, a virtual account number, an expiration date, and a card verification code;

instructions for performing one or more operations based on at least the one-time payment credential token to obtain the financial information;

instructions for providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information; and

instructions for receiving a confirmation that the financial transaction has been completed.

11. The computer-program product of claim **10**, wherein instructions for performing one or more operations include:

instructions for extracting the financial information from the one-time payment credential token.

12. (canceled)

13. The computer-program product of claim **10**, wherein the service object includes a magnetic-stripe-reader service object.

14. (canceled)

15. The computer-program product of claim **10**, wherein the service object executing on the point-of-sale terminal presents the barcode scanner to the point-of-sale terminal as a keyboard.

16. The computer-program product of claim **10**, wherein instructions for performing one or more operations include instructions for extracting the financial information from the one-time payment credential token.

17. The computer-program product of claim **10**, wherein the one-time payment credential token is only valid for the financial transaction.

18. The computer-program product of claim **10**, wherein the peripheral device is selected from the group consisting of: a barcode scanner, a wireless receiver, and a keyboard.

19. A point-of-sale terminal, comprising:

a processor;

memory; and

a program module, wherein the program module is stored in the memory and configurable to be executed by the processor to conduct a financial transaction, the program module including:

instructions for receiving a one-time payment credential token associated with a customer from a portable electronic device via a peripheral device coupled to the point-of-sale terminal and a service object executing on the point-of-sale terminal, wherein the service object acts as a driver for the peripheral device, wherein the peripheral device includes a barcode scanner that scans an 11 digit barcode that includes the one-time payment credential token,

wherein the one-time payment credential token is generated by a trusted execution environment executing a technique known to a third party on the portable electronic device, and wherein said technique does not need to connect to the third party prior to the financial transaction, and

wherein the one-time payment credential token includes financial information of the customer, wherein the financial information includes a 6-digit bank identification number, a virtual account number, an expiration date, and a card verification code;

instructions for performing one or more operations based on at least the one-time payment credential token to obtain the financial information;

instructions for providing the financial information and transaction information associated with the financial transaction to a financial institution specified in the financial information; and

instructions for receiving a confirmation that the financial transaction has been completed.

20. The point-of-sale terminal of claim **19**, wherein instructions for performing one or more operations include:

instructions for extracting the financial information from the one-time payment credential token.

21. (canceled)

22. (canceled)

23. The point-of-sale terminal of claim **19**, wherein the service object executing on the point-of-sale terminal presents the barcode scanner to the point-of-sale terminal as a keyboard.

24. The point-of-sale terminal of claim **19**, wherein instructions for performing one or more operations include instructions for extracting the financial information from the one-time payment credential token.

25. The point-of-sale terminal of claim **19**, wherein the peripheral device is selected from the group consisting of: a barcode scanner, a wireless receiver, and a keyboard.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

KHAN et al.

(10) **Pub. No.: US 2014/0019367 A1**

(43) **Pub. Date: Jan. 16, 2014**

(54) **METHOD TO SEND PAYMENT DATA THROUGH VARIOUS AIR INTERFACES WITHOUT COMPROMISING USER DATA**

(71) Applicant: **APPLE INC.**, Cupertino, CA (US)

(72) Inventors: **Aluner A. KHAN**, Milpitas, CA (US); **Brian J. Tucker**, Sunnyvale, CA (US); **David T. Haggerty**, San Francisco, CA (US); **Scott M. Herz**, San Jose, CA (US)

(73) Assignee: **Apple Inc.**, Cupertino, CA (US)

(21) Appl. No.: **13/631,838**

(22) Filed: **Sep. 28, 2012**

Related U.S. Application Data

(60) Provisional application No. 61/671,677, filed on Jul. 13, 2012.

Publication Classification

(51) **Int. Cl.**

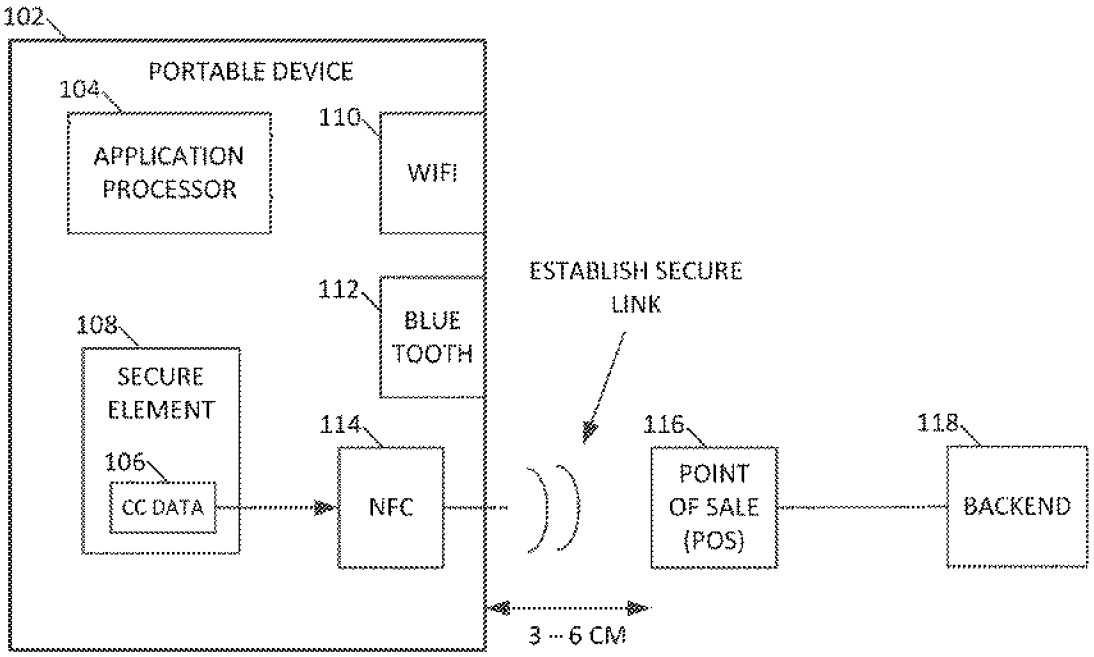
G06Q 30/06	(2012.01)
H04L 9/32	(2006.01)
H04L 9/28	(2006.01)

(52) **U.S. Cl.**

USPC **705/75**; 705/16; 705/78

(57) **ABSTRACT**

A commercial transaction method is disclosed. The method first establishes a secure link over a first air interface by a purchasing device. This secure link is between the purchasing device and a point of sale device. The method further identifies a second air interface, which is different from the first air interface, and the second air interface is used to conduct a secure commercial transaction.



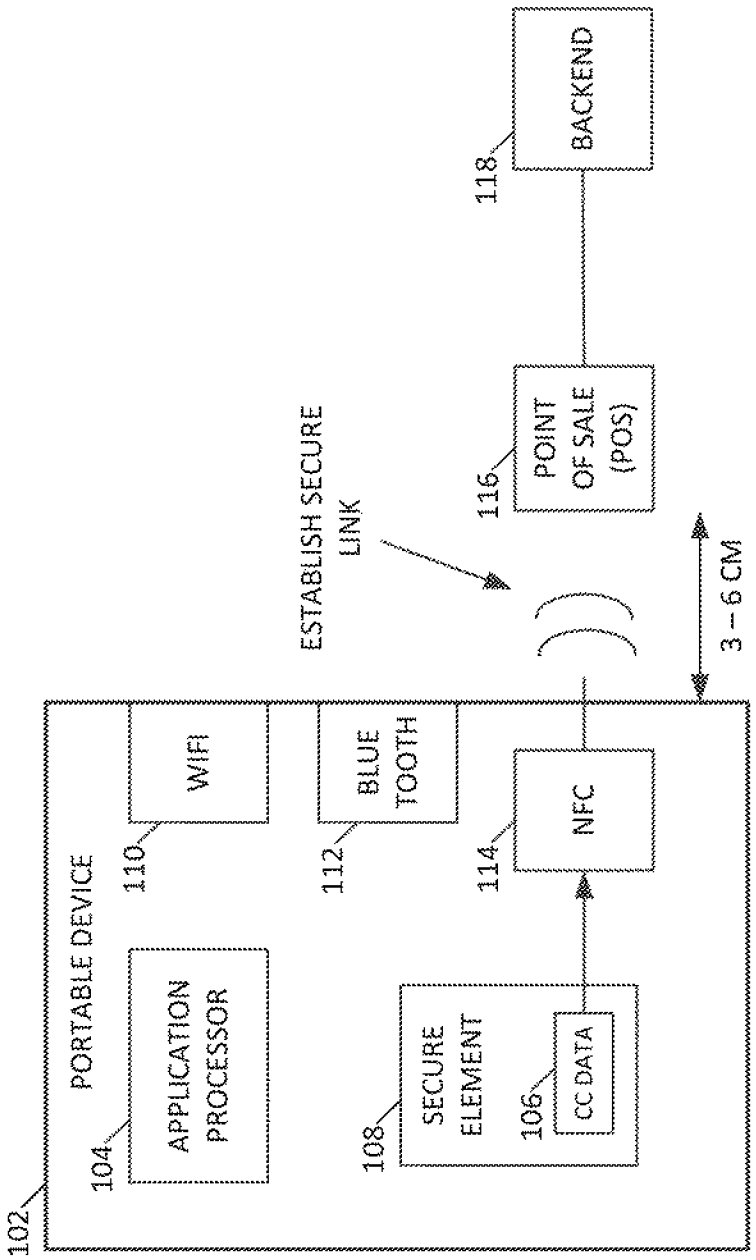

BACKEND
118
POINT OF SALE (POS)
116
ESTABLISH SECURE LINK
3 – 6 CM
PORTABLE DEVICE
102
WIFI
110
BLUE TOOTH
112
NFC
114
APPLICATION PROCESSOR
104
SECURE ELEMENT
108
CC DATA
106

FIG. 1

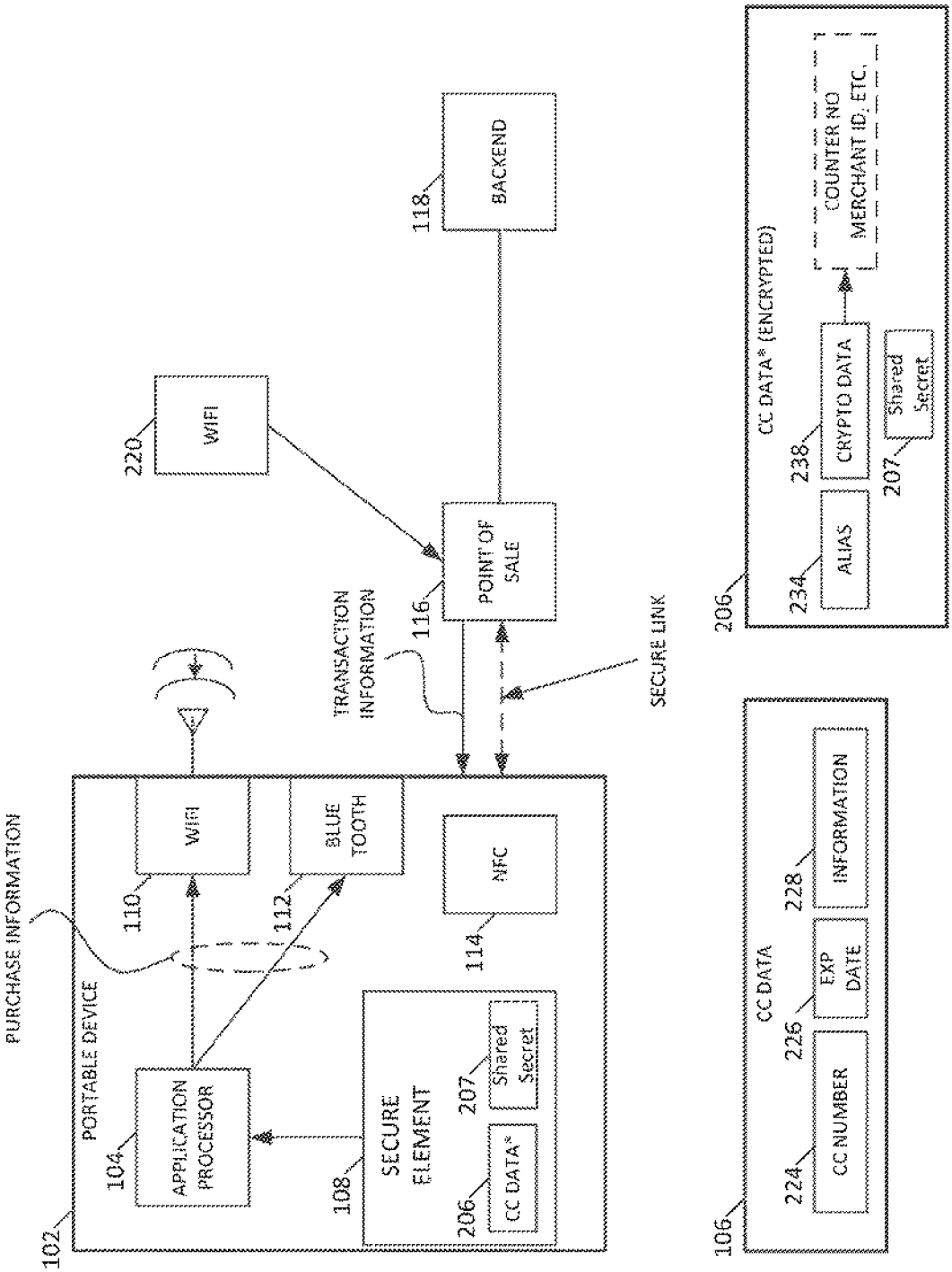

PURCHASE INFORMATION
PORTABLE DEVICE
102
APPLICATION PROCESSOR
104
WIFI
110
BLUE TOOTH
112
NFC
114
SECURE ELEMENT
108
CC DATA*
206
Shared Secret
207
TRANSACTION INFORMATION
116
SECURE LINK
POINT OF SALE
BACKEND
118
WIFI
220
CC DATA
106
CC NUMBER
224
EXP DATE
226
INFORMATION
228
CC DATA* (ENCRYPTED)
206
ALIAS
234
CRYPTO DATA
238
Shared Secret
207
COUNTER NO
MERCHANT ID, ETC.

FIG. 2

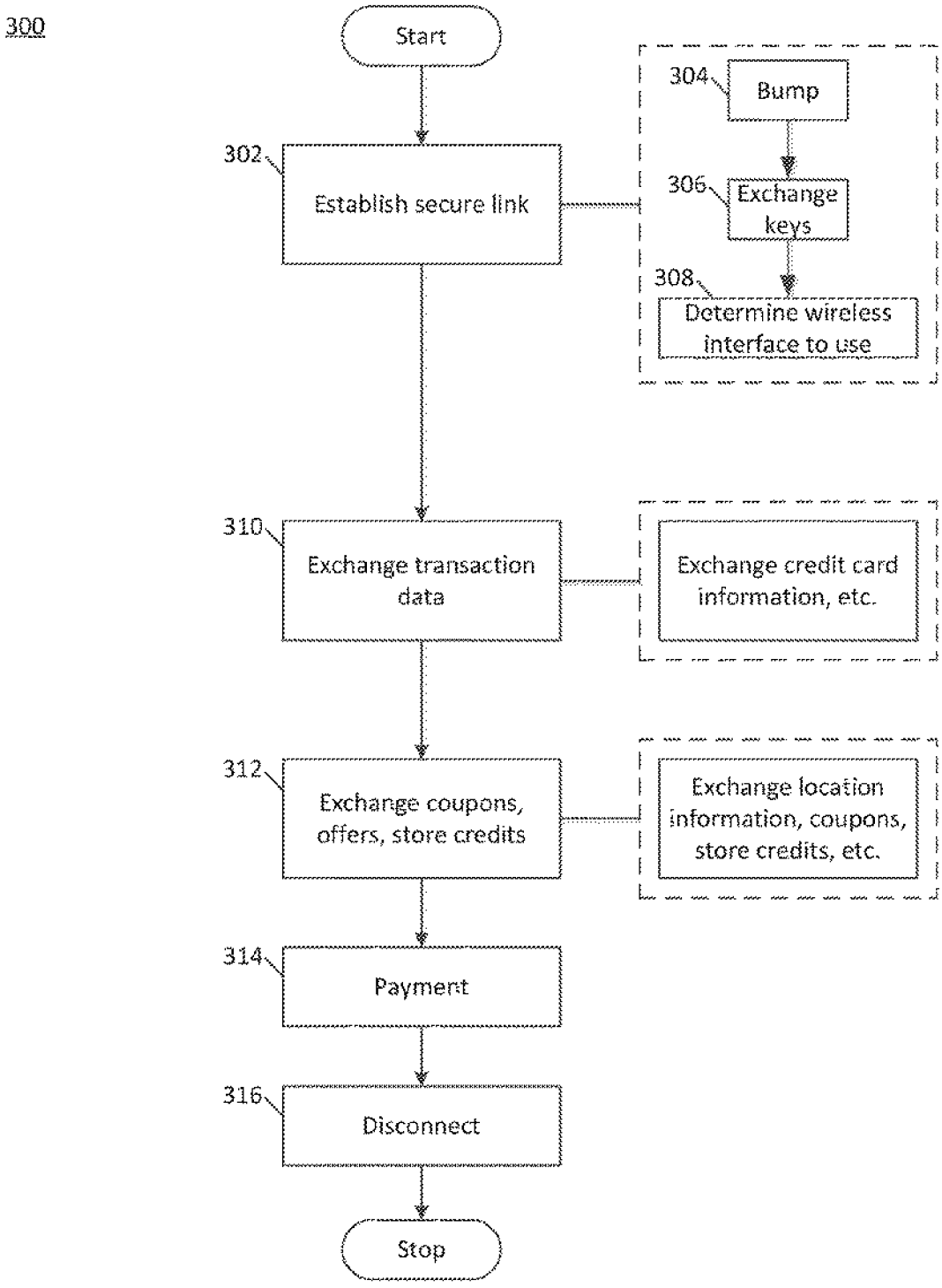

300
Start
302
Establish secure link
304
Bump
306
Exchange keys
308
Determine wireless interface to use
310
Exchange transaction data
Exchange credit card information, etc.
312
Exchange coupons, offers, store credits
Exchange location information, coupons, store credits, etc.
314
Payment
316
Disconnect
Stop

FIG. 3

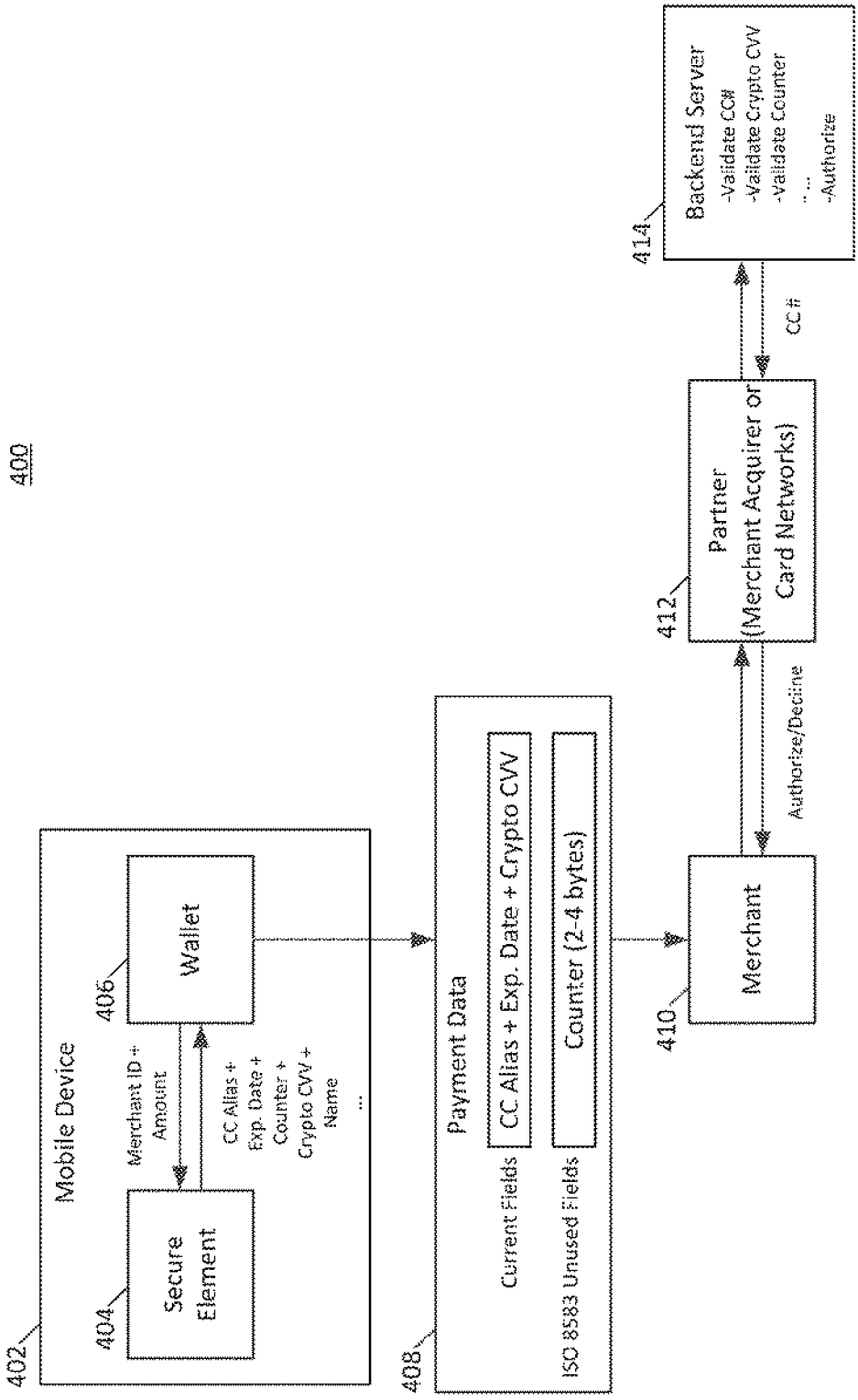

400
402
Mobile Device
404
Secure Element
406
Wallet
Merchant ID + Amount
CC Alias + Exp. Date + Counter + Crypto CVV + Name
...
408
Payment Data
Current Fields
CC Alias + Exp. Date + Crypto CVV
ISO 8583 Unused Fields
Counter (2-4 bytes)
410
Merchant
412
Partner (Merchant Acquirer or Card Networks)
Authorize/Decline
CC #
414
Backend Server
-Validate CCN
-Validate Crypto CVV
-Validate Counter
...
-Authorize

FIG. 4

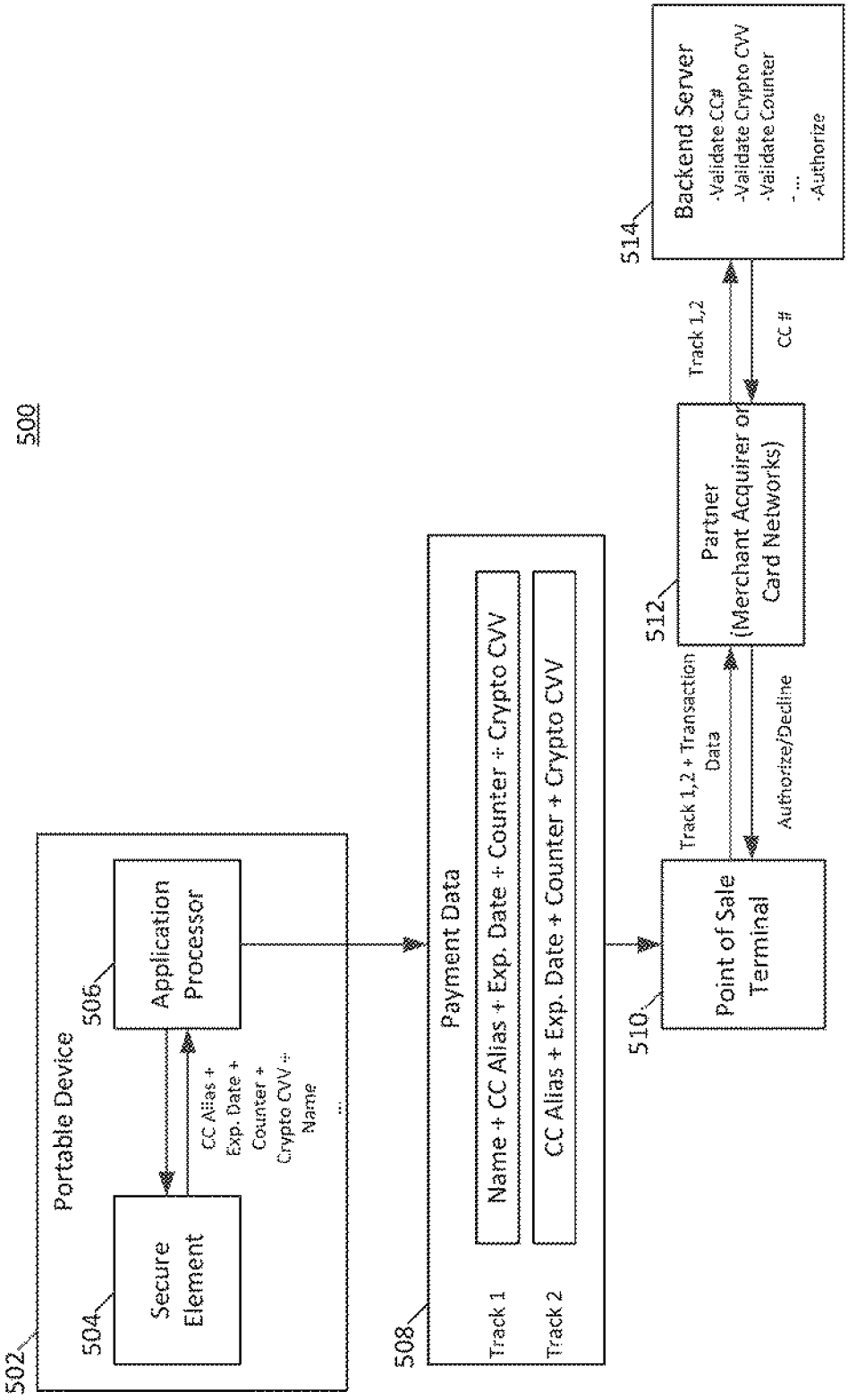

500
502
Portable Device
504
Secure Element
506
Application Processor
CC Alias + Exp. Date + Counter + Crypto CVV + Name
...
508
Payment Data
Track 1
Track 2
Name + CC Alias + Exp. Date + Counter + Crypto CVV
CC Alias + Exp. Date + Counter + Crypto CVV
510
Point of Sale Terminal
Track 1,2 + Transaction Data
Authorize/Decline
512
Partner (Merchant Acquirer or Card Networks)
Track 1,2
CC #
514
Backend Server
-Validate CC#
-Validate Crypto CVV
-Validate Counter
-...
-Authorize

FIG. 5

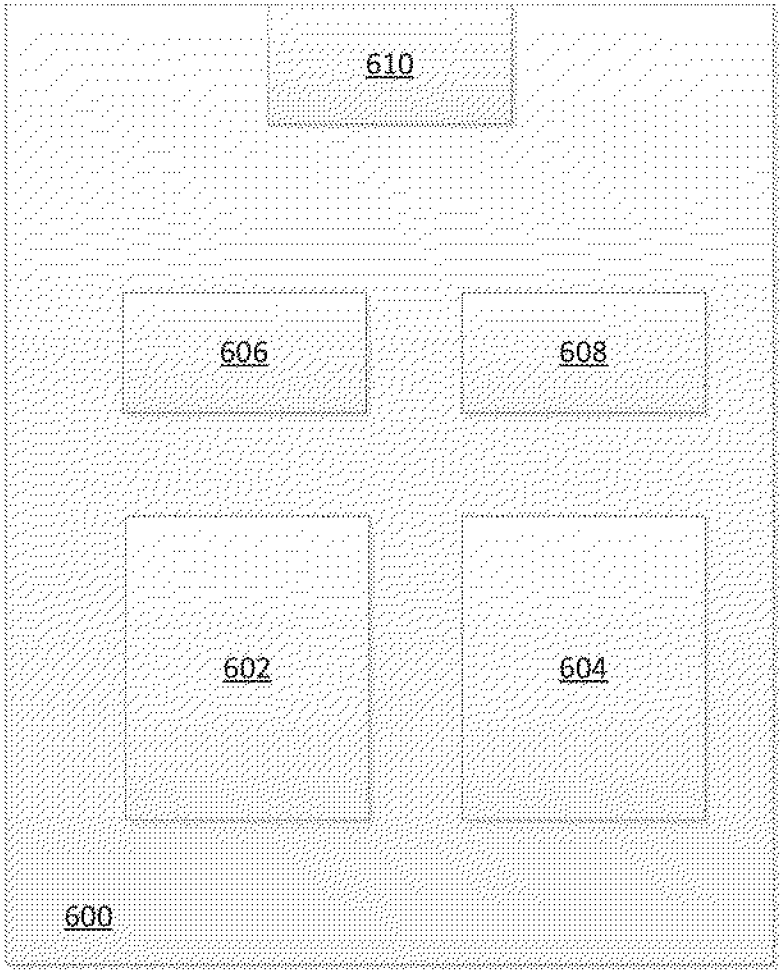


FIG. 6

METHOD TO SEND PAYMENT DATA THROUGH VARIOUS AIR INTERFACES WITHOUT COMPROMISING USER DATA

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/671,677, filed Jul. 13, 2012, and entitled "METHOD TO SEND PAYMENT DATA THROUGH VARIOUS AIR INTERFACES WITHOUT COMPROMISING USER DATA," which is incorporated herein by reference in its entirety and for all purposes.

TECHNICAL FIELD

[0002] The described embodiments generally relate to methods and apparatuses for conducting a wireless commercial transaction that is both user friendly and secure.

BACKGROUND

[0003] Devices located in close proximity to each other can communicate directly using proximity technologies such as Near-Field Communications (NFC), Radio Frequency Identifier (RFID), and the like. These protocols can establish wireless communication links between devices quickly and conveniently, without, for example, performing setup and registration of the devices with a network provider. NFC can be used in electronic transactions, e.g., to securely send order and payment information for online purchases from a purchaser's mobile device to a seller's point of sale (POS) device.

[0004] Currently, payment information such as credit card data in mobile devices is sent directly from a secure element (SE) located in a device such as a mobile phone through proximity interfaces, such as near field communications (NFC), without an associated application processor (AP), such as an application program in the device, accessing the payment information. Preventing the AP from accessing the sensitive payment information is necessary because current payment schemes use real payment information (credit card number, expiration date, etc.) that can be used to make purchases through other means, include online and via the phone, and data in the AP can be intercepted and compromised by rogue applications.

[0005] Thus, there exists a need for a secure method of executing a commercial transaction that is both secure and user friendly.

SUMMARY

[0006] In one or more embodiments, a portable device can make purchases by using near field communications (NFC) to establish a secure link with a point of sale (POS) device connected to a backend system that is configured to execute commercial transactions. This secure link can be established by positioning the portable device to be within close proximity of the point of sale device. Increased mobility is provided to users of the portable device making purchases by establishing a second secure link that uses a different protocol, such as WIFI or Bluetooth, that has more desirable characteristics for maintaining the link over time than NFC.

[0007] In one or more embodiments, a second secure link is established using a shared secret known to the portable device and the backend server, and using an alias to identify a purchasing account such as a credit card. When a request to make a transaction using the credit card is submitted to the backend server, the server determines whether the combination of the alias and crypto data is valid using a shared secret that is known to a secure element in the portable device and the backend server. The backend server uses the shared secret (e.g., symmetric keys, public private keys, etc.) to verify the alias and the crypto data. The backend receives the alias from the portable device via the point of sale device and combines the alias with other information, such as counter value known to both the backend and the secure element **108**. The backend can then generate the same crypto data using the shared secret and received data, and compare the result with the received crypto data. If the comparison indicates that the values are the same, then the credit card that corresponds to the credit card alias is provided back to the partner, and the transaction proceeds as normal. Otherwise, the credit card alias is rejected and the transaction is denied.

[0008] In one or more embodiments, a method of performing a commercial transaction is provided. The method includes establishing a first secure link over a first air interface by a purchasing device, the first secure link between the purchasing device and a point of sale device, identifying a second air interface different from the first air interface, establishing a second secure link over a second air interface, the second secure link between the purchasing device and a backend server, and conducting, using the second air interface, a secure commercial transaction between the purchasing device and the backend server using payment data secured by a shared secret known to a secure element in the purchasing device and to the backend server.

[0009] Embodiments of the invention may include one or more of the following features. The payment data may include an alias associated with a payment account, and establishing the second secure link may include encrypting the payment data by the secure element at the purchasing device using the shared secret as an encryption key. Establishing the second secure link may include decrypting, at the backend server, the payment data using the shared secret, and verifying, at the backend server, the payment data, where verifying includes comparing the payment data to independently known payment data stored at the backend server. Comparing the payment data to independently known payment data may include retrieving an alias from the decrypted received payment data, identifying a credit card account associated with the alias, determining if the alias is associated with the credit card account according to an association stored in a memory of the backend server, and, in response to determining that the alias is associated with the credit card account, approving the commercial transaction. Comparing the payment data may further include retrieving a counter value from the decrypted retrieved payment data, and comparing the counter value to an independently known counter value stored in a memory of the backend server. Establishing the first secure link may include establishing a near field communication link between the purchasing device and the point of sale device. Identifying a second air interface different from the first air interface may include identifying an air interface having properties more desirable than the first air interface to communicate data to a user over a time period longer than the time used to establish the first secure link.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The described embodiments and the advantages thereof may best be understood by reference to the following description taken in conjunction with the accompanying drawings.

[0011] FIG. **1** illustrates a wireless system in accordance with the described embodiments.

[0012] FIG. **2** further illustrates a wireless system in accordance with the described embodiments.

[0013] FIG. **3** illustrates a flow chart of a secure method of executing a commercial transaction in accordance with the described embodiments.

[0014] FIG. **4** illustrates a method of making mobile payments online in accordance with the described embodiments.

[0015] FIG. **5** illustrates a method of making mobile payments offline in accordance with the described embodiments.

[0016] FIG. **6** shows a system block diagram of computer system used to execute the software of an embodiment.

DETAILED DESCRIPTION OF SELECTED EMBODIMENTS

[0017] In the following description, numerous specific details are set forth to provide a thorough understanding of the concepts underlying the described embodiments. It will be apparent, however, to one skilled in the art that the described embodiments may be practiced without some or all of these specific details. In other instances, well known process steps have not been described in detail in order to avoid unnecessarily obscuring the underlying concepts.

[0018] FIG. **1** shows a portable device **102** that includes a secure element (SE) **108** configured to securely store and provide access to credit card information **106** in accordance with one or more embodiments. The device **102** also includes an application processor (AP) **104** that executes applications to, for example, purchase goods and services using the credit card information **106** to send payments to vendor systems such as a point of sale (POS) device **116**. The portable device **102** also includes one or more air interfaces, such as near field communications (NFC) **114**, WIFI **110** (e.g., wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standard) and Bluetooth (BT) **112**. NFC **114**, Bluetooth **112**, and WIFI **110** are wireless communication protocols. In one example, the portable device can make purchases by using near field communications (NFC) to wirelessly establish a secure link with the point of sale (POS) device **116**, which is connected to a backend system **118** configured to execute commercial transactions, e.g., a bank, acquirer, or the like. This secure link using NFC **114** can be established by positioning the portable device to be within close proximity of, within e.g., 3 to 6 cm of, the point of sale device **116**. In this example, credit card information **106** is sent by the secure element **108** as plaintext (i.e., not encrypted) data directly to the NFC **114**. The plaintext credit card data **106** is not sent to the application processor **104**. If the plaintext credit card data **106** were to be sent to the application processor **104**, a rogue program could access the credit card data **106** and use it to make unauthorized purchases. In the example of FIG. **1**, access to the credit card data **106** by rogue programs is prevented because the communication between the secure element **108** and the NFC **114** is not accessible to the application processor **102**.

[0019] In other embodiments, the portable device **102** can use protocols other than NFC to establish the secure link between the portable device **102** and the POS device **116**, particularly protocols that have desirable characteristics for establishing a secure link, e.g., protocols that can establish a secure link quickly and securely. Protocols with desirable characteristics for establishing a secure link can have undesirable characteristics for maintaining the link over time, e.g., such protocols may involve keeping the portable device **102** in the same location for the duration of a transaction. The NFC protocol, for example, establishes a secure link quickly and conveniently at a point of sale. However, transactions that include sending additional data between the POS terminal **106** and the portable device **102**, such as additional payment information, coupon offers, coupon data, and the like, can continue for some time, during which the portable device **102** is kept in the same location within centimeters of the POS terminal **116**. Holding or setting the device **102** near the POS terminal **116** becomes inconvenient for users, so NFC is less desirable for longer transactions such as those that involve transferring more data than used by the payment information or use more time than used in the NFC connection establishment process. The establishment of the NFC link, which occurs quickly, is referred to herein as an initial "bump" because the devices may touch each other momentarily when the NFC connection is being established. NFC is used herein as an example, and other types of proximity technology can be used in other embodiments.

[0020] In one or more embodiments, the NFC secure link can be used to establish a second secure link that uses a different protocol, such as WIFI **110**, Bluetooth **112**, or another wireless protocol that has more desirable characteristics for maintaining the link over time than NFC. The particular protocol that is used for the second link can be selected based on configured information, e.g., depending on the type of communication hardware available in the device, or according to user preferences, signal strength, the amount of data expected to be transferred, and so on.

[0021] FIG. **2** shows the portable device **102** conducting a secure commercial transaction using a second air interface **110** or **112** in accordance with one or more embodiments. The second air interface **110** or **112** is different from the first air interface **114** that was used to establish the secure link. As an example, FIG. **2** shows the portable device **102** conducting a secure commercial transaction using the WIFI air interface **110**, for a secure link that was established using NFC **114**. In this way, purchase information may be transferred through the WIFI interface **110** instead of the NFC interface **114**. WIFI is more convenient than NFC for users, since the limited communication range of NFC requires the portable device to be in close proximity to the POS device, e.g., within 3 to 6 inches. The second air interface **114** can be used, for example, to send information such as offers by customers or merchants, coupon offers and redemptions, receipts, follow up information, and so on. The second air interface **114** link can be closed upon completion of the transaction(s) by, for example, sending a completion or termination message.

[0022] FIG. **2** further shows the secure element **108** passing encrypted credit card data (CC data*) **206** to the application processor **104**. Normal, i.e., plaintext, credit card data (CC data) **106** includes a credit card number, expiration date (exp date) and other information. Encrypted credit card data (CC data*) **206** includes an alias **234** and other cryptographic data **238** such as counter number, merchant ID, etc.

[0023] As described above, the confidentiality of data sent to the application processor **104** may be compromised, e.g., by a rogue application. Therefore, the credit card data **106** is encrypted by the secure element **108** to produce encrypted cryptographic data **206**. The secure element **108** generates an "alias" **234** for the credit card data **206**, which is passed to the application processor **104** instead of the unencrypted credit

card data **106**. The alias **234** is an identifier for the credit card data **206**, but cannot be used to make a payment without valid crypto data **238** that corresponds to the alias **234**. Thus, the alias need not be stored securely, because payments made with the alias **234** are not accepted by the backend **118** unless the corresponding crypto data **238** is also supplied, e.g., in a request to process a payment.

[0024] The crypto data **238** may be, for example, a digitally-signed combination of one or more of the alias **234**, a counter value that is incremented for each alias value, a random number, a merchant identifier, or any other value that is believed to be important. The shared secret **207** may be, for example, a symmetric key distributed to the secure element **108** at the time the device **102** is manufactured, and loaded into the backend **118** via secure communication behind a firewall. In other embodiments, a cryptographic key exchange mechanism may be used to establish the shared secret. Therefore, the alias can be known by the application processor **104** without compromising security. The crypto data is, in one or more embodiments, stored in the secure element **108** and used to generate the crypto data **238** at the portable device **102** based upon the alias received from the application processor **104**. A user may enter the alias **234** into the application processor **104**, and the alias **234** is also known to the backend **118**. The alias is, for example, provided to the user by the organization that operates the backend, e.g., an online merchant.

[0025] In one or more embodiments, when a request to make a transaction using the credit card is submitted to the backend server **414**, the server **414** determines whether the combination of the alias **234** and crypto data **238** are valid using a shared secret **207** that is known to the secure element **108** and the backend server **118**. The backend uses the shared secret (e.g., symmetric keys, public private keys, etc.) to verify the alias **234** and the crypto data **238**. The backend **118** receives the alias from the portable device **102** via the point of sale **116**, combines the alias **234** with other information as described above (e.g., a counter value known to both the backend **118** and the secure element **108**, and so on). The backend **118** can then generate the same crypto data using the shared secret and received data, and compare the result with the received crypto data. If the comparison indicates that the values are the same, then the credit card that corresponds to the credit card alias **234** is provided back to the partner **412**, and the transaction proceeds as normal. Otherwise, the credit card alias is rejected and the transaction is denied.

[0026] FIG. **3** shows the flow chart of an example method **300** to conduct a secure commercial transaction in accordance with one or more embodiments. The method **300** can be implemented as, for example, computer program code encoded on a computer readable medium and executable by a processor of a computer system.

[0027] The method **300** includes, at block **302** establishing a secure link between a portable device and a POS device, exchanging transaction data at block **310**, and exchanging coupons, offers, store credits, location information, etc. at block **312** The method further includes making payment and disconnecting the portable device from the POS device. The establishing a secure link portion **302** includes establishing a bump **304**, e.g., an NFC connection, exchanging keys as described above with reference to FIG. **2**, and determining which wireless interface to use, e.g., NFC, RFID, or another interface. Exchanging transaction data includes exchanging credit card information, etc. as described above with reference to FIG. **2**.

[0028] FIG. **4** shows an example method to make mobile payments online in accordance with one or more embodiments. A mobile device **402** includes a secure element **404** and a wallet **406**, which is similar to the secure element **108** of FIG. **2**. Payment data **408**, including the credit card alias, expiration date, and crypto CVV (e.g., credit card security code) is sent to the merchant **410**, which is analogous to the point of sale **116** of FIG. **2**. The merchant **410** sends an authorization request to a partner **412**, e.g., a credit card network, and a backend server validates the payment information, e.g., credit card number, CVV, counter, alias, and any other information using a secret key that is known to both the backend server **414** and the wallet **406**. If the payment information matches corresponding values independently known to the backend server, then the server **414** authorizes the transaction. Otherwise, the transaction is declined.

[0029] FIG. **5** shows an example method to make mobile payments offline (e.g., in store) in accordance with one or more embodiments. Block **502** is a portable device that includes a secure element **504** and an application processor **506** as described above with reference to FIG. **2**. The application processor **506** sends payment data **408**, e.g., credit card information including a name, alias, expiration data, counter, and security code, to a POS terminal **510**. The POS terminal **510** forwards the payment data to a partner **512**, e.g., a merchant acquirer, which in turn sends an authorization request to the backend **514**. The backend authorizes the request if the received payment data has been encrypted with the same secret key **207** that is known to the backend **514**, and the data that results from decrypting the received payment data matches corresponding values independently known to the backend server **514**.

[0030] FIG. **6** shows a system block diagram of computer system **600** used to execute the software of an embodiment. Computer system **600** includes subsystems such as a central processor **602**, system memory **604**, fixed storage **606** (e.g., hard drive), removable storage **608** (e.g., FLASH), and network interface **610**. The central processor **602**, for example, can execute computer program code (e.g., an operating system) to implement the invention. An operating system is normally, but necessarily) resident in the system memory **604** during its execution. Other computer systems suitable for use with the invention may include additional or fewer subsystems. For example, another computer system could include more than one processor **602** (i.e., a multi-processor system) or a cache memory.

[0031] The various aspects, embodiments, implementations or features of the described embodiments can be used separately or in any combination. Various aspects of the described embodiments can be implemented by software, hardware or a combination of hardware and software.

[0032] The foregoing description, for purposes of explanation, used specific nomenclature to provide a thorough understanding of the described embodiments. However, it will be apparent to one skilled in the art that the specific details are not required in order to practice the described embodiments. Thus, the foregoing descriptions of the specific embodiments described herein are presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the embodiments to the precise forms disclosed. It will be

apparent to one of ordinary skill in the art that many modifications and variations are possible in view of the above teachings.

[0033] The advantages of the embodiments described are numerous. Different aspects, embodiments or implementations can yield one or more of the following advantages. Many features and advantages of the present embodiments are apparent from the written description and, thus, it is intended by the appended claims to cover all such features and advantages of the invention. Further, since numerous modifications and changes will readily occur to those skilled in the art, the embodiments should not be limited to the exact construction and operation as illustrated and described. Hence, all suitable modifications and equivalents can be resorted to as falling within the scope of the invention.

What is claimed is:

1. A method of performing a commercial transaction, comprising:

establishing a first secure link over a first air interface by a purchasing device, the first secure link between the purchasing device and a point of sale device;

identifying a second air interface different from the first air interface;

establishing a second secure link over the second air interface, the second secure link between the purchasing device and a backend server; and

conducting, using the second secure link, a secure commercial transaction between the purchasing device and the backend server using payment data secured by a shared secret known to a secure element in the purchasing device and to the backend server.

2. The method of claim **1**, wherein the payment data comprises an alias associated with a payment account, and establishing the second secure link comprises:

encrypting the payment data by the secnre element at the purchasing device using the shared secret as an encryption key.

3. The method of claim **2**, wherein establishing the second secnre link comprises:

decrypting, at the backend server, the payment data using the shared secret; and

verifying, at the backend server, the payment data,

wherein verifying includes comparing the payment data to independently known payment data stored at the backend server.

4. The method of claim **3**, wherein comparing the payment data to independently known payment data comprises:

retrieving an alias from the decrypted received payment data;

identifying a credit card account associated with the alias;

determining if the alias is associated with the credit card account according to an association stored in a memory of the backend server; and

in response to determining that the alias is associated with the credit card account, approving the commercial transaction.

5. The method of claim **4**, wherein comparing the payment data further comprises:

retrieving a counter value from the decrypted retrieved payment data; and

comparing the counter value to an independently known counter value stored in a memory of the backend server.

6. The method of claim **1**, wherein establishing the first secure link comprises establishing a near field communication link between the purchasing device and the point of sale device.

7. The method of claim **1**, wherein identifying a second air interface different from the first air interface includes identifying an air interface having properties more desirable than the first air interface for communication of data to a user over a time period longer than the time used to establish the first secure link.

8. A system comprising:

a purchasing device

point of sale device; and

a backend server;

the purchasing device configured to:

establish a secure link over a first air interface, the secure link between the purchasing device and a point of sale device; and

identify a second air interface different from the first air interface, the second air interface being used to conduct a secure commercial transaction between the purchasing device and a backend server using payment data secured by a shared secret known to a secure element in the purchasing device and to the backend server.

9. The system of claim **8**, wherein the payment data comprises an alias associated with a payment account, the purchasing device further configured to use a secure element to encrypt the payment data using the shared secret as an encryption key.

10. The system of claim **9**, wherein the backend is configured to:

decrypt the payment data using the shared secret; and

compare the payment data to independently known payment data.

11. The system of claim **10**, wherein to comparing the payment data the backend server is configured to:

retrieve an alias from the decrypted received payment data;

identify a credit card account associated with the alias;

determine if the alias is associated with the credit card account according to an association stored in a memory of the backend server; and

in response to a determination that the alias is associated with the credit card account, approve the commercial transact.

12. The system of claim **11**, wherein to compare the payment data, the backend server is further configured to:

retrieve a counter value from the decrypted retrieved payment data; and

compare the counter value to an independently known counter value stored in a memory of the backend server.

13. The system of claim **8**, wherein the second air interface is established using a security key exchanged between the purchasing device and the backend server via the first air interface.

14. The system of claim **8**, wherein to identify the second air interface different from the first air interface, the purchasing device is configured to identify an air interface having properties desirable for communicating data over a longer period of time more conveniently to a user than the first air interface.

15. A non-transitory computer readable medium for a computer system, the non-transitory computer readable medium

having stored thereon computer program code executable by a processor, the computer program code comprising:

computer program code configured to cause the processor to establish a first secure link over a first air interface by a purchasing device, the first secure link between the purchasing device and a point of sale device,

computer program code configured to cause the processor to identify a second air interface different from the first air interface;

computer program code configured to cause the processor to establish a second secure link over a second air interface, the second secure link between the purchasing device and a backend server; and

computer program code configured to cause the processor to conduct, using the second air interface, a secure commercial transaction between the purchasing device and the backend server using payment data secured by a shared secret known to a secure element in the purchasing device and to the backend server.

16. The computer readable medium of claim **15**, wherein the payment data comprises an alias associated with a payment account, and the computer program code configured to establish the second secure link comprises:

computer program code configured to encrypt the payment data by the secure element at the purchasing device using the shared secret as an encryption key.

17. The computer readable medium of claim **16**, wherein the computer program code configured to establish the second secure link comprises:

computer program code configured to decrypt, at the backend server, the payment data using the shared secret; and

computer program code configured to compare the payment data to independently known payment data stored at the backend server.

18. The computer readable medium of claim **17**, wherein the computer program code configured to compare the payment data to independently known payment data comprises:

computer program code configured to retrieve an alias from the decrypted received payment data;

computer program code configured to identify a credit card account associated with the alias;

computer program code configured to determine if the alias is associated with the credit card account according to an association stored in a memory of the backend server; and

computer program code configured to in response to determining that the alias is associated with the credit card account, approve the commercial transact.

19. The computer readable medium of claim **18**, wherein computer program code configured to compare the payment data further comprises:

computer program code configured to retrieve a counter value from the decrypted retrieved payment data; and

computer program code configured to compare the counter value to an independently known counter value stored in a memory of the backend server.

20. The computer readable medium of claim **15**, wherein the computer program code configured to establish the first secure link comprises computer program code configured to establish a near field communication link between the purchasing device and the point of sale device.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Dunn et al.

(10) **Pub. No.: US 2014/0089186 A1**

(43) **Pub. Date: Mar. 27, 2014**

(54) **MOBILE PAYMENT SERVICE FOR SMALL FINANCIAL INSTITUTIONS**

(71) Applicant: **INTUIT INC.**, Mountain View, CA (US)

(72) Inventors: **Erie C. W. Dunn**, Palo Alto, CA (US); **Alexander S. Ran**, Palo Alto, CA (US)

(73) Assignee: **INTUIT INC.**, Mountain View, CA (US)

(21) Appl. No.: **13/626,776**

(22) Filed: **Sep. 25, 2012**

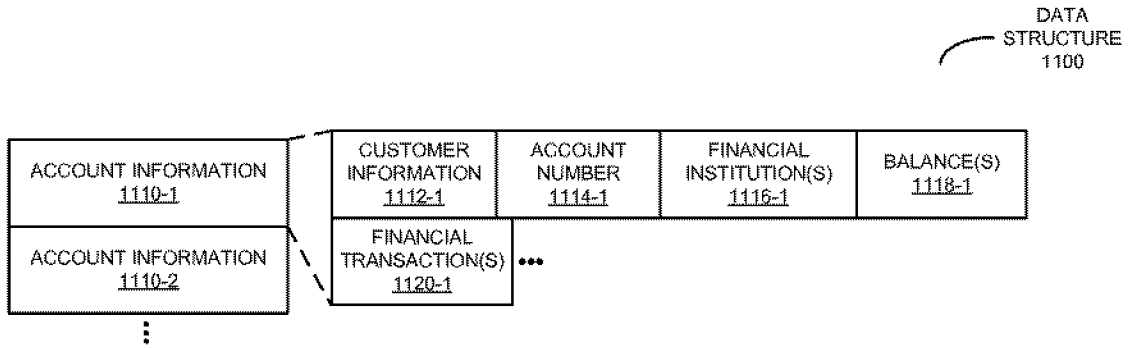
Publication Classification

(51) **Int. Cl.**
G06Q 20/10 (2012.01)
G06Q 40/00 (2012.01)

(52) **U.S. Cl.**
USPC **705/42**; 705/35

(57) **ABSTRACT**

During operation of the system, a user of a portable electronic device provides a request to enroll in a financial service associated with a provider. For example, the financial service may facilitate financial transactions via a financial application that executes on the portable electronic device. Then, an electronic device determines that the user is an existing customer of at least one of a set of financial institutions that have a business relationship with the provider, where the provider is other than one of the financial institutions. Next, the electronic device enrolls the user in the financial service without requesting additional information from the user. By leveraging the business relationship between the user and one of the financial institutions in the set of financial institutions, the user can avoid having to perform a complicated enrollment process in order to start using the financial service.



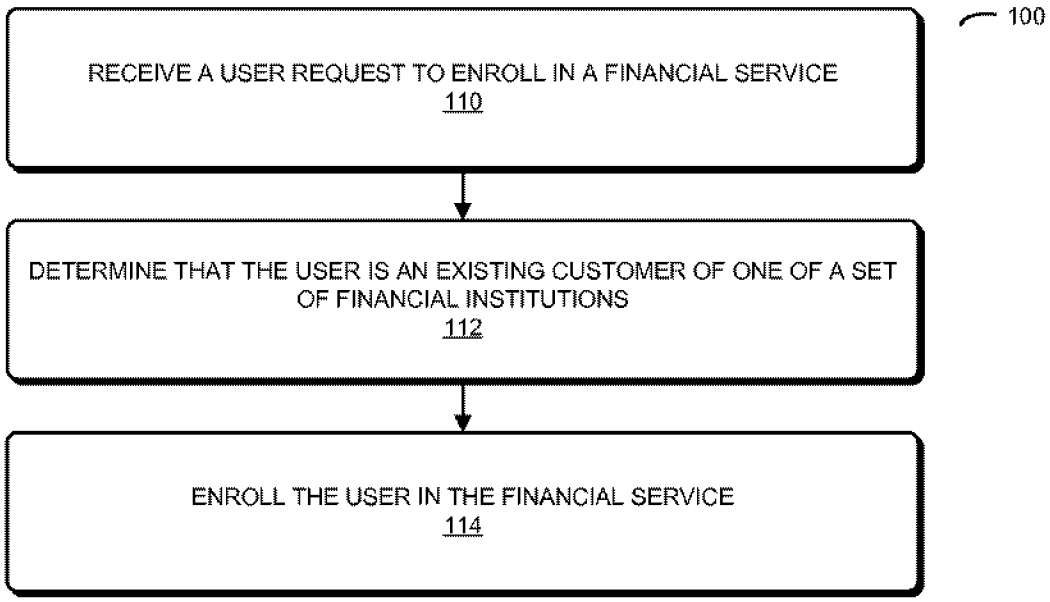

100
RECEIVE A USER REQUEST TO ENROLL IN A FINANCIAL SERVICE
110
DETERMINE THAT THE USER IS AN EXISTING CUSTOMER OF ONE OF A SET OF FINANCIAL INSTITUTIONS
112
ENROLL THE USER IN THE FINANCIAL SERVICE
114

FIG. 1

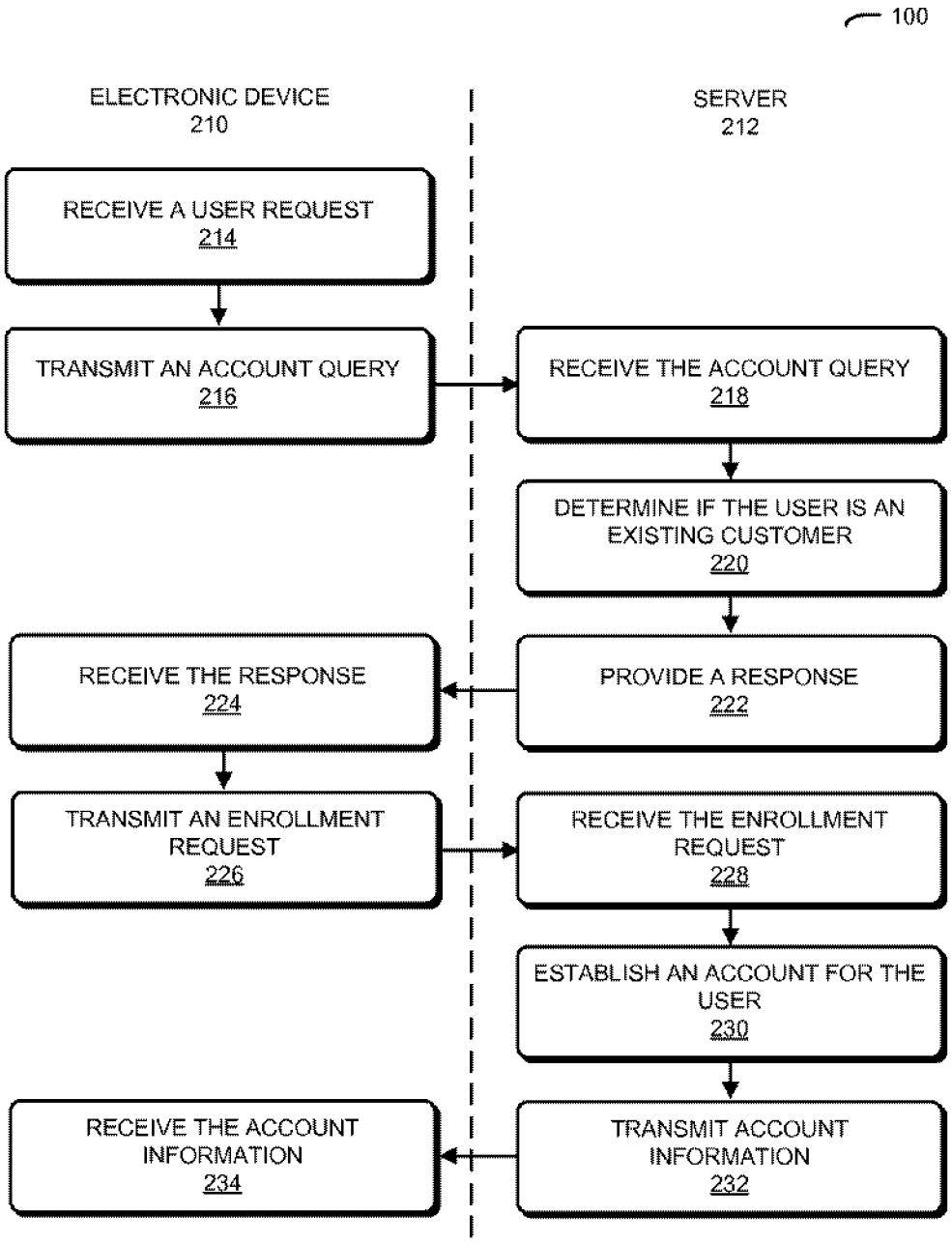

100
ELECTRONIC DEVICE
210
SERVER
212
RECEIVE A USER REQUEST
214
TRANSMIT AN ACCOUNT QUERY
216
RECEIVE THE ACCOUNT QUERY
218
DETERMINE IF THE USER IS AN EXISTING CUSTOMER
220
PROVIDE A RESPONSE
222
RECEIVE THE RESPONSE
224
TRANSMIT AN ENROLLMENT REQUEST
226
RECEIVE THE ENROLLMENT REQUEST
228
ESTABLISH AN ACCOUNT FOR THE USER
230
TRANSMIT ACCOUNT INFORMATION
232
RECEIVE THE ACCOUNT INFORMATION
234

FIG. 2

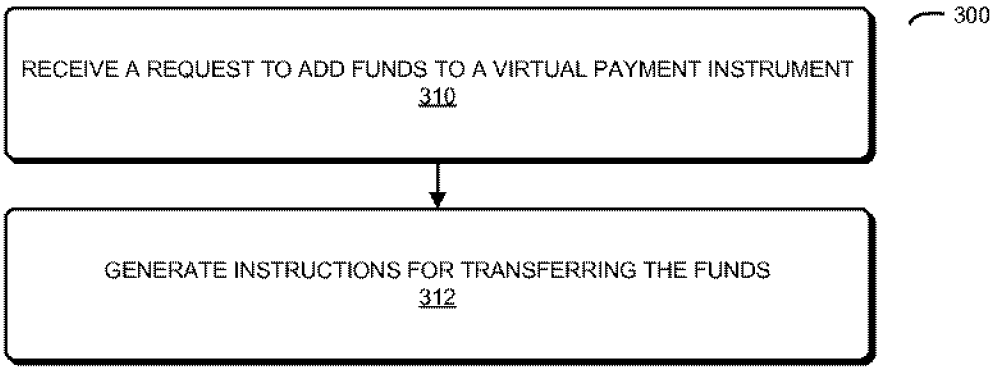

300
RECEIVE A REQUEST TO ADD FUNDS TO A VIRTUAL PAYMENT INSTRUMENT
310
GENERATE INSTRUCTIONS FOR TRANSFERRING THE FUNDS
312

FIG. 3

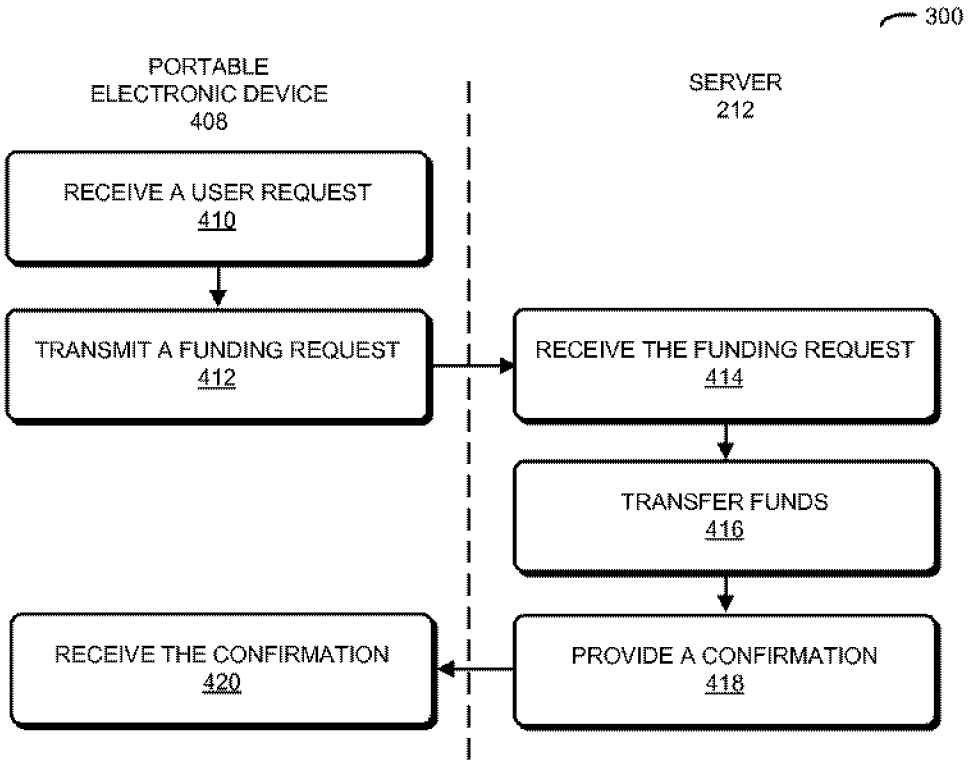

300
PORTABLE ELECTRONIC DEVICE 408
SERVER 212
RECEIVE A USER REQUEST 410
TRANSMIT A FUNDING REQUEST 412
RECEIVE THE FUNDING REQUEST 414
TRANSFER FUNDS 416
PROVIDE A CONFIRMATION 418
RECEIVE THE CONFIRMATION 420

FIG. 4

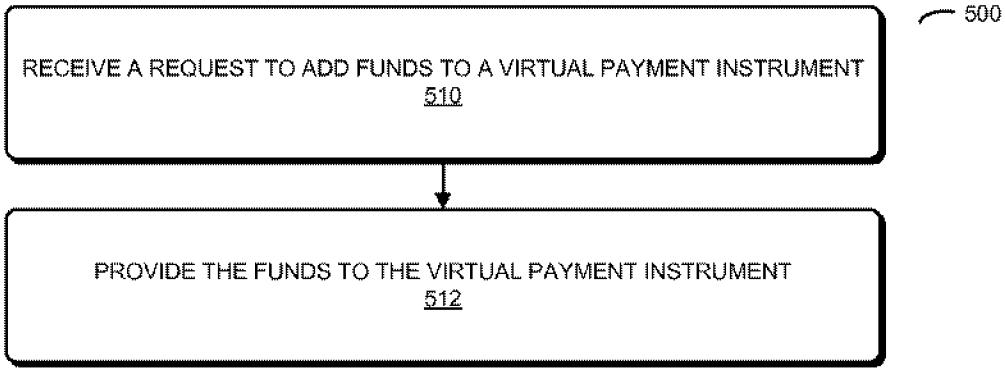

500
RECEIVE A REQUEST TO ADD FUNDS TO A VIRTUAL PAYMENT INSTRUMENT
510
PROVIDE THE FUNDS TO THE VIRTUAL PAYMENT INSTRUMENT
512

FIG. 5

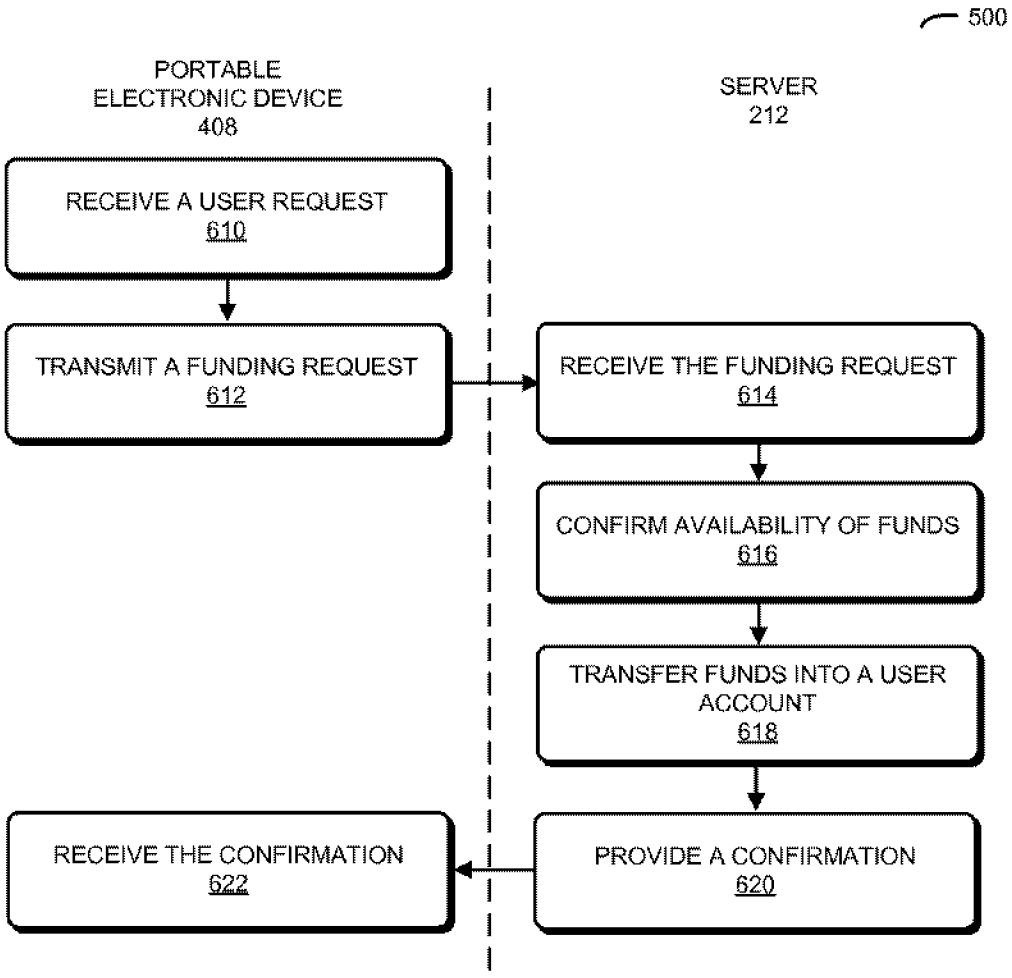

500
PORTABLE ELECTRONIC DEVICE 408
SERVER 212
RECEIVE A USER REQUEST 610
TRANSMIT A FUNDING REQUEST 612
RECEIVE THE FUNDING REQUEST 614
CONFIRM AVAILABILITY OF FUNDS 616
TRANSFER FUNDS INTO A USER ACCOUNT 618
PROVIDE A CONFIRMATION 620
RECEIVE THE CONFIRMATION 622

FIG. 6

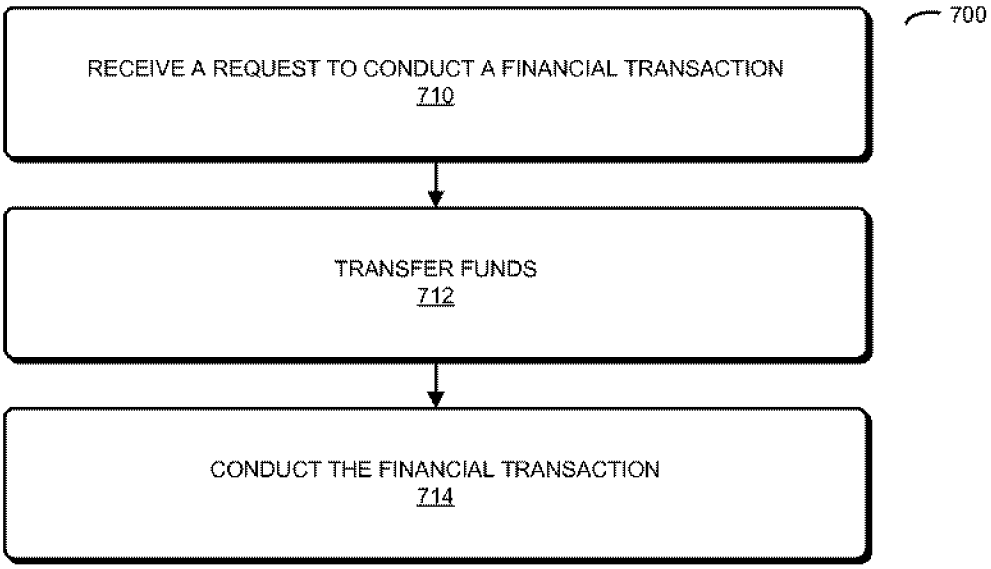

700
RECEIVE A REQUEST TO CONDUCT A FINANCIAL TRANSACTION
710
TRANSFER FUNDS
712
CONDUCT THE FINANCIAL TRANSACTION
714

FIG. 7

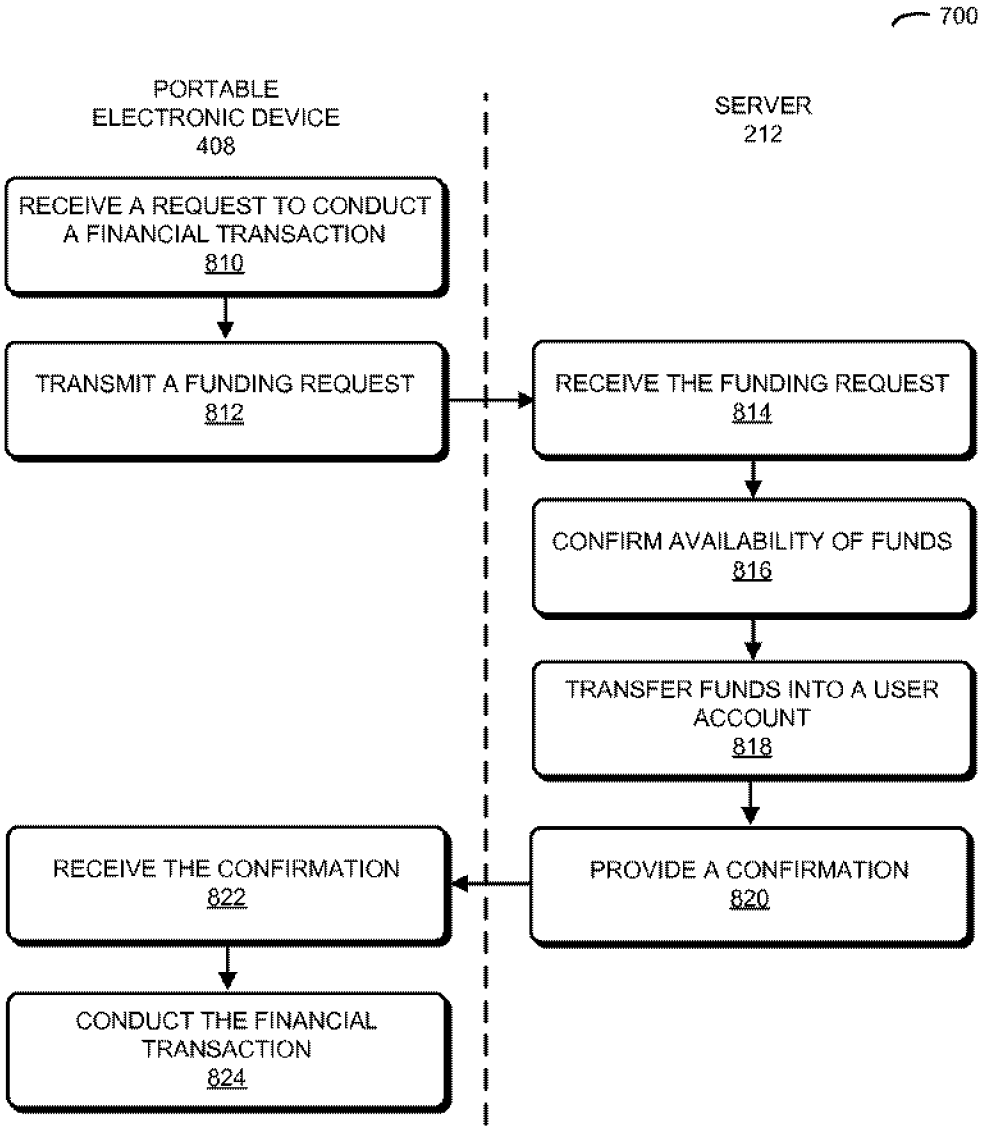

700
PORTABLE ELECTRONIC DEVICE 408
SERVER 212
RECEIVE A REQUEST TO CONDUCT A FINANCIAL TRANSACTION 810
TRANSMIT A FUNDING REQUEST 812
RECEIVE THE FUNDING REQUEST 814
CONFIRM AVAILABILITY OF FUNDS 816
TRANSFER FUNDS INTO A USER ACCOUNT 818
PROVIDE A CONFIRMATION 820
RECEIVE THE CONFIRMATION 822
CONDUCT THE FINANCIAL TRANSACTION 824

FIG. 8

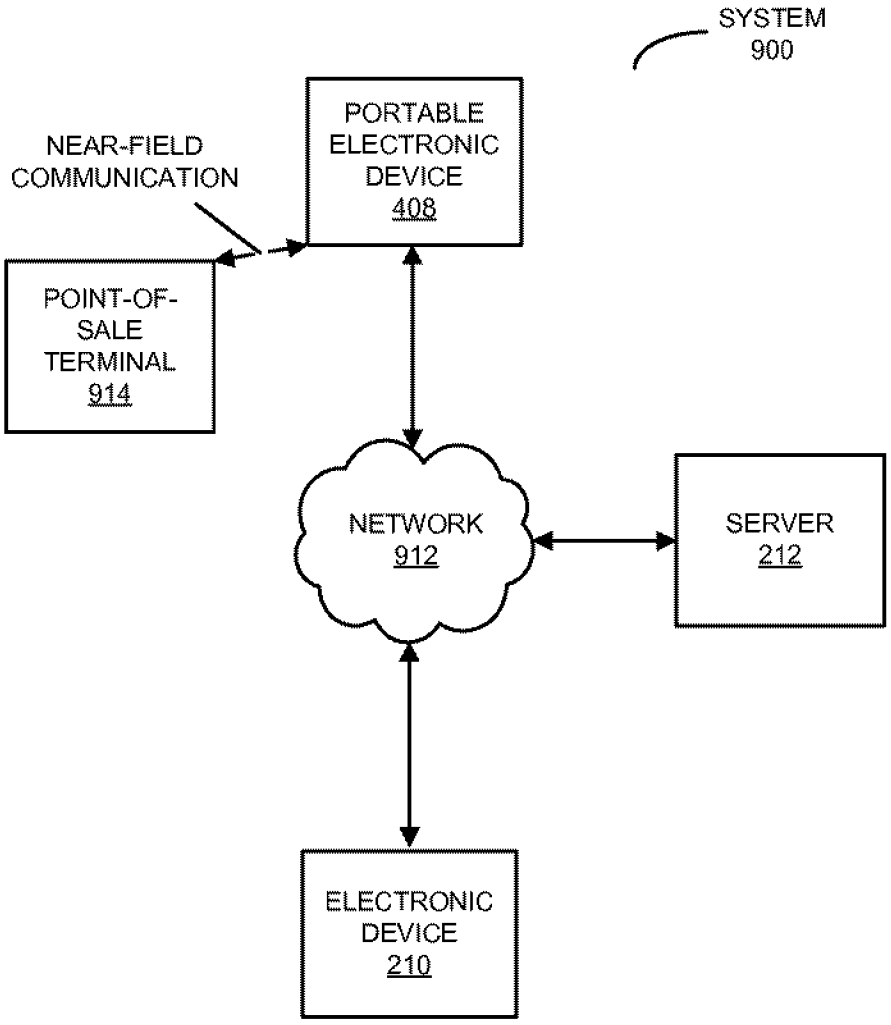

SYSTEM
900
PORTABLE ELECTRONIC DEVICE
408
NEAR-FIELD COMMUNICATION
POINT-OF-SALE TERMINAL
914
NETWORK
912
SERVER
212
ELECTRONIC DEVICE
210

FIG. 9

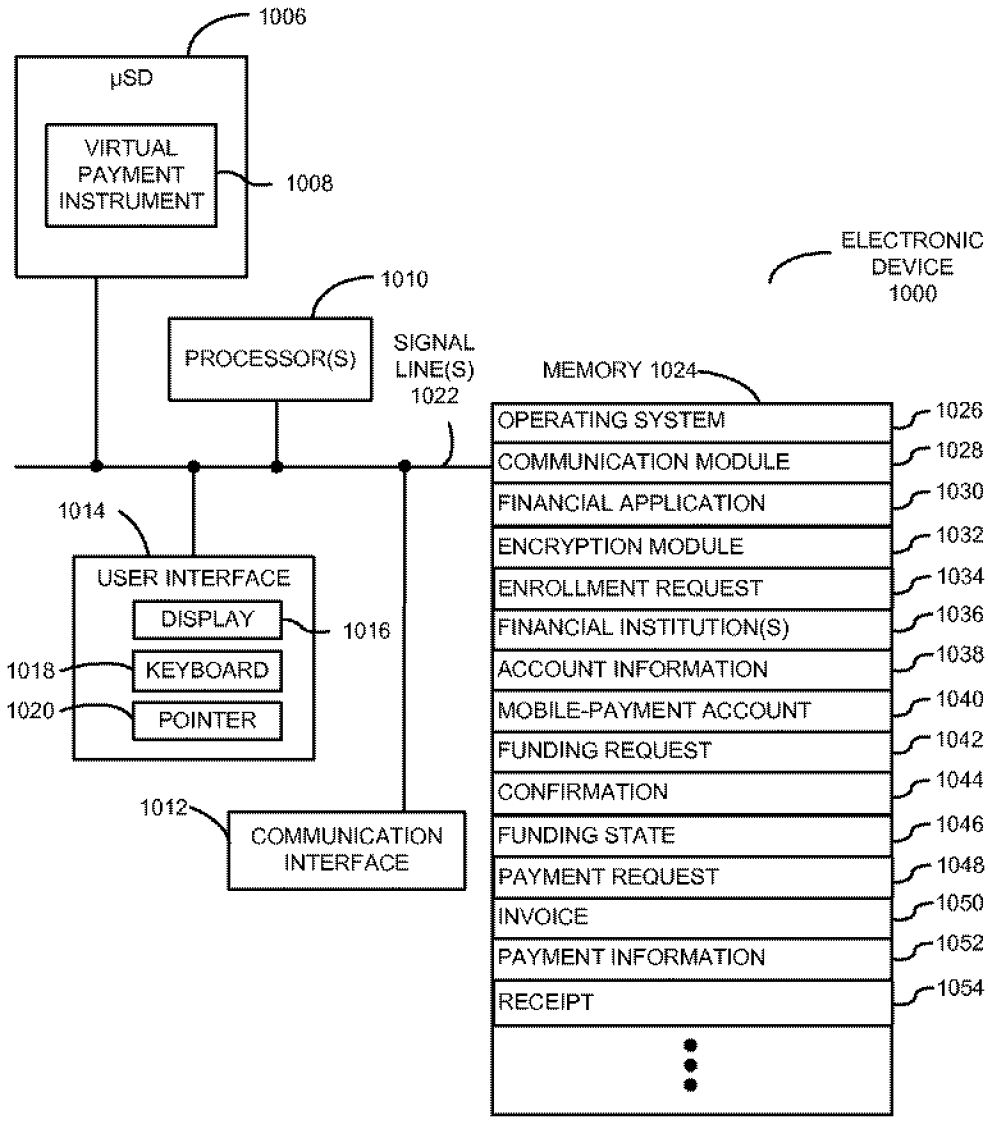

1006
µSD
VIRTUAL PAYMENT INSTRUMENT
1008
ELECTRONIC DEVICE 1000
1010
PROCESSOR(S)
SIGNAL LINE(S) 1022
MEMORY 1024
OPERATING SYSTEM
COMMUNICATION MODULE
FINANCIAL APPLICATION
ENCRYPTION MODULE
ENROLLMENT REQUEST
FINANCIAL INSTITUTION(S)
ACCOUNT INFORMATION
MOBILE-PAYMENT ACCOUNT
FUNDING REQUEST
CONFIRMATION
FUNDING STATE
PAYMENT REQUEST
INVOICE
PAYMENT INFORMATION
RECEIPT
1026
1028
1030
1032
1034
1036
1038
1040
1042
1044
1046
1048
1050
1052
1054
1014
USER INTERFACE
DISPLAY
1016
1018
KEYBOARD
1020
POINTER
1012
COMMUNICATION INTERFACE

FIG. 10

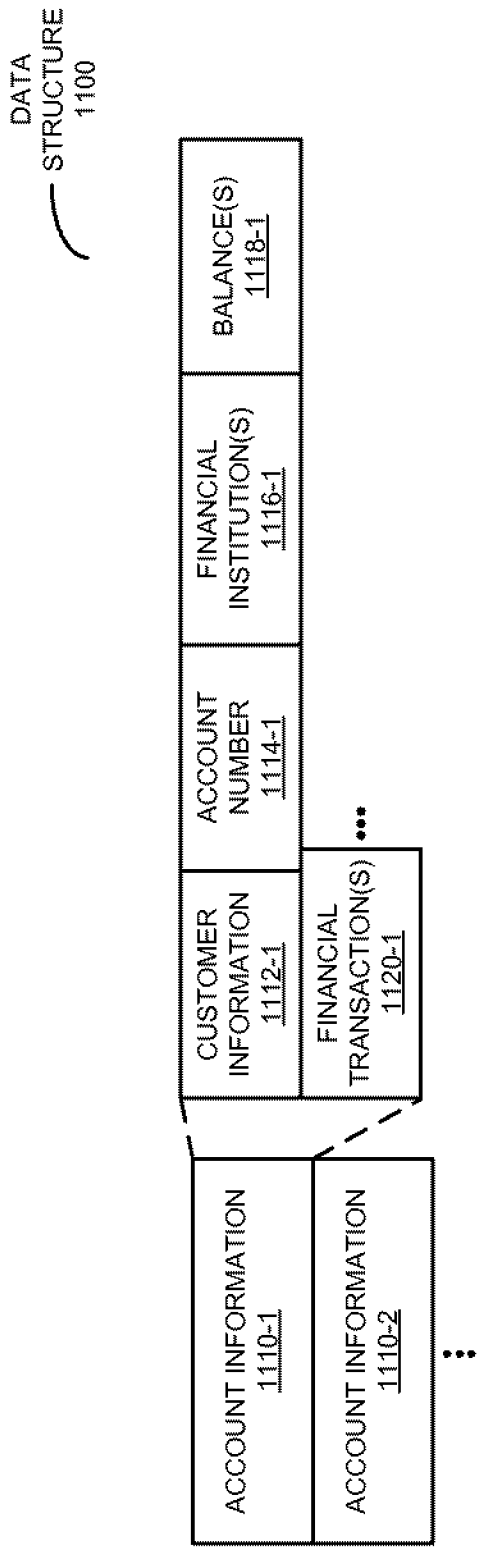

DATA STRUCTURE 1100
ACCOUNT INFORMATION 1110-1
ACCOUNT INFORMATION 1110-2
CUSTOMER INFORMATION 1112-1
ACCOUNT NUMBER 1114-1
FINANCIAL INSTITUTION(S) 1116-1
BALANCE(S) 1118-1
FINANCIAL TRANSACTION(S) 1120-1

FIG. 11

MOBILE PAYMENT SERVICE FOR SMALL FINANCIAL INSTITUTIONS

FIELD

[0001] The present disclosure relates to techniques offering a mobile-payment function to customers of small financial institutions based on a pre-paid financial instrument.

SUMMARY

[0002] The disclosed embodiments relate to an electronic device that enrolls a user in a financial service. During operation, the electronic device receives a user request to enroll in the financial service associated with a provider that facilitates financial transactions via a financial application that executes on the electronic device. Then, the electronic device determines that the user is an existing customer of one of a set of financial institutions that have a business relationship with the provider, where the provider is other than one of the financial institutions. Next, the electronic device enrolls the user in the financial service without requesting additional information from the user.

[0003] Note that the financial transactions may include: making a deposit into a financial account (which may be associated with a pre-paid financial instrument), paying at the point of sale, and/or viewing a summary of the financial account.

[0004] Another embodiment provides a portable electronic device that facilitates transfer of funds for a financial service. During operation, the portable electronic device receives a user request to add funds to a virtual payment instrument associated with the portable electronic device, where the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device. Then, the portable electronic device generates instructions for transferring funds between two financial accounts associated with financial institutions that have a business relationship with a provider of the financial service, where the two financial accounts may be with a financial institution that is associated with the provider, and the funds are transferred without requesting additional (e.g., detailed) payment information from the user.

[0005] Note that the funds may be transferred between the two financial accounts with or without a delay, and/or maybe available to the user with or without a delay.

[0006] Another embodiment provides a portable electronic device that provides funding to a virtual payment instrument. During operation, the portable electronic device receives a user request to add funds to the virtual payment instrument associated with the portable electronic device, where the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device, and the virtual payment instrument is a virtual representation of a financial instrument that is other than a physical financial instrument. In response to the request, the portable electronic device provides the funds to the virtual payment instrument.

[0007] Note that a physical financial instrument corresponding to the virtual payment instrument may not exist. Moreover, the request may be based on proximity of the portable electronic device to another electronic device. Furthermore, note that multiple physical financial instruments may correspond to the virtual payment instrument.

[0008] Another embodiment provides a portable electronic device that facilitates a secure financial transaction. During operation, the portable electronic device receives a request to conduct the financial transaction via a financial application that combines banking on the portable electronic device with mobile payments. In response to the request, the portable electronic device transfers funds from a financial account of a user of the portable electronic device with a financial institution to a virtual payment instrument associated with the portable electronic device, where the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device. Then, the portable electronic device conducts the financial transaction using the financial application.

[0009] Note that the transferring of the funds and the conducting of the financial transaction may occur without user action. Furthermore, if network connectivity between the portable electronic device and the financial institution is unavailable, the portable electronic device may receive an identifier from the user to authenticate the user. Additionally, transferring the funds may leverage historical information about the financial account stored in the virtual payment instrument.

[0010] In some embodiments, conducting the financial transaction within the limit of funds pre-paid to the virtual payment instrument occurs without user authentication or another user action.

[0011] Another embodiment provides one or more methods that include at least some of the operations performed by one or more of the embodiments of the portable electronic device.

[0012] Another embodiment provides one or more computer-program products for use with one or more of the embodiments of the portable electronic device. These one or more computer-program products include instructions for at least some of the operations performed by one or more of the embodiments of the portable electronic device.

BRIEF DESCRIPTION OF THE FIGURES

[0013] FIG. **1** is a flow chart illustrating a method for enrolling a user in a financial service in accordance with an embodiment of the present disclosure.

[0014] FIG. **2** is a flow chart illustrating the method of FIG. **1** in accordance with an embodiment of the present disclosure.

[0015] FIG. **3** is a flow chart illustrating a method for funding a financial service in accordance with an embodiment of the present disclosure.

[0016] FIG. **4** is a flow chart illustrating the method of FIG. **3** in accordance with an embodiment of the present disclosure.

[0017] FIG. **5** is a flow chart illustrating a method for providing funding to a virtual payment instrument in accordance with an embodiment of the present disclosure.

[0018] FIG. **6** is a flow chart illustrating the method of FIG. **5** in accordance with an embodiment of the present disclosure.

[0019] FIG. **7** is a flow chart illustrating a method for providing a secure financial transaction in accordance with an embodiment of the present disclosure.

[0020] FIG. **8** is a flow chart illustrating the method of FIG. **7** in accordance with an embodiment of the present disclosure.

[0021] FIG. **9** is a block diagram illustrating a system that performs the methods of FIGS. **1-8** in accordance with an embodiment of the present disclosure.

[0022] FIG. **10** is a block diagram illustrating a portable electronic device that performs the methods of FIG. **1-8** in accordance with an embodiment of the present disclosure.

[0023] FIG. **11** is a block diagram illustrating a data structure for use with the portable electronic device of FIG. **10** in accordance with an embodiment of the present disclosure.

[0024] Note that like reference numerals refer to corresponding parts throughout the drawings. Moreover, multiple instances of the same part are designated by a common prefix separated from an instance number by a dash.

DETAILED DESCRIPTION

[0025] Embodiments of an electronic device, a portable electronic device, a technique for implementing financial services on the portable electronic device, and a computer-program product (e.g., software) for use with the portable electronic device are described. During this financial technique, a user of the portable electronic device provides a request to enroll in a financial service (such as a mobile-payment service) associated with a provider. For example, the financial service may facilitate financial transactions via a financial application that executes on the portable electronic device. Then, the electronic device determines that the user is an existing customer of at least one of a set of financial institutions that have a business relationship with the provider, where the provider is other than one of the financial institutions. Next, the electronic device enrolls the user in the financial service without requesting additional information from the user.

[0026] By leveraging the business relationship between the user and one of the financial institutions in the set of financial institutions, the user may not have to perform a complicated enrollment process in order to start using the financial service. In particular, the user may not have to provide additional financial information. This 'instant' activation of the financial service may greatly simplify the enrollment process for the user, reducing its duration and eliminating multiple operations. Furthermore, via the set of financial institutions, the provider may be able to instantly fund the financial service on the portable electronic device (for example, by providing funds for mobile payments). Indeed, the portable electronic device may be used as a virtual payment instrument for the user (thereby obviating the need for a corresponding physical payment instrument, such as a debit or credit card). In addition, the financial application may also offer online banking (and other services), thereby offering the user convenience and enhanced security. In this way, the financial technique may improve the user's customer experience and increase their satisfaction, which may make it more likely that the user will use the portable electronic device to conduct financial transactions. Therefore, the financial technique may promote commercial activity.

[0027] In the discussion that follows, a user may include: an individual (for example, an existing customer, a new customer, a service provider, a vendor, a contractor, etc.), an organization, a business and/or a government agency. Furthermore, a 'business' should be understood to include: for-profit corporations, non-profit corporations, organizations, groups of individuals, sole proprietorships, government agencies, partnerships, etc.

[0028] We now describe embodiments of the financial technique, which may be performed by an electronic device (such as electronic device **1000** in FIG. **10**) in a system (such as system **900** in FIG. **9**). Note that the electronic device may or may not be portable. FIG. **1** presents a flow chart illustrating a method **100** for enrolling a user in a financial service. During operation, the electronic device receives a user request (operation **110**) to enroll in the financial service (such as a mobile-payment service) associated with a provider that facilitates financial transactions via a financial application (such as a mobile-payment application) that executes on a portable electronic device. For example, the financial transactions may include: making a deposit into a financial account, paying at a point of sale, and/or viewing a summary of the financial account.

[0029] Then, the electronic device determines that the user is an existing customer of one of a set of financial institutions (operation **112**) that have a business relationship with the provider, where the provider is other than one of the financial institutions. For example, the set of financial institutions may include banks, such as small banks (which do not have the infrastructure needed to offer the financial service to their customers and instead use the service offered by the provider.) Next, the electronic device enrolls the user in the financial service (operation **114**) without requesting additional information from the user by leveraging the existing business relationship between the user and the financial institution and the financial institution and the provider.

[0030] In some embodiments, the electronic device optionally activates a mobile payment financial service without requesting additional information from the user (not shown).

[0031] In an exemplary embodiment, method **100** is implemented using an electronic device (such as a computer or a server) and at least one server (which is associated with and is used by the provider), which communicate through a network, such as a cellular-telephone network and/or the Internet (e.g., using a client-server architecture). This is shown in FIG. **2**, which presents a flow chart illustrating method **100**. During this method, electronic device **210** receives the user request (operation **214**) to enroll in the financial service associated with the provider that facilitates financial transactions via the financial application that executes on a portable electronic device (not shown).

[0032] In response to the user request, electronic device **210** determines if the user is an existing customer of one of the set of financial institutions that have the business relationship with the provider. For example, electronic device **210** may transmit an account query (operation **216**) to server **212** (which is associated with the provider). After receiving the account query (operation **218**), server **212** accesses a data structure to determine if the user is an existing customer (operation **220**). Then, server **212** provides a response (operation **222**) which indicates whether or not the user is an existing customer.

[0033] After receiving the response (operation **224**), electronic device **210** enrolls the user in the financial service without requesting additional (detailed) information from the user. For example, electronic device **210** may transmit an enrollment request (operation **226**) to server **212**. After the enrollment request is received (operation **228**), server **212** may establish an account for the user (operation **230**) based on user financial information that is known to the provider (for example, the financial information, which may be stored in a data structure, may have been shared by one of the financial institutions in the set of financial institutions). Next, server **212** transmits account information (operation **232**), which is subsequently received (operation **234**) by electronic device **210**.

[0034] By leveraging an existing relationship between at least one of the set of financial institutions and the user or the customer, this financial technique may facilitate instant enrollment or provisioning (i.e., instant activation) of mobile payments and/or other financial services via the financial application. Because the user's financial information is known to the provider, the provider does not have to obtain additional information (for example, by asking additional questions) before enrolling the user and activating the mobile-payment service (via the financial application) on electronic device **210**.

[0035] Note that the provider may have previously provided the financial application to the set of financial institutions, which in turn provided it to their customers for use on portable electronic devices. Alternatively, the users or customers may have received the financial application from the provider. As described further below, once installed on the users' portable electronic devices, the financial application can be used to manage the users' relationships with the set of financial institutions.

[0036] FIG. **3** presents a flow chart illustrating a method **300** for facilitating the transfer of funds for a financial service, which may be performed by a portable electronic device (such as electronic device **1000** in FIG. **10**) in a system (such as system **900** in FIG. **9**). During operation, the portable electronic device receives a user request to add funds to a virtual payment instrument (operation **310**) associated with the portable electronic device, where the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device. Then, the portable electronic device generates instructions for transferring the funds (operation **312**) between two financial accounts associated with financial institutions that have a business relationship with a provider of the financial service, where the two financial accounts may be with a financial institution that is associated with the provider, and the funds are transferred without requesting additional (detailed) payment information from the user. Note that the funds may be transferred between the two financial accounts with or without a delay, and/or maybe available to the user with or without a delay.

[0037] In an exemplary embodiment, method **300** is implemented using a portable electronic device (such as a cellular telephone or a computer) and at least one server (which is associated with and is used by the provider), which communicate through a network, such as a cellular-telephone network and/or the Internet (e.g., using a client-server architecture). This is shown in FIG. **4**, which presents a flow chart illustrating method **300**. During this method, portable electronic device **408** receives the user request (operation **410**) to add funds to the virtual payment instrument associated with portable electronic device **408**.

[0038] Then, portable electronic device **408** provides the funds by transferring funds between two financial accounts associated with financial institutions that have the business relationship with the provider of the financial service. For example, portable electronic device **408** may transmit a funding request (operation **412**) to server **212**. After receiving this request (operation **414**), server **212** may transfer the funds (operation **416**) between the two financial accounts. Then, server **212** may provide a confirmation (operation **418**) of the fund transfer that is received (operation **420**) by portable electronic device **408**.

[0039] In some embodiments, portable electronic device **408** includes a virtual payment instrument that is implemented as a software object in a secure element (such as an encrypted chip) on portable electronic device **408**. This virtual payment instrument (or virtual object) may function as a general purpose reloadable card that can be 'instantly' funded (i.e., there is real-time access to funds at little or no cost). This may be possible because the fund transfer needed may not be occurring between two banks, which is usually the case with an automated clearing house. Instead, two different transfers are made, each within a single financial institution. Thus, the money or funds may be 'moved' immediately between the user accounts and the financial accounts maintained by the provider (i.e., the fund transfer occurs inside one financial institution, as opposed to between financial institutions, so it is instantaneous). For example, the user's mobile payment account may be with the provider and, because of the business relationship between the set of financial institutions and the provider, information about the user's financial account (such as a bank account) with at least one of the set of financial institutions may also be available to the provider. Therefore, the provider may have access to an account balance and a financial transaction history associated with the user's financial account. This may allow the provider to temporarily float the funds to the user's mobile-payment account with little or no risk. Subsequently, the funds may be repaid to the provider by at least one of the set of financial institutions that provides financial services (including the financial account) to the user. Note that, because the provider has access to the user's financial information based on the provider's business relationships with the set of financial institutions, the funds may be transferred by the provider (i.e., the mobile-payment service may be provisioned) without requesting (detailed) payment information from the user.

[0040] FIG. **5** presents a flow chart illustrating a method **500** for providing funding to a virtual payment instrument, which may be performed by a portable electronic device (such as electronic device **1000** in FIG. **10**) in a system (such as system **900** in FIG. **9**). During operation, the portable electronic device receives a user request to add funds to the virtual payment instrument (operation **510**) associated with the portable electronic device, where the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device, and the virtual payment instrument is a virtual representation of a financial instrument that is other than a physical financial instrument. In response to the request, the portable electronic device provides the funds to the virtual payment instrument (operation **512**).

[0041] Note that a physical financial instrument corresponding to the virtual payment instrument may not exist. Moreover, note that multiple physical financial instruments may correspond to the virtual payment instrument. Furthermore, the request may be based on proximity of the portable electronic device to another electronic device. For example, by tapping the portable electronic device on a point-of-sale terminal or a bank machine, funds may be provided to or withdrawn from the virtual payment instrument.

[0042] In an exemplary embodiment, method **500** is implemented using a portable electronic device (such as a cellular telephone or a computer) and at least one server (which is associated with and is used by the provider), which communicate through a network, such as a cellular-telephone network and/or the Internet (e.g., using a client-server architecture). This is shown in FIG. **6**, which presents a flow chart illustrating method **500**. During this method, portable elec-

tronic device **408** receives the user request (operation **610**) to add funds to the virtual payment instrument associated with portable electronic device **408**.

[0043] In response to the request, portable electronic device **408** provides the funds to the virtual payment instrument. For example, portable electronic device **408** may transmit a funding request (operation **612**) to server **212**. After receiving the funding request (operation **614**), server **212** may confirm the availability of funds (operation **616**) in one or more financial accounts associated with the user. (Therefore, via this link to the user's financial account with one of the set of financial institutions, the virtual payment instrument may effectively function as a prepaid, general-purpose reloadable virtual payment instrument or card.) Then, server **212** may transfer funds into a user account (operation **618**) associated with the mobile-payment service. Moreover, server **212** may provide a confirmation (operation **620**) of the funding, which is subsequently received (operation **622**) by portable electronic device **408**, thereby enabling the user to conduct financial transactions with the mobile-payment service.

[0044] As noted previously, mobile payments may be implemented using the virtual payment instrument, which is implemented as a software object in a secure element on the portable electronic device. This virtual payment instrument may function as a virtual money clip (and thus funds associated with the virtual payment instrument may be used as 'mobile money'). Moreover, the virtual payment instrument may not have a physical counterpart, i.e., it may not be associated with a real debit or credit card (and, more generally, a financial instrument). Indeed, there may not be a debit or credit card. Thus, in the financial technique the mobile payments may be based on the portable electronic device, as opposed to a debit or credit card.

[0045] In this way, the mobile payments may disconnect or decouple an actual or physical payment instrument from the consumer-facing representation of the payment instrument (which, in this case, is the financial application executing on the portable electronic device). This approach is advantageous, because it enables the use of multiple and different actual or physical payment instruments as the vehicles for financial transactions conducted using the portable electronic device. In this way, the user is freed from complexity of managing multiple payment instruments. This financial technique also enables the provider of the financial service to offer the financial service on behalf of multiple small financial institutions. Additionally, this financial technique may allow the provider to offer a white-label payment service to the customers of multiple small financial institutions without the complexity associated with working with multiple different issuers of payment instruments.

[0046] In method **500**, the user may 'top up' or add funds to the virtual payment instrument via the financial application. For example, when the user activates a physical icon on a keypad or a virtual icon on a touchscreen, the financial application may inquire if the user would you like to make a mobile payment. If yes, a virtual money-clip icon may be displayed. In addition, the user can put 'money' into the virtual money clip, for example, directly from the user's debit account. Thus, the user can top up the virtual money clip, just like using an automated teller machine. If the user taps a point-of-sale terminal that is configured to conduct contactless payments (for example, using near-field communication, wireless communication and/or another type of communication), and funds first need to be added to the user's mobile-payment account, method **500** may be performed before the mobile payment (and, more generally, a financial transaction) is conducted.

[0047] FIG. **7** presents a flow chart illustrating a method **700** for providing a secure financial transaction, which may be performed by a portable electronic device (such as electronic device **1000** in FIG. **10**) in a system (such as system **900** in FIG. **9**). During operation, the portable electronic device receives a request to conduct the financial transaction (operation **710**) via a financial application that combines banking on the portable electronic device with mobile payments. In response to the request, the portable electronic device transfers funds (operation **712**) from a financial account of a user of the portable electronic device with a financial institution to a virtual payment instrument associated with the portable electronic device, where the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device. Then, the portable electronic device conducts the financial transaction (operation **714**) using the financial application.

[0048] Note that the transferring of the funds and the conducting of the financial transaction may occur without user action. Furthermore, if network connectivity between the portable electronic device and the financial institution is unavailable, the portable electronic device may receive an identifier from the user to authenticate the user (for example, based on stored authentication information on the portable electronic device or the secure element). Additionally, transferring the funds may leverage historical information about the financial account stored in the virtual payment instrument. In this way, even if network connectivity is lost, the portable electronic device may be able to confirm that funds are available for a financial transaction.

[0049] In some embodiments, conducting the financial transaction within the limit of funds pre-paid to the virtual payment instrument occurs without user authentication or other user action.

[0050] In an exemplary embodiment, method **700** is implemented using a portable electronic device (such as a cellular telephone or a computer) and at least one server (which is associated with and is used by the provider), which communicate through a network, such as a cellular-telephone network and/or the Internet (e.g., using a client-server architecture). This is shown in FIG. **8**, which presents a flow chart illustrating method **700**. During this method, portable electronic device **408** receives a request (operation **810**) to conduct the financial transaction via the financial application that combines banking on the portable electronic device with mobile payments.

[0051] In response to the request, portable electronic device **408** transfers funds from a financial account of a user of the portable electronic device with a financial institution to the virtual payment instrument associated with the portable electronic device. For example, portable electronic device **408** may transmit a funding request (operation **812**) to server **212**. After receiving the funding request (operation **814**), server **212** may confirm the availability of funds (operation **816**) in one or more financial accounts associated with the user. Then, server **212** may transfer funds into a user account (operation **818**) associated with the mobile-payment service. Moreover, server **212** may provide a confirmation (operation **820**) of the funding, which is subsequently received (operation **822**) by portable electronic device **408**.

[0052] Next, portable electronic device **408** conducts the financial transaction using the financial application (operation **824**). For example, using near-field communication, the financial application may communicate with a point-of-sale terminal to receive an invoice and to provide corresponding payment information.

[0053] Thus, in some embodiments the financial application may combine online banking with mobile payments on portable electronic device **408** (which is collectively sometimes referred to as a 'mobile-banking application'). This approach may provide convenience to the user (for example, the user can review their financial account balance before making a purchase or conducting a financial transaction) and enhance security without requiring that the user provide additional verification information. Furthermore, the user can transfer funds to an account associated with the mobile-payment service and can make payments using a single financial application.

[0054] This integrated solution may also allow the user to use the mobile-payment service even when there is no network connectivity (and, more generally, no communication) between portable electronic device **408** and server **212**. In this case, the user can log in to the financial application by providing a username and password, a PIN or an identifier (and, more generally, authentication information). Then, leveraging cached financial-account information in the secure element on portable electronic device **408** (which may include a latest update of the financial-account balance(s) and recent financial transactions), the financial application may have access to the information needed to transfer funds (if needed) to a financial account associated with the mobile-payment service and to allow the user to conduct one or more financial transactions (such as making a mobile payment). Thus, while embodiments of the financial technique were illustrated using a client-server architecture in FIGS. **2**, **4**, **6** and **8**, in some embodiments the financial technique may be performed by the financial application without real-time interaction with server **212**.

[0055] In some embodiments, the payment capability does not require any authentication and thus can be performed with a single tap of the portable electronic device on the point of sale without any other user action (such as entering a PIN or a password). However, transferring funds to mobile payment account may require authentication. In this way, the risk of loosing the funds if the portable electronic device is lost may be limited to the small balance maintained in the mobile payment account only. This approach trades off the convenience of frictionless payment experience and financial risk.

[0056] In an exemplary embodiment, the financial application enables a mobile-payment service for customers of small banks (and, more generally, small financial institutions). This mobile-payment service may not require consumers to create new financial relationships, or to provide significant amounts of financial information to enroll, fund or use the mobile-payment service. In particular, a customer may be enrolled in the mobile-payment service by their bank, for example, during a visit to a branch, during an online or mobile-banking session, or in another context where a previously established identity of a customer is authenticated. Because the enrollment in the mobile-payment service occurs via the existing relationships with the bank, no new information is required, thereby eliminating the need for any additional interaction with the customer.

[0057] Moreover, a virtual general purpose reloadable (GPR) payment card (i.e., the virtual payment instrument) may be provisioned to the customer's portable electronic device (such as their cellular telephone), either via over-the-air (OTA) provisioning or on a secure hardware add-on device, such as a micro SD (μSD) card. For example, OTA provisioning may be performed to the embedded secure element of the portable electronic device identified by the authenticated customer. Alternatively, a μSD may be mailed to the known address of the customer along with installation instructions.

[0058] After the virtual payment instrument or card has been provisioned to the customer's portable electronic device, when the customer initiates an authenticated mobile-banking session, the newly provisioned virtual payment instrument may be activated without any additional user interaction. Then, the mobile-banking application (i.e., the financial application) can offer the customer new capabilities and services that are enabled by the virtual payment instrument. For example, funds can be moved in real-time between the customer's designated (or default) bank account and the account of the virtual payment instrument (and, thus, the account associated with the mobile-payment service) without requiring a setup procedure. Thus, by leveraging an existing banking relationship in combination with a virtual GPR payment card, instant enrollment, instant funding and efficient provisioning can all be provided to the customer. Furthermore, use of the virtual GPR payment card may be transparent to the customer.

[0059] In an exemplary embodiment, the provider of the mobile-payment service may request that a prepaid processor create prepaid virtual-payment-card accounts for customers of a bank. In response, the prepaid processor may provide vendor card files to a card vendor/personalization bureau.

[0060] If the virtual payment instruments are provisioned on μSD-based add-on devices, the process may involve the provider requesting that an add-on device manufacturer provide a batch of μSDs along with keys for secure elements on the μSDs to the card vendor/personalization bureau. Then, the card vendor/personalization bureau may provision the μSDs with the financial application, and may personalize each μSD with customer-account information.

[0061] When a customer of the bank signs up for the mobile-payment service, they may receive a μSD with a prepaid virtual payment instrument and they may install the μSD in their portable electronic device. Note that the provider may associate the prepaid virtual-payment-card account with the identity of the customer. Then, when the customer logs in to the financial application using their existing credentials, the financial application obtains from the secure element information that allows the provider to identify the prepaid virtual-payment-card account and to associate it (or to verify the association) with the identity of the customer.

[0062] Alternatively, the virtual payment instruments may be provisioned OTA to secure elements that are already embedded in or added-on to portable electronic devices (for example, by a manufacturer of the portable electronic devices). In these embodiments, the vendor card files and the secure-element keys may be provided to a trusted service manager. When a user (such as a customer of a bank) logs in to the financial application and requests to activate the mobile-payment service, the financial application obtains identification information from the secure element and provides it to the trusted service manager. Using secure-element-

specific keys, the trusted service manager establishes a secure channel to the secure element and provisions a virtual payment instrument to the secure element. In this way, the prepaid virtual-payment-card account may be associated with the authenticated user.

[0063] Using either or both of these approaches, the mobile-payment functionality may be activated with minimum user interaction. Furthermore, the financial application may aggregate information about all of the user's financial accounts, and may provide payment-related functionality and mobile-banking functionality (including real-time funding of the mobile-payment or the virtual-payment-card account).

[0064] In some embodiments of methods **100** (FIGS. **1** and **2**), **300** (FIGS. **3** and **4**), **500** (FIGS. **5** and **6**) and/or **700** (FIGS. **7** and **8**), there are additional or fewer operations. Moreover, the order of the operations may be changed, and/or two or more operations may be combined into a single operation.

[0065] In the preceding methods, there are several instances of an enrollment operation of a user in the service. A variety of techniques may be used during this enrollment operation, including: using a mobile application connected the service(s) of the financial institution; using Web interface to the service(s) of the financial institution; via a phone through customer service at the financial institution; in person in a branch of the financial institution; and/or using another technique in which the user can be identified and authenticated as the principal (owner) of the relationship (the financial account) with the financial institution. Thus, using one or more of these techniques, the user may be able to link the information associated with their relationship with the financial institution and their identity with the payment-service provider.

[0066] We now describe embodiments of the system and the portable electronic device, and their use. FIG. **9** presents a block diagram illustrating a system **900** that performs the methods of FIGS. **1-8**. In this system, a user of portable electronic device **408** may use a software application or product, such as a financial software application (which is sometimes referred to as the 'financial application') that is resident on and that executes on portable electronic device **408**. (Alternatively, the user may interact with a web page that is provided by server **212** via network **912**, and which is rendered by a web browser on portable electronic device **408**. For example, at least a portion of the financial software application may be an application tool that is embedded in the web page, and which executes in a virtual environment of the web browser. Thus, the application tool may be provided to the consumer via a client-server architecture.) This financial software application may be a standalone application or a portion of another application that is resident on and which executes on portable electronic device **408** (such as a software application that is provided by server **212** or that is installed and which executes on portable electronic device **408**).

[0067] As discussed previously, the user may provide the user request to enroll in the financial service associated with the provider that facilitates financial transactions via a financial software application that executes on electronic device **210** (such as a computer or a server). For example, the user may click on a physical button or may activate a virtual icon on a touchscreen. In response to the user request, electronic device **210** may transmit the account query to server **212** via network **912**. Then, server **212** may provide a response to electronic device **210** via network **912** that indicates whether the user is an existing customer of one of the set of financial institutions that have the business relationship with the provider.

[0068] If the response indicates that the user is an existing customer, electronic device **210** may transmit an enrollment request to server **212** via network **912**. In response, server **212** may establish an account for the user based on user financial information that is known to the provider. Then, server **212** transmits account information to electronic device **210** via network **912**. In this way, the financial software application can enroll the user in the financial service without requesting additional information from the user.

[0069] After the user is enrolled, the user may request that funds be added to the virtual payment instrument associated with portable electronic device **408**. For example, the user may tap on an 'add funds' icon that is displayed on a touchscreen. In response, portable electronic device **408** may transmit a funding request to server **212** via network **912**. After receiving this request, server **212** may generate instructions for transferring the funds or may transfer the funds between the two financial accounts associated with financial institutions that have the business relationship with the provider of the financial service. Alternatively, server **212** may confirm the availability of funds in one or more financial accounts associated with the user, and may transfer funds into a user account associated with the mobile-payment service. Then, server **212** may provide a confirmation of the fund transfer to portable electronic device **408** via network **912**. In this way, the financial software application may provide real-time funding of the virtual payment instrument without requesting payment information from the user.

[0070] Once funds have been transferred to the virtual payment instrument, the user may use it to conduct mobile payments (and, more generally, financial transactions). In some embodiments, the financial software application also includes mobile-banking functionality, which may allow the user to check account balances, transfer funds, and access other services seamlessly within one integrated application. For example, in response to a request from the user to conduct a financial transaction with point-of-sale terminal **914** (for example, when the user activates a payment icon on a touchscreen), portable electronic device **408** may transmit a funding request to server **212** via network **912**. In response, server **212** may confirm the availability of funds in one or more financial accounts associated with the user, and may transfer funds into a user account associated with the mobile-payment service. Then, server **212** may provide confirmation of the funding to portable electronic device **408** via network **912**. Next, portable electronic device **408** may conduct the financial transaction with point-of-sale terminal **914**, for example, using near-field communication to exchange an invoice, payment information, and a receipt.

[0071] Note that information in system **900** may be stored at one or more locations in system **900** (i.e., locally or remotely). Moreover, because this data may be sensitive in nature, it may be encrypted. For example, stored data and/or data communicated via network **912** may be encrypted.

[0072] FIG. **10** presents a block diagram illustrating an electronic device **1000** (which may or may not be portable) that performs the methods of FIG. **1-8**. Electronic device **1000** includes one or more processing units or processors **1010**, a communication interface **1012**, a user interface **1014**, and one or more signal lines **1022** coupling these components together. Note that the one or more processors **1010** may

support parallel processing and/or multi-threaded operation, the communication interface **1012** may have a persistent communication connection, and the one or more signal lines **1022** may constitute a communication bus. Moreover, the user interface **1014** may include: a display **1016**, a keyboard **1018**, and/or a pointer **1020**, such as a monse.

[0073] Memory **1024** in electronic device **1000** may include volatile memory and/or non-volatile memory. More specifically, memory **1024** may include: ROM, RAM, EPROM, EEPROM, flash memory, one or more smart cards, one or more magnetic disc storage devices, and/or one or more optical storage devices. Memory **1024** may store an operating system **1026** that includes procedures (or a set of instructions) for handling various basic system services for performing hardware-dependent tasks. Memory **1024** may also store procedures (or a set of instructions) in a communication module **1028**. These communication procedures may be used for communicating with one or more computers and/or servers, including computers and/or servers that are remotely located with respect to electronic device **1000**.

[0074] Memory **1024** may also include multiple program modules (or sets of instructions), including: financial application **1030** (or a set of instructions), and/or encryption module **1032** (or a set of instructions). Note that one or more of these program modules (or sets of instructions) may constitute a computer-program mechanism.

[0075] In embodiments where electronic device **1000** is not a portable electronic device, during operation financial application **1030** may receive an enrollment request **1034** (for example, via user interface **1014**) to enroll in the financial service. In response, financial application **1030** may determine whether the user is an existing customer of one of the set of financial institutions **1036**. For example, as further described below with reference to FIG. **11**, financial application **1030** may access account information **1038** associated with existing customers of financial institutions **1036**. If the user is an existing customer, financial application **1030** may establish a mobile-payment account **1040** for the user without requesting additional information from the user.

[0076] Alternatively, if electronic device is a portable electronic device, after the user is enrolled financial application **1030** may receive a funding request **1042** (for example, via user interface **1014**) that funds be added to a virtual payment instrument **1008** in μSD **1006**. In response, financial application **1030** may generate instructions for transferring funds or may transfer the funds between the two financial accounts associated with financial institutions that have the business relationship with the provider of the financial service. For example, financial application **1030** may communicate with server **212** (FIGS. **2**, **4**, **6**, **8** and **9**) using communication module **1028** and communication interface **1012**. Alternatively, financial application **1030** may confirm the availability of funds in one or more financial accounts associated with the user, and may transfer funds into a user account associated with the mobile-payment service. Once the funds are transferred (for example, when financial application **1030** receives a confirmation **1044** from server **212** (FIGS. **2**, **4**, **6**, **8** and **9**) using communication module **1028** and communication interface **1012**), financial application **1030** may update a funding state **1046** associated with the mobile-payment service. Note that the current funding state may be displayed graphically (for example, using an image of a money clip) on display **1016**.

[0077] Then, financial application **1030** may be used to conduct mobile payments. For example, financial application **1030** may receive payment request **1048** (for example, via user interface **1014**). In response, using communication module **1028** and communication interface **1012**, financial application **1030** may: receive an invoice **1050**, provide payment information **1052** and receive a receipt **1054**. When payment is made, funding state **1046** may be appropriately modified.

[0078] If funding state **1046** is insufficient during a financial transaction, financial application **1030** may confirm the availability of funds in one or more financial accounts associated with the user (for example, using account information **1038**), and may transfer funds into a user account associated with the mobile-payment service. In embodiments where financial application **1030** includes mobile-banking functionality, these operations may be performed within financial application **1030**.

[0079] Account information **1038** used by financial application **1030** may be included in a data structure. This is shown in FIG. **11**, which presents a block diagram illustrating a data structure **1100** for use with electronic device **1000** (FIG. **10**). In particular, account information, such as account information **1110-1**, may include: customer information **1112-1** (such as a customer name and contact information), account number **1114-1**, financial institution **1116-1**, balance(s) **1118-1**, and/or financial transactions **1120-1**.

[0080] Referring back to FIG. **10**, because information in electronic device **1000** may be sensitive in nature, in some embodiments at least some of the data stored in memory **1024** and/or at least some of the data communicated using communication module **1028** is encrypted using encryption module **1032**.

[0081] Instructions in the various modules in memory **1024** may be implemented in: a high-level procedural language, an object-oriented programming language, and/or in an assembly or machine language. Note that the programming language may be compiled or interpreted, e.g., configurable or configured, to be executed by the one or more processors **1010**.

[0082] Although electronic device **1000** is illustrated as having a number of discrete items, FIG. **10** is intended to be a functional description of the various features that may be present in electronic device **1000** rather than a structural schematic of the embodiments described herein. In some embodiments, some or all of the functionality of electronic device **1000** may be implemented in one or more application-specific integrated circuits (ASICs) and/or one or more digital signal processors (DSPs).

[0083] Electronic device **1000** may include one of a variety of devices capable of manipulating computer-readable data or communicating such data between two or more computing systems over a network, including: a personal computer, a laptop computer, a tablet computer, a mainframe computer, a portable electronic device (such as a cellular phone or PDA), a server and/or a client computer (in a client-server architecture). Moreover, electronic device **1000** may be capable of communication via a network, such as: the Internet, World Wide Web (WWW), an intranet, a cellular-telephone network, LAN, WAN, MAN, or a combination of networks, or other technology enabling communication between computing systems.

[0084] In some embodiments one or more of the modules in memory **1024** may be associated with and/or included in a financial application **1030**. This financial application may

include planning software capable of processing financial information. Moreover, financial application **1030** may include payroll or accounting software capable of processing payroll information.

[0085] Electronic device **1000** may include fewer components or additional components. Moreover, two or more components may be combined into a single component, and/or a position of one or more components may be changed. In some embodiments, the functionality of electronic device **1000** may be implemented more in hardware and less in software, or less in hardware and more in software, as is known in the art.

[0086] In the preceding description, we refer to 'some embodiments.' Note that 'some embodiments' describes a subset of all of the possible embodiments, but does not always specify the same subset of embodiments.

[0087] The foregoing description is intended to enable any person skilled in the art to make and use the disclosure, and is provided in the context of a particular application and its requirements. Moreover, the foregoing descriptions of embodiments of the present disclosure have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the present disclosure to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present disclosure. Additionally, the discussion of the preceding embodiments is not intended to limit the present disclosure. Thus, the present disclosure is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

1-14. (canceled)

15. A portable-electronic-device-implemented method for providing a secure financial transaction, the method comprising:

using the portable electronic device, receiving a request to conduct the financial transaction via a financial application that combines banking on the portable electronic device with mobile payments;

in response to the request, transferring funds from a financial account of a user of the portable electronic device with a financial institution to a virtual payment instrument associated with the portable electronic device, wherein the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device; and

conducting the financial transaction using the financial application.

16. The method of claim **15**, wherein the transferring of the funds and the conducting of the financial transaction occur without user action.

17. The method of claim **15**, wherein, if network connectivity between the portable electronic device and the financial institution is unavailable, the method further comprises receiving an identifier from the user to authenticate the user; and

wherein transferring the funds leverages historical information about the financial account stored in the virtual payment instrument.

18. The method of claim **15**, wherein conducting the financial transaction within the limit of funds pre-paid to the virtual payment instrument occurs without user authentication.

19. A computer-program product for use in conjunction with a portable electronic device, the computer-program product comprising a non-transitory computer-readable storage medium and a computer-program mechanism embedded therein, to provide a secure financial transaction, the computer-program mechanism including:

instructions for receiving a request to conduct the financial transaction via a financial application that combines banking on the portable electronic device with mobile payments;

instructions for transferring funds from a financial account of a user of the portable electronic device with a financial institution to a virtual payment instrument associated with the portable electronic device in response to the request, wherein the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device; and

instructions for conducting the financial transaction using the financial application.

20. The computer-program product of claim **19**, wherein the transferring of the funds and the conducting of the financial transaction occur without user action.

21. The computer-program product of claim **19**, wherein, if network connectivity between the portable electronic device and the financial institution is unavailable, the computer-program mechanism further includes instructions for receiving an identifier from the user to authenticate the user; and

wherein transferring the funds leverages historical information about the financial account stored in the virtual payment instrument.

22. A portable electronic device, comprising:

a processor;

memory; and

a program module, wherein the program module is stored in the memory and configurable to be executed by the processor to provide a secure financial transaction, the program module including:

instructions for receiving a request to conduct the financial transaction via a financial application that combines banking on the portable electronic device with mobile payments;

instructions for transferring funds from a financial account of a user of the portable electronic device with a financial institution to a virtual payment instrument associated with the portable electronic device in response to the request, wherein the virtual payment instrument is implemented as a software object in a secure element on the portable electronic device; and

instructions for conducting the financial transaction using the financial application.

23. The computer-program product of claim **19**, wherein conducting the financial transaction within the limit of funds pre-paid to the virtual payment instrument occurs without user authentication.

24. The portable electronic device of claim **22**, wherein the transferring of the funds and the conducting of the financial transaction occur without user action.

25. The portable electronic device of claim **22**, wherein, if network connectivity between the portable electronic device and the financial institution is unavailable, the method further comprises receiving an identifier from the user to authenticate the user; and

wherein transferring the funds leverages historical information about the financial account stored in the virtual payment instrument.

26. The portable electronic device of claim **22**, wherein conducting the financial transaction within the limit of funds pre-paid to the virtual payment instrument occurs without user authentication.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Monroe

(10) **Pub. No.: US 2014/0099886 A1**

(43) **Pub. Date: Apr. 10, 2014**

(54) **SYSTEM AND METHOD FOR PAYMENT USING A MOBILE DEVICE**

(71) Applicant: **Joshua G. Monroe**, Wentzville, MO (US)

(72) Inventor: **Joshua G. Monroe**, Wentzville, MO (US)

(73) Assignee: **MasterCard International Incorporated**, Purchase, NY (US)

(21) Appl. No.: **13/647,560**

(22) Filed: **Oct. 9, 2012**

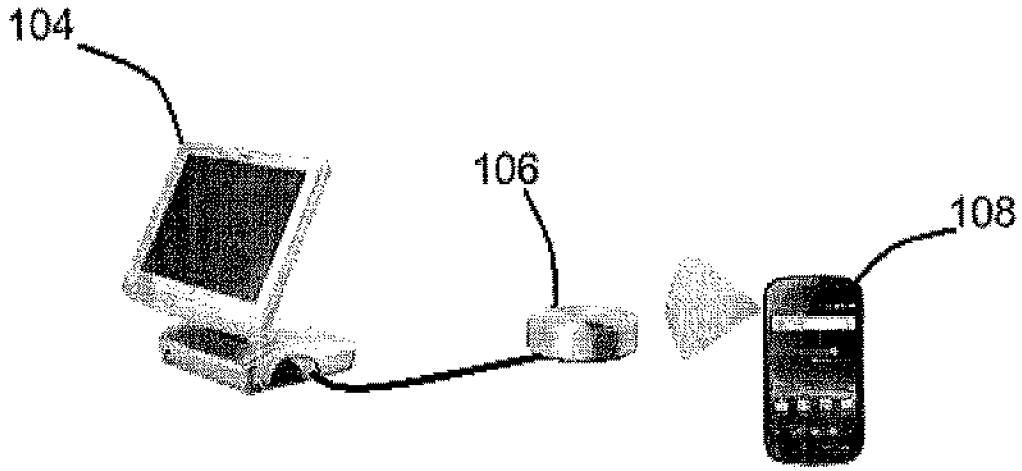
Publication Classification

(51) **Int. Cl.**
H04B 5/02 (2006.01)

(52) **U.S. Cl.**
USPC **455/41.1**

(57) **ABSTRACT**

A system and method is disclosed for a contactless payment enabled smartphone in which a user can toggle between multiple payment methods, i.e. multiple different credit/debit card accounts, by predefined user actions, alone or in combination with the act of changing the physical orientation of the smartphone, and complete a payment transaction using the selected payment method via a contactless, wireless transmission.



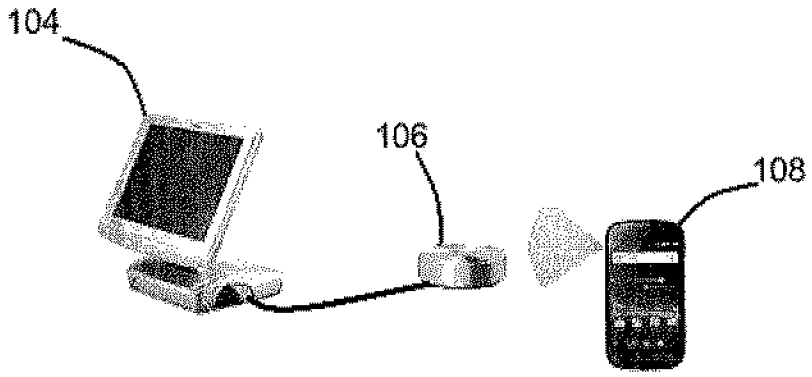

104
106
108
100

FIG. 1

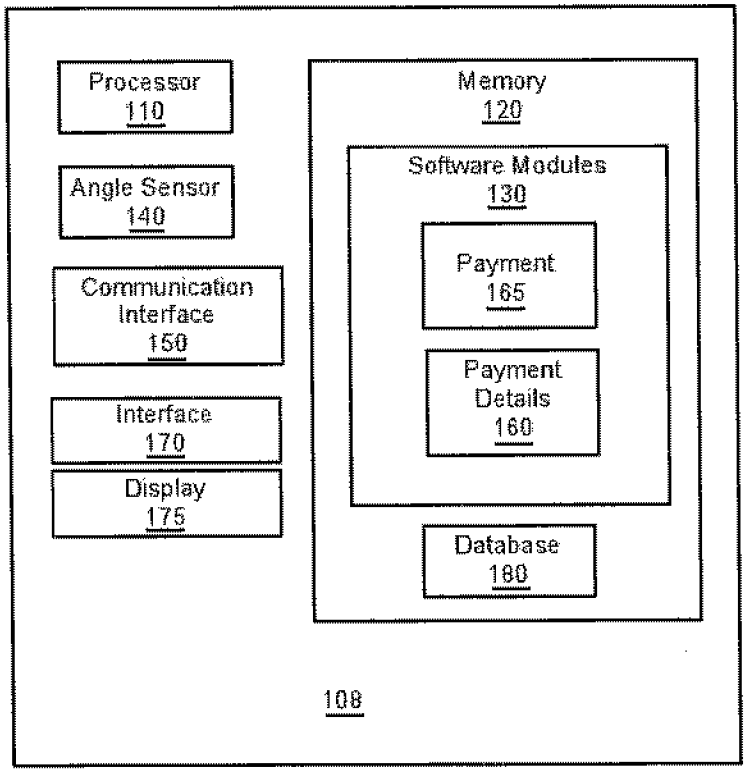

Processor
110
Angle Sensor
140
Communication Interface
150
Interface
170
Display
175
Memory
120
Software Modules
130
Payment
165
Payment Details
160
Database
180
108

FIG. 2

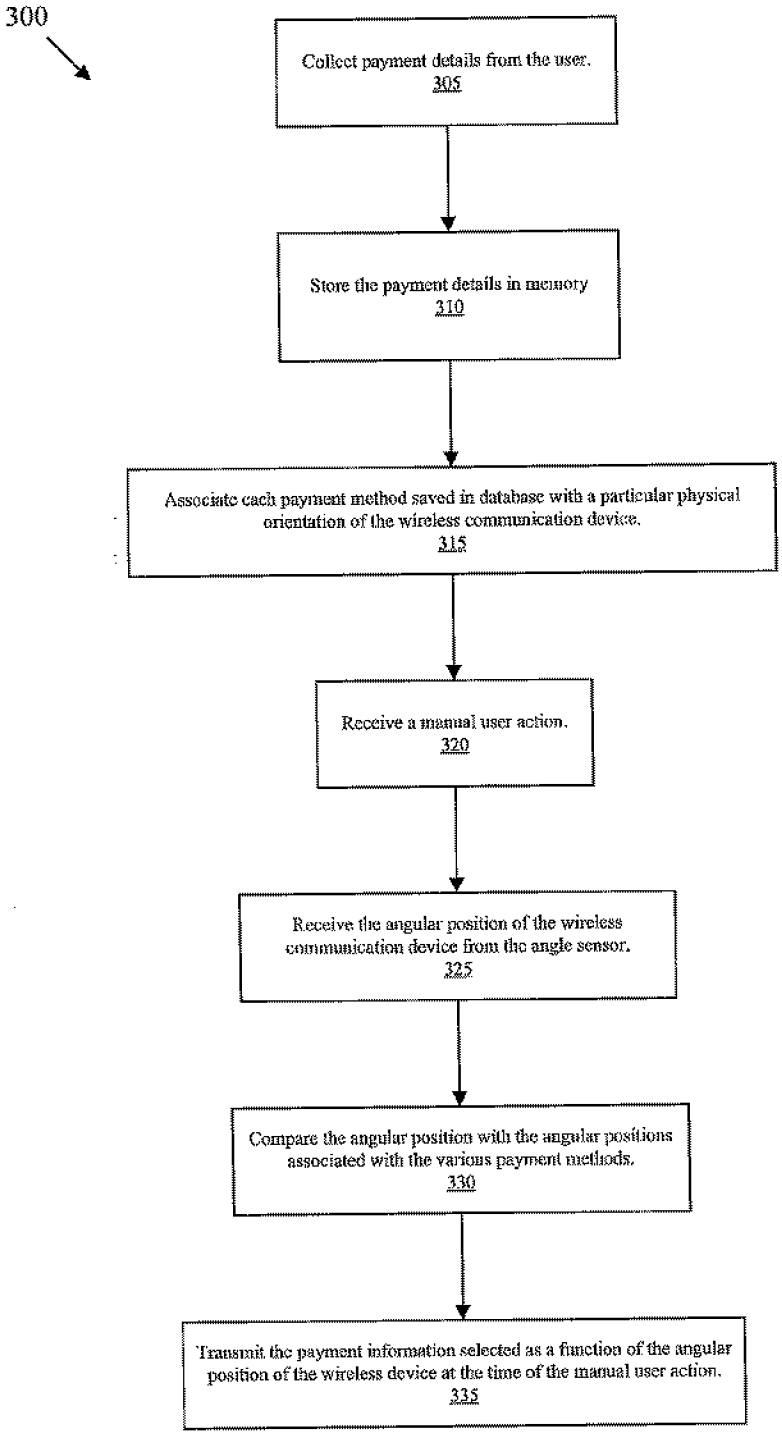

300
Collect payment details from the user.
305
Store the payment details in memory
310
Associate each payment method saved in database with a particular physical orientation of the wireless communication device.
315
Receive a manual user action.
320
Receive the angular position of the wireless communication device from the angle sensor.
325
Compare the angular position with the angular positions associated with the various payment methods.
330
Transmit the payment information selected as a function of the angular position of the wireless device at the time of the manual user action.
335

Fig. 3

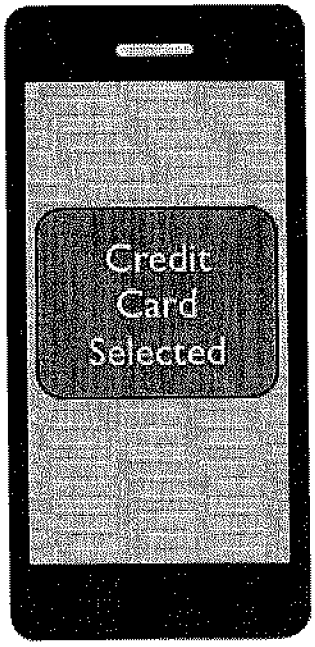


FIG. 4-A

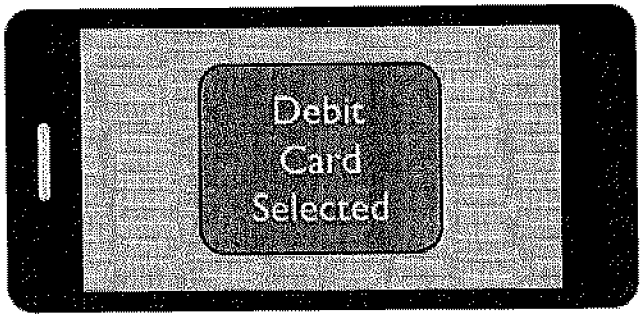


FIG. 4-B

SYSTEM AND METHOD FOR PAYMENT USING A MOBILE DEVICE

TECHNICAL FIELD OF THE INVENTION

[0001] This patent application relates generally to the field of electronic transactions and, in particular, wireless electronic devices configured to select a payment method and wirelessly transmit payment information.

BACKGROUND OF THE INVENTION

[0002] Many individuals carry cash currency, debit cards or credit cards to complete daily purchases. A more modern payment method for completing debit/credit transactions is a "contactless" payment transaction, such as can be done using with PayPass® by MasterCard International Incorporated, the assignee of the present invention. That system provides cardholders with a simpler way to complete a credit/debit transaction by bringing a contactless-enabled payment card or other payment device, such as a key fob, within proximity of a point-of-sale terminal reader, rather than swiping or inserting a card.

[0003] Contactless payment generally employs "Near Field Communication" (NFC) technology, which facilitates secure, short range communication between electronic devices. More specifically, NFC is a short range high frequency wireless communication technology that enables the exchange of data between devices over a relatively short distance. NFC is based on Radio Frequency Identification ("RFID") technology and uses many of the same working principles.

[0004] NFC is a set of short-range wireless technologies, typically requiring a distance of 4 cm or less. Typically, NFC involves an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take very simple form factors such as tags, stickers, key fobs, or cards that do not require batteries. NFC peer-to-peer communication is possible, provided both devices are powered.

[0005] NFC tags contain data and are typically read-only, but can be rewriteable. The tags can securely store personal data, such as debit and credit card information, loyalty program data, PINs and networking contacts, among other information.

[0006] NFC tags for contactless payment have only added to the number of devices that users carry on a day to day basis, including cash, credit cards, keys, NFC tags, and mobile phones/smartphones. In an effort to consolidate the myriad of electronic devices used on a daily basis, some mobile phones now include wireless transponders, including but not limited, to NFC tags.

[0007] With the rising popularity of NFC equipped mobile phones, more consumers are completing contactless payment transactions using their mobile phones instead of the traditional wireless payment key fobs. In addition, "mobile wallet" applications on a smart phone allow the user to select one of multiple stored cards in order to make a payment as many consumers use more than one card in a given day. However, with mobile phones acting as payment devices, selecting a particular card often involves awaking the phone from sleep, unlocking the phone, launching the mobile wallet application, selecting the card and then tapping the phone to the terminal. This is a lengthy process that ultimately can hinder the use of these technologies. When faced with a lengthy multi-step process of selecting a card on their phone or simply pulling the desired card out of their physical wallet, the consumer may prefer to reach for their old physical wallet and card.

[0008] It would be beneficial to provide a mobile phone and/or smartphone configured to allow a user to toggle between multiple payment methods and complete a wireless/contactless payment transaction quickly, easily and without requiring multiple user input actions.

[0009] It is with respect to these and other considerations that the disclosure made herein is presented.

SUMMARY OF THE INVENTION

[0010] Technologies are presented herein in support of a system and method to facilitate wireless payment transactions. In particular, a wireless communication device is configured to select a payment method and to wirelessly transmit payment information without unlocking a phone or other electronic device. In one implementation, a payment is selectable as a function of a predefined (e.g., manual) user action/interaction. In another further implementation, the payment selector further takes into consideration the angular position of the communication device.

[0011] According to a first aspect, a wireless communication device is disclosed. Particularly, a wireless communication device adapted to conduct a financial transaction over a communication network of the type having one or more processors configured to interact with a wireless transceiver, an angle sensor, and a computer readable storage medium wherein the one or more processors execute one or more software modules stored on the storage medium. The device includes a payment details module configured to receive one or more sets of payment information and associate the one or more sets of payment information with the two or more angular positions. The device also includes a payment module configured to transmit payment information obtained from the payment details module in response to a particular angular position provided by the angle sensor and a manual user action, wherein the payment details are selected automatically as a function of the angular position of the wireless communication device at the time of the manual user action.

[0012] According to another aspect, a method for conducting a financial transaction over a communication network using a wireless communication device is provided. The method comprises: receiving one or more sets of payment information and associating the one or more sets of payment information with the two or more angular positions of the wireless device, receiving a manual user action, and transmitting payment information in response to the particular angular position provided by the angle sensor and a manual user action. In this method, the payment details are selected automatically as a function of the angular position of the wireless device at the time of the manual user action.

[0013] According to another aspect, a wireless communication device is disclosed. Particularly, the wireless communication device is adapted to conduct a financial transaction over a communication network and is of the type that has one or more processors configured to interact with a wireless transceiver, and a user interface, a computer readable storage medium, wherein the one or more processors execute one or more software modules stored on the storage medium. The device includes a payment details module configured to receive one or more sets of payment information and associate the one or more sets of payment information with one or

more predefined user interactions with the user interface. The device also includes a payment module configured to transmit payment information obtained from the payment details module in response to a particular predefined user interaction with the user interface wherein the payment details are selected automatically as a function of the predefined user interaction.

[0014] According to another aspect, a method for conducting a financial transaction over a communication network using a wireless communication device is provided. The method comprises: receiving one or more sets of payment information, associating the one or more sets of payment information with one or more predefined user interactions, receiving a user action, and transmitting payment information in response to the user action. In this method, the payment details are selected automatically as a function of the user action.

[0015] These and other aspects, features, and advantages can be appreciated from the accompanying description of certain embodiments of the invention and the accompanying drawing figures and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] FIG. **1** is a high-level diagram illustrating an exemplary configuration of a wireless transaction processing system;

[0017] FIG. **2** is a block diagram illustrating an exemplary configuration of a wireless communication device according to an embodiment of the present invention;

[0018] FIG. **3** is a flow diagram showing a routine that illustrates facilitating a transaction according to an embodiment of the present invention;

[0019] FIG. **4**-A is a diagram illustrating an exemplary orientation of a wireless communication device; and

[0020] FIG. **4**-B is a diagram illustrating an exemplary orientation of a wireless communication device.

DETAILED DESCRIPTION OF CERTAIN EMBODIMENTS OF THE INVENTION

[0021] By way of overview and introduction, a system and method is disclosed for a contactless, payment-enabled smartphone in which a user can toggle between multiple payment methods, i.e., multiple different credit/debit card accounts, by changing the physical orientation of the smartphone and complete a transaction using the selected payment method via a contactless, wireless transmission.

[0022] It can be appreciated that, from the consumer's standpoint, that there is a demand for a system that removes the inconvenience of carrying credit cards and contactless payment key fobs in addition to carrying a smartphone, and for a solution that reduces the input required from the user to select one of a plurality of payment methods in order to conduct a transaction using a contactless, payment enabled-smartphone.

[0023] The referenced systems and methods are now described more fully with reference to the accompanying drawings, in which one or more illustrated embodiments and/or arrangements of the systems and methods are shown. The systems and methods are not limited in any way to the illustrated embodiments and/or arrangements as the illustrated embodiments and/or arrangements described below are merely exemplary of the systems and methods, which can be embodied in various forms, as appreciated by one skilled in the art. Therefore, it is to be understood that any structural and functional details disclosed herein are not to be interpreted as limiting the systems and methods, but rather are provided as a representative embodiment and/or arrangement for teaching one skilled in the art one or more ways to implement the systems and methods. Accordingly, aspects of the present systems and methods can take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.), or an embodiment combining software and hardware. One of skill in the art can appreciate that a software process can be transformed into an equivalent hardware structure, and a hardware structure can itself be transformed into an equivalent software process. Thus, the selection of a hardware implementation versus a software implementation is one of design choice and left to the implementer. Furthermore, the teems and phrases used herein are not intended to be limiting, but rather are to provide an understandable description of the systems and methods.

[0024] FIG. **1** is a high level diagram illustrating an exemplary contactless transaction processing system **100**. The system consists of a point of sale (POS) system **104** equipped with a wireless transceiver **106**, and a wireless communication device **108** adapted to select a payment method and conduct a contactless financial transaction according to the present invention. POS systems that are enabled to receive and/or transmit transaction information wirelessly by contactless payment methods are well known in the art. Similarly, wireless communication devices that are enabled to transmit and receive transaction information, including payment information, wirelessly through contactless payment methods are well known in the art.

[0025] In the exemplary wireless transaction processing system **100** of FIG. **1**, the POS system **104** is operated by a merchant for processing transactions for goods or services. Wireless communication device **108** can be a mobile phone or a smartphone and is operated by a user/consumer. When a transaction is ready to be completed, the consumer is prompted to conduct a contactless payment transaction in order to submit payment. The consumer can present wireless communication device to the POS wireless transceiver **106**. In this exemplary embodiment wireless transceiver can be an NFC transceiver. The wireless communication device can emulate an NFC or RFID tag so as to provide data, including personal information (i.e., name, billing address and the like) and payment information (i.e., credit card number, expiration date and security code) to the POS system via the POS wireless transceiver.

[0026] NFC wirelessly operates over a short range, typically under about 4 cm. NFC may operate in various modes such as, for example, Card Emulation Mode, Peer-to-Peer Mode, and Reader-Writer Mode. Card Emulation Mode permits the wireless communication device to be used to perform secure transactions such as mobile payments, including smart card like transactions. Peer-to-Peer Mode permits data transfer between two NFC devices in proximity to one another for services as diverse as mobile ticketing transactions and exchange of business cards. Reader-Writer Mode permits a one-way data acquisition of information.

[0027] In addition, the wireless communication device can also read a NFC tag or RFID tag to acquire information such as, for example, transaction, payment or merchant related information. For RFID tag reading and emulation, a communication interface within the wireless communication device may be configured for operating at a suitable radio frequency

and includes an antenna suitable for inductively coupling at one or more RF frequencies with an RFID reader. The term "NFC" as used herein is a broad term which is inclusive of RFID but is not essentially defined by RFID. In this sense, a RFID tag may be considered a type of NFC tag, but a NFC tag does not require the particular attributes of a RFID tag. Similarly, a RFID reader may be considered to be a type of NFC reader, but a NFC reader does not require the ability to read RFID tags. Further, although the exemplary embodiments described herein are discussed in relation to NFC wireless payment systems, it should be understood that the present invention can facilitate wireless transmission of payment data over other wireless communication systems including but not limited to, Bluetooth, WIFI, cellular and the like.

[0028] It should be noted that while FIG. **1** depicts credit transaction processing system **100** with respect to a wireless communication device **108** and a merchant POS system **104**, it should be understood that any number of wireless communication devices and merchant POS systems can interact with one another in the manner described herein. It should be further understood that while the various electronic devices and machines referenced herein, including but not limited to merchant POS system and wireless communication device, are referred to herein as individual/single devices and/or machines, in certain implementations the referenced devices and machines, and their associated and/or accompanying operations, features, and/or functionalities can be arranged or otherwise employed across any number of devices and/or machines, as is known to those of skill in the art.

[0029] FIG. **2** is a block diagram illustrating an exemplary configuration of a wireless communication device **108** according to an embodiment of the present invention. Wireless communication device includes, various hardware and software components that serve to select a payment method and conduct a financial transaction according to the present invention. Wireless communication device includes, inter alia, a processor **110** in communication with a memory **120**, an angle sensor **140** and a communication interface **150**. Processor serves to execute software instructions that can be loaded into memory **120**. Processor **110** can be a number of processors, a multi-processor core, or some other type of processor, depending on the particular implementation.

[0030] Preferably, memory **120** is accessible by processor **110**, thereby enabling processor to receive and execute instructions stored on memory. Memory can be, for example, a random access memory (RAM) or any other suitable volatile or non-volatile computer readable storage medium. In addition, memory can be fixed or removable and can contain one or more components or devices such as a hard drive, a flash memory, a rewritable optical disk, a rewritable magnetic tape, or some combination of the above.

[0031] The angle sensor **140** is also operatively connected to processor. Angle sensor can be any type of sensor that detects an angular position and generates an electric signal indicative of the physical orientation of the wireless communication device. Angle sensors are well known smartphone components and can include, but are not limited to accelerometers, gyroscopes, compasses and the like.

[0032] One or more software modules **130** are encoded in memory **120**. The software modules can comprise one or more software programs or applications having computer program code or a set of instructions executed in processor **110**. Such computer program code or instructions for carrying out operations for aspects of the systems and methods disclosed herein can be written in any combination of one or more programming languages.

[0033] Preferably, included among the software modules are payment details module **160** and payment module **165** that are executed by processor. During execution of the software modules, the processor configures the wireless communication device to perform various operations relating to the facilitating and processing of transactions, as will be described in greater detail below.

[0034] In addition, it should be noted that other information and/or data relevant to the operation of the present systems and methods (such as database **180**) can also be stored on memory, as will be discussed in greater detail below.

[0035] Also preferably stored in memory is database **180**. Database **180** contains and/or maintains various data items and elements that are utilized throughout the various operations of contactless payment system. The information stored in database can include but is not limited to, credit card details and billing information unique to the consumer and/or payment method, personal information for each consumer, banking information and a history of transactions by the consumer. It should be noted that although database **180** is depicted as being configured locally to wireless communication device **108**, in certain implementations database and/or various of the data elements stored therein can be located remotely (such as on a remote device or server—not shown) and connected to wireless communication device **108** through a network in a manner known to those of ordinary skill in the art, in order to be loaded into a processor and executed.

[0036] It can also be said that the program code of software modules **130** and one or more computer readable storage devices (such as memory **120** and/or storage **190**) form a computer program product that can be manufactured and/or distributed in accordance with the present invention, as is known to those of ordinary skill in the art.

[0037] Communication interface **150** is also operatively connected to the processor **110** and can be any interface that enables communication between the wireless communication device and external devices, machines and/or elements including a merchant's POS system. Preferably, communication interface includes an NFC transceiver that is configured to operate at a suitable radio frequency, includes an antenna suitable for inductively coupling at one or more RF frequencies with an RFID reader and is capable of transmitting and/or receiving data. Alternatively, communication interface can include but is not limited to a Bluetooth, or cellular transceiver, a satellite communication transmitter/receiver, an optical port and/or any other such interfaces for wirelessly connecting electronic device **108** to a merchant's POS system.

[0038] An interface **170** is also operatively connected to the processor. The interface can be one or more input device(s) such as switch(es), button(s), key(s), a touch screen, etc. Interface serves to facilitate the capture of certain information about the user and payment methods, such as credit card numbers and billing information, as discussed in greater detail below. Interface also serves to facilitate the capture of commands from the user such as an on-off commands or settings related to operation of the contactless payment system.

[0039] A display **175** is also operatively connected to the processor. Display includes a screen or any other such presentation device that enables the user to view various options,

parameters, and results. By way of example, display **175** can be a digital display such as a dot matrix display or other 2-dimensional display.

[0040] By way of further example, interface **170** and display **175** can be integrated into a touch screen display. Accordingly, the screen is used to show a graphical user interface, which can display various data and provide "forms" that include fields that allow for the entry of information by the user. Touching the touch screen at locations corresponding to the display of a graphical user interface allows the person to interact with the device to enter data, change settings, control functions, etc. So, when the touch screen is touched, interface communicates this change to processor, and settings can be changed or user entered information can be captured and stored in the memory.

[0041] The operation of the wireless communication device **108** and the various elements and components described above will be further appreciated with reference to the method for selecting a payment method and conducting a financial transaction over a communication network using a wireless communication device as described below, in conjunction with FIG. **3**.

[0042] Turning now to FIG. **3**, a flow diagram illustrates a routine **300** for selecting a payment method and facilitating a wireless payment in accordance with at least one embodiment disclosed herein. It should be appreciated that several of the logical operations described herein are implemented (1) as a sequence of computer implemented acts or program modules running on wireless communication device **108**; and/or (2) as interconnected machine logic circuits or circuit modules within the wireless communication device. The implementation is a matter of choice dependent on the requirements of the device (e.g., size, energy, consumption, performance, etc.). Accordingly, the logical operations described herein are referred to variously as operations, steps, structural devices, acts, or modules. As referenced above, various of these operations, steps, structural devices, acts and modules can be implemented in software, in firmware, in special purpose digital logic, and any combination thereof. It should also be appreciated that more or fewer operations can be performed than shown in the figures and described herein. These operations can also be performed in a different order than those described herein.

[0043] The process begins at step **305**, in which processor **110** executing one or more software modules **130**, including, preferably, payment details module **160**, configures wireless communication device **108** to collect payment details from a user of the system. Wireless communication device **108** can be a smartphone as described in detail above. The display **175** of the wireless communication device **108**, such as a smartphone, can display one or more interactive forms for inputting information including but not limited to a form for inputting a credit card number, a billing address associated with that card and personal information for security purposes. Alternatively, payment details can be obtained in other ways such as through electronic access to the details kept on another device, via a camera image of the debit card or credit card, and so on. Using user interface **170**, the user can input a variety of different payment methods for completing transactions. For example, a user can enter a personal credit card as a first payment method and a personal debit card as a second payment method. While this exemplary embodiment describes two possible payment methods, it should be understood that the present invention can accommodate any number of payment methods. Further, payment methods are not limited to credit/debit cards but can include, without limitation, bank accounts or other electronic money transfer methods (e.g., PayPal® by PayPal, Inc.).

[0044] At step **310**, processor executing one or more software modules **130**, including, preferably, payment details module **160**, configures the wireless communication device **108** to store the payment methods gathered at step **305** in memory **120**, and more specifically in database **180**.

[0045] At step **315**, processor **110** executing one or more software modules **130**, including, preferably, payment details module **160**, configures the wireless communication device **108** to associate each payment method saved in database, with a particular physical orientation of the wireless communication device **108**. For example, the system can associate a first payment method with a generally horizontal orientation, commonly referred to as landscape, and associate a second payment method with a vertical orientation, commonly referred to as portrait. FIG. **4**-A depicts a wireless communication device in a portrait orientation according to an exemplary embodiment. FIG. **4**-B depicts a smartphone in a landscape orientation. While only two possible orientations in a two dimensional plane (x-y) have been mentioned, it should be understood that angle sensors, such as accelerometers, can also allow for the detection of the wireless communication device's orientation in three dimensions (x-y-z).

[0046] At step **320**, processor **110** executing one or more software modules **130**, configures the wireless communication device **108** to receive a manual user action. A manual user action can be any kind of user input to the wireless communication device **108** that can be interpreted as an indication that the user intends to complete a transaction using the wireless communication device **108**. This can be a user input via a user interface **170**, such as depressing one or more buttons a prescribed number of times (e.g., three times) or interacting with a touch screen or by a voice command to a microphone on the device. Alternatively, user action can include placing the wireless communication device in proximity of a merchant's POS system wireless transceiver **106**. For example, merchant's POS system employing NFC technology can be actively generating an RF field. The detection of an RF field by the wireless communication device's communication interface **150**, can be interpreted by the processor **110** as a manual user action. It should be understood that the wireless communication device **108** can be configured to receive and act upon a manual user action regardless of whether the device is in a locked or sleep state or in an unlocked or active state.

[0047] At step **325**, responsive to detecting a manual user input at step **320**, processor **110** executing one or more software modules **130** configures the wireless communication device **108** to receive the angular position of the wireless communication device **108** from the angle sensor **140**. In an exemplary embodiment, the angle sensor **140** can be an accelerometer that generates an electric signal indicative of the physical orientation of the wireless communication device as is well known in the art. Optionally, the electric signal undergoes pre-processing to provide information that is of the same value range as used with the stored angular positions that were stored within the payment details at step **310**.

[0048] At step **330**, processor **110** executing one or more software modules **130**, configures the wireless communication device **108** to compare the angular position received at step **320** with the angular positions associated with the vari-

ous payment methods stored at step **310**. If the processor determines that the angular position of the angle sensor **140** is within a pre-determined range of the angular position associated with a particular payment method, the processor **110** will set the matching payment method as the payment method to be transmitted.

[0049] At step **335**, processor **110** executing one or more software modules **130**, including, preferably, payment module **165**, configures the wireless communication device **108** to transmit the payment information selected as a function of the angular position of the wireless communication device **108** at the time of the manual user action as determined in step **325**.

[0050] Furthermore, the wireless communication device **108** can also be configured to open up a bi-directional communication link with the POS device to receive information. As mentioned above, NFC can operate in various modes. Peer-to-Peer mode permits data transfer between two NFC devices in proximity to one another for services as diverse as mobile ticketing transactions and exchange of business cards. Reader-Writer Mode permits a one-way data acquisition of information. For example, the wireless communication device **108** can acquire information such as transaction details, payment and or merchant related information. This information can be stored in the database **180** and can be used to generate a transaction history log or interface with other programs, including but not limited to, accounting/money management applications or rewards programs.

[0051] In addition, the wireless communication device **108** can be configured to enable rapid toggle between payment methods prior to completing a contactless payment transaction free of any angle sensor data. According to such an arrangement, a user can quickly toggle between a first payment method and a second payment method with two predefined user interactions with the user interface **170**. For example, first payment method saved at step **310** can be set as the default payment method for contactless payment. Further, user interface **170** can include a sleep/wake push button that is commonly found on smartphones and typically pushed once to awaken the phone or force it to hibernate. The processor **110**, executing one or more software modules **130**, can configure the wireless communication device **108** to change the payment method to be used for contactless payment from the default first payment method to a second payment method upon detection of the user depressing the sleep/wake button twice in a set period of time. Similarly the user can toggle to a third or fourth payment method by depressing the sleep wake button three or four times within a set period of time, respectively. It should be understood that toggling between any number of payment methods can be done in this way. It should also be understood that toggling between payment methods can also be accomplished by depressing a combination of buttons, or gestures on a touch screen, or voice command, in a predefined manner. In addition, the wireless communication device **108** can be configured to allow the user to define any number of custom predefined user interactions.

[0052] At this juncture, it should be noted that although much of the foregoing description has been directed to a wireless communication device **108** configured to select a payment method and facilitate a wireless transaction and method of use, the systems and methods disclosed herein can be similarly deployed and/or implemented in scenarios, situations, and settings far beyond the referenced scenarios. It can be readily appreciated that the wireless communication device **108** can be effectively employed in practically any scenario in which a transaction is being made between one or more parties wirelessly (e.g., by 'bumping' phones). For example, two or more individuals using wireless communication devices as described herein can set their devices into a bi-directional communication mode and complete a transfer of funds between themselves simply by tonching or 'bumping' phones together, allowing their respective communication interfaces to exchange the transaction data. Similarly such phone bump transfers can also be used load pre-paid credit cards and the like.

[0053] It is to be understood that like numerals in the drawings represent like elements through the several figures, and that not all components and/or steps described and illustrated with reference to the figures are required for all embodiments or arrangements.

[0054] Thus, illustrative embodiments and arrangements of the present systems and methods provide a method, system, and computer program product for facilitating wireless payment transactions. The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments and arrangements. In this regard, each block in the flowchart or block diagrams can represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function (s). It should, also be noted that, in some alternative implementations, the functions noted in the block may occur ont of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0055] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising", when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0056] Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of "including," "comprising," or "having," "containing," "involving," and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

[0057] The subject matter described above is provided by way of illustration only and should not be construed as limiting. Various modifications and changes can be made to the subject matter described herein without following the example embodiments and applications illustrated and described, and without departing from the true spirit and scope of the present invention, which is set forth in the following claims.

What is claimed is:

1. A wireless communication device adapted to conduct a financial transaction over a communication network of the type having one or more processors configured to interact with a wireless transceiver, an angle sensor, and a computer readable storage medium, wherein the one or more processors execute one or more software modules stored on the storage medium, comprising:

a payment details module configured to receive one or more sets of payment information and associate the one or more sets of payment information with two or more angular positions of the wireless device; and

a payment module configured to transmit payment information obtained from the payment details module in response to a particular angular position provided by the angle sensor and a manual user action;

wherein the payment details are selected automatically as a function of the angular position of the wireless device at the time of the manual user action.

2. The wireless communication device of claim **1** wherein the payment information is transmitted if the wireless communication device is in an active state or an inactive state.

3. The wireless communication device of claim **1** further comprising a user display and a user interface.

4. A wireless communication device adapted to conduct a financial transaction over a communication network having one or more processors configured to interact with a wireless transceiver, a user interface, a computer readable storage medium wherein the one or more processors execute one or more software modules stored on the storage medium, comprising:

a payment details module configured to receive one or more sets of payment information and associate the one or more sets of payment information with one or more predefined user interactions with the user interface; and

a payment module configured to transmit payment information obtained from the payment details module in response to a particular predefined user interactions with the user interface;

wherein the payment details are selected automatically as a function of the predefined user interaction.

5. The wireless communication device of claim **4**, wherein the user interface includes a sleep/wake button.

6. A method for selecting a payment method and conducting a financial transaction over a communication network using a wireless communication device, the method comprising:

receiving one or more sets of payment information;

associating the one or more sets of payment information with one or more predefined angular positions of the wireless device;

receiving a manual user action; and

transmitting payment information in response to the particular angular position provided by the angle sensor and a manual user action, wherein the payment details are selected automatically as a function of the angular position of the wireless device at the time of the manual user action.

7. The method of claim **6**, further comprising the step of comparing the particular position provided by the angle sensor with the one or more predefined angular positions.

8. The method of claim **6**, further comprising the step of defining the predefined angular positions.

9. The method of claim **6**, further comprising the step of receiving transaction information relating to the financial transaction.

10. A method for selecting a payment method and conducting a financial transaction over a communication network using a wireless communication device, the method comprising:

receiving one or more sets of payment information;

associating the one or more sets of payment information with one or more predefined user interactions;

receiving a user action; and

transmitting payment information in response to the user action, wherein the payment details are selected automatically as a function of the user action.

11. The method of claim **10** further comprising the step of comparing the user action to the one or more predefined user interactions.

12. The method of claim **10** further comprising the step of defining the one or more predefined user interactions.

13. The method of claim **10** further comprising the step of associating the one or more sets of payment information with one or more predefined angular positions of the wireless device; and wherein the payment details are selected automatically as a function of the manual user action and angular position of the wireless device at the time of the manual user action.

14. The wireless communication device of claim **4**, further comprising an angle sensor, and wherein the payment module is configured to transmit payment information obtained from the payment details module in response to a particular predefined user interaction with the user interface and in response to a particular angular position provided by the angle sensor.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

KIM et al.

(10) **Pub. No.: US 2014/0214664 A1**

(43) **Pub. Date: Jul. 31, 2014**

(54) **PAYMENT SUPPORT METHOD AND SYSTEM**

(71) Applicant: **Samsung Electronics Co., Ltd.**, Suwon-si (KR)

(72) Inventors: **Kyungdong KIM**, Namyangju-si (KR); **Shinwoo LEE**, Seoul (KR)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Suwon-si (KR)

(21) Appl. No.: **14/163,017**

(22) Filed: **Jan. 24, 2014**

(30) **Foreign Application Priority Data**

Jan. 25, 2013 (KR) 10-2013-0008505

Publication Classification

(51) **Int. Cl.**
G06Q 20/36 (2006.01)

(52) **U.S. Cl.**
CPC *G06Q 20/363* (2013.01)
USPC **705/41**

(57) **ABSTRACT**

A method and a system for payment support are provided. The payment support method may include creating an account used for a payment service via a wallet server apparatus, connecting to the wallet server apparatus using the account, registering personal identification information including hardware information of a terminal device in the account, and associating at least one payment option with the personal identification information stored in the wallet server apparatus.

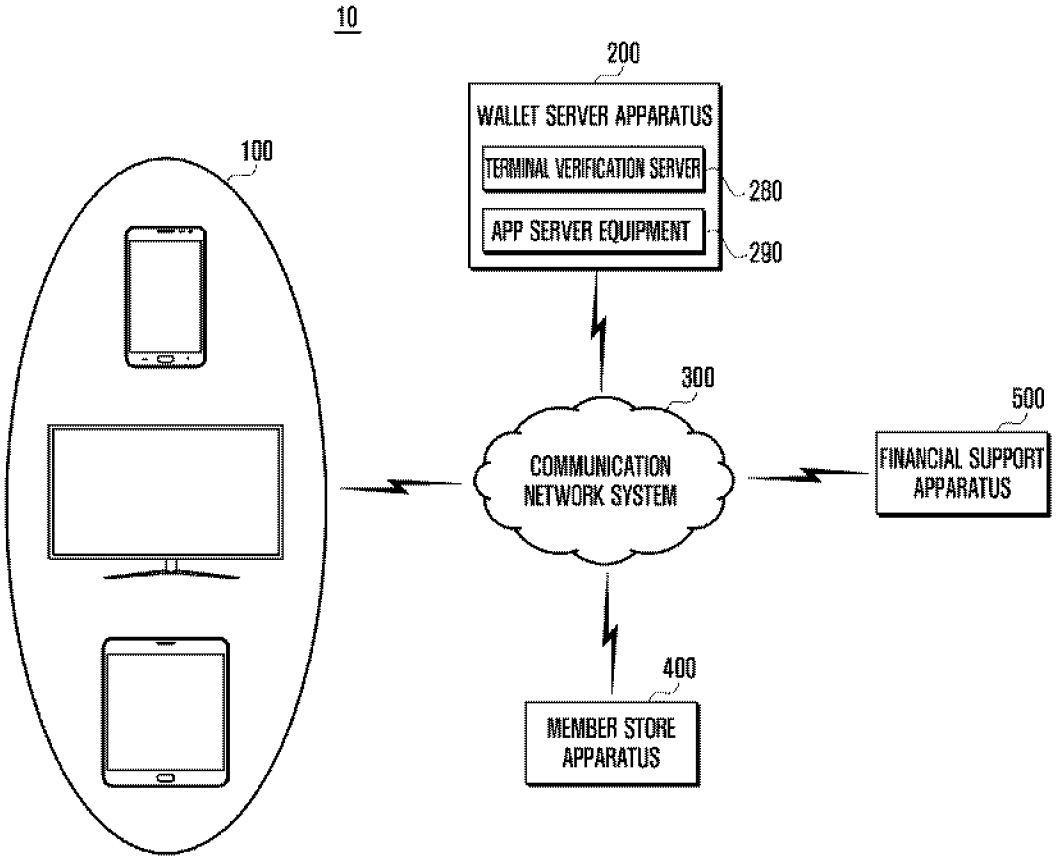


FIG. 1

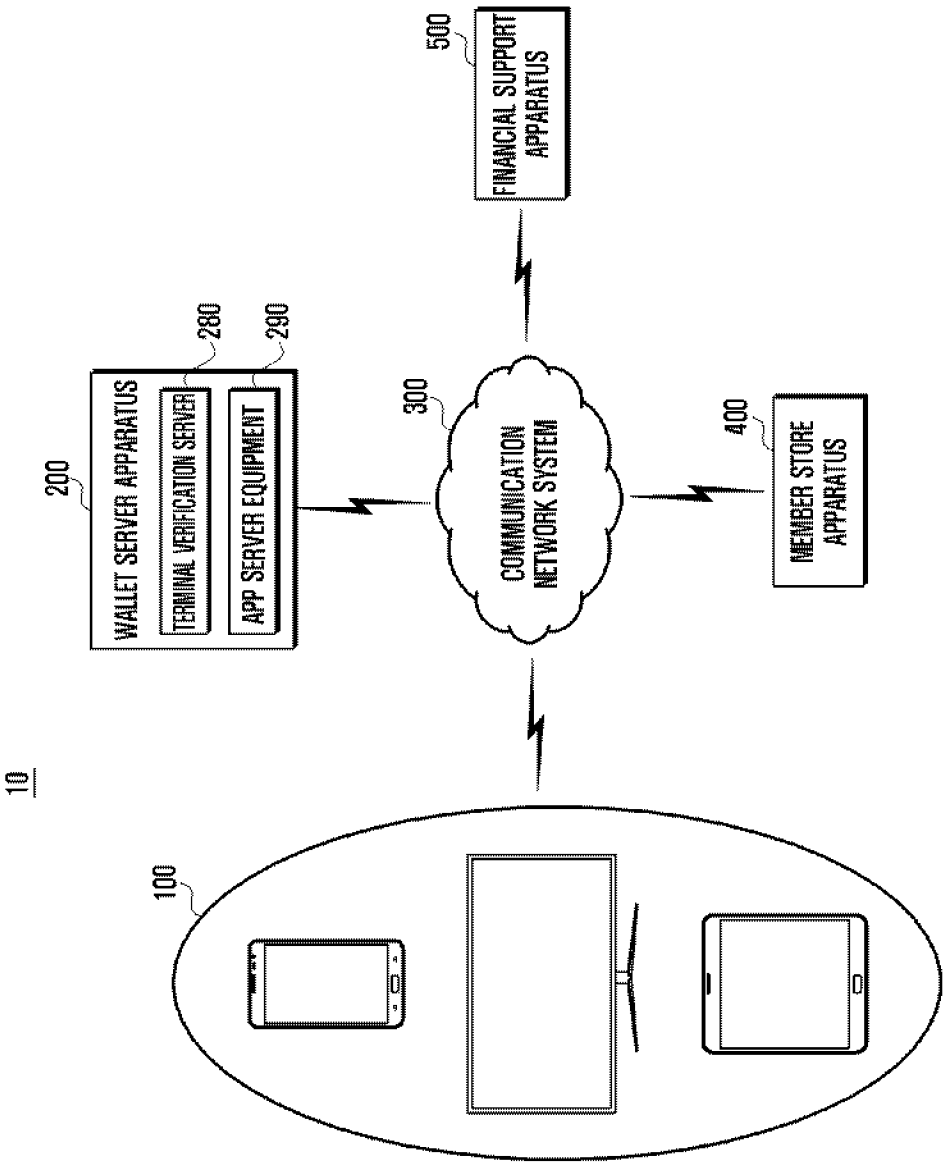

10
100
200
WALLET SERVER APPARATUS
TERMINAL VERIFICATION SERVER
280
APP SERVER EQUIPMENT
290
300
COMMUNICATION NETWORK SYSTEM
400
MEMBER STORE APPARATUS
500
FINANCIAL SUPPORT APPARATUS

FIG. 2

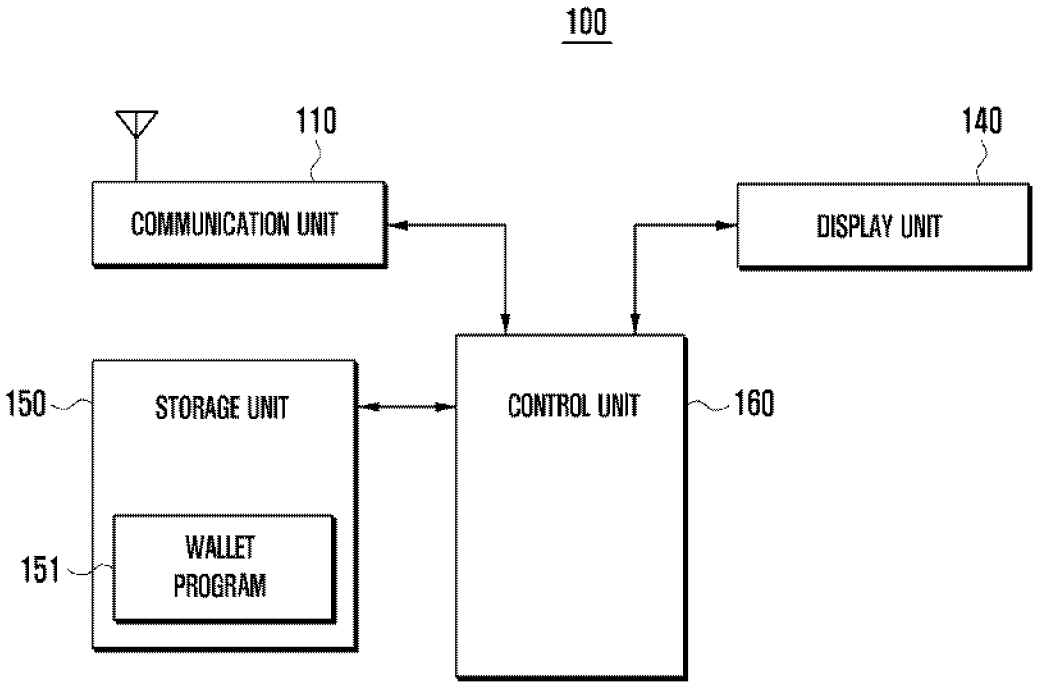

100
110
COMMUNICATION UNIT
140
DISPLAY UNIT
150
STORAGE UNIT
151
WALLET PROGRAM
CONTROL UNIT
160

FIG. 3

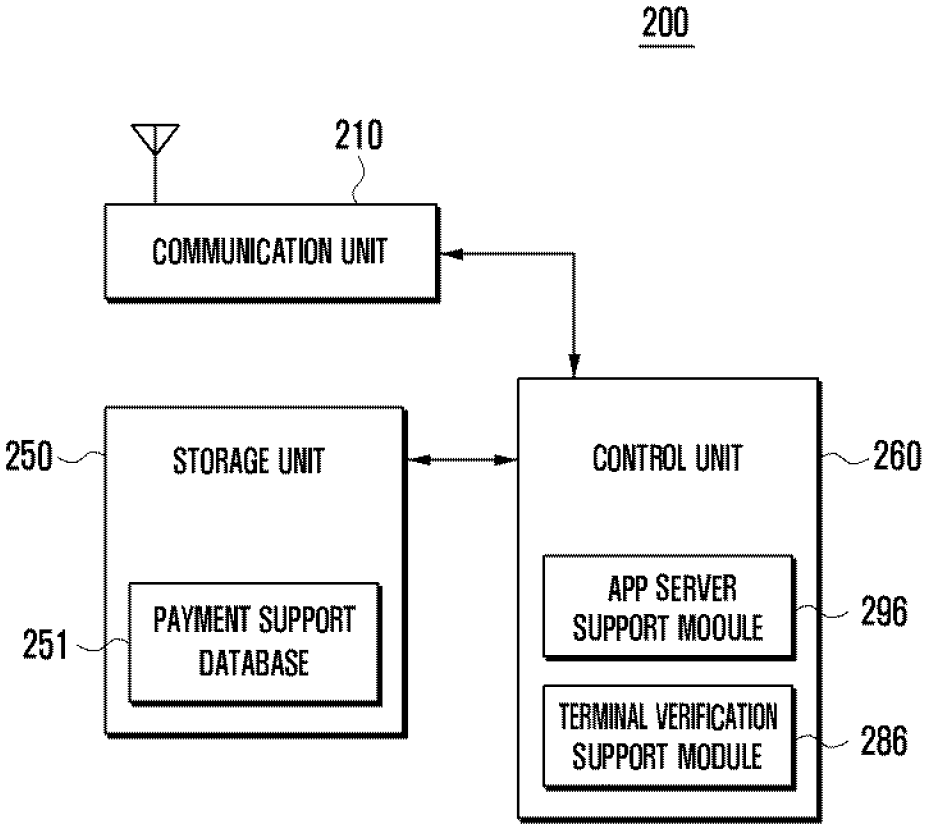

200
210
COMMUNICATION UNIT
250
STORAGE UNIT
251
PAYMENT SUPPORT DATABASE
CONTROL UNIT
260
APP SERVER SUPPORT MOOULE
296
TERMINAL VERIFICATION SUPPORT MODULE
286

FIG. 4

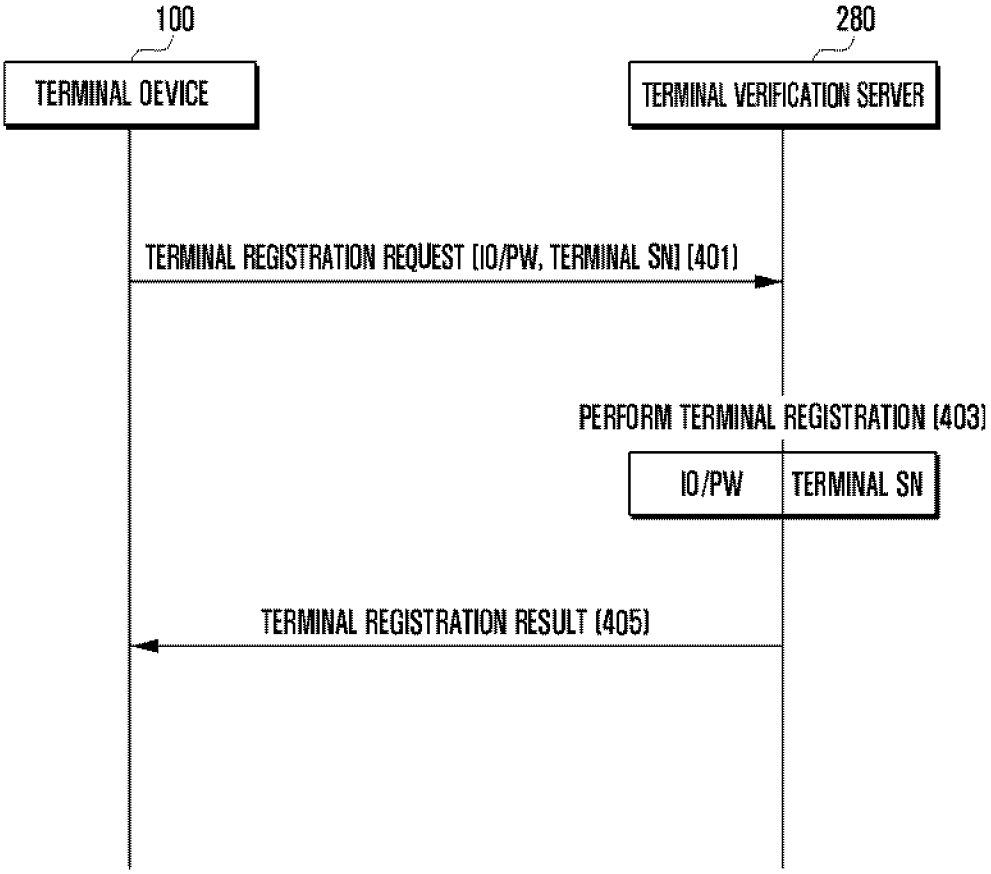

100
TERMINAL DEVICE
280
TERMINAL VERIFICATION SERVER
TERMINAL REGISTRATION REQUEST (ID/PW, TERMINAL SN) (401)
PERFORM TERMINAL REGISTRATION (403)
ID/PW
TERMINAL SN
TERMINAL REGISTRATION RESULT (405)

FIG. 5

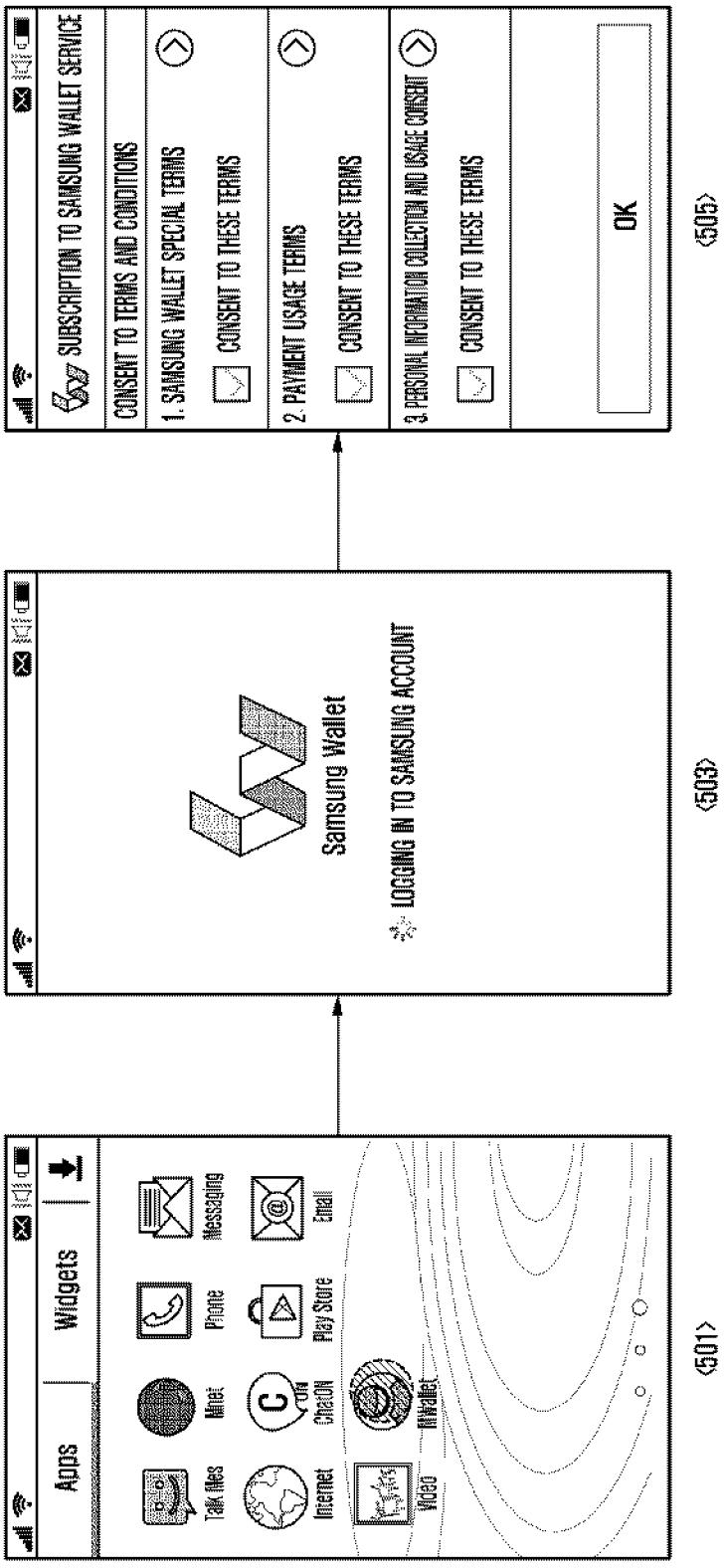

Apps
Widgets
Talk Mes
Mnet
Phone
Messaging
Internet
ChatON
Play Store
Email
Video
MiWallet
<501>
Samsung Wallet
LOGGING IN TO SAMSUNG ACCOUNT
<503>
SUBSCRIPTION TO SAMSUNG WALLET SERVICE
CONSENT TO TERMS AND CONDITIONS
1. SAMSUNG WALLET SPECIAL TERMS
CONSENT TO THESE TERMS
2. PAYMENT USAGE TERMS
CONSENT TO THESE TERMS
3. PERSONAL INFORMATION COLLECTION AND USAGE CONSENT
CONSENT TO THESE TERMS
OK
<505>

FIG. 6A

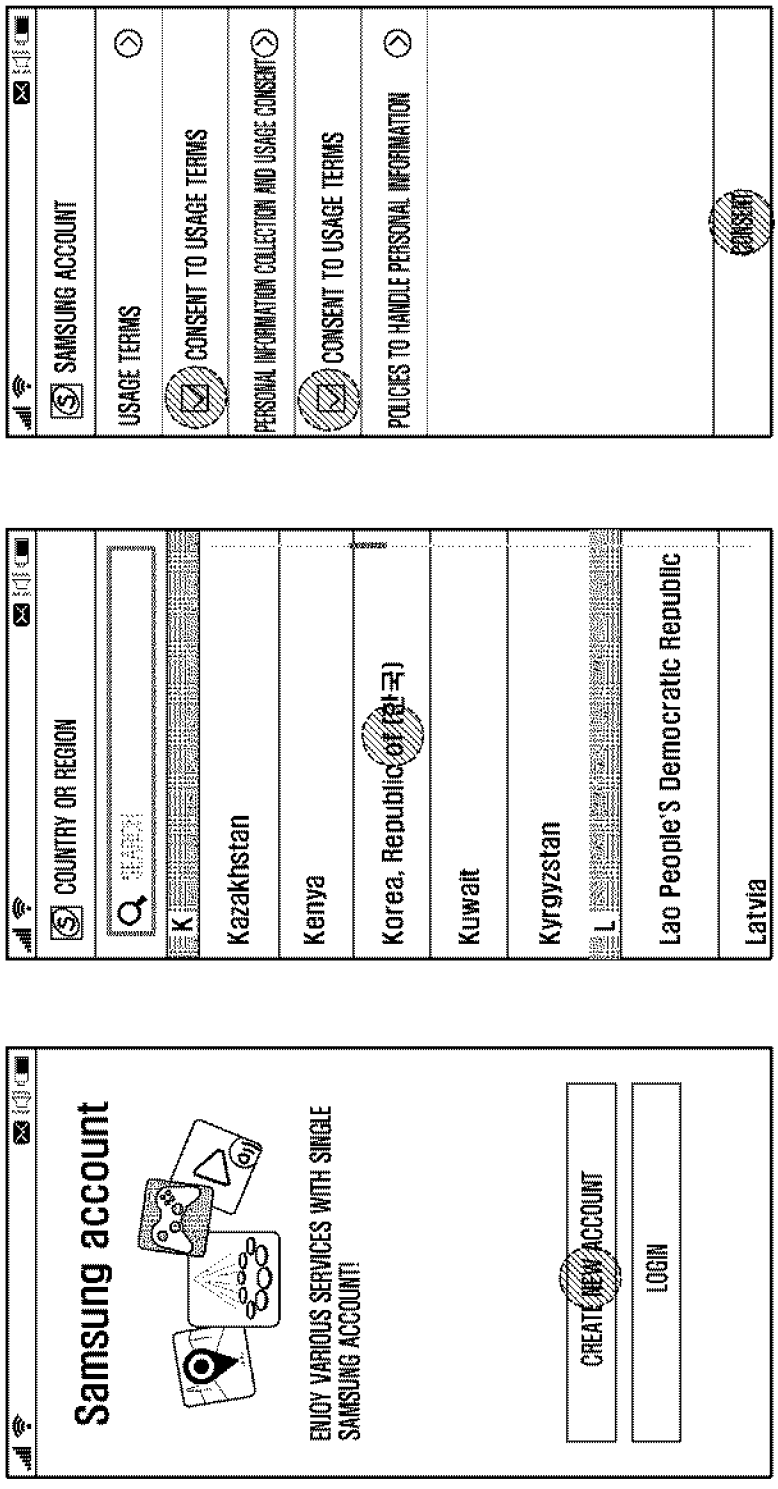

Samsung account
ENJOY VARIOUS SERVICES WITH SINGLE SAMSUNG ACCOUNT!
CREATE NEW ACCOUNT
LOGIN
<601>
COUNTRY OR REGION
K
Kazakhstan
Kenya
Korea, Republic of (대한민국)
Kuwait
Kyrgyzstan
L
Lao People'S Democratic Republic
Latvia
<603>
SAMSUNG ACCOUNT
USAGE TERMS
CONSENT TO USAGE TERMS
PERSONAL INFORMATION COLLECTION AND USAGE CONSENT
CONSENT TO USAGE TERMS
POLICIES TO HANDLE PERSONAL INFORMATION
CONSENT
<605>

FIG. 6B

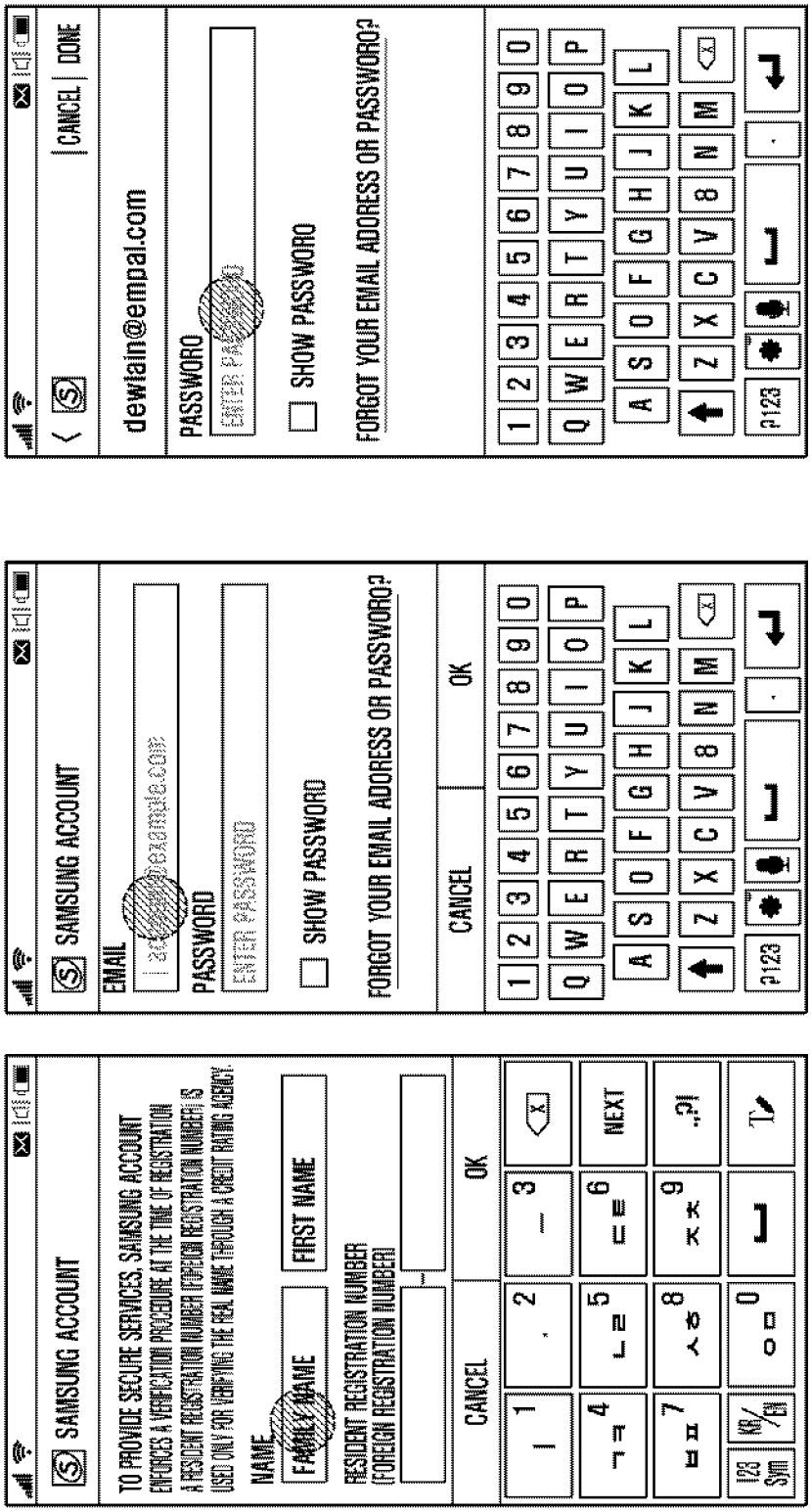

SAMSUNG ACCOUNT
TO PROVIDE SECURE SERVICES, SAMSUNG ACCOUNT ENFORCES A VERIFICATION PROCEDURE AT THE TIME OF REGISTRATION A RESIDENT REGISTRATION NUMBER (FOREIGN REGISTRATION NUMBER) IS USED ONLY FOR VERIFYING THE REAL NAME THROUGH A CREDIT RATING AGENCY.
NAME
FAMILY NAME
FIRST NAME
RESIDENT REGISTRATION NUMBER (FOREIGN REGISTRATION NUMBER)
CANCEL
OK
NEXT
SAMSUNG ACCOUNT
EMAIL
PASSWORD
ENTER PASSWORD
SHOW PASSWORD
FORGOT YOUR EMAIL ADDRESS OR PASSWORD?
CANCEL
OK
dewtain@empal.com
CANCEL
DONE
PASSWORD
SHOW PASSWORD
FORGOT YOUR EMAIL ADDRESS OR PASSWORD?
〈607〉
〈609〉
〈611〉

FIG. 7

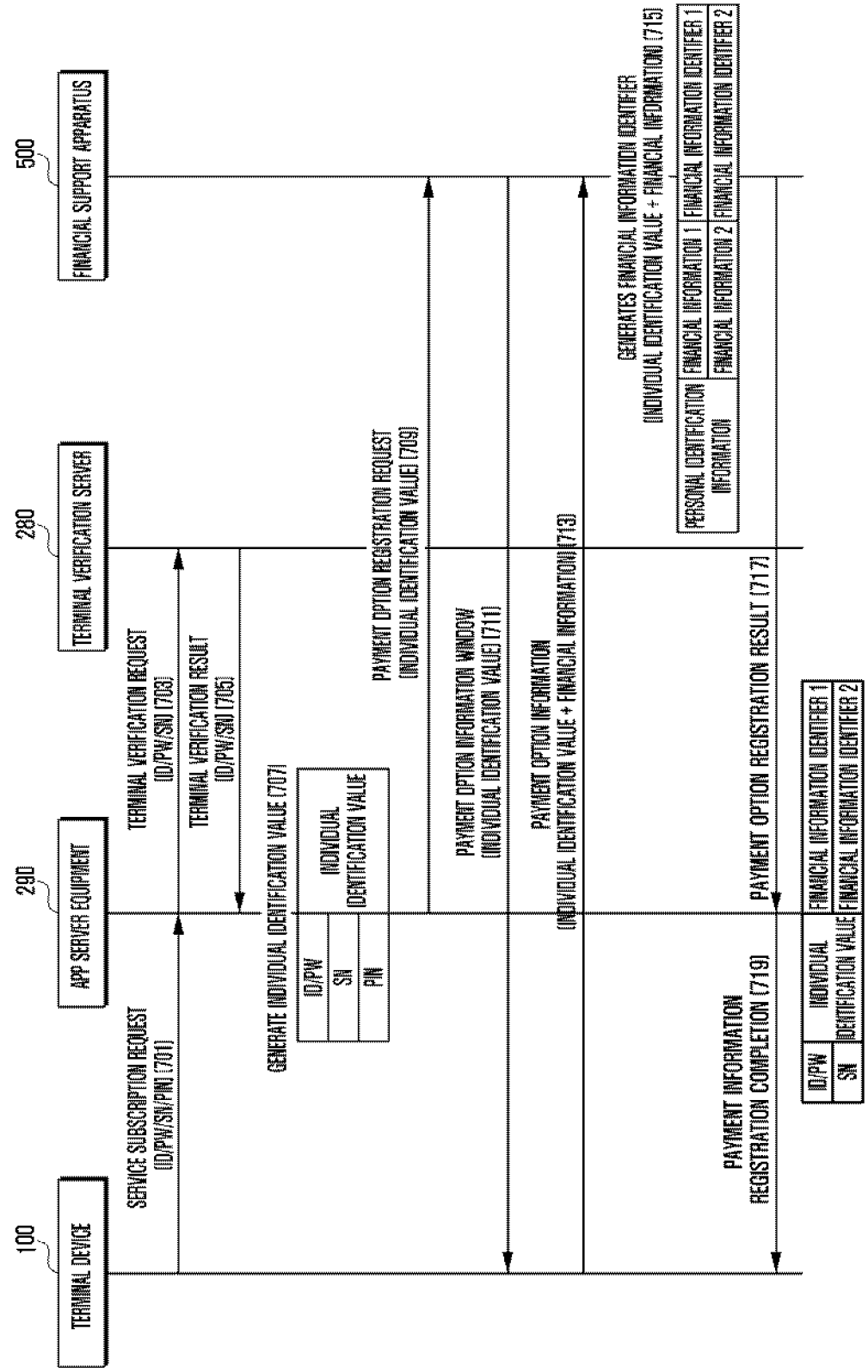

100
TERMINAL DEVICE
290
APP SERVER EQUIPMENT
280
TERMINAL VERIFICATION SERVER
500
FINANCIAL SUPPORT APPARATUS
SERVICE SUBSCRIPTION REQUEST (ID/PW/SSN/PIN) [701]
TERMINAL VERIFICATION REQUEST (ID/PW/SSN) [703]
TERMINAL VERIFICATION RESULT (ID/PW/SSN) [705]
PAYMENT OPTION REGISTRATION REQUEST (INDIVIDUAL IDENTIFICATION VALUE) [709]
GENERATES FINANCIAL INFORMATION IDENTIFIER (INDIVIDUAL IDENTIFICATION VALUE + FINANCIAL INFORMATION) [715]
GENERATE INDIVIDUAL IDENTIFICATION VALUE [707]
ID/PW
SSN
PIN
INDIVIDUAL IDENTIFICATION VALUE
PAYMENT OPTION INFORMATION WINDOW (INDIVIDUAL IDENTIFICATION VALUE) [711]
PAYMENT OPTION INFORMATION (INDIVIDUAL IDENTIFICATION VALUE + FINANCIAL INFORMATION) [713]
PERSONAL IDENTIFICATION INFORMATION
FINANCIAL INFORMATION 1
FINANCIAL INFORMATION 2
FINANCIAL INFORMATION IDENTIFIER 1
FINANCIAL INFORMATION IDENTIFIER 2
PAYMENT INFORMATION REGISTRATION COMPLETION [719]
PAYMENT OPTION REGISTRATION RESULT [717]
ID/PW
SSN
INDIVIDUAL IDENTIFICATION VALUE
FINANCIAL INFORMATION IDENTIFIER 1
FINANCIAL INFORMATION IDENTIFIER 2

FIG. 8A

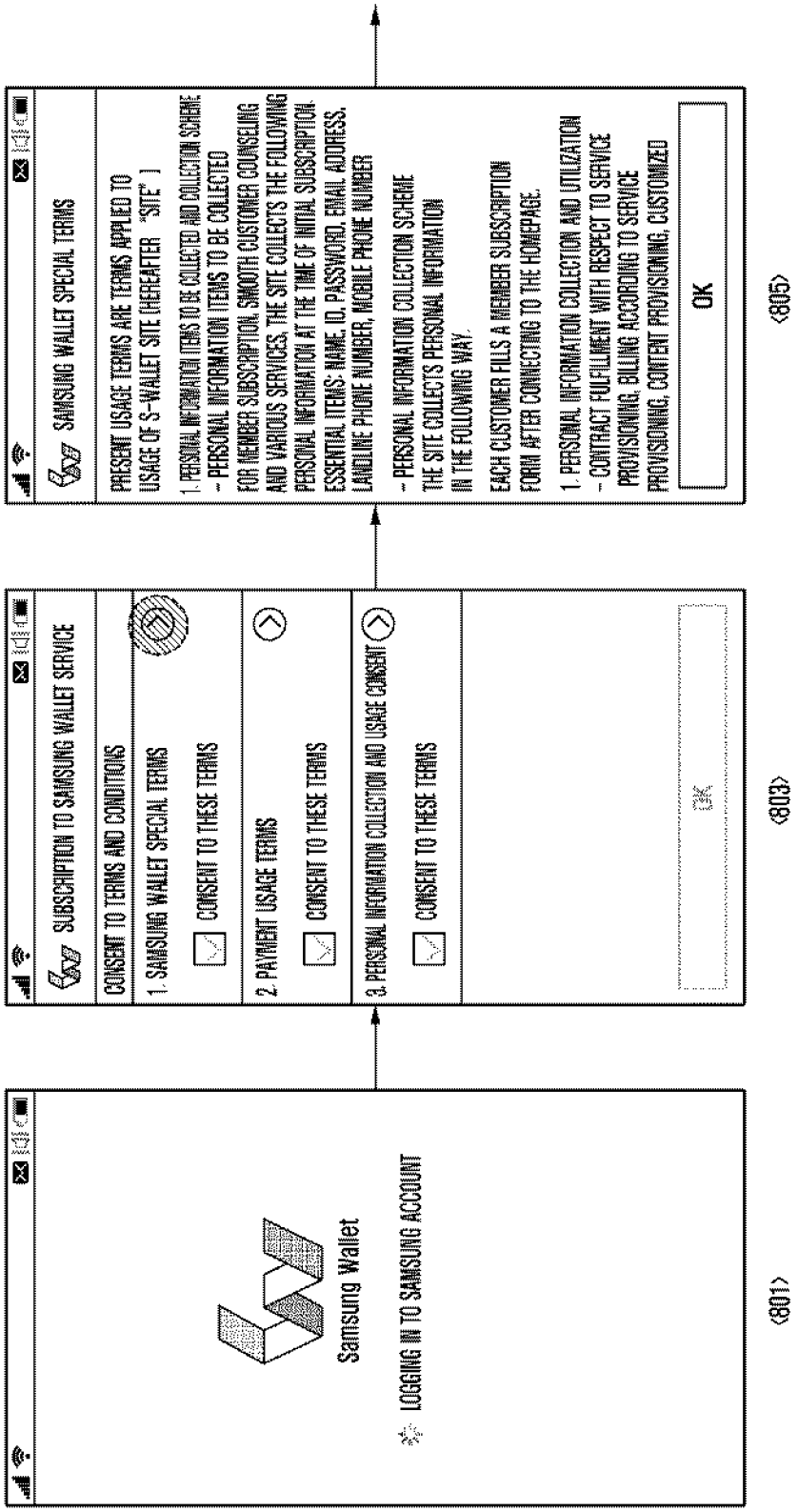

Samsung Wallet
LOGGING IN TO SAMSUNG ACCOUNT
<801>
SUBSCRIPTION TO SAMSUNG WALLET SERVICE
CONSENT TO TERMS AND CONDITIONS
1. SAMSUNG WALLET SPECIAL TERMS
CONSENT TO THESE TERMS
2. PAYMENT USAGE TERMS
CONSENT TO THESE TERMS
3. PERSONAL INFORMATION COLLECTION AND USAGE CONSENT
CONSENT TO THESE TERMS
OK
<803>
SAMSUNG WALLET SPECIAL TERMS
PRESENT USAGE TERMS ARE TERMS APPLIED TO USAGE OF S-WALLET SITE (HEREAFTER "SITE")
1. PERSONAL INFORMATION ITEMS TO BE COLLECTED AND COLLECTION SCHEME
- PERSONAL INFORMATION ITEMS TO BE COLLECTED FOR) MEMBER SUBSCRIPTION, SMOOTH CUSTOMER COUNSELING AND VARIOUS SERVICES, THE SITE COLLECTS THE FOLLOWING PERSONAL INFORMATION AT THE TIME OF INITIAL SUBSCRIPTION.
ESSENTIAL ITEMS: NAME, ID, PASSWORD, EMAIL ADDRESS, LANDLINE PHONE NUMBER, MOBILE PHONE NUMBER
- PERSONAL INFORMATION COLLECTION SCHEME
THE SITE COLLECTS PERSONAL INFORMATION IN THE FOLLOWING WAY.
EACH CUSTOMER FILLS A MEMBER SUBSCRIPTION FORM AFTER CONNECTING TO THE HOMEPAGE.
1. PERSONAL INFORMATION COLLECTION AND UTILIZATION
- CONTRACT FULFILLMENT WITH RESPECT TO SERVICE PROVISIONING, BILLING ACCORDING TO SERVICE PROVISIONING, CONTENT PROVISIONING, CUSTOMIZED
OK
<805>

FIG. 8B

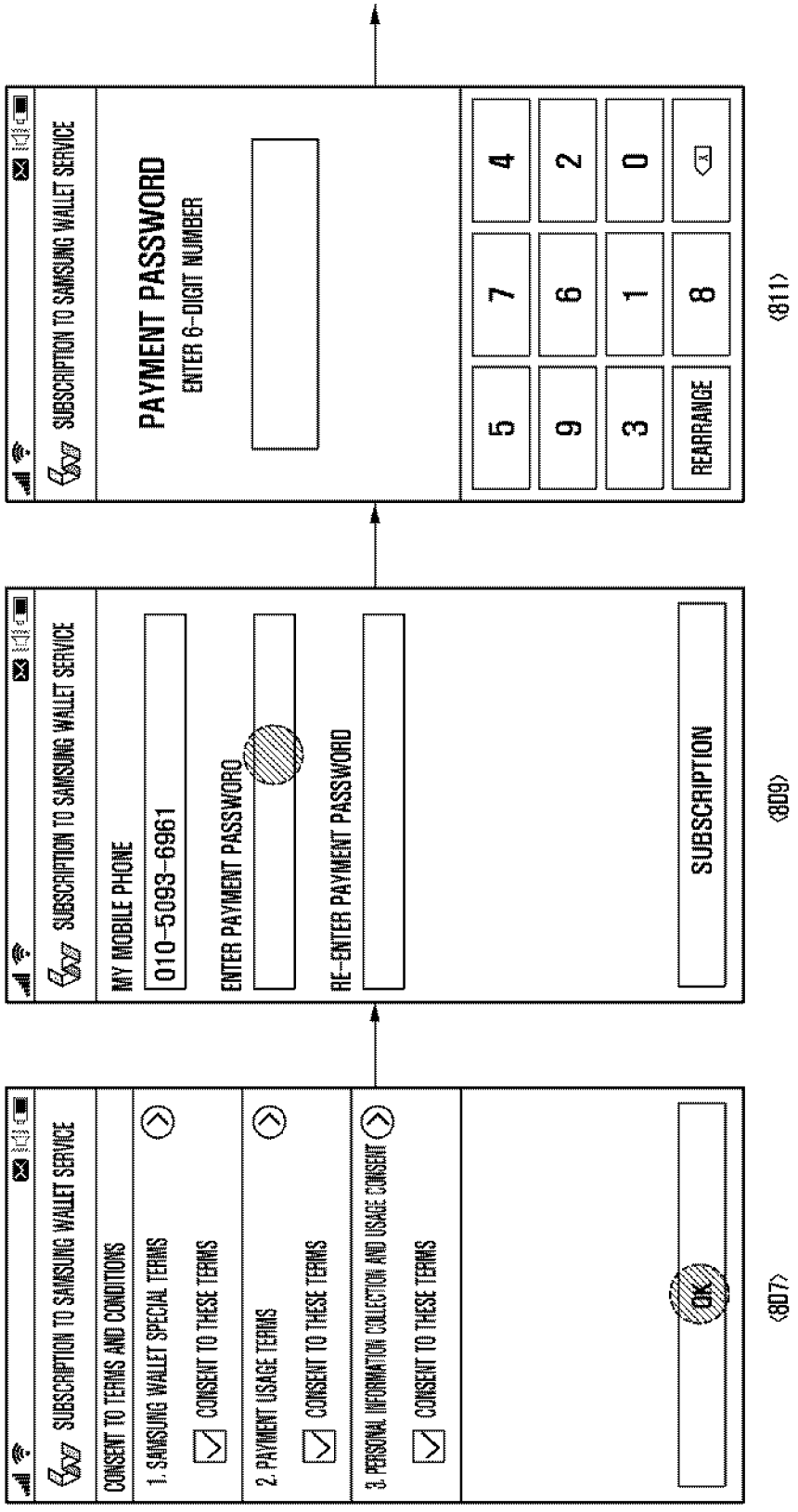

SUBSCRIPTION TO SAMSUNG WALLET SERVICE
CONSENT TO TERMS AND CONDITIONS
1. SAMSUNG WALLET SPECIAL TERMS
CONSENT TO THESE TERMS
2. PAYMENT USAGE TERMS
CONSENT TO THESE TERMS
3. PERSONAL INFORMATION COLLECTION AND USAGE CONSENT
CONSENT TO THESE TERMS
OK
<807>
SUBSCRIPTION TO SAMSUNG WALLET SERVICE
MY MOBILE PHONE
010-5093-6961
ENTER PAYMENT PASSWORD
RE-ENTER PAYMENT PASSWORD
SUBSCRIPTION
<809>
SUBSCRIPTION TO SAMSUNG WALLET SERVICE
PAYMENT PASSWORD
ENTER 6-DIGIT NUMBER
5 7 4
9 6 2
3 1 0
REARRANGE 8
<811>

FIG. 9

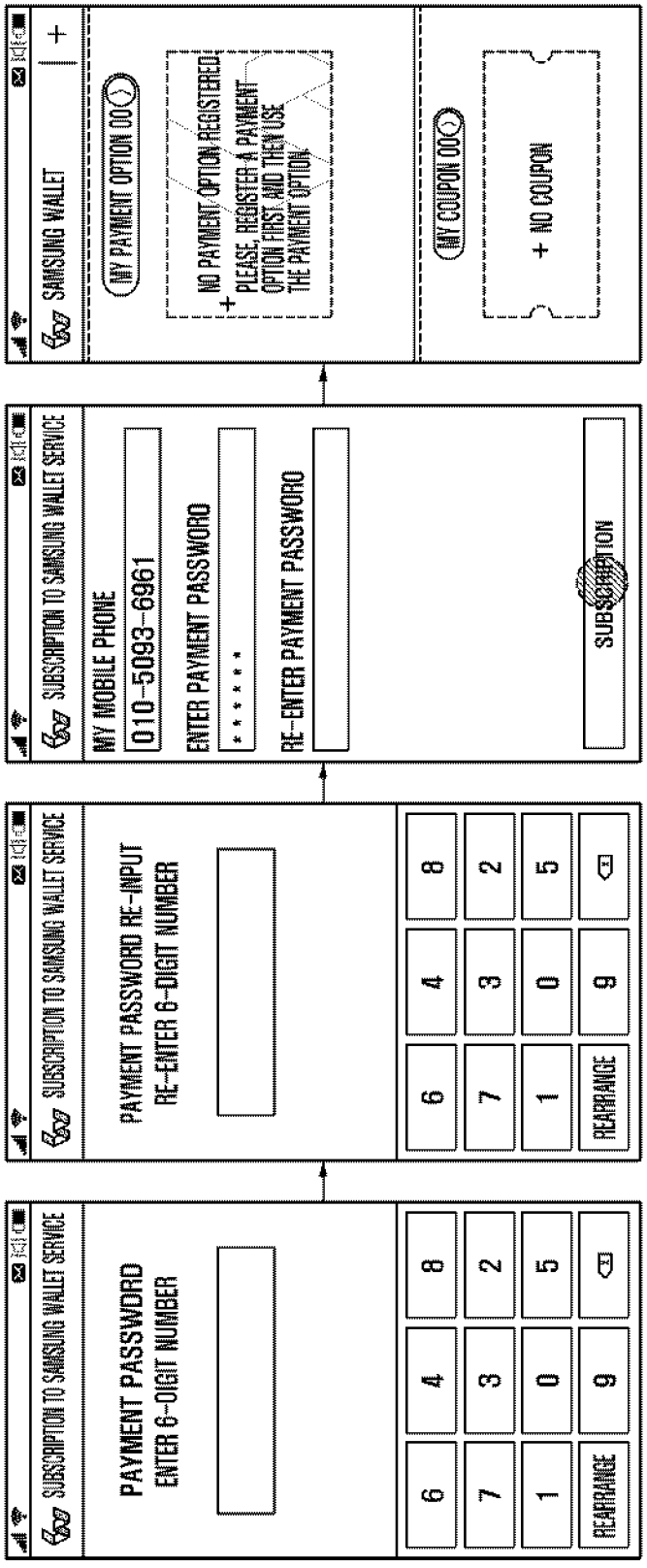

SUBSCRIPTION TO SAMSUNG WALLET SERVICE
PAYMENT PASSWORD
ENTER 6-DIGIT NUMBER
6 4 8
7 3 2
1 0 5
REARRANGE 9
<901>
SUBSCRIPTION TO SAMSUNG WALLET SERVICE
PAYMENT PASSWORD RE-INPUT
RE-ENTER 6-DIGIT NUMBER
6 4 8
7 3 2
1 0 5
REARRANGE 9
<903>
SUBSCRIPTION TO SAMSUNG WALLET SERVICE
MY MOBILE PHONE
010-5093-6961
ENTER PAYMENT PASSWORD
******
RE-ENTER PAYMENT PASSWORD
SUBSCRIPTION
<905>
SAMSUNG WALLET
MY PAYMENT OPTION 00
NO PAYMENT OPTION REGISTERED
+ PLEASE, REGISTER A PAYMENT OPTION FIRST, AND THEN USE THE PAYMENT OPTION
MY COUPON 00
+ NO COUPON
<907>

FIG. 10A

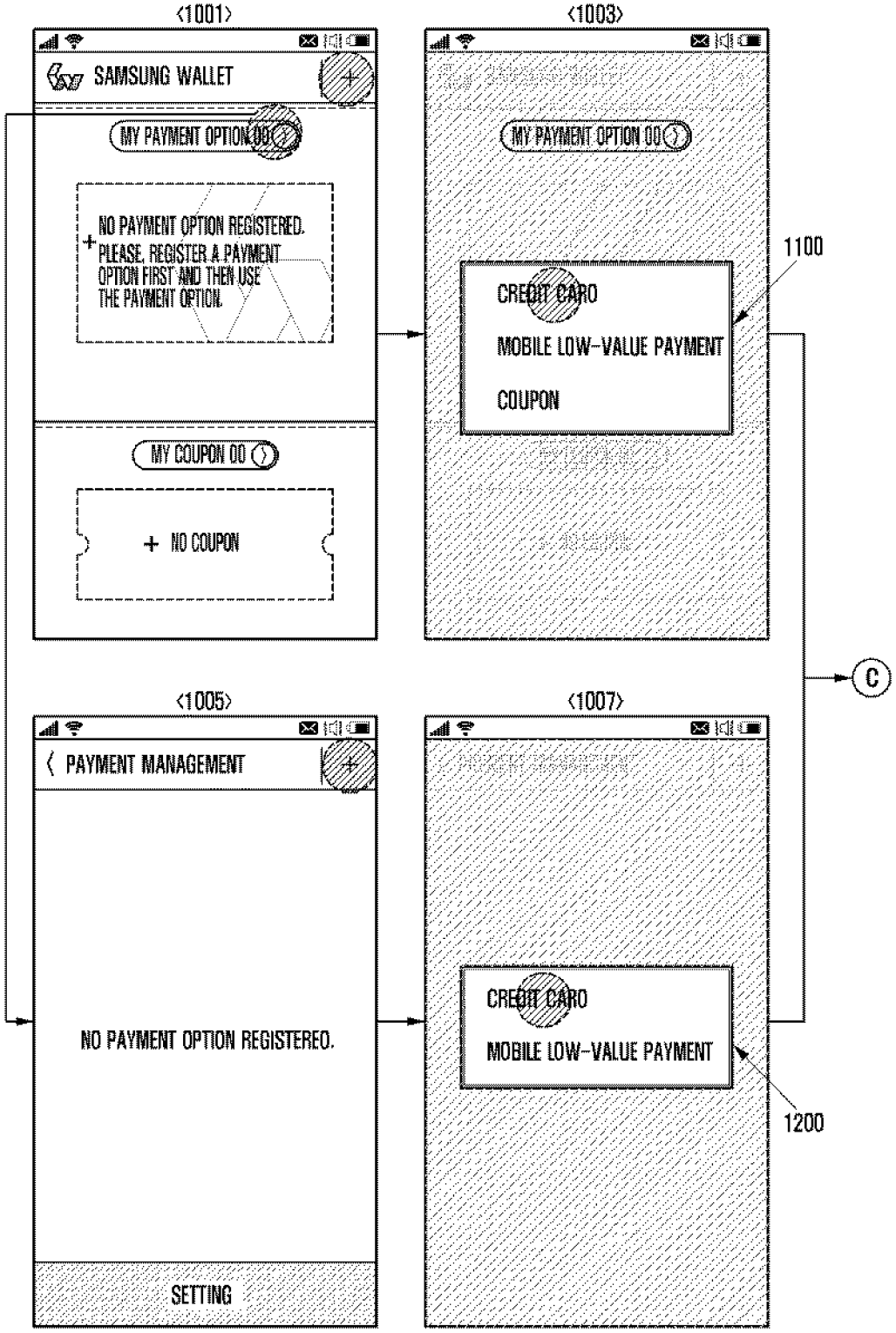

〈1001〉
SAMSUNG WALLET
MY PAYMENT OPTION 00
NO PAYMENT OPTION REGISTERED. PLEASE, REGISTER A PAYMENT OPTION FIRST AND THEN USE THE PAYMENT OPTION.
MY COUPON 00
NO COUPON
〈1003〉
MY PAYMENT OPTION 00
CREDIT CARD
MOBILE LOW-VALUE PAYMENT
COUPON
1100
C
〈1005〉
PAYMENT MANAGEMENT
NO PAYMENT OPTION REGISTERED.
SETTING
〈1007〉
CREDIT CARD
MOBILE LOW-VALUE PAYMENT
1200

FIG. 10B

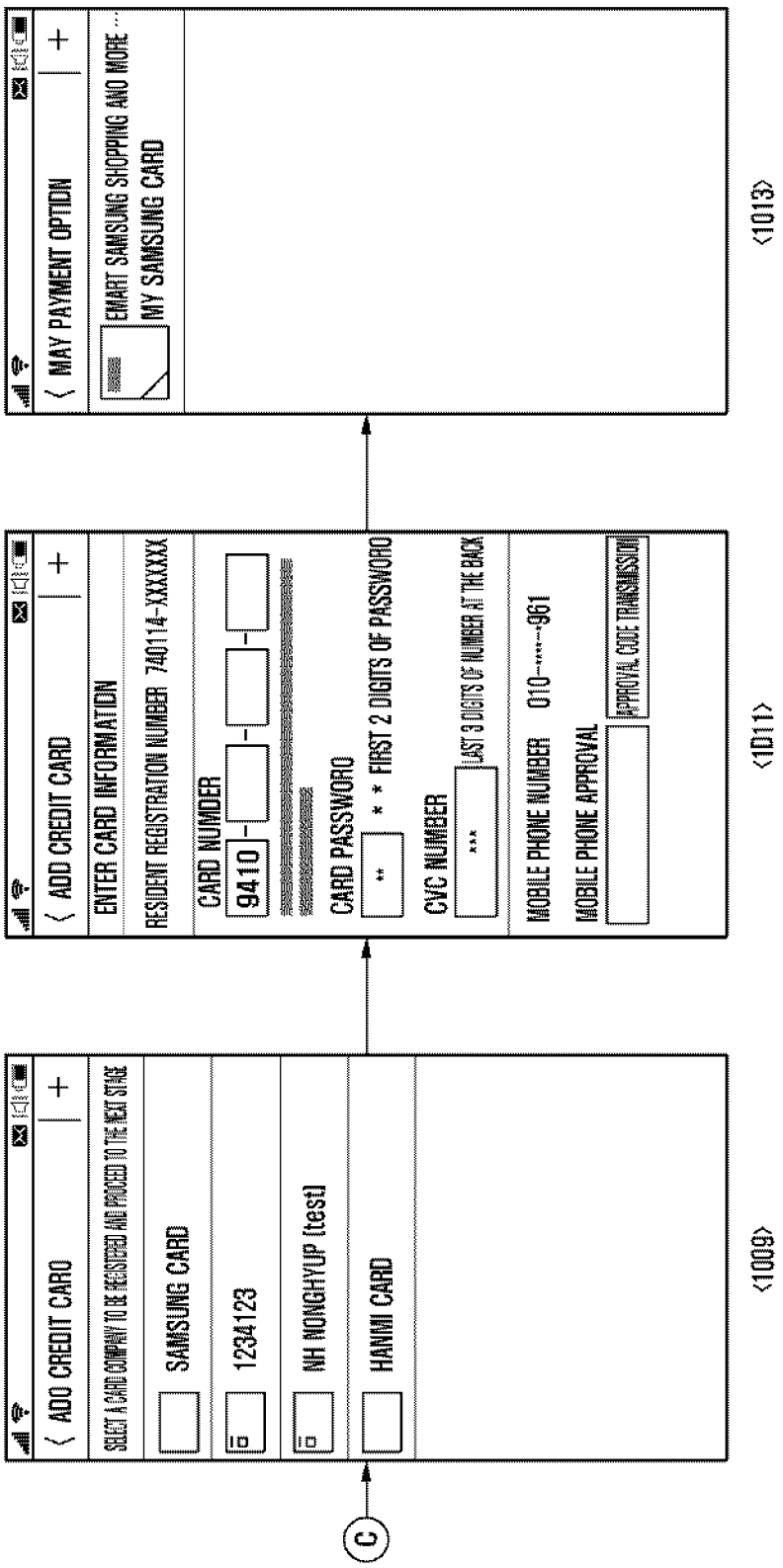

C
ADD CREDIT CARD
SELECT A CARD COMPANY TO BE REGISTERED AND PROCEED TO THE NEXT STAGE
SAMSUNG CARD
1234123
NH NONGHYUP (test)
HANMI CARD
<1009>
ADD CREDIT CARD
ENTER CARD INFORMATION
RESIDENT REGISTRATION NUMBER 740114-XXXXXXX
CARD NUMBER
9410
CARD PASSWORD
** FIRST 2 DIGITS OF PASSWORD
CVC NUMBER
*** LAST 3 DIGITS OF NUMBER AT THE BACK
MOBILE PHONE NUMBER 010-****-961
MOBILE PHONE APPROVAL
APPROVAL CODE TRANSMISSION
<1011>
MAY PAYMENT OPTION
EMART SAMSUNG SHOPPING AND MORE ...
MY SAMSUNG CARD
<1013>

FIG. 11

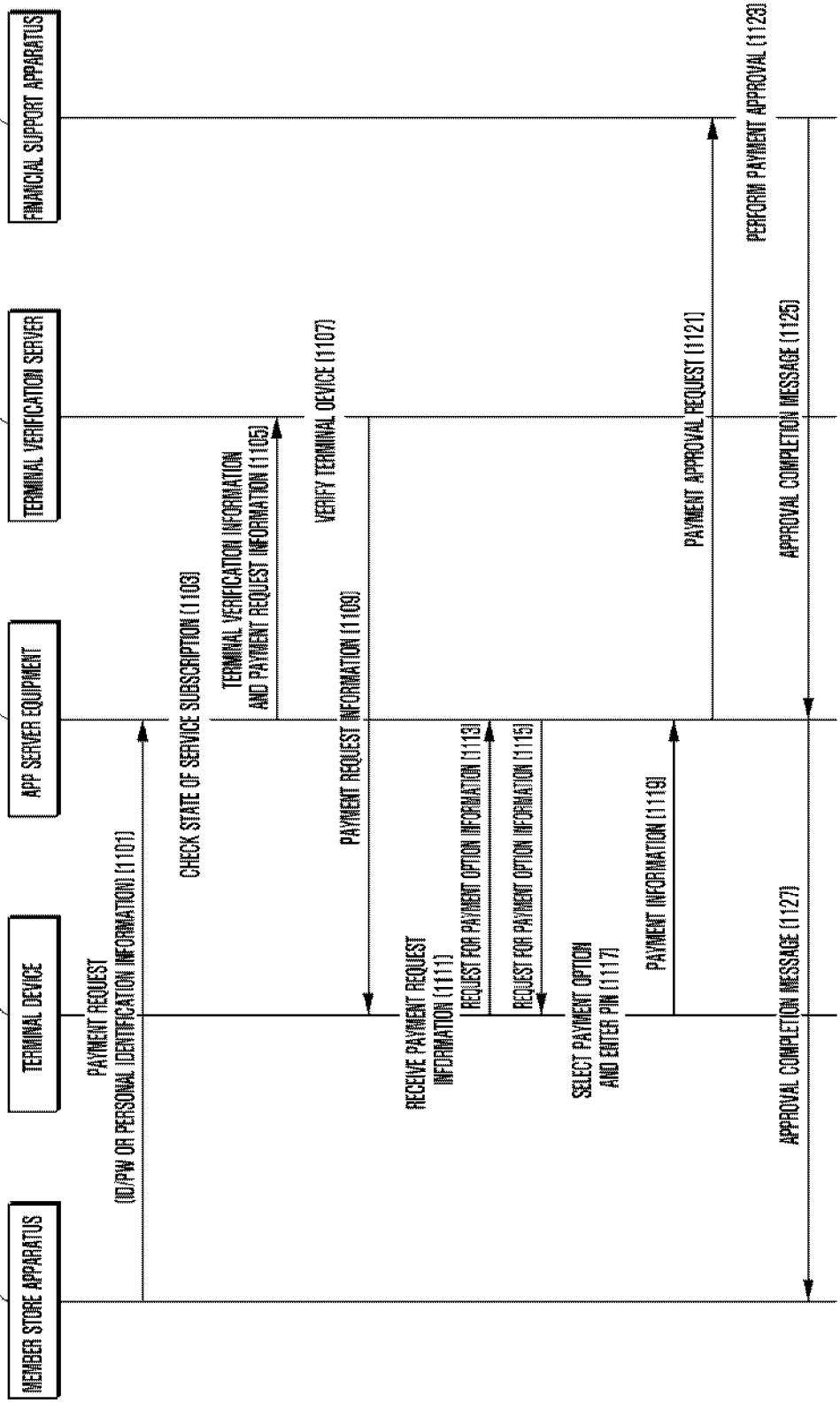

400
MEMBER STORE APPARATUS
100
TERMINAL DEVICE
290
APP SERVER EQUIPMENT
280
TERMINAL VERIFICATION SERVER
500
FINANCIAL SUPPORT APPARATUS
PAYMENT REQUEST (ID/PW OR PERSONAL IDENTIFICATION INFORMATION) (11101)
CHECK STATE OF SERVICE SUBSCRIPTION (11103)
TERMINAL VERIFICATION INFORMATION AND PAYMENT REQUEST INFORMATION (11105)
VERIFY TERMINAL DEVICE (11107)
PAYMENT REQUEST INFORMATION (11109)
RECEIVE PAYMENT REQUEST INFORMATION (11111)
REQUEST FOR PAYMENT OPTION INFORMATION (11113)
REQUEST FOR PAYMENT OPTION INFORMATION (11115)
SELECT PAYMENT OPTION AND ENTER PIN (11117)
PAYMENT INFORMATION (11119)
PAYMENT APPROVAL REQUEST (11121)
PERFORM PAYMENT APPROVAL (11123)
APPROVAL COMPLETION MESSAGE (11125)
APPROVAL COMPLETION MESSAGE (11127)

FIG. 12

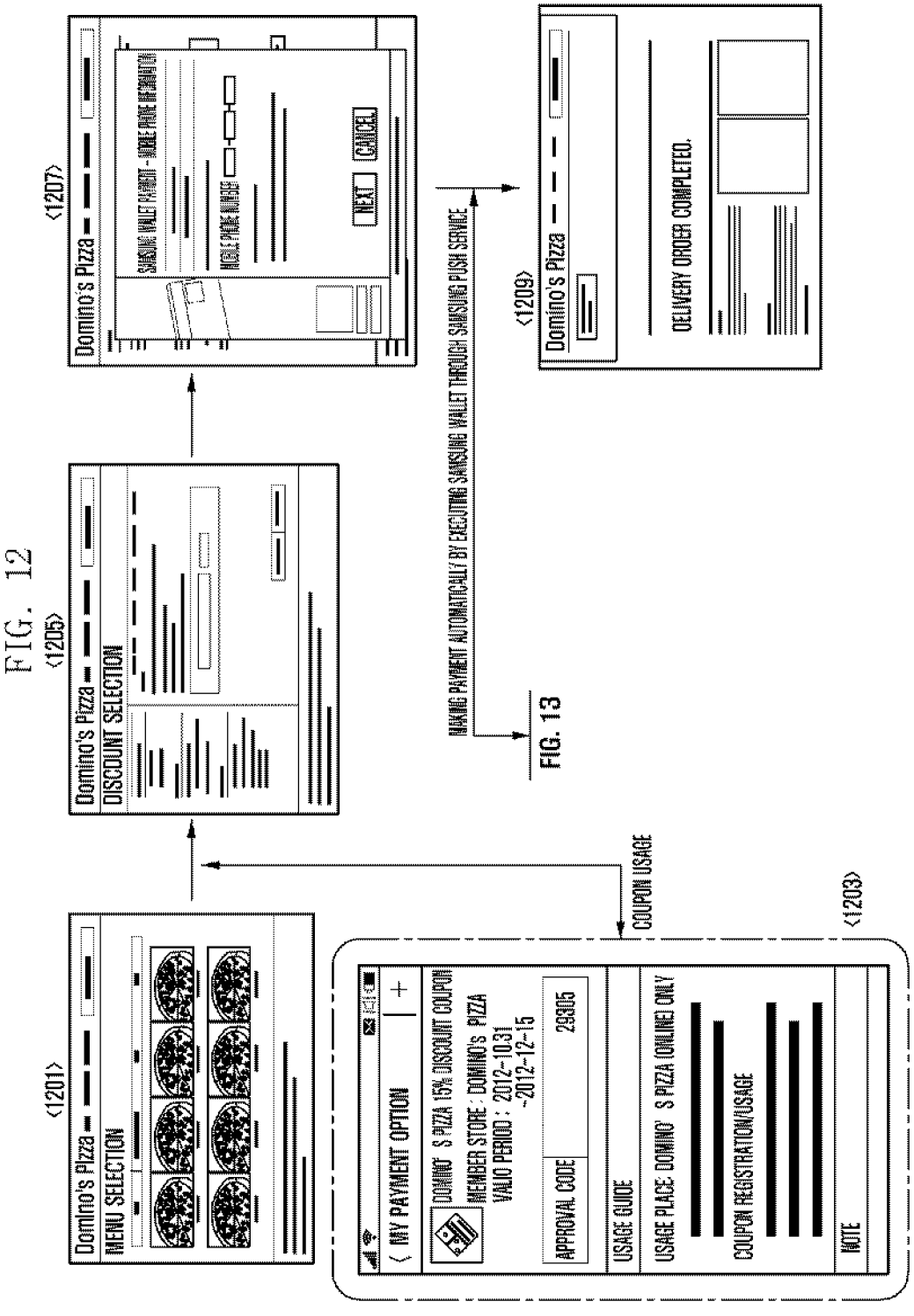

<1201>
Domino's Pizza
MENU SELECTION
<1205>
Domino's Pizza
DISCOUNT SELECTION
<1207>
Domino's Pizza
SAMSUNG WALLET PAYMENT - MOBILE PHONE PAYMENT(0)
MOBILE PHONE NUMBER
NEXT
CANCEL
MAKING PAYMENT AUTOMATICALLY BY EXECUTING SAMSUNG WALLET THROUGH SAMSUNG PUSH SERVICE
<1209>
Domino's Pizza
DELIVERY ORDER COMPLETED.
COUPON USAGE
<1203>
< MY PAYMENT OPTION
DOMINO'S PIZZA 15% DISCOUNT COUPON
MEMBER STORE : DOMINO's PIZZA
VALID PERIOD : 2012-10-31
~2012-12-15
APPROVAL CODE
29305
USAGE GUIDE
USAGE PLACE: DOMINO'S PIZZA (ONLINE) ONLY
COUPON REGISTRATION/USAGE
NOTE

FIG. 13

FIG. 13

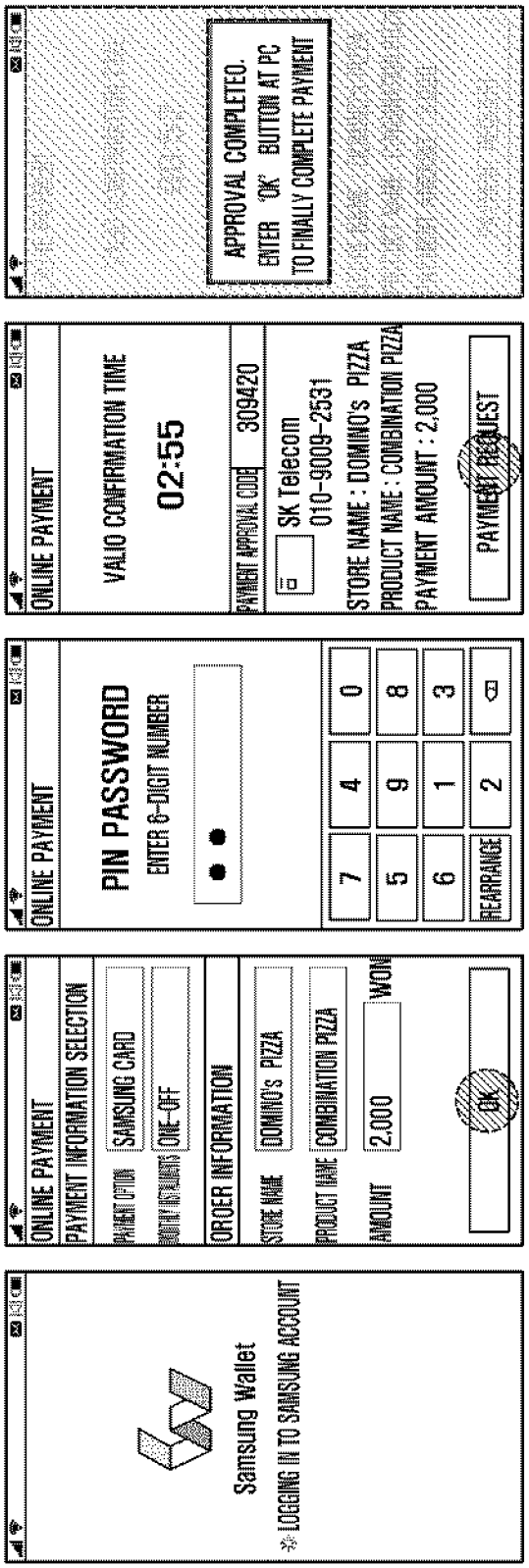

1301
Samsung Wallet
LOGGING IN TO SAMSUNG ACCOUNT
1303
ONLINE PAYMENT
PAYMENT INFORMATION SELECTION
PAYMENT OPTION
SAMSUNG CARD
DISCOUNT INFORMATION
ONE-OFF
ORDER INFORMATION
STORE NAME
DOMINO's PIZZA
PRODUCT NAME
COMBINATION PIZZA
AMOUNT
2,000
WON
OK
1305
ONLINE PAYMENT
PIN PASSWORD
ENTER 6-DIGIT NUMBER
7
4
0
5
9
8
6
1
3
REARRANGE
2
1307
ONLINE PAYMENT
VALID CONFIRMATION TIME
02:55
PAYMENT APPROVAL CODE
309420
SK Telecom
010-9009-2531
STORE NAME : DOMINO's PIZZA
PRODUCT NAME : COMBINATION PIZZA
PAYMENT AMOUNT : 2,000
PAYMENT REQUEST
1309
APPROVAL COMPLETED.
ENTER 'OK' BUTTON AT PC
TO FINALLY COMPLETE PAYMENT

FIG. 14

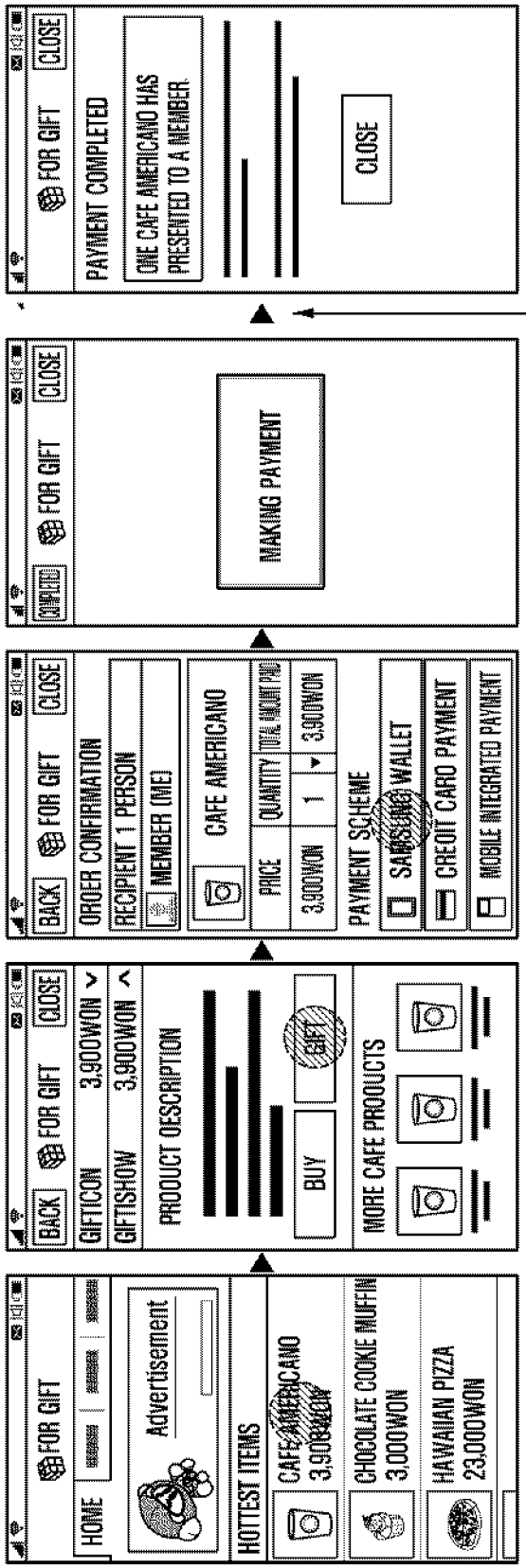

〈1401〉
FOR GIFT
HOME
Advertisement
HOTTEST ITEMS
CAFE AMERICANO
3,900WON
CHOCOLATE COOKIE MUFFIN
3,000WON
HAWAIIAN PIZZA
23,000WON
〈1403〉
BACK
FOR GIFT
CLOSE
GIFTICON
3,900WON
GIFTISHOW
3,900WON
PRODUCT DESCRIPTION
BUY
GIFT
MORE CAFE PRODUCTS
〈1405〉
BACK
FOR GIFT
CLOSE
ORDER CONFIRMATION
RECIPIENT 1 PERSON
MEMBER (ME)
CAFE AMERICANO
PRICE
QUANTITY
TOTAL AMOUNT PAID
3,900WON
1
3,900WON
PAYMENT SCHEME
SAMSUNG WALLET
CREDIT CARD PAYMENT
MOBILE INTEGRATED PAYMENT
〈1407〉
COMPLETED
FOR GIFT
CLOSE
MAKING PAYMENT
〈1409〉
FOR GIFT
CLOSE
PAYMENT COMPLETED
ONE CAFE AMERICANO HAS PRESENTED TO A MEMBER
CLOSE

FIG. 15

FIG. 15

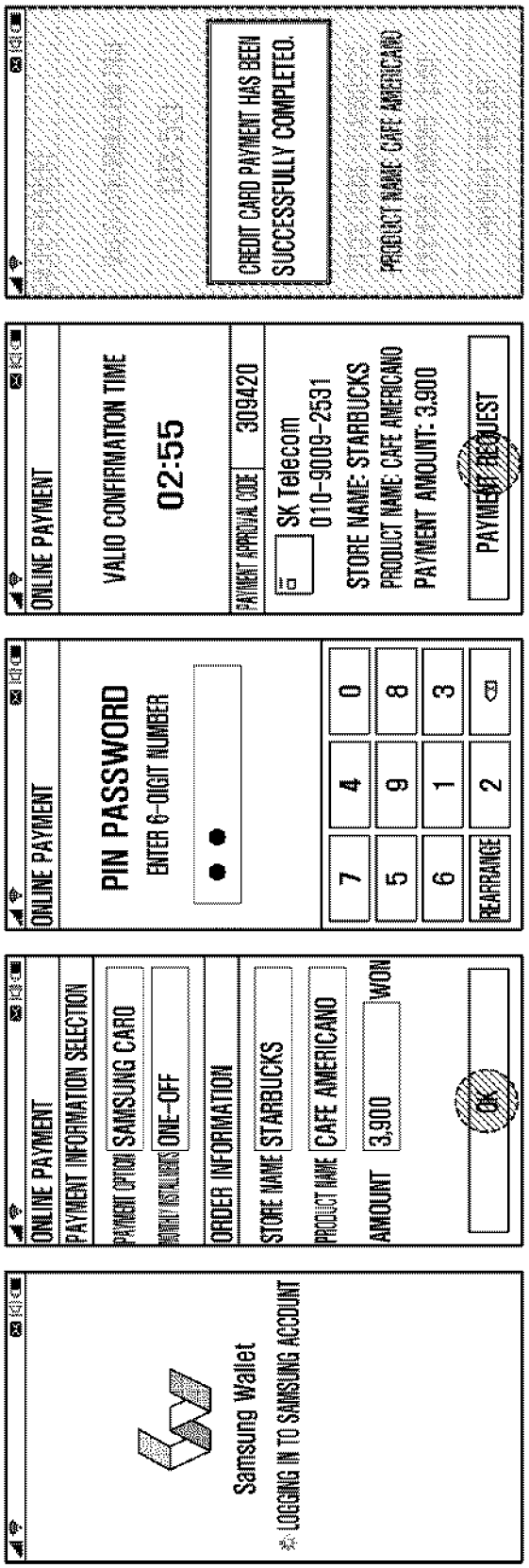

1501
Samsung Wallet
LOGGING IN TO SAMSUNG ACCOUNT
1503
ONLINE PAYMENT
PAYMENT INFORMATION SELECTION
PAYMENT OPTION SAMSUNG CARD
ONE-OFF
ORDER INFORMATION
STORE NAME STARBUCKS
PRODUCT NAME CAFE AMERICANO
AMOUNT 3,900 WON
OK
1505
ONLINE PAYMENT
PIN PASSWORD
ENTER 6-DIGIT NUMBER
7 4 0
5 9 8
6 1 3
REARRANGE 2
1507
ONLINE PAYMENT
VALID CONFIRMATION TIME
02:55
PAYMENT APPROVAL CODE 309420
SK Telecom
010-9009-2531
STORE NAME: STARBUCKS
PRODUCT NAME: CAFE AMERICANO
PAYMENT AMOUNT: 3,900
PAYMENT REQUEST
1509
CREDIT CARD PAYMENT HAS BEEN SUCCESSFULLY COMPLETED.
PRODUCT NAME: CAFE AMERICANO

FIG. 16

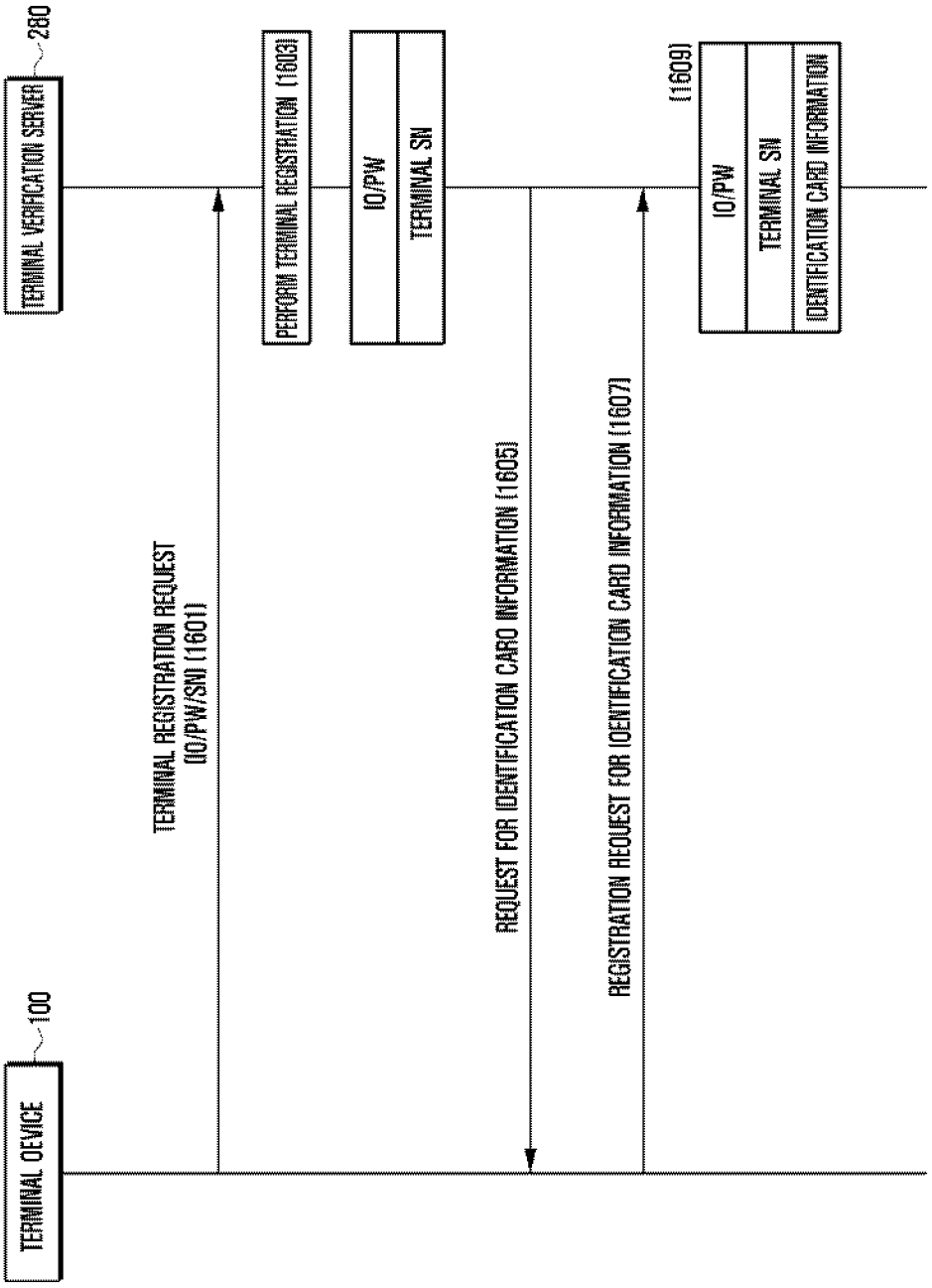

TERMINAL DEVICE
100
TERMINAL VERIFICATION SERVER
280
TERMINAL REGISTRATION REQUEST (ID/PW/SN) (1601)
PERFORM TERMINAL REGISTRATION (1603)
ID/PW
TERMINAL SN
REQUEST FOR IDENTIFICATION CARD INFORMATION (1605)
REGISTRATION REQUEST FOR IDENTIFICATION CARD INFORMATION (1607)
(1609)
ID/PW
TERMINAL SN
IDENTIFICATION CARD INFORMATION

FIG. 17

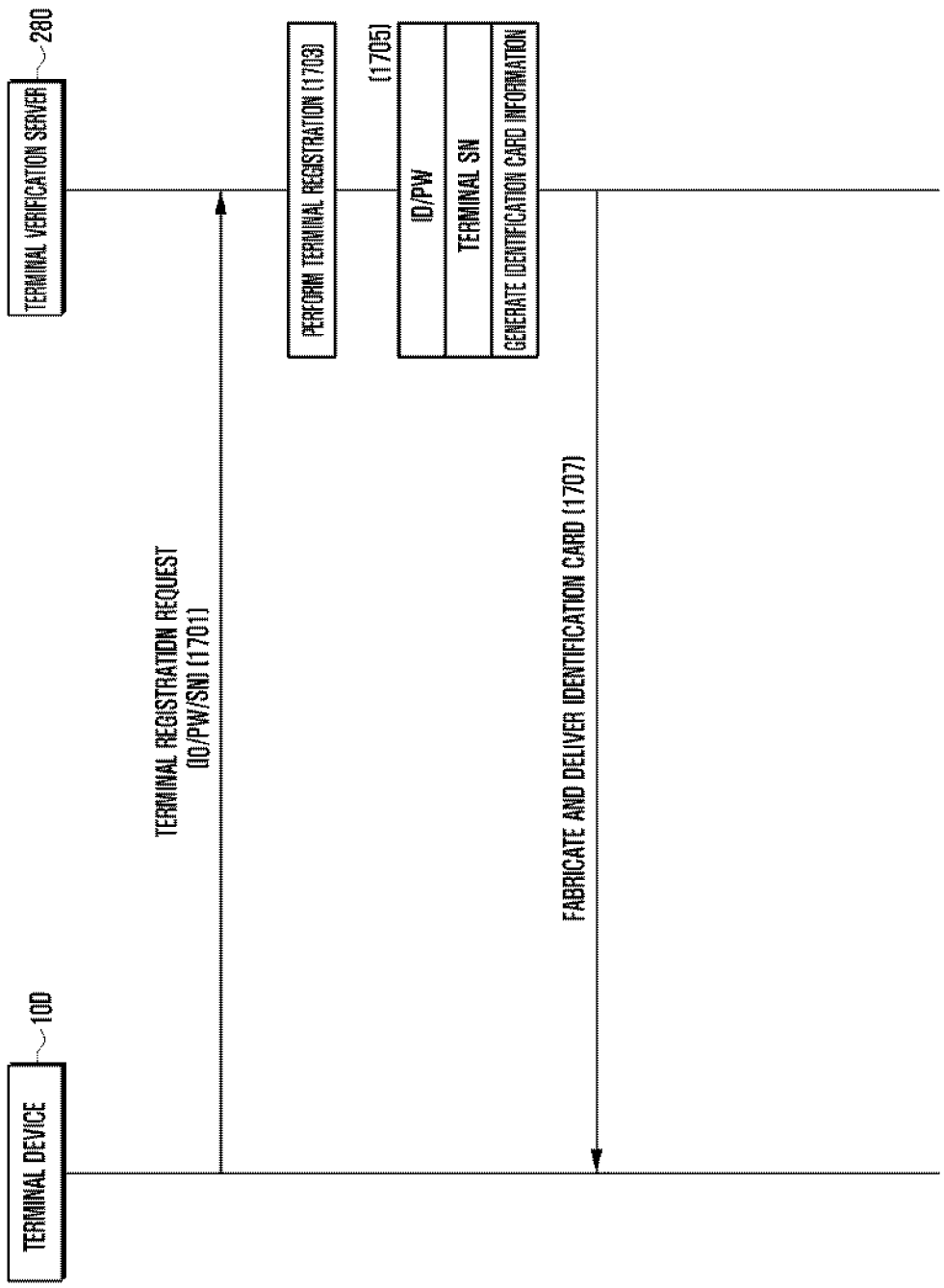

TERMINAL DEVICE
100
TERMINAL VERIFICATION SERVER
280
TERMINAL REGISTRATION REQUEST
(ID/PW/SN) (1701)
PERFORM TERMINAL REGISTRATION (1703)
(1705)
ID/PW
TERMINAL SN
GENERATE IDENTIFICATION CARD INFORMATION
FABRICATE AND DELIVER IDENTIFICATION CARD (1707)

FIG. 18

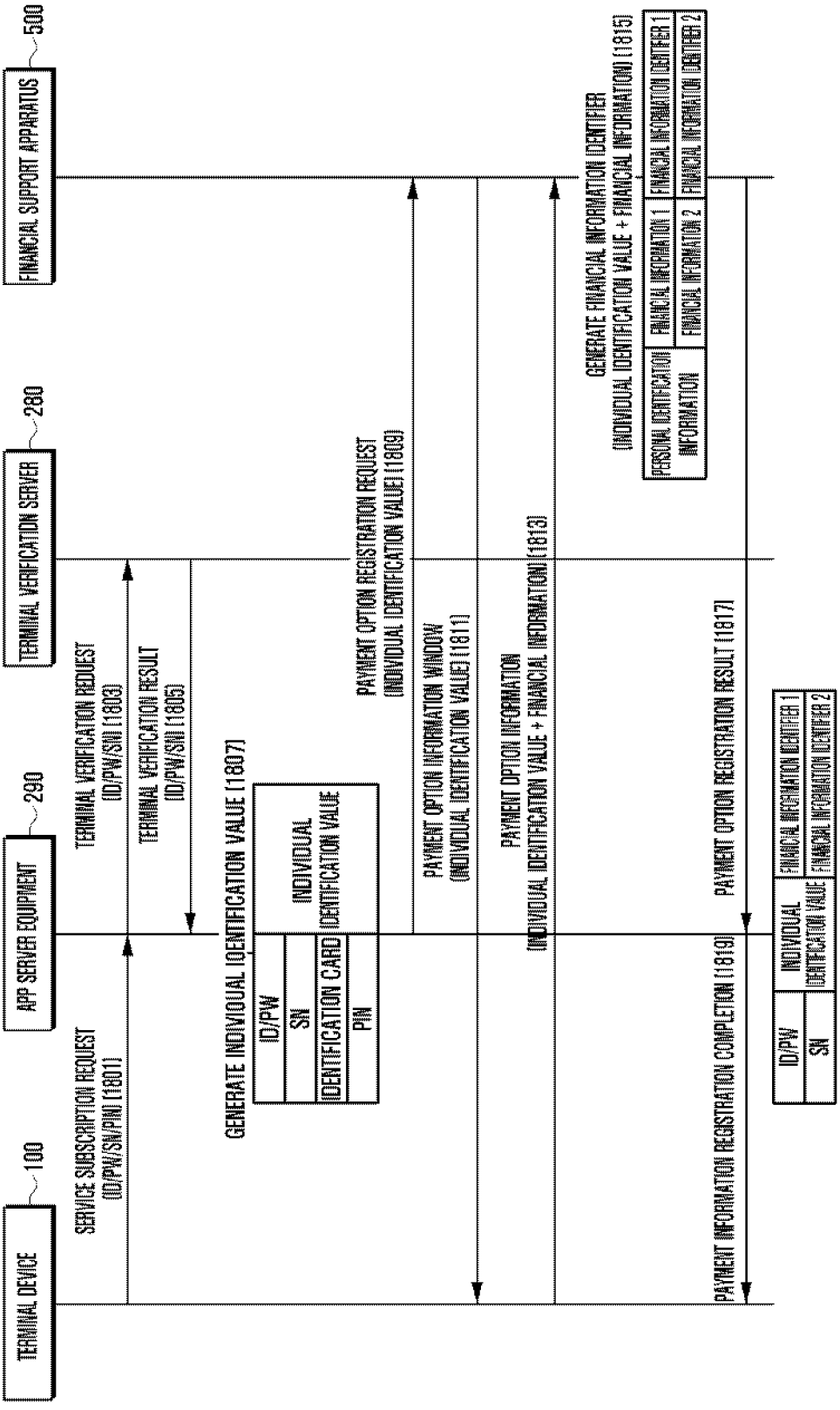

TERMINAL DEVICE
100
APP SERVER EQUIPMENT
290
TERMINAL VERIFICATION SERVER
280
FINANCIAL SUPPORT APPARATUS
500
SERVICE SUBSCRIPTION REQUEST (ID/PW/SN/PIN) (1801)
TERMINAL VERIFICATION REQUEST (ID/PW/SN) (1803)
TERMINAL VERIFICATION RESULT (ID/PW/SN) (1805)
GENERATE INDIVIDUAL IDENTIFICATION VALUE (1807)
ID/PW
SN
IDENTIFICATION CARD
PIN
INDIVIDUAL IDENTIFICATION VALUE
PAYMENT OPTION REGISTRATION REQUEST (INDIVIDUAL IDENTIFICATION VALUE) (1809)
PAYMENT OPTION INFORMATION WINDOW (INDIVIDUAL IDENTIFICATION VALUE) (1811)
PAYMENT OPTION INFORMATION (INDIVIDUAL IDENTIFICATION VALUE + FINANCIAL INFORMATION) (1813)
GENERATE FINANCIAL INFORMATION IDENTIFIER (INDIVIDUAL IDENTIFICATION VALUE + FINANCIAL INFORMATION) (1815)
PERSONAL IDENTIFICATION INFORMATION
FINANCIAL INFORMATION 1
FINANCIAL INFORMATION 2
FINANCIAL INFORMATION IDENTIFIER 1
FINANCIAL INFORMATION IDENTIFIER 2
PAYMENT OPTION REGISTRATION RESULT (1817)
PAYMENT INFORMATION REGISTRATION COMPLETION (1819)
ID/PW
SN
INDIVIDUAL IDENTIFICATION VALUE
FINANCIAL INFORMATION IDENTIFIER 1
FINANCIAL INFORMATION IDENTIFIER 2

FIG. 19

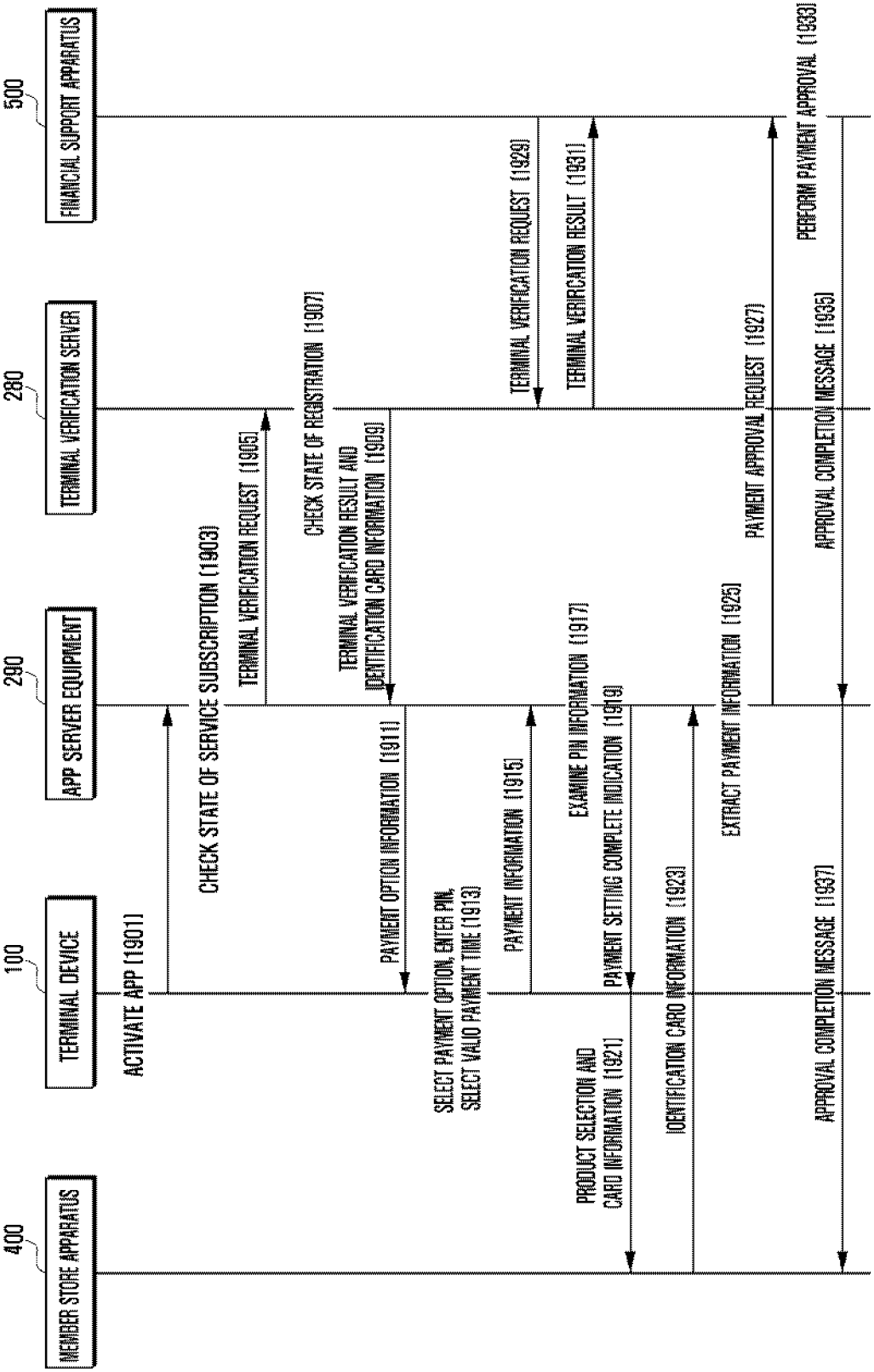

400
MEMBER STORE APPARATUS
100
TERMINAL DEVICE
290
APP SERVER EQUIPMENT
280
TERMINAL VERIFICATION SERVER
500
FINANCIAL SUPPORT APPARATUS
ACTIVATE APP (19901)
CHECK STATE OF SERVICE SUBSCRIPTION (19903)
TERMINAL VERIFICATION REQUEST (19905)
CHECK STATE OF REGISTRATION (19907)
TERMINAL VERIFICATION RESULT AND IDENTIFICATION CARD INFORMATION (19909)
TERMINAL VERIFICATION REQUEST (19929)
TERMINAL VERIFICATION RESULT (19931)
PAYMENT OPTION INFORMATION (19911)
SELECT PAYMENT OPTION, ENTER PIN, SELECT VALID PAYMENT TIME (19913)
PAYMENT INFORMATION (19915)
EXAMINE PIN INFORMATION (19917)
PAYMENT SETTING COMPLETE INDICATION (19919)
PRODUCT SELECTION AND CARD INFORMATION (19921)
IDENTIFICATION CARD INFORMATION (19923)
EXTRACT PAYMENT INFORMATION (19925)
PAYMENT APPROVAL REQUEST (19927)
PERFORM PAYMENT APPROVAL (19933)
APPROVAL COMPLETION MESSAGE (19935)
APPROVAL COMPLETION MESSAGE (19937)

FIG. 20

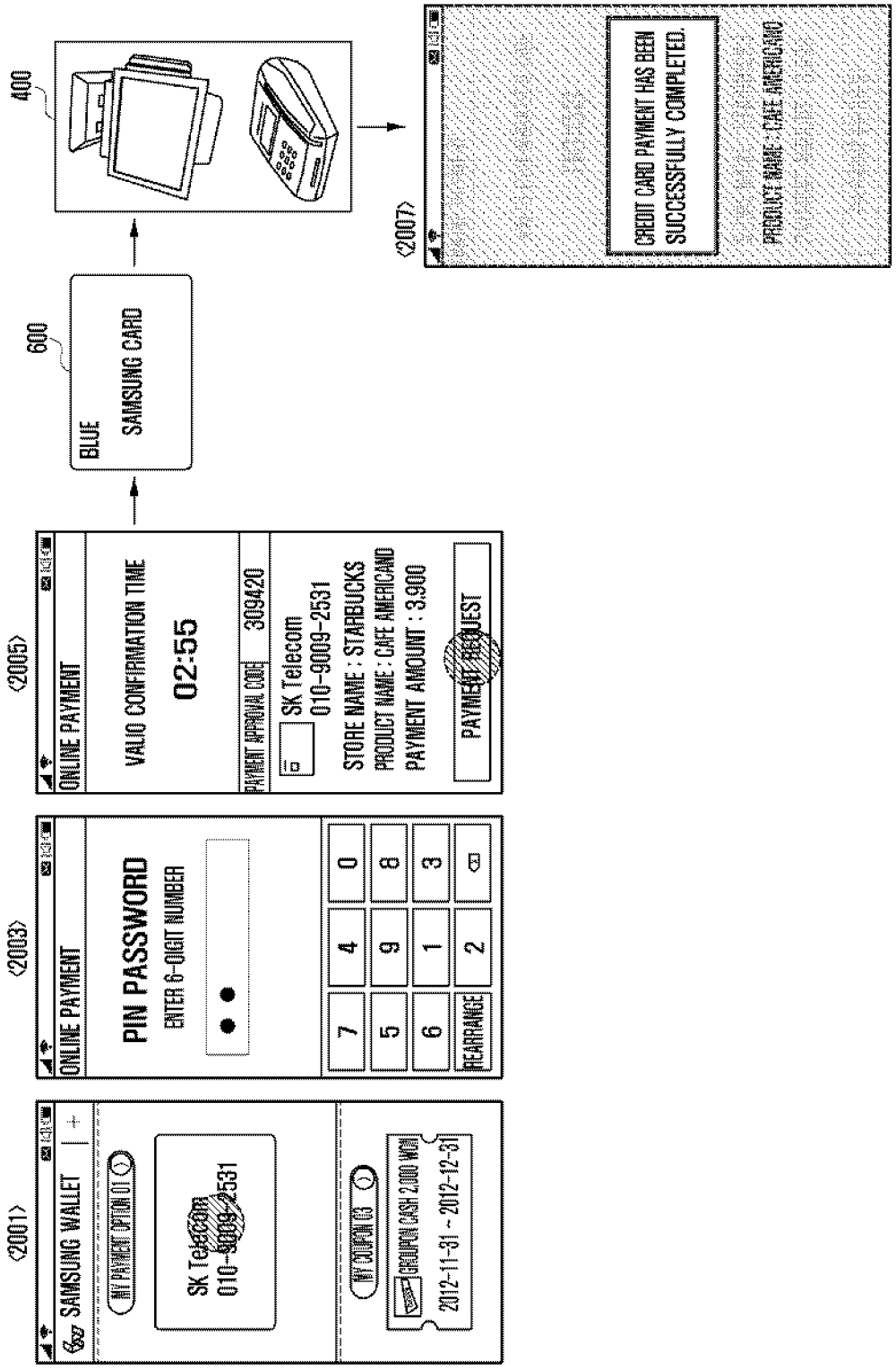

〈2001〉
SAMSUNG WALLET
MY PAYMENT OPTION 01
SK Telecom
010-9009-2531
MY COUPON 03
2012-11-31 ~ 2012-12-31
〈2003〉
ONLINE PAYMENT
PIN PASSWORD
ENTER 6-DIGIT NUMBER
REARRANGE
〈2005〉
ONLINE PAYMENT
VALID CONFIRMATION TIME
02:55
PAYMENT APPROVAL CODE 309420
SK Telecom
010-9009-2531
STORE NAME : STARBUCKS
PRODUCT NAME : CAFE AMERICANO
PAYMENT AMOUNT : 3,900
PAYMENT REQUEST
600
BLUE
SAMSUNG CARD
400
〈2007〉
CREDIT CARD PAYMENT HAS BEEN SUCCESSFULLY COMPLETED.
PRODUCT NAME : CAFE AMERICANO

FIG. 21

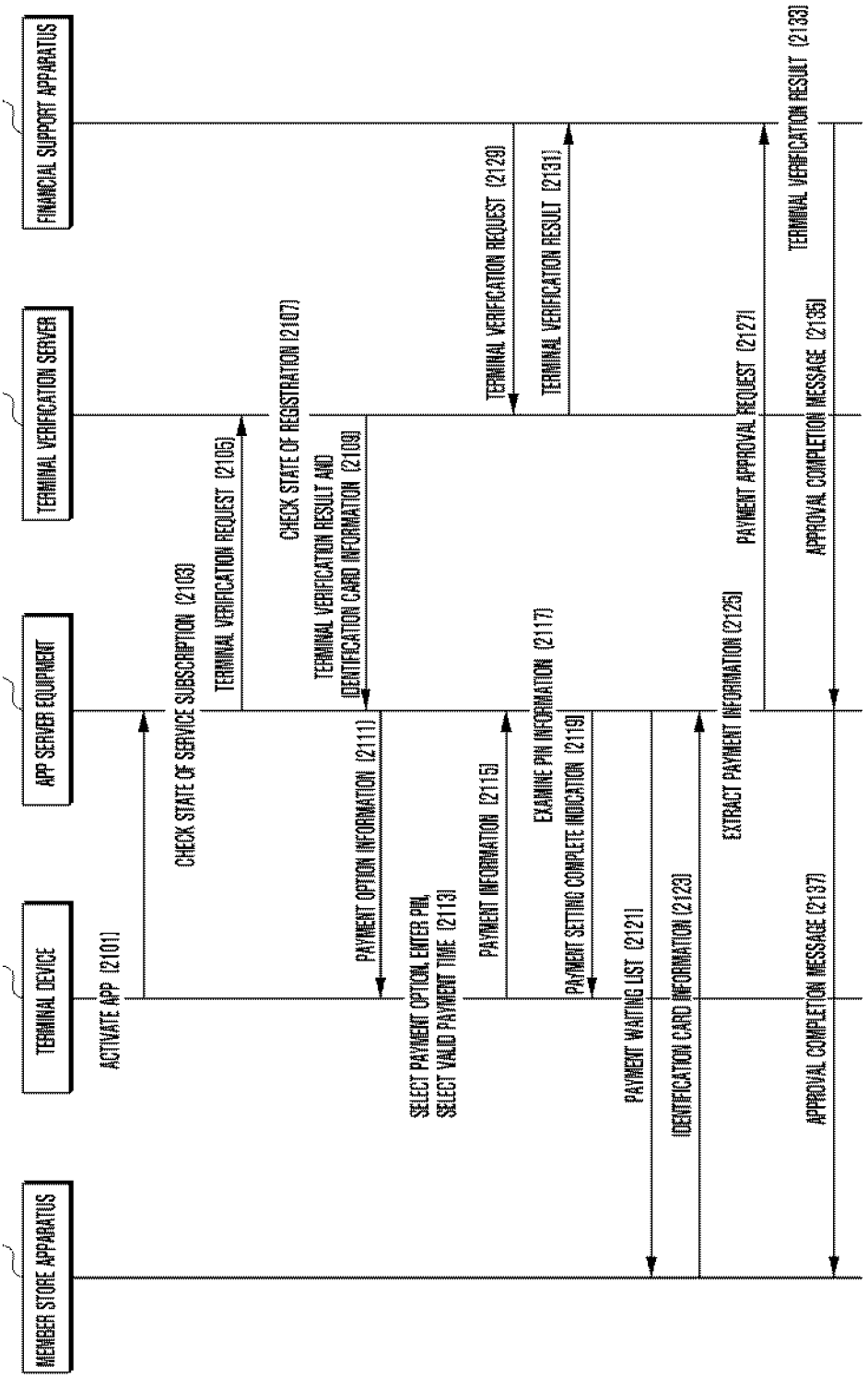
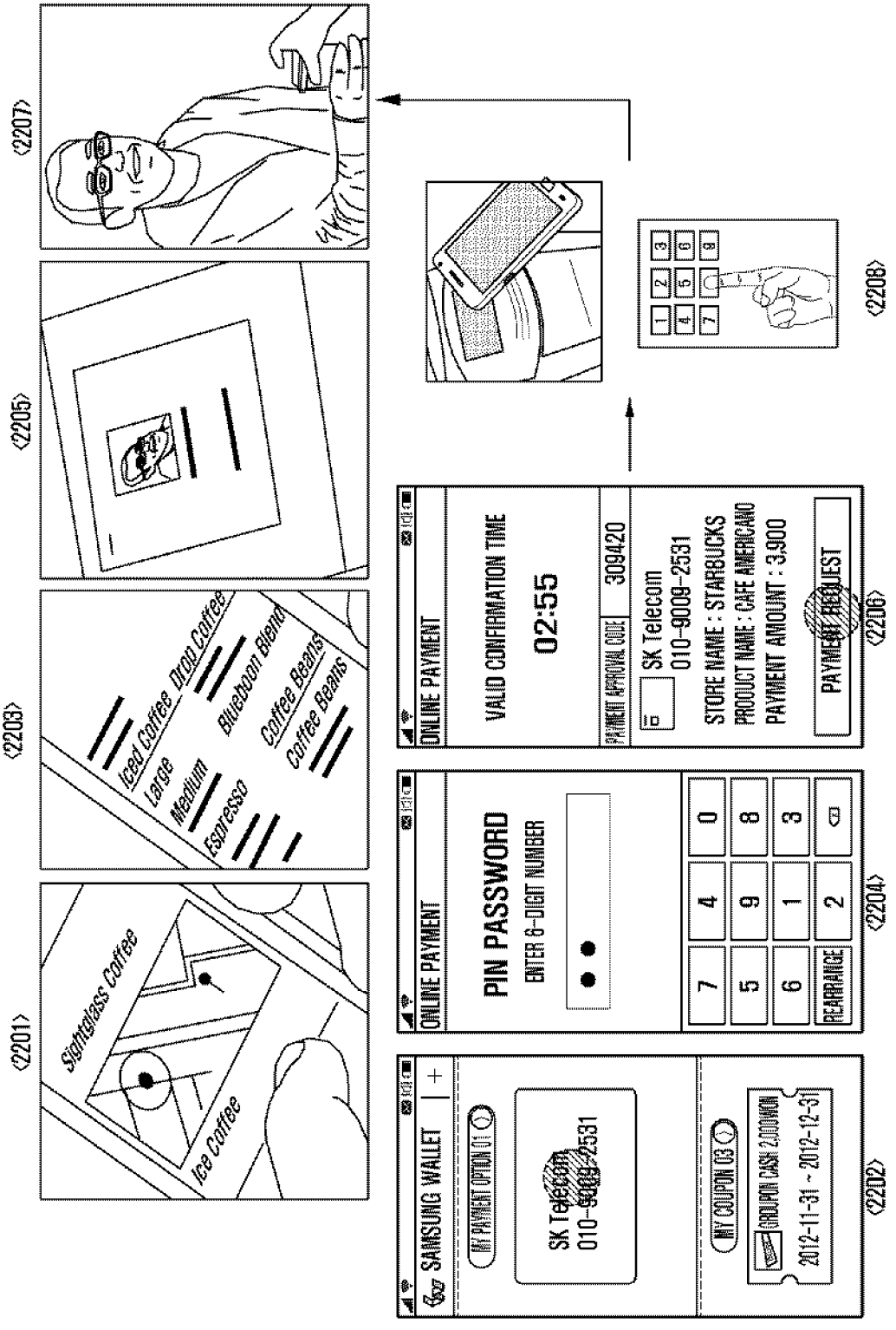

400
MEMBER STORE APPARATUS
100
TERMINAL DEVICE
290
APP SERVER EQUIPMENT
280
TERMINAL VERIFICATION SERVER
500
FINANCIAL SUPPORT APPARATUS
ACTIVATE APP (2101)
CHECK STATE OF SERVICE SUBSCRIPTION (2103)
TERMINAL VERIFICATION REQUEST (2105)
CHECK STATE OF REGISTRATION (2107)
TERMINAL VERIFICATION RESULT AND IDENTIFICATION CARD INFORMATION (2109)
TERMINAL VERIFICATION REQUEST (2129)
TERMINAL VERIFICATION RESULT (2131)
PAYMENT OPTION INFORMATION (2111)
SELECT PAYMENT OPTION, ENTER PIN, SELECT VALID PAYMENT TIME (2113)
PAYMENT INFORMATION (2115)
EXAMINING PIN INFORMATION (2117)
PAYMENT SETTING COMPLETE INDICATION (2119)
PAYMENT APPROVAL REQUEST (2127)
TERMINAL VERIFICATION RESULT (2133)
APPROVAL COMPLETION MESSAGE (2135)
PAYMENT WAITING LIST (2121)
IDENTIFICATION CARD INFORMATION (2123)
EXTRACT PAYMENT INFORMATION (2125)
APPROVAL COMPLETION MESSAGE (2137)

FIG. 22


〈2201〉
Sightglass Coffee
Ice Coffee
〈2203〉
Iced Coffee Drop Coffee
Large
Medium
Espresso
Bluebean Blend
Coffee Beans
Coffee Beans
〈2205〉
〈2207〉
SAMSUNG WALLET
MY PAYMENT OPTION 01
SK Telecom
010-9009-2531
MY COUPON 03
2012-11-31 ~ 2012-12-31
〈2202〉
ONLINE PAYMENT
PIN PASSWORD
ENTER 6-DIGIT NUMBER
CLEAR
CANCEL
〈2204〉
ONLINE PAYMENT
VALID CONFIRMATION TIME
02:55
PAYMENT APPROVAL CODE
309420
SK Telecom
010-9009-2531
STORE NAME : STARBUCKS
PRODUCT NAME : CAFE AMERICANO
PAYMENT AMOUNT : 3,900
PAYMENT REQUEST
〈2206〉
〈2208〉

PAYMENT SUPPORT METHOD AND SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION(S)

[0001] This application claims the benefit under 35 U.S.C. §119(a) of a Korean patent application filed on Jan. 25, 2013 in the Korean Intellectual Property Office and assigned Serial number 10-2013-0008505, the entire disclosure of which is hereby incorporated by reference.

TECHNICAL FIELD

[0002] The present disclosure relates to a payment method. More particularly, the present disclosure relates to a payment support method and system that enables a terminal device to perform payment in a more secure and convenient manner.

BACKGROUND

[0003] With widespread usage of credit cards, consumers may make payments for goods and services using credit cards instead of cash. Currently, due to advances in Internet technology, an increasing number of financial transactions are now performed in cyberspace rather than in person, and payment methods in cyberspace have been diversified accordingly.

[0004] For purchase and payment using a credit card in cyberspace, a user provides preregistered credit card information to a service equipment requesting payment for a product, and a related financial institution pays requested money to the service equipment. More specifically, when a user buys a product using a credit card, a financial institution ensuring credit of the credit card pays the seller for the product and the user makes a credit card payment to the financial institution. The user may directly enter the credit card information at the time of purchase or may use credit card information prestored in a terminal device. In most cases, the terminal device used to store credit card information is a mobile terminal carried by the user.

[0005] In the payment process, the financial institution simply confirms information directly input by a cardholder, in which case a serious security problem may arise. For example, a malicious user having already stolen financial information of an innocent user, in some way or another, may make a purchase and payment in cyberspace using the stolen financial information.

[0006] Accordingly there is a need for an improved method and system that permit only a properly authorized user to obtain approval for purchase and payment by verifying card information in a multifaceted way with respect to preregistered terminal hardware information, financial information and personal identification information so as to improve security.

[0007] The above information is presented as background information only to assist with an understanding of the present disclosure. No determination has been made, and no assertion is made, as to whether any of the above might be applicable as prior art with regard to the present disclosure.

SUMMARY

[0008] Aspects of the present disclosure are to address at least the above-mentioned problems and/or disadvantages and to provide at least the advantages described below. Accordingly, an aspect of the present disclosure is to provide a payment support method and system that permit only a properly authorized user to obtain approval for purchase and payment by verifying card information in a multifaceted way with respect to preregistered terminal hardware information, financial information and personal identification information so as to improve security.

[0009] Another aspect of the present disclosure is to provide a payment support method and system that permit a user to manage multiple terminals based on a single account so that the user may obtain approval for payment in a convenient manner using one of the multiple terminals.

[0010] Another aspect of the present disclosure is to provide a payment support method and system that enable organizational entities involved in a transaction to enhance security without modification of existing procedures.

[0011] In accordance with another aspect of the present disclosure, a payment support system is provided. The payment support system includes a wallet server apparatus configured to support generation of an account of a payment service, and a terminal device configured to connect to the wallet server apparatus using the account, wherein the terminal device registers personal identification information including hardware information of the terminal device in the account and associates at least one payment option with the personal identification information stored in the wallet server apparatus.

[0012] In accordance with an aspect of the present disclosure, a payment support method is provided. The payment support method includes creating an account used for a payment service via a wallet server apparatus, connecting to the wallet server apparatus using the account, registering personal identification information including hardware information of a terminal device in the account, and associating at least one payment option with the personal identification information stored in the wallet server apparatus.

[0013] The present disclosure applies an optimized payment approval scheme without significant modification of existing payment system components, promoting system expandability through an independent system configuration.

[0014] Other aspects, advantages, and salient features of the disclosure will become apparent to those skilled in the art from the following detailed description, which, taken in conjunction with the annexed drawings, discloses various embodiments of the present disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The above and other aspects, features, and advantages of certain embodiments of the present disclosure will be more apparent from the following description taken in conjunction with the accompanying drawings, in which:

[0016] FIG. **1** illustrates an overall configuration of a payment support system according to an embodiment of the present disclosure;

[0017] FIG. **2** is a block diagram of a terminal device shown in FIG. **1** according to an embodiment of the present disclosure;

[0018] FIG. **3** is a block diagram of a wallet server apparatus shown in FIG. **1** according to an embodiment of the present disclosure;

[0019] FIG. **4** is a sequence diagram illustrating a terminal registration procedure according to an embodiment of the present disclosure;

[0020] FIGS. **5**, **6**A, and **6**B illustrate screen representations for terminal registration according to an embodiment of the present disclosure;

EWS-004388

[0021] FIG. **7** is a sequence diagram illustrating a procedure for payment information registration according to an embodiment of the present disclosure;

[0022] FIGS. **8**A, **8**B, **9**, **10**A, and **10**B illustrate screen representations for payment information registration according to an embodiment of the present disclosure;

[0023] FIG. **11** is a sequence diagram illustrating a payment making procedure according to an embodiment of the present disclosure;

[0024] FIGS. **12**, **13**, **14**, and **15** illustrate screen representations that may be presented in a payment making procedure according to an embodiment of the present disclosure;

[0025] FIG. **16** is a sequence diagram illustrating a procedure for terminal registration based on an identification card according to an embodiment of the present disclosure;

[0026] FIG. **17** is a sequence diagram illustrating another procedure for terminal registration based on an identification card according to an embodiment of the present disclosure;

[0027] FIG. **18** is a sequence diagram illustrating a procedure for payment information registration based on an identification card according to an embodiment of the present disclosure;

[0028] FIG. **19** is a sequence diagram illustrating a payment making procedure based on an identification card according to an embodiment of the present disclosure;

[0029] FIG. **20** illustrates screen representations of a payment making procedure based on an identification card according to an embodiment of the present disclosure;

[0030] FIG. **21** is a sequence diagram illustrating another payment making procedure based on an identification card according to an embodiment of the present disclosure; and

[0031] FIG. **22** depicts a payment making procedure based on identification card information input according to an embodiment of the present disclosure.

[0032] Throughout the drawings, it should be noted that like reference numbers are used to depict the same or similar elements, features, and structures.

DETAILED DESCRIPTION

[0033] The following description with reference to the accompanying drawings is provided to assist in a comprehensive understanding of various embodiments of the present disclosure as defined by the claims and their equivalents. It includes various specific details to assist in that understanding but these are to be regarded as merely exemplary. Accordingly, those of ordinary skill in the art will recognize that various changes and modifications of the various embodiments described herein can be made without departing from the scope and spirit of the present disclosure. In addition, descriptions of well-known functions and constructions may be omitted for clarity and conciseness.

[0034] The terms and words used in the following description and claims are not limited to the bibliographical meanings, but, are merely used by the inventor to enable a clear and consistent understanding of the present disclosure. Accordingly, it should be apparent to those skilled in the art that the following description of various embodiments of the present disclosure is provided for illustration purpose only and not for the purpose of limiting the present disclosure as defined by the appended claims and their equivalents.

[0035] It is to be understood that the singular forms "a," "an," and "the" include plural referents unless the context clearly dictates otherwise. Thus, for example, reference to "a component surface" includes reference to one or more of such surfaces.

[0036] FIG. **1** illustrates an overall configuration of a payment support system **10** supporting terminal based payment according to an embodiment of the present disclosure.

[0037] Referring to FIG. **1**, the payment support system **10** may include one or more terminal devices **100** owned by a user, a wallet server apparatus **200**, a member store apparatus **400**, a financial support apparatus **500**, and a communication network system **300**.

[0038] In the payment support system **10** having the above configuration, the user of a terminal device **100** connects to the wallet server apparatus **200** through the communication network system **300** and registers an account used for payment approval in the wallet server apparatus **200**. The account may contain text, images or biometric information suitable for personal identification. The user of the terminal device **100** may register at least one piece of payment approval information in the account. The payment approval information is information used by the user making payment for a purchase and may include personal identification information such as an individual ID and password, terminal information, and financial information. The terminal information may include various information contained in a terminal, such as information on the Universal Subscriber Identity Module (USIM) installed in the terminal device **100**, information on the embedded Security Element (eSE) installed in the terminal device **100**, unique hardware information such as a serial number of the terminal device **100**, MAC address information of the terminal device **100**, and unique identification information of a memory module installed in the terminal device **100**. In the following description, the serial number of the terminal device **100** is mainly used as the terminal hardware information.

[0039] As the user may use multiple terminal devices, payment approval information for each terminal device may be registered in the same account. Not only a mobile communication terminal, but also other types of terminals capable of accessing the wallet server apparatus **200** and the financial support apparatus **500** through the communication network system **300** may serve as the terminal device **100**. For example, a smart TV, desktop computer, laptop computer, and electronic note pad may act as a terminal device **100**. In the following description, a mobile terminal equipped with a USIM supporting mobile communication is mainly used as the terminal device **100**.

[0040] The terminal device **100** may connect to the wallet server apparatus **200** through the communication network system **300**, receive a wallet program from the wallet server apparatus **200** and install the wallet program. The wallet program may support user verification when a financial payment request is made. The terminal device **100** may use the wallet program to connect to the wallet server apparatus **200**, receive a wallet page from the wallet server apparatus **200**, and display the received wallet page on a display unit. The user may manipulate the wallet page to create an account for payment and to register payment approval information including terminal hardware information, USIM information, eSE information, personal identification information and financial information in the account. The payment approval information may be registered together with multiple terminals according to user consent. Hence, the same payment approval information may be used by multiple ter-

minals for payment. Components of the terminal device **100** and their operations are described in more detail later with reference to the drawings.

[0041] The wallet server apparatus **200** may perform user verification for the terminal device **100** and support information exchange between the member store apparatus **400** and the financial support apparatus **500**. The wallet server apparatus **200** may provide a wallet program to a terminal device **100** connected to the communication network system **300** and making a request for payment operation of the present disclosure. The wallet server apparatus **200** may associate an account with the user of the terminal device **100** according to activation of the wallet program and support payment operation of the user for a purchase through the account. In particular, the wallet server apparatus **200** stores personal identification information such as individual ID and password information, terminal hardware information, and financial information in conjunction as payment approval information. When a payment request message is received from a terminal device **100**, the wallet server apparatus **200** verifies whether information contained in the payment request message matches with all of the corresponding payment approval information. For example, although a match is found in the personal identification information, USIM information and financial information, if the terminal hardware information does not match, the wallet server apparatus **200** may not send an approval code indicating successful verification to the terminal device **100**. The wallet server apparatus **200** may send such an approval code to a terminal device **100** corresponding to the preregistered terminal hardware information. As a result, an approval code is not sent to a terminal device **100** whose terminal hardware information does not match the preregistered terminal hardware information. The wallet server apparatus **200** may be configured to include a terminal verification server **280** and an app server equipment **290**. The configuration and operation of the wallet server apparatus **200** are described in more detail later with reference to the drawings.

[0042] The member store apparatus **400** may receive and install a merchant wallet program from the wallet server apparatus **200**. The merchant wallet program may be a wallet program designed for a vendor or store. For example, the merchant wallet program may include a routine for forwarding information received from a terminal device **100** to the wallet server apparatus **200**, and a routine for receiving and outputting an approval code from the wallet server apparatus **200**. The member store apparatus **400** may provide a service page built to sell products to terminal devices **100**. When a purchase request for a particular product is received through the service page from a terminal device **100**, the member store apparatus **400** may send an approval request for payment for the purchase to the wallet server apparatus **200**. After the wallet server apparatus **200** successfully verifies the terminal device **100** and payment information is transferred to the financial support apparatus **500**, the member store apparatus **400** may receive an approval code from at least one of the wallet server apparatus **200** and the financial support apparatus **500**. To support usage of an identification card, the member store apparatus **400** may further include a reader (not shown) to recognize an identification card, and a communication module to receive electronic identification card information. Upon collection of identification card information, the member store apparatus **400** may provide the identification card information to the app server equipment **290** of the wallet server apparatus **200**.

[0043] When a payment approval request is received from the wallet server apparatus **200**, the financial support apparatus **500** tries to obtain confirmation for payment from the corresponding terminal device **100** and performs payment approval upon successfully obtaining confirmation. The financial support apparatus **500** may be composed of multiple entities to deal with distinct payment options such as credit cards, account transfer, payment gateway, membership cards and coupons. The payment option may be selected from a preregistered list of payment options or may be set by default.

[0044] The communication network system **300** supports exchange of signals and data between the components of the payment support system **10**. For data exchange between the components, the communication network system **300** may be composed of various communication instruments and modules supporting one or more communication schemes. For example, for payment support, the communication network system **300** may include various communication instruments to establish a communication channel for sending a service page from the member store apparatus **400** to a terminal device **100**, a communication channel for sending a payment request from a terminal device **100** to the wallet server apparatus **200**, a communication channel for sending a payment request from the member store apparatus **400** to the wallet server apparatus **200**, a communication channel for exchanging data between the wallet server apparatus **200** and the financial support apparatus **500**, and a communication channel for exchanging data between the financial support apparatus **500** and a terminal device **100**.

[0045] FIG. **2** is a block diagram of a terminal device **100** supporting improved secure payment operation according to an embodiment of the present disclosure.

[0046] Referring to FIG. **2**, the terminal device **100** may include a communication unit **110**, a display unit **140**, a storage unit **150** and a control unit **160**. The display unit **140** supports touch functionality and may act as an input means. The terminal device **100** may further include hard keys for user input, and an audio processing unit to process audio information needed for payment support operation.

[0047] The terminal device **100** having the above configuration may receive a service page of purchasable products through the communication unit **110** from the member store apparatus **400** and output the received service page on the display unit **140**. The terminal device **100** may use a preinstalled wallet program **151** to connect to the wallet server apparatus **200**. The wallet program **151** may be received from the wallet server apparatus **200**, be downloaded from a specific website or be received through USB serial communication, and may be stored and managed in the storage unit **150**.

[0048] The terminal device **100** may collect a product from the service page and send a purchase request for the selected product to the member store apparatus **400**. The terminal device **100** may connect to the wallet server apparatus **200** through the communication unit **110** and send login information to the wallet server apparatus **200**. The terminal device **100** may receive various payment related pages from the wallet server apparatus **200** and output the received pages on the display unit **140**. The user of the terminal device **100** may enter terminal hardware information, individual ID and password information matched with the preregistered payment approval information, and may also enter payment option

information registered in the corresponding account. The terminal device **100** sends the information entered by the user to the wallet server apparatus **200**.

[0049] In addition, the terminal device **100** may electronically store information on an identification card used for payment. The terminal device **100** may directly receive identification card information as user input from the user or receive the same from the wallet server apparatus **200**. The identification card information may be one-off information according to the policy of the wallet server apparatus **200**. One-off identification card information may be mapped with at least one of the account, the terminal and the identification card. One-off identification card information may be provided as text, barcode, QR code or RFID information. One-off identification card information may be received through direct key input or a barcode reader, or through short-range communication in a form of RFID information.

[0050] To use a payment option using identification card information, the terminal device **100** may receive identification card information from the terminal verification server **280** in advance.

[0051] As described before, the terminal device **100** may register its hardware information together with an account in the wallet server apparatus **200**. Hence, when the USIM of the terminal device **100** is transferred to a different terminal, the different terminal may be prohibited from using the payment service of the present disclosure. Hence, the user may register multiple terminal devices, which may be used to receive the payment service, on the account managed by the wallet server apparatus **200**. For example, the user may register hardware information of a mobile terminal, hardware information of a desktop computer, and hardware information of a smart TV on the same account. In this case, the user may receive the payment service using the mobile terminal, the desktop computer or the smart TV. For example, the user may use the desktop computer or the smart TV to connect to the wallet server apparatus **200**, which regards the connection as valid.

[0052] The terminal device **100** may register a piece of PIN information for each payment option as part of registration of the payment approval information. The PIN information serving as a payment password may be biometric information related to a fingerprint, voice sound, iris scan or other biometric feature. The PIN information may be stored in at least one of the wallet server apparatus **200** and the terminal device **100**.

[0053] The terminal device **100** may also register a piece of PIN information for multiple payment options. In this case, the payment support system **10** permits the user to enter the same PIN information even if the user selects any one of the multiple payment options. In addition, the terminal device **100** may register a piece of PIN information for one account.

[0054] A payment procedure using the terminal device **100** is described in more detail later with reference to the drawings.

[0055] FIG. **3** is a block diagram of a wallet server apparatus **200** according to an embodiment of the present disclosure.

[0056] Referring to FIG. **3**, the wallet server apparatus **200** may include a communication unit **210**, a storage unit **250**, and a control unit **260**. The wallet server apparatus **200** having the above configuration may establish communication channels to the terminal device **100**, the member store apparatus **400** and the financial support apparatus **500** to exchange payment information through the communication unit **210**. In the wallet server apparatus **200**, the storage unit **250** may store a payment support database **251**, which may maintain registered account information of terminal devices **100**, terminal information registered in the accounts, and financial information mapped to the terminal information. The terminal information stored in the payment support database **251** may include not only a telephone number but also hardware information of a terminal device **100**. The payment support database **251** may store an individual ID generated by mapping the terminal information. The payment support database **251** may also store a financial ID generated by the financial support apparatus **500** in connection with payment approval information of a registered terminal device **100**. The financial ID may be generated for each payment option.

[0057] The control unit **260** of the wallet server apparatus **200** may include an app server support module **296** to operate the app server equipment **290**, and a terminal verification support module **286** to operate the terminal verification server **280**. The control unit **260** may operate the app server equipment **290** and the terminal verification server **280** as separate entities. Operations of the app server equipment **290** and the terminal verification server **280** are described in more detail later with reference to the drawings.

[0058] As described above, the wallet server apparatus **200** stores hardware information of a terminal device **100** as part of registration of payment approval information of the terminal device **100**, improving security of payment operation.

[0059] FIG. **4** is a sequence diagram illustrating a terminal registration procedure in a payment support method according to an embodiment of the present disclosure.

[0060] Referring to FIG. **4**, at operation **401**, a terminal device **100** sends a registration request to the terminal verification server **280** of the wallet server apparatus **200**. To this end, the terminal device **100** installs a wallet program received from the terminal verification server **280**. The terminal device **100** may activate the wallet program to connect to the terminal verification server **280**. After activation of the wallet program, the terminal verification server **280** may receive an individual ID, password information and a terminal serial number from the terminal device **100**. The terminal verification server **280** may provide a window having input fields for an individual ID, a password and a serial number to the terminal device **100**. The terminal serial number may be directly entered by the user using an input unit or may be automatically found from hardware configuration information.

[0061] At operation **403**, the terminal verification server **280** performs registration of the individual ID, password and serial number received from the terminal device **100**. The terminal verification server **280** may register the serial number at an account created for the terminal device **100**. The account may be associated with the individual ID and password. A user may create an account by connecting to the terminal verification server **280**, entering personal information such as a social security number and address, and entering additional information requested by the terminal verification server **280**. The created account may be used to access the terminal verification server **280** by entering individual ID and password information. When an account is already registered for the user of the terminal device **100** and a serial number of the terminal device **100** is received, the terminal verification server **280** registers the terminal device **100**. At operation **405**, the terminal verification server **280** sends a registration result to the terminal device **100**.

EWS-004391

[0062] Upon reception of a registration result from the terminal verification server **280**, the terminal device **100** may output the registration result on the display unit **140**. When an account for the user is not present in the terminal verification server **280**, the user may create an account first.

[0063] FIGS. **5** to **6**B illustrate screen representations for terminal registration in a payment support method according to an embodiment of the present disclosure.

[0064] Referring to FIG. **5**, the terminal device **100** may output various icons associated with menu items and widgets on the display unit **140** in a standby state. In particular, as in a screen **501**, the terminal device **100** may output a wallet icon linked with a wallet program. Upon generation of an input event selecting the wallet icon, the terminal device **100** may output a screen for entering account information on the display unit **140**. Upon reception of individual ID and password information, the terminal device **100** may output a screen **503** for logging in to a specific account on the display unit **140**. The account information for login may be entered through manual character input, individual ID card, barcode recognition or the like. Previously entered account information may be reused for login if possible. Login to the account may further require verification of a password, fingerprint or the like.

[0065] After successful account login, the terminal device **100** may output a screen **505** for wallet service subscription. Upon generation of an input signal for wallet service subscription, the terminal device **100** may proceed to the next stage, for example, registration of payment approval information.

[0066] Meanwhile, when a registered account is not present after activation of the wallet program, the terminal device **100** may proceed to a phase depicted in FIGS. **6**A and **6**B.

[0067] Referring to FIGS. **6**A and **6**B, when no account is found in relation to the terminal device **100** after selection of the wallet icon in a state as in a screen **501**, the terminal device **100** outputs an account creation screen as in a screen **601**. When a preregistered individual ID and password are entered in the state as in screen **501**, the terminal device **100** performs screen transition via a screen **503** to a screen **505**.

[0068] When an item "new account creation" is selected in the screen **601**, the terminal device **100** may output a screen **603** for country selection, a screen **605** for consenting to general, a screen **607** for real name verification, and a screen **609** for ID and password input in sequence. The output sequence of the screens for new account creation may differ according to design. The above screens may be a screen that is received from the wallet server apparatus **200** or the terminal verification server **280**. The user may create a new account by selecting the country, consenting to general conditions, entering a real name, and entering an ID and password.

[0069] Upon completion of account creation, the terminal device **100** may output a screen **611** for account login received from the wallet server apparatus **200** on the display unit **140**. When the user enters account login information, the terminal device **100** may proceed to the state indicated by screen **503**. In this example, the account is identified by email information. However, the present disclosure is not limited thereto. For example, accounts may be identified by any distinct pieces of information such as combinations of characters, numerals, and special characters.

[0070] FIG. **7** is a sequence diagram illustrating a procedure for payment information registration according to an embodiment of the present disclosure.

[0071] Referring to FIG. **7**, to register payment information, at operation **701**, the terminal device **100** sends a service subscription request to the app server equipment **290**. Optionally, the terminal device **100** may create an account in the app server equipment **290** in advance. The service subscription request may contain subscription information such as individual ID, password, terminal serial number, and PIN information. Optionally, the terminal device **100** may output an input window for entering ID, password, terminal serial number and PIN information received from the app server equipment **290**. The user may enter necessary information in the input window using an input unit of the terminal device **100**.

[0072] Upon reception of a service subscription request containing subscription information from the terminal device **100**, at operation **703**, the app server equipment **290** sends a terminal verification request to the terminal verification server **280**. The terminal verification request may contain the individual ID, password, and terminal serial number extracted from the subscription information received from the terminal device **100**. The terminal verification server **280** verifies whether the user is a registered user by examining the received individual ID, password, and terminal serial number. At operation **705**, the terminal verification server **280** sends a terminal verification result to the app server equipment **290**.

[0073] If the terminal verification result received from the terminal verification server **280** indicates a registered user, at operation **707**, the app server equipment **290** generates an individual identification value using the individual ID, password, terminal serial number and PIN information. If the terminal verification result received from the terminal verification server **280** indicates an unregistered user, the app server equipment **290** may send a registration recommendation message (not shown) notifying an unregistered user to the terminal device **100**.

[0074] Upon generation of an individual identification value, at operation **709**, the app server equipment **290** sends a payment option registration request containing the individual identification value to the financial support apparatus **500**. At operation **711**, the financial support apparatus **500** sends a payment option information window containing the individual identification value to the terminal device **100**.

[0075] Upon reception of a payment option information window, at operation **713**, the terminal device **100** provides payment option information to the financial support apparatus **500** by entering card information in the payment option information window. The card information may include a card identifier, valid duration or other information defined by the financial support apparatus **500**. The payment option information sent by the terminal device **100** to the financial support apparatus **500** may contain the received individual identification value to thereby indicate payment option registration.

[0076] Upon reception of payment option information, at operation **715**, the financial support apparatus **500** generates a financial information identifier based on financial information. Multiple financial information identifiers may be generated. For example, for a given individual identification value, the financial support apparatus **500** may associate one financial information identifier with one piece of financial information. When multiple pieces of card information are registered, multiple financial information identifiers are associated respectively with multiple pieces of financial information. After generation of the financial information identifier, at operation **717**, the financial support apparatus **500** sends a

payment option registration result to the app server equipment **290**. The app server equipment **290** may store the individual ID, password, terminal serial number, individual identification value, and at least one financial information identifier. Upon reception of a payment option registration result from the financial support apparatus **500**, at operation **719**, the app server equipment **290** notifies the terminal device **100** of payment information registration completion.

[0077] FIGS. **8**A to **10**B illustrate screen representations for payment information registration according to an embodiment of the present disclosure.

[0078] Referring to FIG. **8**A, in response to an input event for selecting the wallet icon or a wallet service, the terminal device **100** activates the wallet program and connects to the wallet server apparatus **200** through the wallet program. The wallet server apparatus **200** may provide an account login screen to the terminal device **100**. When the user enters an account ID and password, the terminal device **100** forwards the ID and password to the wallet server apparatus **200** to log in to the associated account, and may output a login progress screen **801** received from the wallet server apparatus **200**. When account login is successful (i.e. the input account ID and password match the preregistered account ID and password), the terminal device **100** may receive a terms-and-conditions screen **803** from the wallet server apparatus **200** and output the same on the display unit **140** to obtain user consent. When an item "wallet special terms" is selected in the screen **803**, the terminal device **100** may receive detailed information of the selected item from the wallet server apparatus **200** and output the detailed information in a screen **805** on the display unit **140** as.

[0079] Referring to FIG. **8**B, when all terms and conditions are checked ("OK") as in a screen **807**, the terminal device **100** sends information on the checked items to the wallet server apparatus **200**, which may provide a payment information registration screen to the terminal device **100**. Then, the terminal device **100** may output in a screen **811**, a password input window received from the wallet server apparatus **200**. The phone number or serial number of the terminal device **100** may be automatically input to a password input field of the password input window. The phone number or serial number may also be manually input by the user.

[0080] When the password input field is selected in the screen in screen **809**, the terminal device **100** may output a virtual keypad for password input at a region of the display unit **140** as in the screen **811**.

[0081] Referring to FIG. **9**, when a password is input as in a screen **901**, to ensure that the password is correct, the terminal device **100** may output a password verification window received from the wallet server apparatus **200** as in a screen **903**. When password verification is successful, the terminal device **100** may output the input password as special characters for security in the corresponding field on the service subscription screen as in a screen **905**. When a field "subscription" is selected on the screen **905**, payment information registration is completed, and the terminal device **100** may output a wallet service home screen received from the wallet server apparatus **200** on the display unit **140** as in a screen **907**.

[0082] Referring to FIG. **10**A, when an add button such as a '+' button is selected on the wallet service home screen as in a screen **1001**, the terminal device **100** may output a first selection window **1100** for selection of payment options including a coupon as in a screen **1003**.

[0083] Meanwhile, when an item "my payment options" is selected on the screen **1001** in a state where payment option registration is not performed yet, the terminal device **100** may output a screen **1005** indicating an absence of a registered payment option. When an add button is selected on the screen, the terminal device **100** may output a second selection window **1200** for selection of payment options not including a coupon as in a screen **1007**.

[0084] Referring to FIG. **10**B, when an item "credit card" is selected on the first selection window **1100** or second selection window **1200**, the terminal device **100** may output a card information input screen **1009**. The card information input screen may contain a list of card issuing companies in partnership with the wallet service received from the wallet server apparatus **200**. When the user selects a card issuing company (e.g. "Samsung Card") from the list, the terminal device **100** may output a web view screen **1011** for card information input. In this process, the terminal device **100** may check validity of input card information in cooperation with the financial support apparatus **500** associated with the selected card issuing company. In addition, the user may enter card information, password or other code information requested by the financial support apparatus **500** and the financial support apparatus **500** may verify the entered information.

[0085] Upon reception of an indication to completion of payment option registration from the wallet server apparatus **200**, the terminal device **100** may output information on the issued credit card as my payment option as in a screen **1013**. In this process, the financial support apparatus **500** may provide the payment option registration information to the wallet server apparatus **200**, which may store the received payment option registration information and provide the same to the terminal device **100**.

[0086] FIG. **11** is a sequence diagram illustrating a payment making procedure based on a wallet service according to an embodiment of the present disclosure.

[0087] Referring to FIG. **11**, at operation **1101**, a member store apparatus **400** sends a payment request for a product purchased by the terminal device **100** to the app server equipment **290**. The terminal device **100** may connect to a server page hosted by the member store apparatus **400** and send a purchase request for a product to the member store apparatus **400**. For example, the terminal device **100** may log in to the server page of the member store apparatus **400** and provide personal identification information such as an ID and password to the member store apparatus **400**. The member store apparatus **400** sends the personal identification information such as an ID and password received from the terminal device **100** to the app server equipment **290**. For payment support, the member store apparatus **400** may download and store a merchant wallet program from the wallet server apparatus **200** and subscribe to the wallet service in advance. The merchant wallet program is a version of the wallet program adapted for a vendor or store. For example, the merchant wallet program may include routines for validating information received from the terminal device **100** and forwarding the validated information to the wallet server apparatus **200** in a payment process.

[0088] Upon reception of a payment request from the member store apparatus **400**, at operation **1103**, the app server equipment **290** checks whether the member store apparatus **400** is subscriber of the wallet service. If the member store apparatus **400** is a subscriber of the wallet service, the app server equipment **290** proceeds to operation **1105** at which the

app server equipment **290** sends terminal verification information and payment request information to the terminal verification server **280**. If the member store apparatus **400** is not a subscriber of the wallet service, the app server equipment **290** may send a message recommending service subscription (not shown) to the member store apparatus **400**.

[0089] Upon reception of terminal verification information and payment request information from the app server equipment **290**, at operation **1107**, the terminal verification server **280** checks whether the terminal device **100** is registered. If the terminal device **100** is registered, the terminal verification server **280** proceeds to operation **1109** at which terminal verification server **280** forwards the payment request information to the terminal device **100**. If the terminal device **100** is not registered, the terminal verification server **280** may send a message indicating an unregistered terminal (not shown) to the app server equipment **290**, which may forward the message indicating an unregistered terminal (not shown) to the member store apparatus **400** and the terminal device **100**.

[0090] At operation **1111**, the terminal device **100** receives the payment request information from the terminal verification server **280** and executes the wallet program. At operation **1113**, the terminal device **100** sends a request for payment option information to the app server equipment **290**. Payment option information may be card information and/or coupon information registered by a user in the app server equipment **290**. In response to the request for payment option information, at operation **1115**, the app server equipment **290** locates payment option information registered by the terminal device **100** and sends the payment option information to the terminal device **100**. Upon reception of payment option information, the terminal device **100** may output the payment option information on the display unit **140**. The terminal device **100** may output a list of cards or coupons. At operation **1117**, the terminal device **100** receives user input for selecting a card and/or other coupon as a payment option and entering PIN information (preregistered in the app server equipment **290**).

[0091] When no payment option is included in the payment option information, the app server equipment **290** may send a message recommending payment option registration (not shown) to the terminal device **100**. In response to the message, the terminal device **100** may perform a procedure for payment option registration (not shown) according to user control.

[0092] Upon reception of user input for payment option selection and PIN information, at operation **1119**, the terminal device **100** sends payment information to the app server equipment **290**. At operation **1121**, the app server equipment **290** checks whether the received PIN information matches the PIN information preregistered for the terminal device **100** and sends, if the received PIN information matches the preregistered PIN information, a payment approval request to the financial support apparatus **500**. If the received PIN information does not match the preregistered PIN information, the app server equipment **290** may notify the terminal device **100** of a PIN error and request the terminal device **100** to reenter PIN information (not shown). When the number of times of PIN input failure exceeds a preset value, the app server equipment **290** may prohibit use of the related payment option, use of the registration information of the terminal device **100** or use of the account created for a terminal device **100** according to preset policies. This prohibition may be enforced by the financial support apparatus **500** rather than the app server equipment **290**.

[0093] Upon reception of a payment approval request from the app server equipment **290**, at operation **1123**, the financial support apparatus **500** verifies payment approval information. The financial support apparatus **500** may check validity of the card information and PIN information sent by the app server equipment **290**. Validity of the PIN information may be checked by the app server equipment **290** rather than the financial support apparatus **500**. To check whether the terminal device **100** is registered as a payment terminal, the financial support apparatus **500** may send a push message (not shown) to the terminal device **100** and examine a corresponding response message (not shown) from the terminal device **100**. The terminal device **100** may process such a push message in the background without display. Upon successful validation, at operation **1125**, the financial support apparatus **500** sends an approval completion message to the app server equipment **290**.

[0094] Upon reception of an approval completion message, at operation **1127**, the app server equipment **290** forwards the approval completion message to the member store apparatus **400**. The approval completion message may include a payment statement.

[0095] FIGS. **12** and **13** illustrate screen representations for a payment making procedure based on a wallet service according to an embodiment of the present disclosure. The procedure described in FIGS. **12** and **13** may be performed jointly by a desktop computer and a mobile terminal serving as a terminal device **100** of the present disclosure. Screen representations in FIG. **12** may be related to the desktop computer, and screen representations in FIG. **13** may be related to the mobile terminal

[0096] Referring to FIG. **12**, in response to user input, a desktop computer may connect to a server page hosted by a member store apparatus **400** operated by a pizza store. The desktop computer may output a pizza menu screen **1201** received from the member store apparatus **400** on the display unit **140**. When the user generates an input event for selecting desired pizza on the pizza menu screen, the desktop computer sends information on the selected product to the member store apparatus **400**. The desktop computer may output a discount coupon screen **1203**. For example, the desktop computer may maintain information on discount coupons owned by the user and output guidance information on use of a discount coupon when a member store apparatus **400** accepting the discount coupon is connected.

[0097] Upon completion of product and coupon selection, the desktop computer may output a screen **1205** containing selection information and a field for payment initiation. When the field for payment initiation is selected by the user, the desktop computer may output a screen **1207** for verifying personal identification information received from the member store apparatus **400**. The member store apparatus **400** may request input of information on a mobile terminal registered for payment. The user may enter mobile terminal information using an input unit or the like.

[0098] Upon reception of mobile terminal information from the desktop computer, the member store apparatus **400** sends a payment approval request to the app server equipment **290**. The payment approval procedure is depicted in FIG. **13**. Upon reception of an approval completion response from the financial support apparatus **500**, the member store apparatus

400 may provide a page containing information on approval completion and product delivery to the desktop computer, which displays the received page as in a screen 1209. When the policy of the financial support apparatus 500 requires final user confirmation, the desktop computer may output a window for obtaining user confirmation. When user confirmation is obtained, the desktop computer may output the screen.

[0099] In the above description, a desktop computer rather than a mobile terminal is used to make a purchase and payment. However, the present disclosure is not limited thereto. For example, a smart TV or other electronic appliance supporting bidirectional communication may be utilized instead of a desktop computer.

[0100] The app server equipment 290 may perform a payment approval procedure in cooperation with a mobile terminal whose information is provided during a purchase and payment process initiated by a desktop computer. In the following description, a mobile terminal is referred to as a terminal device 100.

[0101] Referring to FIG. 13, upon reception of a confirmation request from the app server equipment 290 according to the personal identification information and terminal selection information entered by the desktop computer for handling a payment approval request, the terminal device 100 may automatically activate the wallet program and output a login screen. When the user successfully enters login information, the terminal device 100 may output a login progress indication on the display unit as in a screen 1301. Upon login completion, the terminal device 100 sends a request for payment option information to the app server equipment 290 of the wallet server apparatus 200, and receives registered payment option information and outputs the payment option information as in a screen 1303. For example, the terminal device 100 may output a screen containing a payment information selection region for a payment option and monthly installments and an order information region. The order information region may be filled in by the app server equipment 290 based on information of a purchased product sent by the member store apparatus 400.

[0102] If information elements on the screen 1303 match the product to buy, the user may enter a confirmation input to thereby proceed to the next stage. Upon reception of a confirmation input, the terminal device 100 may output a PIN input request (corresponding to the selected payment option) received from the app server equipment 290 as in a screen 1305. When PIN information is input, the app server equipment 290 sends payment approval information such as information on the payment option, PIN and purchase value to the financial support apparatus 500. The financial support apparatus 500 validates the received information and sends a final confirmation request to the terminal device 100, which may output the final confirmation request as in a screen 1307. The financial support apparatus 500 may set a time limit to final confirmation of the user. For example, the financial support apparatus 500 may set a time limit of three minutes to user confirmation. The user may review the displayed information and make a confirmation by issuing a payment request within the confirmation time limit. The terminal device 100 sends user confirmation information to the financial support apparatus 500. After completion of payment approval, the financial support apparatus 500 sends a payment approval completion indication to the terminal device 100 and may send the payment approval completion indication to the desktop computer having initiated the payment making procedure. The terminal device 100 outputs a payment approval completion screen as in a screen 1309, and may output a guide message requesting final confirmation at the terminal device having initiated the payment making procedure (e.g. the desktop computer) according to the policy set by the financial support apparatus 500.

[0103] FIGS. 14 and 15 illustrate screen representations for another payment making procedure based on a wallet service according to an embodiment of the present disclosure. The procedure described in FIGS. 14 and 15 is performed by one terminal device making a purchase request and making a payment confirmation.

[0104] Referring to FIG. 14, the user may use the terminal device 100 to connect to a server page hosted by a member store apparatus 400 operated by a merchant store. The terminal device 100 may output the server page received from the member store apparatus 400 as in a screen 1401. The user may browse various items on the server page and select a particular item. The terminal device 100 may receive a screen describing selectable actions applicable to the selected item (e.g., purchase or presentation as a gift) from the member store apparatus 400 and output the received screen as in a screen 1403.

[0105] When the user selects an item "gift", the terminal device 100 may send information on the selected item to the member store apparatus 400. The member store apparatus 400 may send a page containing a short description of the selected product and a payment option region for payment option selection to the terminal device 100. Upon reception of the page, the terminal device 100 may output the received page as in a screen 1405. The member store apparatus 400 may be a device registered in the wallet server apparatus 200, and hence may insert an item for a payment option based on the wallet service in the payment option region. When the user selects a payment option based on the wallet service, the terminal device 100 may support a payment procedure using an individual identification value. For example, the terminal device 100 may output various items describing the progress of payment as in a screen 1407. Upon completion of payment, the terminal device 100 may output a screen indicating payment completion as in a screen 1409. The progress of payment is described in more detail with reference to FIG. 15.

[0106] Referring to FIG. 15, when the app server equipment 290 receives a request for payment based on a selected payment option, it may provide various screen data for payment approval to the terminal device 100. Accordingly, the terminal device 100 may output various screens for payment approval, such as a screen 1501 for account login after activation of the wallet program, a screen 1503 for payment option selection, a screen 1505 for PIN input, a screen 1507 for entering a "one time approval code" given by the financial support apparatus 500 or app server equipment 290 within a time limit, and a screen 1509 indicating payment completion after user confirmation. The user may enter requested information (identical to the information preregistered in the wallet server apparatus 200 or the financial support apparatus 500) in the above screens.

[0107] FIG. 16 is a sequence diagram illustrating a procedure for identification card registration according to an embodiment of the present disclosure.

[0108] Referring to FIG. 16, the terminal device 100 may register payment information at an account provided by the wallet server apparatus 200. To this end, the terminal device 100 may install the wallet program and activate the wallet

program to connect to the wallet server apparatus **200** by entering login information to a login page of the wallet server apparatus **200**. The terminal device **100** may register itself to the account associated with the login information. When no account is present, the terminal device **100** may output an account creation screen for entering user information such as registration number or address. For terminal registration, at operation **1601**, the terminal device **100** sends a terminal registration request to the terminal verification server **280**. The terminal registration request may contain an ID, password and terminal serial number. Alternatively, the terminal device **100** may log in to the account first by entering an ID and password, and enter the terminal serial number through a page provided by the wallet server apparatus **200**.

[0109] Upon reception of a terminal registration request from the terminal device **100**, at operation **1603**, the terminal verification server **280** performs terminal registration. For example, the terminal verification server **280** stores the ID, password and serial number in an interrelated manner in the storage unit. At operation **1605**, the terminal verification server **280** sends a request for identification card information to the terminal device **100**. Upon reception of the request, the terminal device **100** outputs a screen for entering identification card information. The user enters identification card information verified by the wallet server apparatus **200**. For example, to use a wallet service, the user may obtain an identification card issued by an organization operating the wallet server apparatus **200**, and register the identification card at a specific account managed by the wallet server apparatus **200**. At operation **1607**, the terminal device **100** sends identification card information registered to the terminal verification server **280**. Upon reception of the identification card information, at operation **1609**, the terminal verification server **280** stores and manages the ID, password, serial number and identification card information in an interrelated manner.

[0110] FIG. **17** is a sequence diagram illustrating another procedure for identification card registration according to an embodiment of the present disclosure.

[0111] Referring to FIG. **17**, in response to selection of the wallet program, the terminal device **100** activates the wallet program and output a screen for login to the wallet server apparatus **200** on the display unit. When the user enters login information, at operation **1701**, the terminal device **100** may send a terminal registration request containing the login information and terminal serial number to the terminal verification server **280** of the wallet server apparatus **200**.

[0112] Upon reception of the terminal registration request, at operation **1703**, the terminal verification server **280** performs terminal registration. At operation **1705**, the terminal verification server **280** generates identification card information according to the ID, password, and terminal serial number contained in the terminal registration request, and stores and manages the identification card information, ID, password and terminal serial number in an interrelated manner.

[0113] At operation **1707**, the terminal verification server **280** may support fabrication of an identification card corresponding to the identification card information and support delivery of the identification card to the terminal device **100**.

[0114] FIG. **18** is a sequence diagram illustrating a procedure for payment information registration based on an identification card according to an embodiment of the present disclosure.

[0115] Referring to FIG. **18**, to register payment information using an identification card, at operation **1801**, the terminal device **100** sends a service subscription request to the app server equipment **290**. The service subscription request may contain an ID, password, terminal serial number and PIN information. The terminal device **100** may output an input window for entering ID, password and terminal serial number first, and output an input window for entering PIN information.

[0116] Upon reception of a service subscription request from the terminal device **100**, at operation **1803**, the app server equipment **290** sends a terminal verification request to the terminal verification server **280**. The terminal verification request may contain the ID, password and terminal serial number. The terminal verification server **280** verifies whether the information contained in the terminal verification request matches the preregistered information. At operation **1805**, the terminal verification server **280** sends a terminal verification result to the app server equipment **290**.

[0117] When the terminal verification result indicates that the terminal device **100** is valid, at operation **1807**, the app server equipment **290** generates an individual identification value, and stores and manages the individual identification value, ID, password, terminal serial number, identification card information and PIN information in an interrelated manner. The identification card information may be received from the terminal device **100**, or an identification card may be fabricated and sent together with identification card information to the terminal device **100**.

[0118] At operation **1809**, the app server equipment **290** sends a payment option registration request containing the individual identification value to the financial support apparatus **500**. At operation **1811**, the financial support apparatus **500** sends a payment option information window containing the individual identification value to the terminal device **100**. The terminal device **100** outputs the payment option information window and receives payment option information entered by the user. For example, the user may enter financial information including card information in the payment option information window. At operation **1813**, the terminal device **100** sends payment option information including an individual identification value and financial information to the financial support apparatus **500**.

[0119] At operation **1815**, the financial support apparatus **500** generates a financial information identifier based on the received individual identification value and financial information, and maintains the financial information identifier. Multiple financial information identifiers may be generated. For example, for a given individual identification value, the financial support apparatus **500** may associate one financial information identifier with one piece of financial information. When multiple pieces of card information are registered, multiple financial information identifiers are associated respectively with multiple pieces of financial information.

[0120] At operation **1817**, the financial support apparatus **500** sends a payment option registration result to the app server equipment **290**. The app server equipment **290** may store at least one financial information identifier and other information such as ID, password, terminal serial number and individual identification value in an interrelated manner. At operation **1819**, the app server equipment **290** notifies the terminal device **100** of payment information registration completion depending upon the received payment option registration result.

[0121] FIG. **19** is a sequence diagram illustrating a payment making procedure based on an identification card according to an embodiment of the present disclosure.

[0122] Referring to FIG. **19**, at operation **1901**, the terminal device **100** activates the wallet program and connects to the app server equipment **290**. At operation **1903**, the app server equipment **290** checks whether the terminal device **100** is a subscriber of the service. When the terminal device **100** is a subscriber, the app server equipment **290** proceeds to operation **1905** at which the app server equipment **290** sends a terminal verification request to the terminal verification server **280**. At operation **1907**, the terminal verification server **280** checks whether the terminal device **100** is registered based on terminal information such as ID, password and serial number. At operation **1909**, the terminal verification server **280** sends a terminal verification result and identification card information registered for the terminal device to the app server equipment **290**.

[0123] When the terminal device **100** is determined to be registered, at operation **1911**, the app server equipment **290** sends payment option information to the terminal device **100**. Upon reception of payment option information, at operation **1913**, the terminal device **100** outputs the payment option information and receives user input for selecting a payment option and entering PIN information. Additionally, the terminal device **100** may support selection of a valid payment time and receive user input for selecting a valid payment time. At operation **1915**, the terminal device **100** sends payment information related to a payment option, PIN information and valid payment time to the app server equipment **290**. At operation **1917**, the app server equipment **290** checks whether the received PIN information matches the preregistered PIN information. At operation **1919**, the app server equipment **290** sends a payment setting complete indication to the terminal device **100**. At operation **1921**, the terminal device **100** selects a desired one of products provided by the member store apparatus **400** and sends identification card information to the member store apparatus **400**. The identification card information may be provided through a plastic card, through short-range communication as electronic information, or through a tag having identification card information and a reader attached to the member store apparatus **400**.

[0124] At operation **1923**, the member store apparatus **400** sends product information and identification card information entered by the user to the app server equipment **290**. The app server equipment **290** may check whether the received identification card information is identical to the identification card information provided by the terminal verification server **280**. At operation **1925**, the app server equipment **290** extracts payment information including payment option information, PIN information and product information from the information provided by the member store apparatus **400**. At operation **1927**, the app server equipment **290** sends a payment approval request containing the payment information to the financial support apparatus **500**.

[0125] At operation **1933**, when information contained in the received payment approval request matches the preregistered information, the financial support apparatus **500** performs payment approval. At operation **1935**, the financial support apparatus **500** sends a payment approval completion message to the app server equipment **290**. At operation **1937**, the app server equipment **290** forwards the payment approval completion message to the member store apparatus **400**, which may send a payment approval completion indication to the terminal device **100**.

[0126] FIG. **20** illustrates screen representations of a payment making procedure based on an identification card according to an embodiment of the present disclosure.

[0127] Referring to FIG. **20**, upon activation of the wallet program and login completion, the terminal device **100** may output a screen **2001** containing payment option and coupon information. When the user selects a payment option on the screen, the terminal device **100** may output a PIN input window received from the app server equipment **290** as in a screen **2003**. Upon successful PIN input, the app server equipment **290** may send information provided by the terminal device **100**, personal identification information and identification card information to the financial support apparatus **500**.

[0128] To verify the terminal owner, the financial support apparatus **500** sends a screen containing a payment approval code and a time limit to the terminal device **100**, which outputs a screen **2005**. The user may initiate the payment procedure by entering payment request input within the time limit.

[0129] To limit the usage time of an identification card **600**, the user of the terminal device **100** may send a request for setting a valid payment time to the financial support apparatus **500** or the wallet server apparatus **200**. The user presents the preregistered identification card **600** to the member store apparatus **400**. The identification card information collected by the member store apparatus **400** is treated as effective when the identification card information is sent to the financial support apparatus **500** or the wallet server apparatus **200** within the valid payment time set by the user. The valid payment time may indicate the time taken from completion of payment approval to recognition of the identification card **600** by a member store apparatus. Similarly to the valid confirmation time, the valid payment time may be output or not output on the display unit of a terminal device according to design.

[0130] The member store apparatus **400** may obtain information contained in the identification card **600** using a reader and send the identification card information to the wallet server apparatus **200** through a communication network. The wallet server apparatus **200** may verify the received identification card information and send a payment approval request to the financial support apparatus **500**. The wallet server apparatus **200** may not verify the received identification card information and may forward the identification card information to the financial support apparatus **500**. Alternatively, the member store apparatus **400** may directly provide the identification card information and product purchase information to the financial support apparatus **500**. Upon reception of a payment approval completion message from the financial support apparatus **500**, the app server equipment **290** may send the payment approval completion message to at least one of the member store apparatus **400** and the terminal device **100** as in a screen **2007**.

[0131] When the user selects a desired product from the server page of the member store apparatus **400**, the terminal device **100** may activate the wallet program and output a screen **2001**.

[0132] FIG. **21** is a sequence diagram illustrating another payment making procedure based on an identification card according to an embodiment of the present disclosure. As the

procedure depicted in FIG. **21** is similar to that of FIG. **19** except for use of a payment waiting list, a relatively brief description thereof is given.

[0133] Referring to FIG. **21**, at operation **2101**, the terminal device **100** activates the wallet program **151** and connects to the app server equipment **290**. At operation **2103**, the app server equipment **290** checks whether the terminal device **100** is a subscriber of the service. When the terminal device **100** is a subscriber, the app server equipment **290** proceeds to operation **2105** at which the app server equipment **290** sends a terminal verification request to the terminal verification server **280**. At operation **2107**, the terminal verification server **280** checks whether the terminal device **100** is registered based on the preregistered information. At operation **2109**, the terminal verification server **280** sends a terminal verification result and registered identification card information to the app server equipment **290**.

[0134] At operation **2111**, the app server equipment **290** sends payment option information for payment option selection to the terminal device **100**. At operation **2113**, the terminal device **100** may output the payment option information and receives user input for selecting a payment option, entering PIN information and selecting a valid payment time. At operation **2115**, the terminal device **100** sends payment information related to a payment option, PIN information and valid payment time to the app server equipment **290**. At operation **2117**, the app server equipment **290** checks whether the received PIN information matches the preregistered PIN information. When a match is found, at operation **2119**, the app server equipment **290** sends a payment setting complete indication to the terminal device **100**. At operation **2121**, the app server equipment **290** sends a payment waiting list to the member store apparatus **400**.

[0135] The terminal device **100** presents identification card information to the member store apparatus **400**. At operation **2123**, the member store apparatus **400** sends the identification card information to the app server equipment **290**. At operation **2125**, the app server equipment **290** extracts payment information corresponding to the identification card information such as financial information (financial information identifier) mapped with the identification card. At operation **2127**, the app server equipment **290** sends a payment approval request containing the payment information to the financial support apparatus **500**.

[0136] At operation **2129**, the financial support apparatus **500** sends a terminal verification request to the terminal verification server **280**. At operation **2131**, the financial support apparatus **500** receives a terminal verification result from the terminal verification server **280**.

[0137] At operation **2133**, when information contained in the received payment approval request is valid, the financial support apparatus **500** performs payment approval. At operation **2135**, the financial support apparatus **500** sends a payment approval completion message to the app server equipment **290**. At operation **2137**, the app server equipment **290** forwards the payment approval completion message to the member store apparatus **400**.

[0138] FIG. **22** depicts a payment making procedure based on identification card information according to an embodiment of the present disclosure.

[0139] Referring to FIG. **22**, the user of the terminal device **100** may locate nearby coffee shops through an application as in a screen **2201**. The terminal device **100** may output the menu of a selected coffee shop as in a screen **2203**. To this end, the terminal device **100** may activate the communication unit **110**, connect to a member store apparatus **400** operated by the selected coffee shop, and receive a server page containing the menu from the member store apparatus **400**. The user selects an item from the screen **2201** and makes payment for the item.

[0140] More specifically, when the user selects a menu item, the terminal device **100** may automatically activate the wallet program. Upon login completion, the terminal device **100** may output a page for payment option selection received from the app server equipment **290** as in a screen **2202**. When a payment option is selected, the terminal device **100** may output a screen for PIN input as in a screen **2204**. Upon completion of PIN input, the terminal device **100** sends the PIN information via the app server equipment **290** to the financial support apparatus **500**. When the PIN information is correct, the financial support apparatus **500** sends a confirmation page having a valid confirmation time to the terminal device **100**. The terminal device **100** outputs the confirmation page and waits for user input for terminal verification within the valid confirmation time as in a screen **2206**. Meanwhile, before or after PIN input (state indicated by the screen **2204**), the terminal device **100** may set a time limit for the identification card. When the user sets a valid payment time for the identification card, the terminal device **100** may send information on the valid payment time to the financial support apparatus **500** or the wallet server apparatus **200**. Upon reception of information on the valid payment time, the wallet server apparatus **200** or the like may determine validity of received identification card information by examining whether the identification card information is received within the valid payment time. The valid payment time may be output or not output by the terminal device **100**.

[0141] The terminal device **100** may send identification card information (received from the input unit or pre-stored) to the member store apparatus **400** through short-range wireless communication as illustrated at **2208**. The member store apparatus **400** may be equipped with a reader or may support short-range wireless communication.

[0142] When identification card information is obtained, the terminal device **100** may send the same to the wallet server apparatus **200**. The app server equipment **290** may determine validity of the identification card information by comparing the identification card information received from the terminal device **100** with the identification card information received from the terminal verification server **280**.

[0143] When the identification card information received from the terminal device **100** is valid, the app server equipment **290** sends corresponding payment information to the financial support apparatus **500**. The finaucial support apparatus **500** performs payment approval and sends a payment approval completion message to the member store apparatus **400**, which may output the payment approval completion message as in a screen **2205**. The member store apparatus **400** may output user information such as a photograph for user identification. Optionally, the user may register a headshot together with the terminal device **100** in the app server equipment **290** or the financial support apparatus **500** that is additionally displayed in the screen **2205**. The user is delivered his coffee as illustrated at **2207**.

[0144] As described hereinabove, the payment support method of the present disclosure enables registration of hardware information of a terminal device **100** such as a serial number, MAC address, memory ID in conjunction with reg-

istration of payment information to thereby enhance security of payment operation. In particular, the app server equipment **290** of the wallet server apparatus **200** may store hardware information of the terminal device **100** and payment related information in an interrelated manner, providing a more stable security function.

[0145] Meanwhile, the terminal device **100** may further include various components according to design. For example, when the terminal device **100** is a communication terminal, the terminal device **100** may further include a local area communication module for local area communication, a data communication interface based on wired and wireless communication, an Internet communication module for Internet access and communication, and a digital broadcast reception module for receiving and playing digital broadcasts. Although possible variations according to the trend of digital convergence are too numerous to enumerate, it should be apparent to those skilled in the art that the terminal device **100** may further include a unit comparable to the above-described units, and one unit of the terminal device **100** may be removed or replaced with another unit.

[0146] The terminal device **100** of the present disclosure may be any information and communication appliance or multimedia appliance, such as a mobile communication terminal based on communication protocols supporting various communication systems, a Portable Multimedia Player (PMP), a digital broadcast receiver, a Personal Digital Assistant (PDA), a music player like an MP3 player, a portable game console, a smartphone, a laptop computer, or a handheld computer.

[0147] Various aspects of the present disclosure can also be embodied as computer readable code on a non-transitory computer readable recording medium. A non-transitory computer readable recording medium is any data storage device that can store data which can be thereafter read by a computer system. Examples of the non-transitory computer readable recording medium include Read-Only Memory (ROM), Random-Access Memory (RAM), CD-ROMs, magnetic tapes, floppy disks, and optical data storage devices. The non-transitory computer readable recording medium can also be distributed over network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion. Also, functional programs, code, and code segments for accomplishing the present disclosure can be easily construed by programmers skilled in the art to which the present disclosure pertains.

[0148] At this point it should be noted that various embodiments of the present disclosure as described above typically involve the processing of input data and the generation of output data to some extent. This input data processing and output data generation may be implemented in hardware or software in combination with hardware. For example, specific electronic components may be employed in a mobile device or similar or related circuitry for implementing the functions associated with the various embodiments of the present disclosure as described above. Alternatively, one or more processors operating in accordance with stored instructions may implement the functions associated with the various embodiments of the present disclosure as described above. If such is the case, it is within the scope of the present disclosure that such instructions may be stored on one or more non-transitory processor readable mediums. Examples of the processor readable mediums include Read-Only Memory (ROM), Random-Access Memory (RAM), CD-ROMs, magnetic tapes, floppy disks, and optical data storage devices. The processor readable mediums can also be distributed over network coupled computer systems so that the instructions are stored and executed in a distributed fashion. Also, functional computer programs, instructions, and instruction segments for accomplishing the present disclosure can be easily construed by programmers skilled in the art to which the present disclosure pertains.

[0149] While the present disclosure has been shown and described with reference to various embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the present disclosure as defined by the appended claims and their equivalents. cm What is claimed is:

1. A payment support method comprising:
- creating an account used for a payment service via a wallet server apparatus;
- connecting to the wallet server apparatus using the account;
- registering personal identification information including hardware information of a terminal device in the account; and
- associating at least one payment option with the personal identification information stored in the wallet server apparatus.

2. The payment support method of claim **1**, wherein the creating of the account comprises operating an electronic device configured to access a communication network to connect to the wallet server apparatus and send personal information to the wallet server apparatus.

3. The payment support method of claim **1**, wherein the hardware information of the terminal device comprises at least one of a serial number of the terminal device, Media Access Control (MAC) information of the terminal device, and memory ID of the terminal device.

4. The payment support method of claim **1**, further comprising:
- receiving, by the terminal device, a payment request for a product purchase;
- accessing the wallet server apparatus;
- sending the personal identification information including the hardware information of the terminal device to the wallet server apparatus;
- performing, by the wallet server apparatus, terminal verification based on the personal identification information;
- sending, upon completion of the terminal verification, by the wallet server apparatus, the payment request for the product purchase to a financial support apparatus; and
- performing, by the financial support apparatus, payment approval.

5. The payment support method of claim **4**, wherein the accessing of the wallet server apparatus comprises one of:
- connecting to the wallet server apparatus using a program installed to access the wallet server apparatus when the program is selected for activation; and
- automatically activating the program according to a request from the wallet server apparatus.

6. The payment support method of claim **4**, further comprising sending, after the terminal verification, by the wallet server apparatus, payment option information preregistered by the terminal device to the terminal device.

7. The payment support method of claim 1, further comprising one of:

generating, by the wallet server apparatus, identification card information related to the account, providing the identification card information to the terminal device, and storing, according to a request from the terminal device, the identification card information so that the identification card information is mapped with information on the terminal device; and

registering identification card information provided by the terminal device in the account open for the terminal device, and storing the identification card information so that the identification card information is mapped with information on the terminal device.

8. The payment support method of claim 7, further comprising:

receiving, by the terminal device, a payment request for a product purchase;

connecting to the wallet server apparatus, sending the personal identification information to the wallet server apparatus, selecting one of payment options preregistered in the terminal device, and waiting for payment;

obtaining, by a member store apparatus, the identification card information and sending the identification card information to the wallet server apparatus; and

performing, by a financial support apparatus, payment approval for the payment request according to validity of the identification card information.

9. The payment support method of claim 7, wherein the providing of the identification card information comprises one of:

fabricating, by the wallet server apparatus, an identification card containing the identification card information and delivering the identification card to the terminal device; and

generating, by the wallet server apparatus, the identification card information as disposable information and sending the disposable identification card information to the terminal device.

10. The payment support method of claim 9, wherein the disposable identification card information is sent through at least one of key input, a barcode reader, and short-range wireless communication.

11. A payment support system comprising:

a wallet server apparatus configured to support generation of an account of a payment service; and

a terminal device configured to connect to the wallet server apparatus using the account,

wherein the terminal device registers personal identification information including hardware information of the terminal device in the account and associates at least one payment option with the personal identification information stored in the wallet server apparatus.

12. The payment support system of claim 11, wherein the hardware information of the terminal device comprises at least one of a serial number of the terminal device, Media Access Control (MAC) information of the terminal device, and memory ID of the terminal device.

13. The payment support system of claim 11, further comprising:

a member store apparatus configured to receive a payment request for a product purchase from the terminal device,

wherein the member store apparatus collects the personal identification information of the terminal device and sends the product purchase information and the personal identification information to the wallet server apparatus.

14. The payment support system of claim 13, wherein the wallet server apparatus comprises:

a terminal verification server configured to verify the terminal device according to the payment request from the member store apparatus; and

an app server equipment configured to provide, upon completion of the terminal verification, payment option information registered by the terminal device to the terminal device.

15. The payment support system of claim 11, wherein the terminal device connects to the wallet server apparatus by using a program installed for access to the wallet server apparatus when the program is selected for activation or by automatically activating the program according to a request from the wallet server apparatus.

16. The payment support system of claim 11, wherein the wallet server apparatus generates identification card information related to the account, provides the identification card information to the terminal device, and stores, according to a request from the terminal device, the identification card information so that the identification card information is mapped with information on the terminal device.

17. The payment support system of claim 16, wherein, when a payment request for a product purchase is received, the terminal device connects to the wallet server apparatus, sends the personal identification information to the wallet server apparatus, selects one of payment options preregistered in the terminal device, and waits for payment.

18. The payment support system of claim 17, wherein the wallet server apparatus sends the payment request to a financial support apparatus that approves the payment request according to validity of the identification card information.

19. The payment support system of claim 16, wherein the wallet server apparatus fabricates an identification card containing the identification card information and delivers the identification card to the terminal device, or generates the identification card information as disposable information and sends the disposable identification card information to the terminal device.

20. The payment support system of claim 19, wherein the disposable identification card information is sent through at least one of key input, a barcode reader, and short-range wireless communication.

* * * * *

(19) **United States**

(12) **Patent Application Publication**

Verma et al.

(10) **Pub. No.: US 2014/0279566 A1**

(43) **Pub. Date: Sep. 18, 2014**

(54) **SECURE MOBILE PAYMENT USING MEDIA BINDING**

(71) Applicant: **Samsung Electronics Co., Ltd.**, Suwon (KR)

(72) Inventors: **Sanjeev Verma**, San Jose, CA (US); **Glen D. Stone**, Los Gatos, CA (US)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Suwon (KR)

(21) Appl. No.: **14/015,611**

(22) Filed: **Aug. 30, 2013**

Related U.S. Application Data

(60) Provisional application No. 61/789,457, filed on Mar. 15, 2013.

Publication Classification

(51) **Int. Cl.**

G06Q 20/38 (2006.01)

G06Q 20/32 (2006.01)

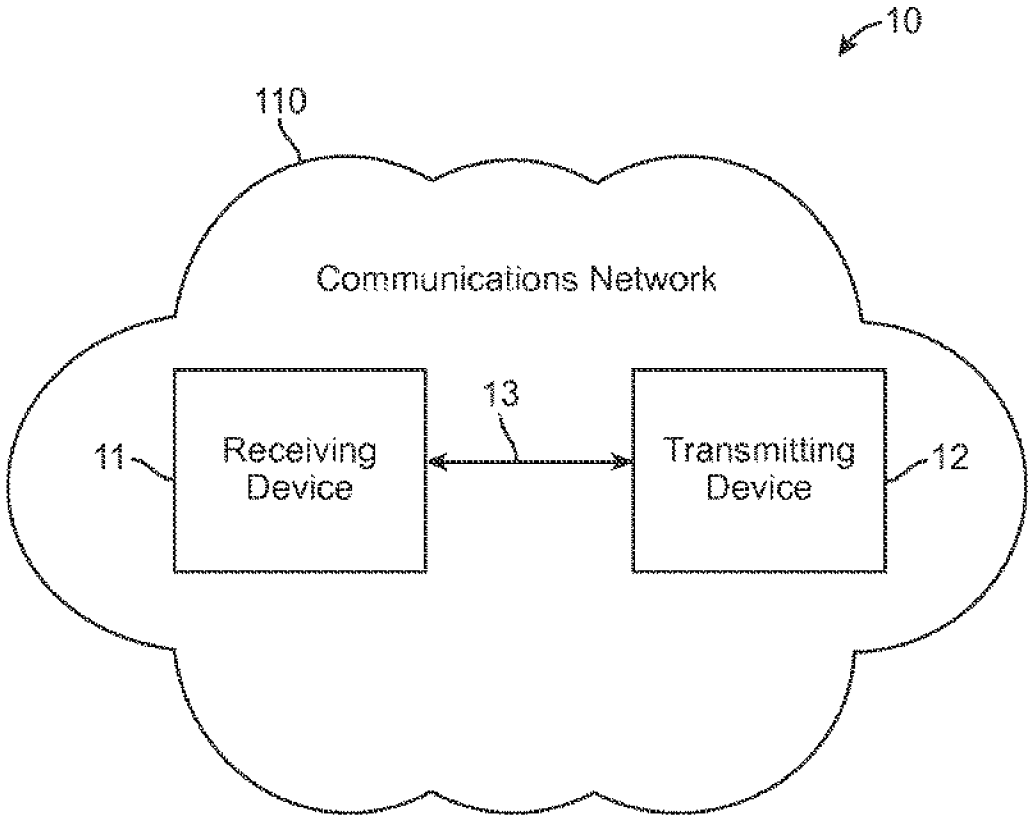
(52) **U.S. Cl.**

CPC ***G06Q 20/38215*** (2013.01); ***G06Q 20/322*** (2013.01)

USPC **705/76**

(57) **ABSTRACT**

A method for mobile payment includes generating, by a financial institution, a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification. The financial institution stores the credential and media binding information in the form of authentication code in a memory used by an electronic device. The stored credential and media binding information is accessed using the user access information for a payment transaction. A digital certificate is generated using the credential and media binding information. The digital certificate is presented to the financial institution for the payment transaction. The memory is authenticated and binding of the credential to the memory is verified prior to completing the payment transaction.



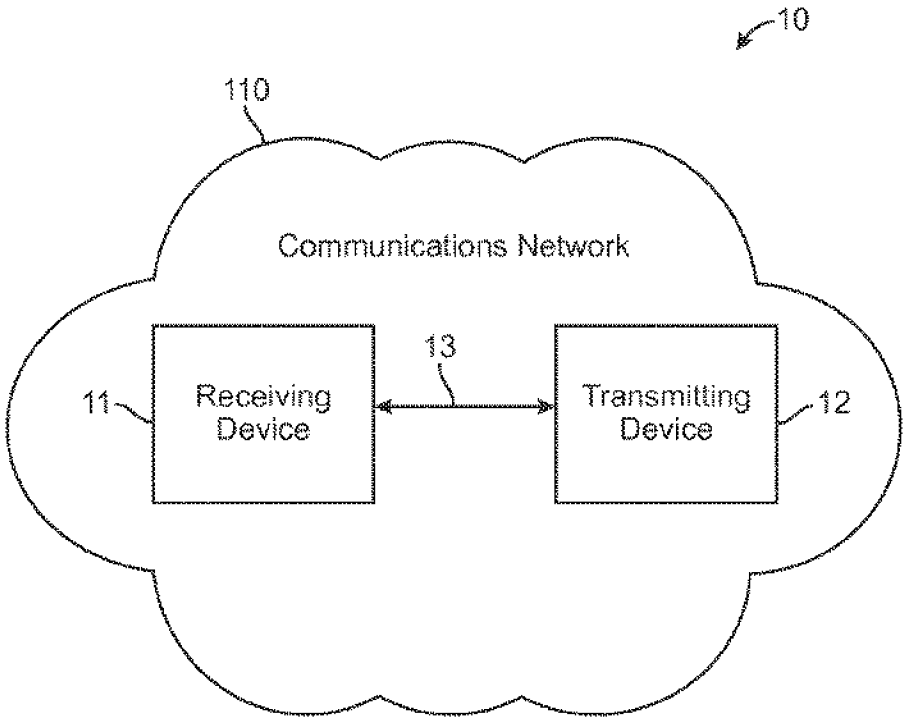

10
110
Communications Network
11
Receiving Device
13
Transmitting Device
12

FIG. 1

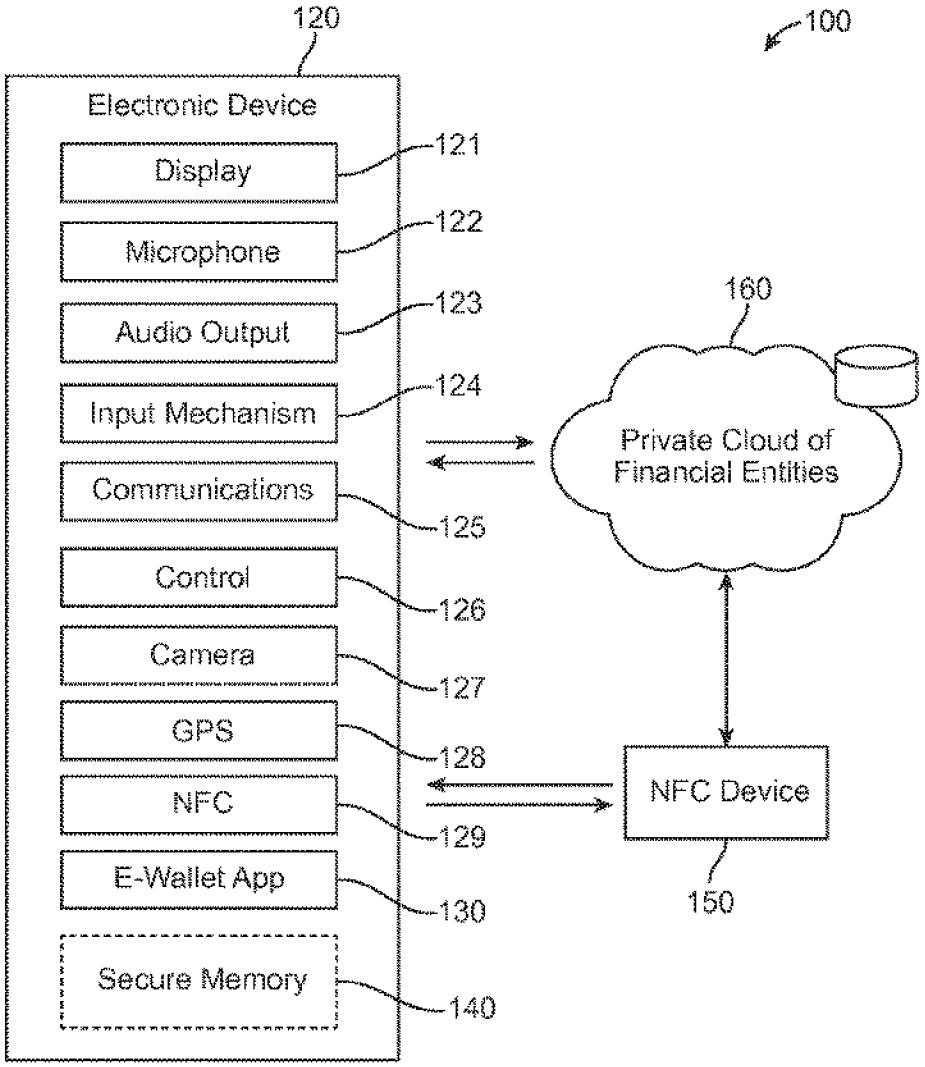

120
100
Electronic Device
Display
121
Microphone
122
Audio Output
123
Input Mechanism
124
Communications
125
Control
126
Camera
127
GPS
128
NFC
129
E-Wallet App
130
Secure Memory
140
160
Private Cloud of Financial Entities
NFC Device
150

FIG. 2

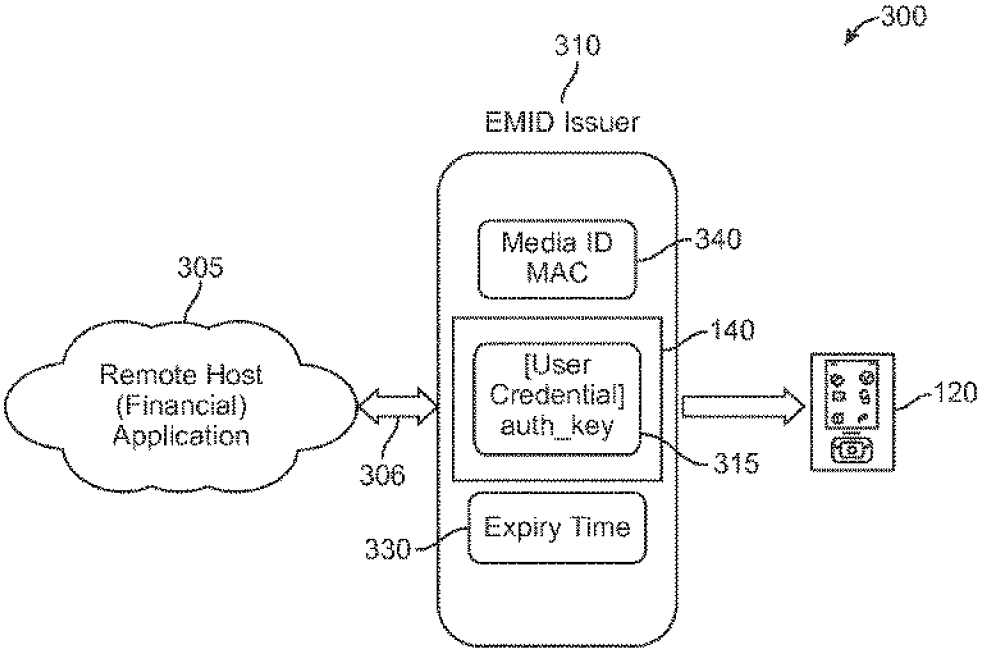

300
310
EMID Issuer
Media ID
MAC
340
305
140
Remote Host
(Financial)
Application
[User
Credential]
auth_key
120
306
315
330
Expiry Time

FIG. 3

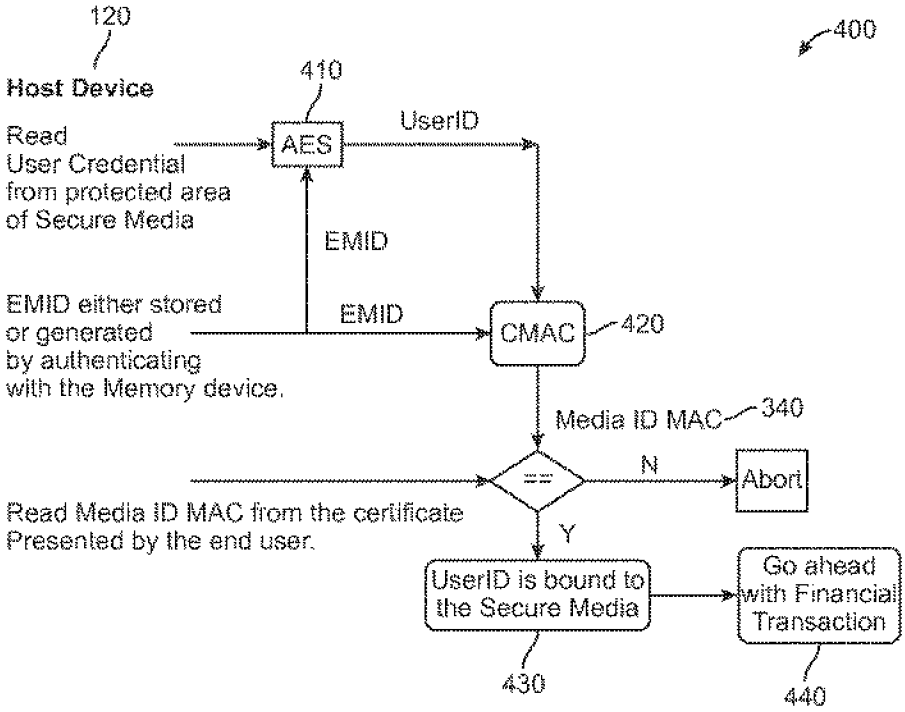

120
400
Host Device
410
Read
User Credential
from protected area
of Secure Media
AES
UserID
EMID
EMID either stored
or generated
by authenticating
with the Memory device.
EMID
CMAC
420
Media ID MAC
340
==
N
Abort
Read Media ID MAC from the certificate
Presented by the end user.
Y
UserID is bound to
the Secure Media
Go ahead
with Financial
Transaction
430
440

FIG. 4

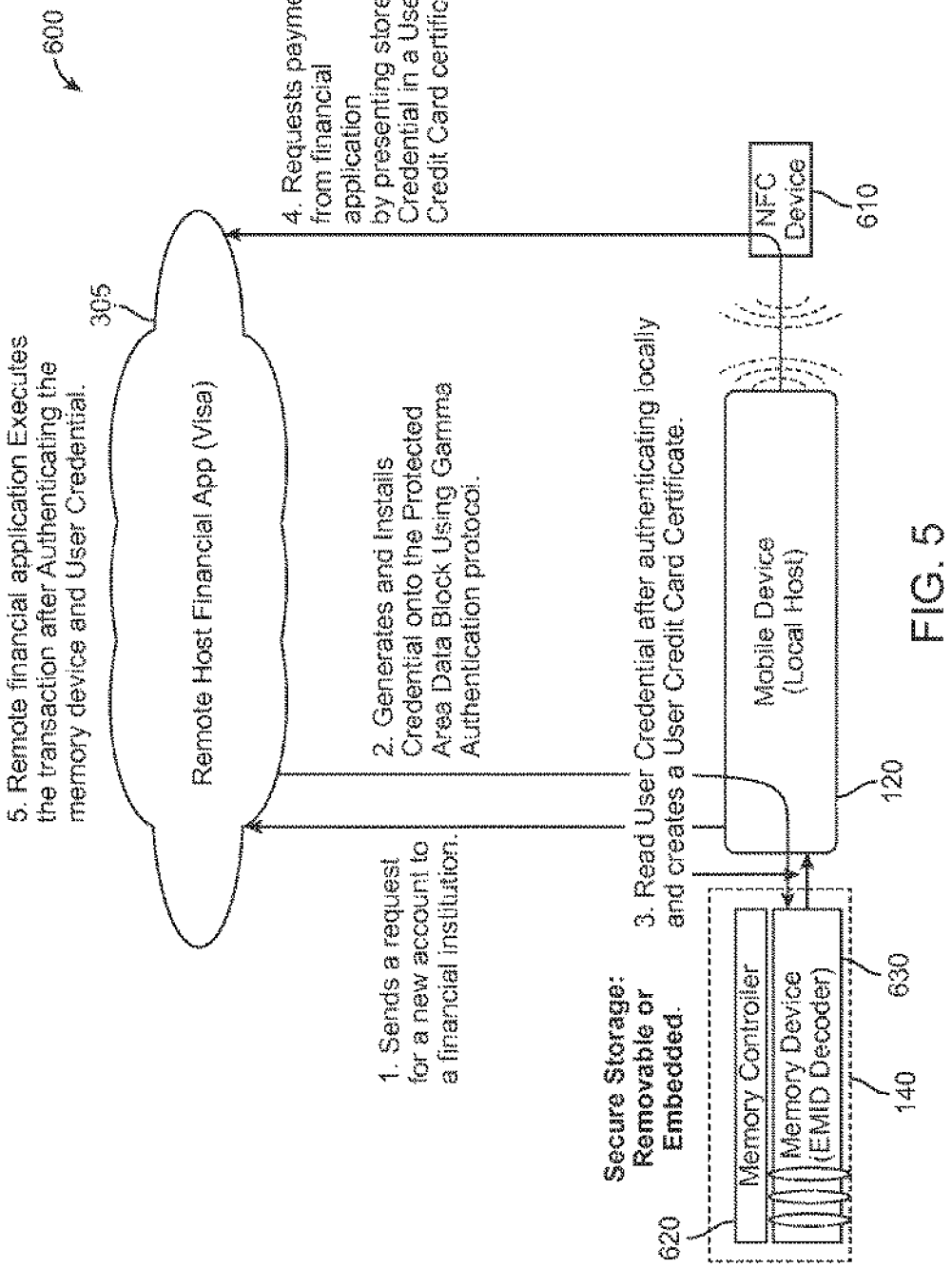

600
5. Remote financial application Executes the transaction after Authenticating the memory device and User Credential.
305
Remote Host Financial App (Visa)
4. Requests payment from financial application by presenting stored Credential in a User Credit Card certificate.
2. Generates and Installs Credential onto the Protected Area Data Block Using Gamma Authentication protocol.
1. Sends a request for a new account to a financial institution.
3. Read User Credential after authenticating locally and creates a User Credit Card Certificate.
NFC Device
610
Mobile Device (Local Host)
120
Secure Storage: Removable or Embedded.
620
Memory Controller
Memory Device (EMID Decoder)
630
140

FIG. 5

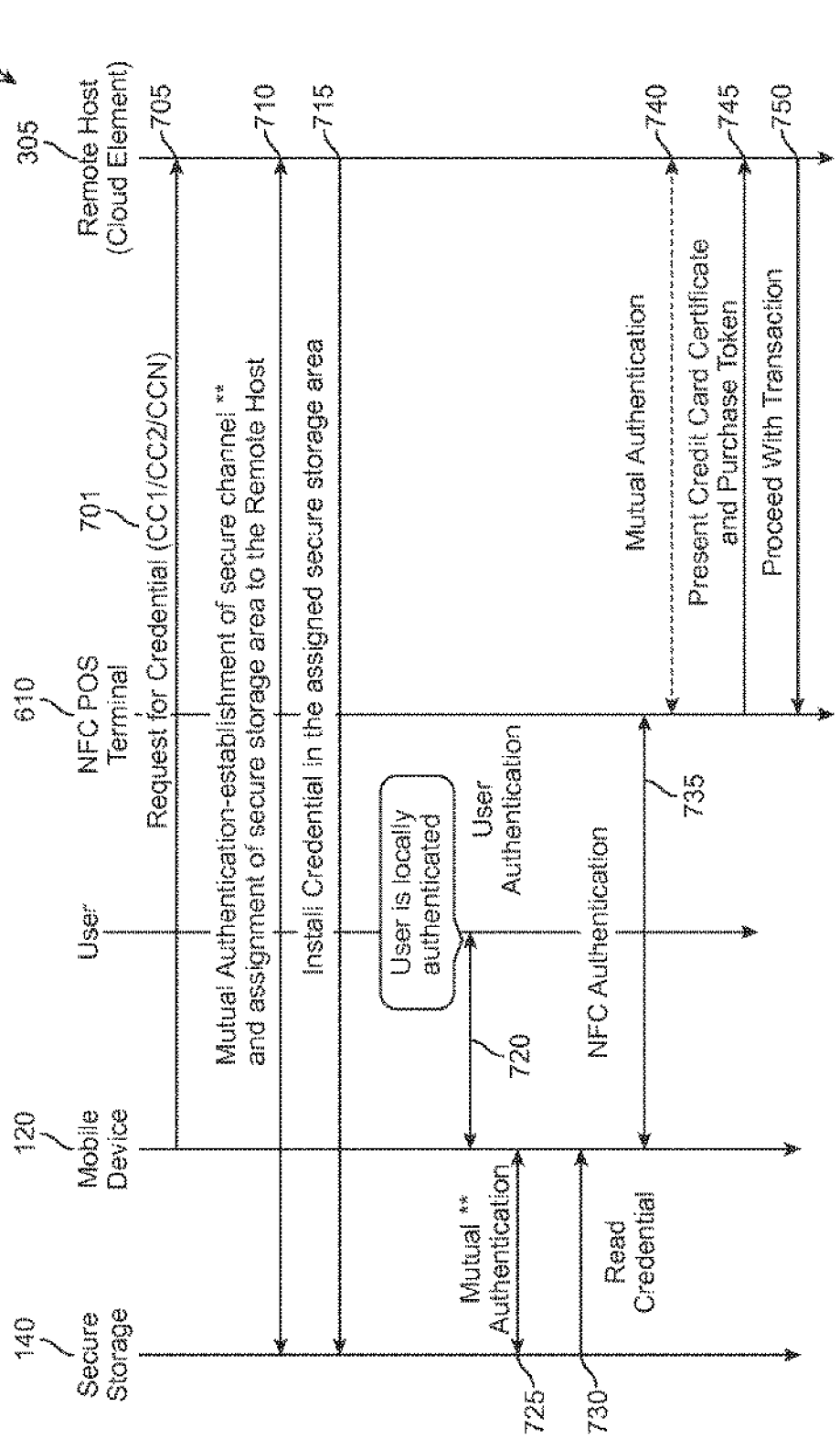

700
140
Secure Storage
120
Mobile Device
610
NFC POS Terminal
User
305
Remote Host (Cloud Element)
705
Request for Credential (CC1/CC2/CCN)
701
Mutual Authentication-establishment of secure channel ** and assignment of secure storage area to the Remote Host
710
Install Credential in the assigned secure storage area
715
User is locally authenticated
User Authentication
720
NFC Authentication
735
Mutual Authentication
740
Present Credit Card Certificate and Purchase Token
745
Proceed With Transaction
750
Mutual ** Authentication
725
Read Credential
730

FIG. 6

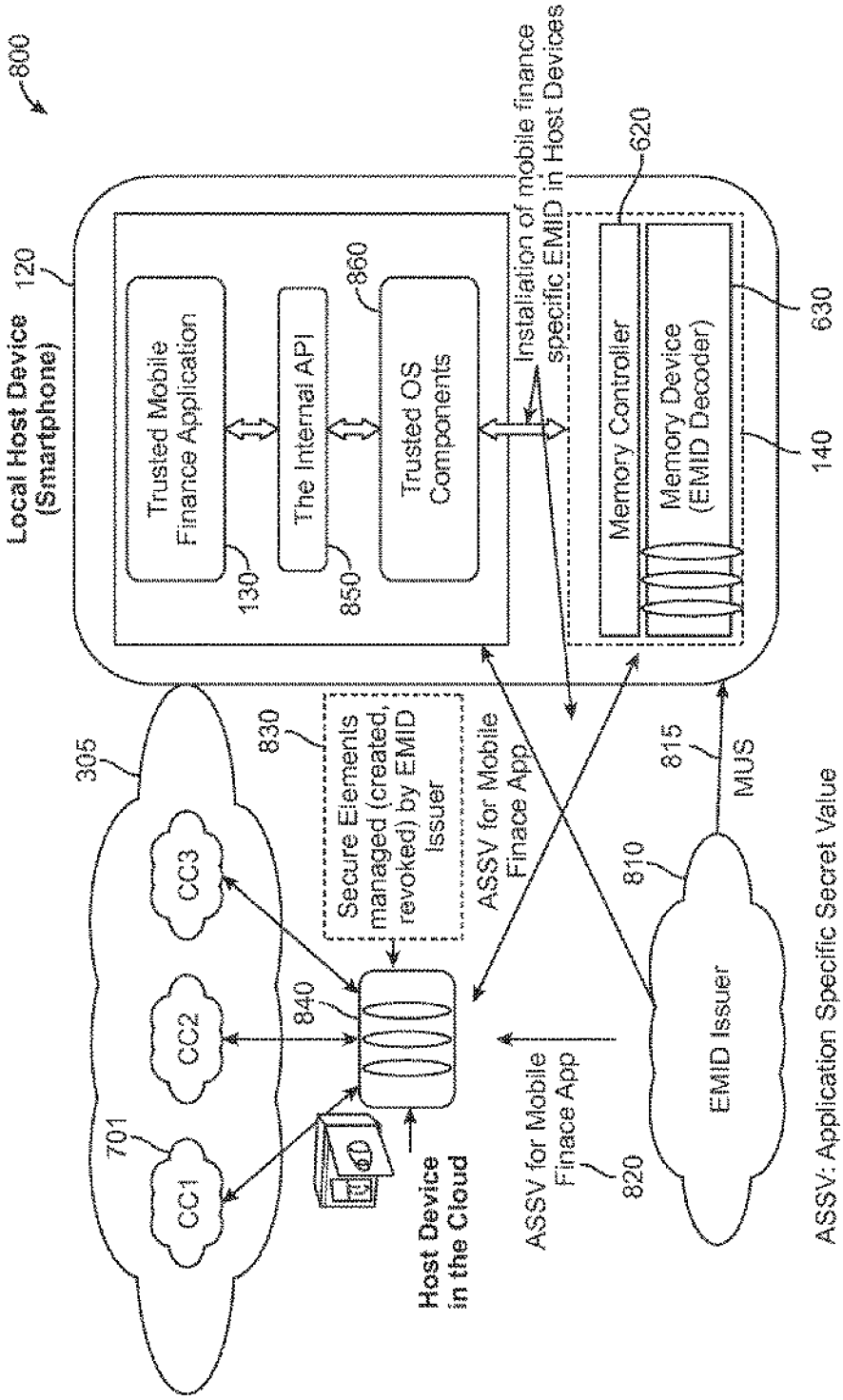

800
Local Host Device (Smartphone)
120
Trusted Mobile Finance Application
130
The Internal API
850
860
Trusted OS Components
Installation of mobile finance specific EMID in Host Devices
620
Memory Controller
Memory Device (EMID Decoder)
630
140
305
CC1
CC2
CC3
701
Secure Elements managed (created, revoked) by EMID Issuer
830
840
ASSV for Mobile Finace App
Host Device in the Cloud
ASSV for Mobile Finace App
820
810
EMID Issuer
815
MUS
ASSV: Application Specific Secret Value
MUS: Memory Unique Secret

FIG. 7

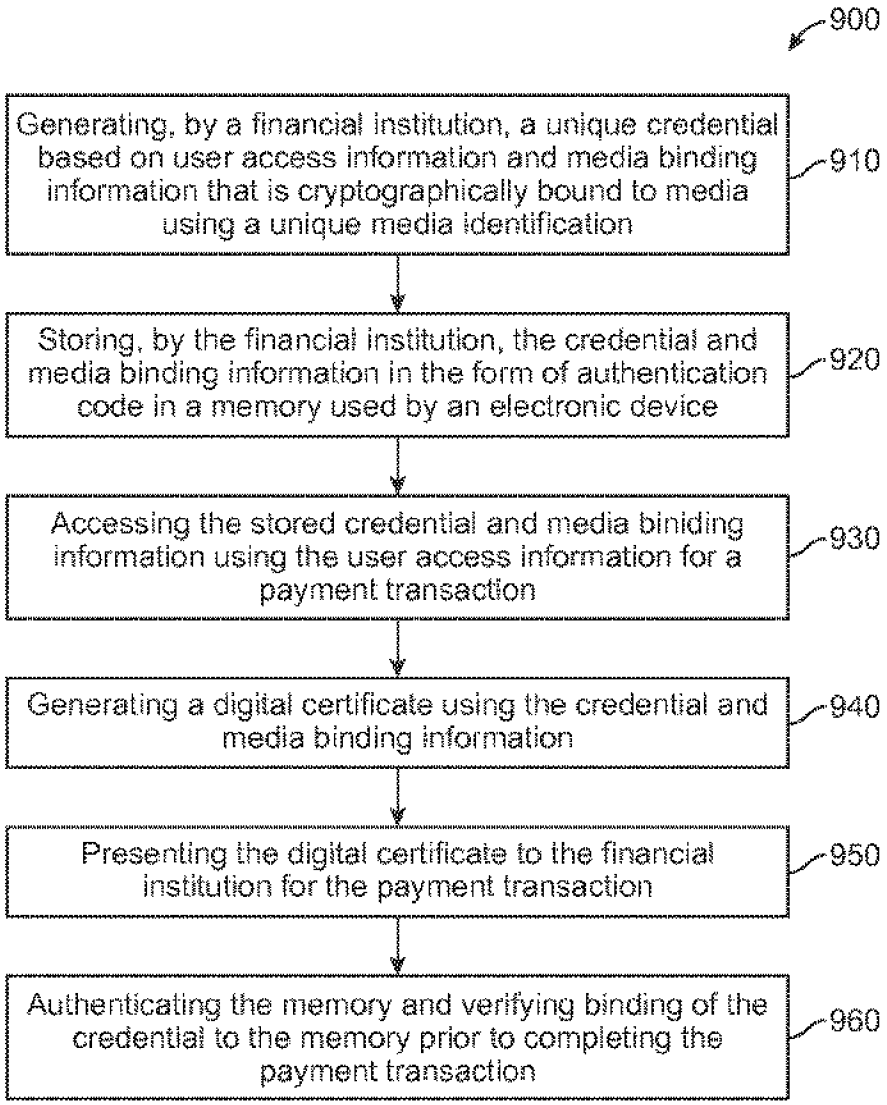

900
Generating, by a financial institution, a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification
910
Storing, by the financial institution, the credential and media binding information in the form of authentication code in a memory used by an electronic device
920
Accessing the stored credential and media biniding information using the user access information for a payment transaction
930
Generating a digital certificate using the credential and media binding information
940
Presenting the digital certificate to the financial institution for the payment transaction
950
Authenticating the memory and verifying binding of the credential to the memory prior to completing the payment transaction
960

FIG. 8

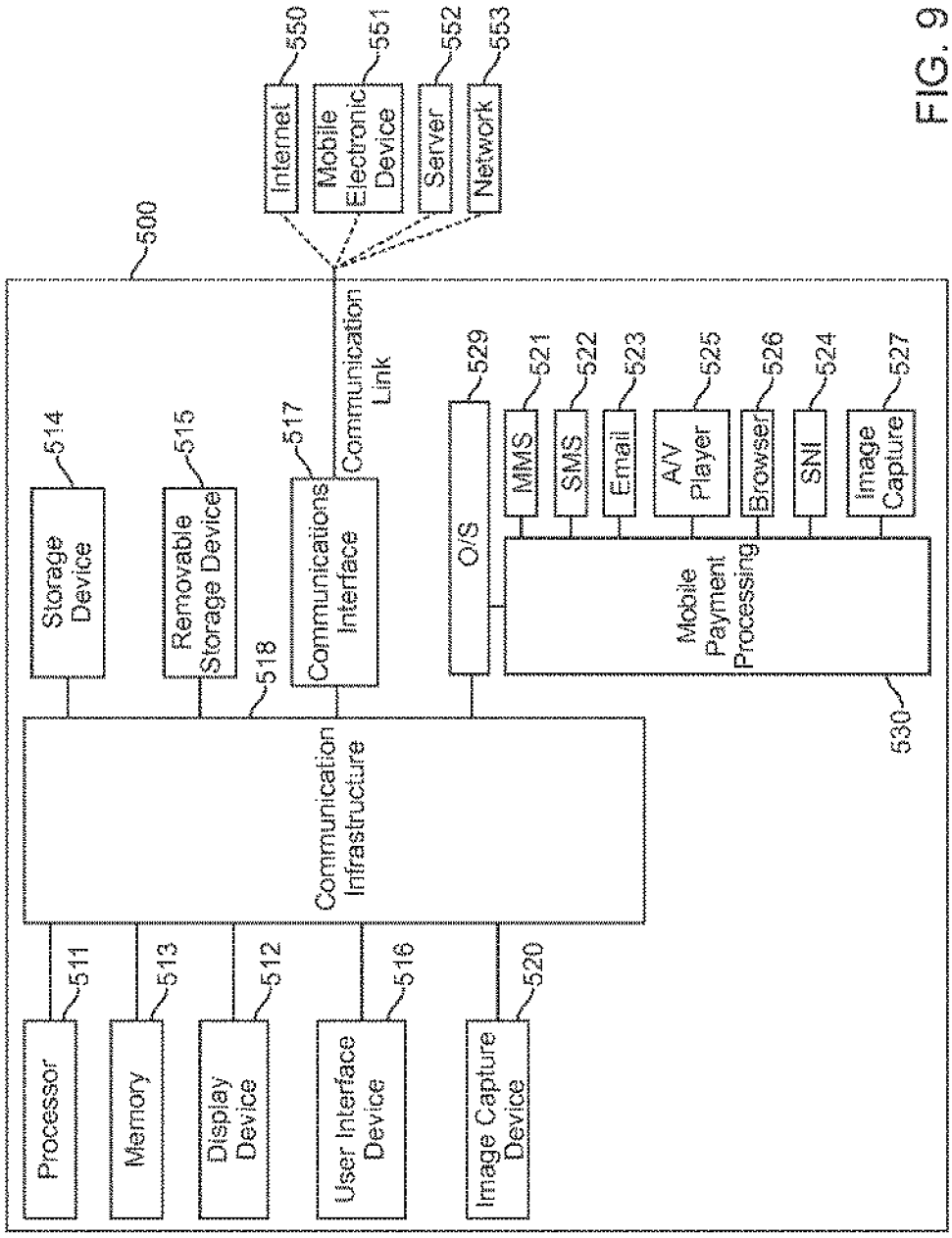

500
Internet
550
Mobile Electronic Device
551
Server
552
Network
553
Communication Link
517
Communications Interface
518
Storage Device
514
Removable Storage Device
515
Communication Infrastructure
O/S
529
MMS
521
SMS
522
Email
523
A/V Player
525
Browser
526
SNI
524
Image Capture
527
Mobile Payment Processing
530
Processor
511
Memory
513
Display Device
512
User Interface Device
516
Image Capture Device
520

FIG. 9

SECURE MOBILE PAYMENT USING MEDIA BINDING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the priority benefit of U.S. Provisional Patent Application Ser. No. 61/789,457, filed Mar. 15, 2013, incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] One or more embodiments relate generally to mobile payment and, in particular, to secure mobile payment using media binding.

BACKGROUND

[0003] Credit card payment typically uses a four party payment system including the bank customer/cardholder that desires to obtain goods or services, a merchant or retailer that uses a point-of-service (POS) card reader and provides goods or services, the issuer (e.g., bank) that provides the customer with a means to pay for the goods or services (e.g., through billing, online payment options, etc.), and the Acquirer with whom the merchant interacts to receive funds for the goods or services.

SUMMARY

[0004] In one embodiment, a method provides mobile payment. One embodiment comprises a method that includes generating, by a financial institution, a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification. In one embodiment, the financial institution stores the credential and media binding information in the form of authentication code in a memory used by an electronic device. In one embodiment, the stored credential and media binding information is accessed using the user access information for a payment transaction. In one embodiment, a digital certificate is generated using the credential and media binding information. In one embodiment, the digital certificate is presented to the financial institution for the payment transaction. In one embodiment, the memory is authenticated and binding of the credential to the memory is verified prior to completing the payment transaction.

[0005] One embodiment provides a system for mobile payment. In one embodiment a server generates a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification, and stores the credential and media binding information in the form of authentication code in a memory used by an electronic device through a secure channel. In one embodiment, an electronic device accesses the stored credential and media binding information from the memory using the user access information for a payment transaction, and generates a digital certificate using the credential. In one embodiment, a near field communication (NFC) interface passes the digital certificate to the server for the payment transaction. In one embodiment, the server authenticates the memory and verifies binding of the credential to the memory prior to completing the payment transaction.

[0006] Another embodiment provides a server for mobile payment that comprises a credential service that uses a processor to generate a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification, and stores the credential and media binding information in a memory used by an electronic device through a secure channel. In one embodiment an authorization service authenticates the memory and verifies the binding of the credential to the memory prior to completing a requested payment transaction based on a digital certificate generated by the electronic device using the credential and media binding information.

[0007] These and other aspects and advantages of the embodiments will become apparent from the following detailed description, which, when taken in conjunction with the drawings, illustrate by way of example the principles of the embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] For a fuller understanding of the nature and advantages of the embodiments, as well as a preferred mode of use, reference should be made to the following detailed description read in conjunction with the accompanying drawings, in which:

[0009] FIG. **1** shows a schematic view of a communications system, according to an embodiment.

[0010] FIG. **2** shows a block diagram of an architecture system for mobile payment using an electronic device, according to an embodiment.

[0011] FIG. **3** shows an architecture for storage and access control for mobile payment using an electronic device, according to an embodiment.

[0012] FIG. **4** shows a memory binding authentication flow, according to an embodiment.

[0013] FIG. **5** shows an example flow for a mobile transaction with a cloud computing environment for mobile payment using an electronic device, according to an embodiment.

[0014] FIG. **6** shows a flow diagram for mobile payment using an electronic device, according to an embodiment.

[0015] FIG. **7** shows an architecture implementation for mobile payment using an electronic device, according to an embodiment.

[0016] FIG. **8** shows a block diagram of a flow chart for mobile payment using an electronic device, according to an embodiment.

[0017] FIG. **9** is a high-level block diagram showing an information processing system comprising a computing system implementing an embodiment.

DETAILED DESCRIPTION

[0018] The following description is made for the purpose of illustrating the general principles of the embodiments and is not meant to limit the inventive concepts claimed herein. Further, particular features described herein can be used in combination with other described features in each of the various possible combinations and permutations. Unless otherwise specifically defined herein, all terms are to be given their broadest possible interpretation including meanings implied from the specification as well as meanings understood by those skilled in the art and/or as defined in dictionaries, treatises, etc.

[0019] One or more embodiments relate generally to payment for point-of-service (POS) purchases using an electronic device. One embodiment provides secured purchasing using authentication of a memory device and secure creden-

tial. In one embodiment, the electronic device comprises a mobile electronic device capable of data communication over a communication link, such as a wireless communication link. Examples of such mobile device include a mobile phone device, a mobile tablet device, a wearable device, portable computing device, etc.

[0020] In one embodiment, a method provides mobile payment using an electronic device. One embodiment comprises a method that includes generating, by a financial institution, a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification. In one embodiment, the financial institution stores the credential and media binding information in a memory used by an electronic device. In one embodiment, the stored credential and media binding information is accessed using the user access information for a payment transaction. In one embodiment, a digital certificate is generated using the credential and media binding information. In one embodiment, the digital certificate is presented to the financial institution for the payment transaction. In one embodiment, the memory is authenticated and binding of the credential to the memory is verified prior to completing the payment transaction.

[0021] One or more embodiments address the security in a mobile payment ecosystem by using enhanced media identification (EMID) technology and a private cloud computing environment managed and authenticated by financial institutions (e.g., credit card issuers). In one embodiment, a security issue arising out of a theft of a mobile device is handled by revoking a credential of a memory device by financial institutions. One embodiment provides for replacement of plastic credit cards by digital credit cards, such as digital certificates generated by electronic devices.

[0022] In one embodiment, the installation and management of a mobile payment credential in the mobile electronic device takes place directly between the private computing environment (e.g., of financial institutions, a cloud computing environment, etc.) and the electronic device without any involvement of other entities, such as a mobile network operator (MNO).

[0023] FIG. **1** is a schematic view of a communications system in accordance with one embodiment. Communications system **10** may include a communications device that initiates an outgoing communications operation (transmitting device **12**) and communications network **110**, which transmitting device **12** may use to initiate and conduct communications operations with other communications devices within communications network **110**. For example, communications system **10** may include a communication device that receives the communications operation from the transmitting device **12** (receiving device **11**). Althongh communications system **10** may include several transmitting devices **12** and receiving devices **11**, only one of each is shown in FIG. **1** to simplify the drawing.

[0024] Any suitable circuitry, device, system or combination of these (e.g., a wireless communications infrastructure including communications towers and telecommunications servers) operative to create a communications network may be used to create communications network **110**. Communications network **110** may be capable of providing communications using any suitable communications protocol. In some embodiments, communications network **110** may support, for example, traditional telephone lines, cable television, Wi-Fi (e.g., a 802.11 protocol), Bluetooth®, high frequency systems (e.g., 900 MHz, 2.4 GHz, and 5.6 GHz communication systems), infrared, other relatively localized wireless communication protocol, or any combination thereof. In some embodiments, communications network **110** may support protocols used by wireless and cellular phones and personal email devices (e.g., a Blackberry®). Such protocols may include, for example, GSM, GSM plus EDGE, CDMA, quadband, and other cellular protocols. In another example, a long range communications protocol may include Wi-Fi and protocols for placing or receiving calls using VOIP or LAN. Transmitting device **12** and receiving device **11**, when located within communications network **110**, may communicate over a bidirectional communication path such as path **13**. Both transmitting device **12** and receiving device **11** may be capable of initiating a communications operation and receiving an initiated communications operation.

[0025] Transmitting device **12** and receiving device **11** may include any suitable device for sending and receiving communications operations. For example, transmitting device **12** and receiving device **11** may include a cellular telephone or a landline telephone, a personal e-mail or messaging device with audio and/or video capabilities, pocket-sized personal computers such as an iPAQ Pocket PC, available by Hewlett Packard Inc., of Palo Alto, Calif., personal digital assistants (PDAs), wearable devices, a desktop computer, a laptop computer, tablet computers, pad-type computing devices, a media player, and any other device capable of communicating wirelessly (with or without the aid of a wireless-enabling accessory system) or via wired pathways (e.g., using traditional telephone wires). The communications operations may include any suitable form of communication, including for example, voice communication (e.g., telephone calls), data communication (e.g., e-mails, text messages, media messages), near field communication (NFC), or combinations of these (e.g., video conferences).

[0026] FIG. **2** shows a functional block diagram of an architecture system **100** that may be used for mobile payment using an electronic device **120**, according to an embodiment. Both transmitting device **12** and receiving device **11** may include some or all of the features of electronics device **120**. In one embodiment, the electronic device **120** may comprise a display **121**, a microphone **122**, an audio output **123**, an input mechanism **124**, communications circuitry **125**, control circuitry **126**, a camera **127**, a global positioning system (GPS) receiver module **128**, an NFC interface **129**, a secure memory module **140**, and any other suitable components. In one embodiment, a mobile payment application **130** (e.g., an e-wallet application) executes on the electronic device **120**. In one embodiment, an e-wallet table or list may store information associated with multiple credit cards. In one embodiment, the electronic device **120** may communicate with the private computing environment **160** (e.g., a clond computing environment, local or remote server, etc.) that comprises financial entities (e.g., banks, credit card issuers, etc.) that process credit cards and use thereof. In one embodiment, the NFC interface **129** communicates with the NFC device **150** that may be coupled with or part of a POS system that accepts credit card payments for a merchant.

[0027] In one embodiment, the secure memory module **140** may comprise a removable memory device or card, or may comprise a memory device embedded in the electronic device **120**. In one embodiment, the memory modnle **140** comprises memory that is secure and separate from other memory available for the electronic device **120**.

[0028] In one embodiment, all of the applications employed by an audio output **123**, a display **121**, an input mechanism **124**, communications circuitry **125** and a microphone **122** may be interconnected and managed by control circuitry **126**. In one embodiment, the audio output **123** may include any suitable audio component for providing audio to the user of the electronics device **120**. For example, the audio output **123** may include one or more speakers (e.g., mono or stereo speakers) built into the electronics device **120**. In some embodiments, the audio output **123** may include an audio component that is remotely coupled to electronics device **120**. For example, the audio output **123** may include a headset, headphones or earbuds that may be coupled to communications device with a wire (e.g., coupled to the electronics device **120** with a jack) or wirelessly (e.g., Bluetooth® headphones or a Bluetooth® headset).

[0029] In one embodiment, the display **121** may include any suitable screen or projection system for providing a display visible to the user. For example, the display **121** may include a screen (e.g., an LCD screen) that is incorporated in electronics device **120**. As another example, the display **121** may include a movable display or a projecting system for providing a display of content on a surface remote from the electronics device **120** (e.g., a video projector). The display **121** may be operative to display content (e.g., information regarding communications operations or information regarding available media selections) under the direction of control circuitry **126**.

[0030] In one embodiment, the input mechanism **124** may be any suitable mechanism or user interface for providing user inputs or instructions to the electronics device **120**. The input mechanism **124** may take a variety of forms, such as a button, keypad, dial, a click wheel, or a touch screen. The input mechanism **124** may include a multi-touch screen. The input mechanism **124** may include a user interface that may emulate a rotary phone or a multi-button keypad, which may be implemented on a touch screen or the combination of a click wheel or other user input device and a screen.

[0031] In one embodiment, communications circuitry **125** may be any suitable communications circuitry operative to connect to a communications network (e.g., communications network **110**, FIG. **1**) and to transmit communications operations and media from the electronics device **120** to other devices within the communications network. Communications circuitry **125** may be operative to interface with the communications network using any suitable communications protocol such as, for example, Wi-Fi (e.g., a 802.11 protocol), Bluetooth®, high frequency systems (e.g., 900 MHz, 2.4 GHz, and 5.6 GHz communication systems), infrared, GSM, GSM plus EDGE, CDMA, quadband, and other cellular protocols, VOIP, or any other suitable protocol.

[0032] In some embodiments, communications circuitry **125** may be operative to create a communications network using any suitable communications protocol. For example, communications circuitry **125** may create a short-range communications network using a short-range communications protocol to connect to other communications devices. For example, communications circuitry **125** may be operative to create a local communications network using the Bluetooth® protocol to couple the electronics device **120** with a Bluetooth® headset.

[0033] In one embodiment, control circuitry **126** may be operative to control the operations and performance of the electronics device **120**. Control circuitry **126** may include, for example, a processor, a bus (e.g., for sending instructions to the other components of the electronics device **120**), memory, storage, or any other suitable component for controlling the operations of the electronics device **120**. In some embodiments, a processor may drive the display and process inputs received from the user interface. The memory and storage may include, for example, cache, flash memory, ROM, and/or RAM. In some embodiments, the memory may be specifically dedicated to storing firmware (e.g., for device applications such as an operating system, user interface functions, and processor functions). In some embodiments, memory may be operative to store information related to other devices with which the electronics device **120** performs communications operations (e.g., saving contact information related to communications operations or storing information related to different media types and media items selected by the user).

[0034] In one embodiment, the control circuitry **126** may be operative to perform the operations of one or more applications implemented on the electronics device **120**. Any suitable number or type of applications may be implemented. Although the following discussion will enumerate different applications, it will be understood that some or all of the applications may be combined into one or more applications. For example, the electronics device **120** may include an ASR application, a dialog application, a map application, a media application (e.g., QuickTime®, MobileMusic.app, or MobileVideo.app). In some embodiments, the electronics device **120** may include one or several applications operative to perform communications operations. For example, the electronics device **120** may include a messaging application, a mail application, a telephone application, a voicemail application, an instant messaging application (e.g., for chatting), a videoconferencing application, a fax application, or any other suitable application for performing any suitable communications operation.

[0035] In some embodiments, the electronics device **120** may include a microphone **122**. For example, electronics device **120** may include the microphone **122** to allow the user to transmit audio (e.g., voice audio) during a communications operation or as a means of establishing a communications operation or as an alternate to using a physical user interface. The microphone **122** may be incorporated in electronics device **120**, or may be remotely coupled to the electronics device **120**. For example, the microphone **122** may be incorporated in wired headphones, or the microphone **122** may be incorporated in a wireless headset.

[0036] In one embodiment, the electronics device **120** may include any other component suitable for performing a communications operation. For example, the electronics device **120** may include a power supply, ports, or interfaces for coupling to a host device, a secondary input mechanism (e.g., an ON/OFF switch), or any other suitable component.

[0037] In one embodiment, a user may direct the electronics device **120** to perform a communications operation using any suitable approach. As one example, a user may receive a communications request from another device (e.g., an incoming telephone call, an email or text message, an instant message) and may initiate a communications operation by accepting the communications request. As another example, the user may initiate a communications operation by identifying another communications device and transmitting a request to initiate a communications operation (e.g., dialing a telephone number, sending an email, typing a text message, or selecting a chat screen name and sending a chat request).

[0038] In one embodiment, the electronic device **120** may comprise a mobile device that may utilize mobile device hardware functionality including: the display **121**, the GPS receiver module **128**, the camera **127**, a compass module, and an accelerometer and gyroscope module. The GPS receiver module **128** may be used to identify a current location of the mobile device (i.e., user). The compass module is used to identify direction of the mobile device. The accelerometer and gyroscope module is used to identify tilt of the mobile device. In other embodiments, the electronic device may comprise a television or television component system.

[0039] FIG. **3** shows an architecture **300** for storage and access control for mobile payment using an electronic device **120**, according to an embodiment. In one embodiment, an EMID issuer **310** provides the remote host **305** (e.g., a financial institution application running on a server in the computing environment **160**) with information including a secure location on a memory device of the secure memory module **140** that contains a secret or code.

[0040] In one embodiment, EMID technology is used to provide secure mobile finance services on the electronic device **120**. EMID technology enables a unique way of identifying flash memory by embedding a unique secret (e.g., code) in the secure area (e.g., in the secure memory module **140**) of memory (e.g., flash memory) at the time of manufacturing the memory device. In one embodiment, the unique secret never leaves the flash memory. In one embodiment, the remote host **305** transmits and stores a user credential authorization key **315** in the memory module **140**. In one embodiment, an authorized host device (e.g., the remote host **305**) may access the secret value to generate a unique identification (ID) for a certain application (e.g., application **130**). The EMID is not stored anywhere in the memory device. In one embodiment, the access to the unique secret is provided through a family key. The family key is derived by using one key from a set of device key sets that every host device is provided with by an EMID issuer **310**. The family key is decrypted by reading a family key block area of the memory in the memory module **140** (e.g., a flash memory device). The memory manufacturer may revoke a host device by updating the family key block so that a revoked Host is not able to derive a family key needed to decrypt the unique secret.

[0041] In one embodiment, a user credential (determined by the remote host **305**, e.g., a financial institution) binds to the memory device of the memory module **140** so that the credential may be revoked by the remote host **305** (e.g., a financial institution) application if the device is lost or stolen. In one embodiment, direct remote credential management is allowed on the secure memory module **140** by the remote host **305** without the direct involvement of the end user of the electronic device **120**. This provides a flexible solution where the credential (or secure element) may be easily moved around between the computing environment **160** and the secure memory module **140**.

[0042] In one embodiment, the remote host **305** also stores an expiry time element **330** in order to limit the access of the credential that may be accessed and decrypted by the electronic device **120**. In one embodiment, the expiry time element **330** includes a time limitation (e.g., a time stamp, code, etc.) that must be periodically updated by the remote host **305**. In one embodiment, the remote host **305** also stores a media ID message authentication code (MAC) on the electronic device **120** to bind the UserID to the media of the secure memory module **140**. In one embodiment, the remote host **305** first authenticates the binding of the credential of the memory device of the secure memory module **140** before accepting the credential from the end user. In one embodiment, the media ID MAC **340** is generated as follows: Media ID MAC=CMAC (EMID, Credentials), where CMAC represents a cipher-based MAC.

[0043] In one embodiment, a user of the electronic device **120** first establishes an account at the financial institution (e.g., remote host **305**) by using user access information (e.g., a username and a password). In one embodiment, the financial institution then generates an authorization key (auth_key) using the user access information (e.g., user name and password) as input to a function, such as a hash function-auth_key=PRF (username, password).

[0044] In one embodiment, the remote host **305** stores the encrypted credential (encrypted using auth_key) at its assigned protected area in the memory device of the secure memory module **140**. In one embodiment, the credential is generated by cryptographically binding the UserID to the media (through EMID). In one embodiment, the credential may be read by the electronic device **120** over a secure channel. In one embodiment, the electronic device **120** (Host device) uses the auth_key **315** to decrypt the credentials stored at the protected area in the secure memory module **140**. In one embodiment, the auth_key is generated locally by first prompting a user to enter their username and password via the electronic device **120**. In this embodiment, the credential may be decrypted correctly only by the rightful owner of the credential. The credential is then presented to the remote host **305** (e.g., the financial institution) through a merchant in the form of a user digital (e.g., credit card) certificate. The remote host (e.g., financial institution) then makes sure that the credential is bound to the secure memory module **140** and originating from the authorized user before completing the transaction.

[0045] In one embodiment, the remote host **305** (e.g., a financial institution such as a Bank, credit card companies, etc.) installs and binds encrypted user credential (encrypted by the auth_key **315**) for the corresponding application (financial institution) on its assigned protected memory area (removable or embedded) of the secure memory module **140** over a secure channel. In one embodiment, the remote host **305** may both read and write the credential on the secure memory module **140**. In one embodiment, the access control information is provided in the Host certificate issued by the EMID issuer **310**.

[0046] In one embodiment, the local Host is the electronic device **120**, and may (Mobile Device) read the encrypted stored credential over the secure channel when desired to use the credential at the time of a financial transaction. In one embodiment, the electronic device **120** decrypts the credential using the auth_key **315** by prompting a user to enter a username and password. In one embodiment, the electronic device **120** cannot modify the credential stored in the secure area of the secure memory module **140**.

[0047] In one embodiment, the user credential is cryptographically bound by the remote host **305** (e.g., financial institution) to the media of the secure memory module **140**, and the credential is generated as: User credential=PRF (UserID, EMID); where PRF indicated pseudo-random function, such as advanced encryption standard (AES) and UserID is the user identity of the end user at the remote host **305** (e.g., at the financial institution). In one embodiment, the expiry time **330** is stored along with the credential, and the credential

is valid only for a certain time period as determined by the remote host **305** (e.g., financial institution) issuing the credential.

[0048] FIG. **4** shows a memory binding authentication flow **400**, according to an embodiment. In one embodiment, the remote host **305** first authenticates the binding of the credential of the memory device of the secure memory module **140** before accepting the credential from the end user. This ensures that the source of the credential is a valid device containing the authenticated memory (embedded or removable). In one embodiment, the credential is generated at **410** using a PRF, such as AES. In one embodiment, the media ID MAC is generated at **420** (e.g., CMAC (EMID, Credentials).

[0049] In one embodiment, when the end user wants to initiate a financial transaction, the local Host device (electronic device **120**) creates a digital certificate (e.g., a User Credit Card certificate) by reading the User credential and Media ID MAC from the memory device of the secure memory module **140** and signs it using its private key at **340**. If the user credential is expired then it asks the remote host **305** (e.g., financial institution) to create a new user credential and store it in the memory device of the secure memory module **140**. In one embodiment, if the media ID MAC that is read from the secure memory module **140** does not match the known media ID MAC known by the remote host **305**, the payment transaction process is aborted. Otherwise, in one embodiment, the UserID is found to be bound to the secure media at **430** and the transaction is processed at **440**.

[0050] FIG. **5** shows an example flow **600** for a mobile transaction with a cloud computing environment for mobile payment using an electronic device **120**, according to an embodiment. In one embodiment, the flow **600** starts with a request for a new account from the electronic device **120** to the remote host **305**. In one embodiment, a user first requests a credit card at the website of a financial institution (e.g., the remote host **305**) by presenting his/her user name and password along with other information. In one embodiment, the financial institution then generates a unique UserID by performing a selected cryptographic operation (e.g., a PRF, such as AES) on the user access information. In one embodiment, the secure memory module **140** includes a memory controller **620** and a memory device **630** including an EMID decoder.

[0051] In one embodiment, the remote host **305** establishes a secure channel to the memory device of the secure memory module **140** through the electronic device **120** and installs the encrypted credential in the assigned protected area of the memory device of the secure memory module **140**, along with the expiry time **330** (FIG. **3**) of the credential. In one embodiment, the remote host **305** also generates the memory ID MAC **340** and stores it in the memory device of the secure memory module **140**. It should be noted that the request for a new account and the generation and storing of the credential and memory ID MAC are needed only when either the user first establishes an account with the financial institution or when the User credential expires.

[0052] In one embodiment, an end user using the electronic device **120** goes to a POS (Point Of Sale) device (e.g., NFC device **610**) and selects a credit card from his eWallet application (e.g., application **130**, FIG. **2**). In one embodiment, the user is prompted on the display **121** to enter his/her username and password. In one embodiment, the electronic device **120** reads and decrypts the stored credentials in the protected area of the secure memory module **140**. In one embodiment, the electronic device **120** generates a digital certificate (e.g., a user credit card certificate) by using the credential and then presents it to a merchant over the NFC interface **129**.

[0053] In one embodiment, a merchant uses the financial institution network to present the user digital certificate (e.g., credit card certificate) to the financial institution. In one embodiment, the remote host application of the remote host **305** (e.g., the financial institution) first authenticates the memory device of the secure memory module **140** and then authenticates the credential in order to authorize the user. In one embodiment, the remote host **305** (i.e., the financial institution) completes the requested transaction after performing the authorizations in order to determine that the request is issued from an authorized user using a certified device.

[0054] In one embodiment, the hosting of the application **130** and the stored encrypted credentials are provided by the remote hosts for one or more credit cards, where credit card issuers (e.g., financial institutions) provide the processing for their respective credentials. In one embodiment, the computing environment **160** is private and only hosted by a numbers of banks and financial institutions.

[0055] FIG. **6** shows a flow diagram **700** for mobile payment using an electronic device **120**, according to an embodiment. In one embodiment, the flow diagram **700** includes the flow interactions for the secure memory module **140**, the electronic device **120**, the user, the NFC device **610** (e.g., POS device), credit or bank card **701**, remote host **305** and the application **130** executing on the electronic device **130**. In one embodiment, at flow **705** the user uses the electronic device **120** to request for a credential from a particular credit card entity **701** at the remote host **305**. At flow **710**, the remote host **305** uses a secure channel over a network in order to access the secure storage module **140** for assignment of the secure storage area of the secure memory module **140**.

[0056] In one embodiment, in flow **715** the remote host **305** installs the credential, media ID MAC **340** and expiry time element **330** in the secure memory module **140**. In one embodiment, in flow **720**, upon a user requesting a financial transaction using the application **130**, the user is locally authenticated based on the user access information (e.g., username and password) and EMID technology authentication of the media of the secure memory module **140** (flow **725**). In flow **730**, the credential is read from the secure memory module **140** by the electronic device **120** using the application **130**, and NFC authentication occurs in flow **735**.

[0057] In one embodiment, in flow **740**, mutual authentication by the remote host **305** occurs. In flow **745**, the digital certificate generated (e.g., credit card certificate) and a purchase token are forwarded to the remote host **305**. In one embodiment, upon processing by the remote host **305**, in flow **750** the purchase is approved to proceed.

[0058] FIG. **7** shows an architecture implementation **800** for mobile payment using an electronic device **120**, according to an embodiment. In one embodiment, the implementation **800** includes a remote host **305** that may be anyone of multiple credit card financial institutions, banks, etc, an EMID issuer **810** and the electronic device **120** including the secure memory module **140** (either removable or embedded). In one embodiment, the electronic device **120** executes the application **130** that communicates with a trusted execution environment (TEE) API **850** and trusted operating system (OS) **860** implementation.

[0059] In one embodiment, the EMID issuer **810** forwards the application specific secret value (ASSV) **820** to the mobile financial application that interacts in the cloud **840**

with the secure elements **830** managed (i.e., created, revoked) by the EMID issuer. In one embodiment, the EMID issuer included the memory unique secret (MUS) at the time of manufacturing the memory device **630** in the secure memory module **140**. In one embodiment, the mobile application **130** on the electronic device **120** is developed and deployed by device manufacturers, such as Samsung®. In other embodiments, all the stakeholders (involved in the payment processing) may jointly develop requirements and standard protocols.

[0060] In one embodiment, device manufacturers may develop mobile wallet technologies based on the specifics of their devices (e.g., using a mobile trusted module (MTM)/trusted platform module (TPM), Trustzone or any other relevant technology). In one embodiment, financial institutions may develop their own technologies on the cloud side that may function properly in a mobile wallet ecosystem by following standards.

[0061] In one embodiment, the mobile application **130** in the electronic device **120** has a counterpart in the private computing environment **160** of financial institutions. In one embodiment, the mobile application **130** in the electronic device **120** maintains an e-wallet table or list of the credit cards owned by the user.

[0062] In one embodiment, Trusted Computing (TC) based technologies are used to authenticate and authorize the mobile application **130** in the electronic device **120**. In one embodiment, TC-based technology (e.g., presence of trusted platform module (TPM)/mobile trusted module (MTM) chip in the electronic device **120**) may be used for secure communication and processing.

[0063] FIG. **8** shows a flow diagram showing a process **900** for mobile payment nsing the electronic device **120**, according to an embodiment. In one embodiment, in block **910**, a financial institution (e.g., remote host **305**, FIG. **3**), generates a unique credential based on user access information (e.g., username and password) and media binding information (e.g., EMID information) that is cryptographically bound to media using a unique media identification. In one embodiment, in block **920**, the financial institution stores the credential and media binding identification in the form of authentication code in a memory (e.g., secure memory module **140**, FIG. **2**) used by an electronic device **120**.

[0064] In one embodiment, a mobile wallet application (e.g., mobile application **130**, FIG. **1**) is launched at a merchant POS machine/system, where a user selects a particular credit card of available credit cards (e.g., e-wallet table or list) to use for a purchase/payment. In one embodiment, the user launches the mobile wallet application manually by, for example, tapping on a touch screen (e.g., display **121**). In one embodiment, in block **930** the stored credential and media binding information is accessed using the user access information for a payment transaction. In one embodiment, in block **940**, a digital certificate (e.g., credit card certificate) is generated using the credential and the media binding information. In one embodiment, in block **950** the digital certificate is presented to the financial institution for the payment transaction (e.g., from an NFC POS device). In one embodiment, in block **960** the memory is authenticated and the binding of the credential is verified by the financial institution (e.g., the remote host **305**) prior to completing the payment transaction.

[0065] In one embodiment, the mobile device may use one or a combination of the following: (1) TrustZone to provide secure storage and domain to run the mobile wallet application (e.g., mobile application **130**) and store the digital credit card information; (2) TC primitives to ensure the integrity of the software (s/w) stack that runs the mobile wallet application and to provide secured (e.g., sealed or separated) storage for digital credit cards; or (3) a similar technology to provide isolated and integrity-protected execution environment for the mobile wallet application execution and secure storage for digital credit cards.

[0066] FIG. **9** is a high-level block diagram showing an information processing system comprising a computing system **500** implementing an embodiment. The system **500** includes one or more processors **511** (e.g., ASIC, CPU, etc.), and can further include an electronic display device **512** (for displaying graphics, text, and other data), a main memory **513** (e.g., random access memory (RAM)), storage device **514** (e.g., hard disk drive), removable storage device **515** (e.g., removable storage drive, removable memory module, a magnetic tape drive, optical disk drive, computer-readable medium having stored therein computer software and/or data), user interface device **516** (e.g., keyboard, touch screen, keypad, pointing device), and a communication interface **517** (e.g., modem, wireless transceiver (such as Wi-Fi, Cellular), a network interface (such as an Ethernet card), a communications port, or a PCMCIA slot and card). The communication interface **517** allows software and data to be transferred between the computer system and external devices. The system **500** further includes a communications infrastructure **518** (e.g., a communications bus, cross-over bar, or network) to which the aforementioned devices/modules **511** through **517** are connected.

[0067] The information transferred via communications interface **517** may be in the form of signals such as electronic, electromagnetic, optical, or other signals capable of being received by communications interface **517**, via a communication link that carries signals to/from a plurality of sinks/sources, such as, the Internet **550**, a mobile electronic device **551**, a server **552**, or a network **553**, and may be implemented using wire or cable, fiber optics, a phone line, a cellular phone link, an radio frequency (RF) link, and/or other communication channels.

[0068] In one implementation, in a mobile wireless device such as a mobile phone, the system **500** further includes an image capture device such as a camera **520**. The system **500** may further include application modules as MMS module **521**, SMS module **522**, email module **523**, social network interface (SNI) module **524**, audio/video (AV) player **525**, web browser **526**, image capture module **527**, etc.

[0069] The system **500** further includes a mobile payment processing module **530** as described herein, according to an embodiment. In one implementation of mobile payment processing module **530** along with an operating system **529** may be implemented as executable code residing in a memory of the system **500**. In another embodiment, such modules are in firmware, etc.

[0070] One or more embodiments leverage EMID technology to bind a financial credential to the identity of the user at the corresponding financial organization and the device that is being used to access the financial service. In one or more embodiments, the credential management in the device occurs from the cloud computing environment using EMID technology without the direct involvement of the user.

[0071] One or more embodiments provide for simplified security mechanisms that allow the revocation of credentials

by a remote host when a device is lost using EMID to bind financial credential to a certain device and user. In one or more embodiments, the use of cloud based technology allows the temporary storage of secure element (credential) in the device memory/removable memory or the cloud host. In one or more embodiments, the financial institution may update the credential and reinstall the credential if the device is lost or stolen. In one or more embodiments, the cloud host acts as an escrow that may update the credential immediately in case the device is lost or stolen. One or more embodiments provide for the periodic update of the credential by associating an expiry time associated with it to further improve the security.

[0072] In one or more embodiments, the use of cloud based approach is used to move secure storage elements (credentials) between the device and the cloud. In one or more embodiments, the credential stored in a stolen device cannot be decrypted correctly without the knowledge of username and password of the rightful owner of the credential.

[0073] As is known to those skilled in the art, the aforementioned example architectures described above, according to said architectures, can be implemented in many ways, such as program instructions for execution by a processor, as software modules, microcode, as computer program product on computer readable media, as analog/logic circuits, as application specific integrated circuits, as firmware, as consumer electronic devices, AV devices, wireless/wired transmitters, wireless/wired receivers, networks, multi-media devices, etc. Further, embodiments of said Architecture can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements.

[0074] Embodiments have been described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to one or more embodiments. Each block of such illustrations/diagrams, or combinations thereof, can be implemented by computer program instructions. The computer program instructions when provided to a processor produce a machine, such that the instructions, which execute via the processor create means for implementing the functions/operations specified in the flowchart and/or block diagram. Each block in the flowchart/block diagrams may represent a hardware and/or software module or logic, implementing one or more embodiments. In alternative implementations, the functions noted in the blocks may occur out of the order noted in the figures, concurrently, etc.

[0075] The terms "computer program medium," "computer usable medium," "computer readable medium", and "computer program product," are used to generally refer to media such as main memory, secondary memory, removable storage drive, a hard disk installed in hard disk drive. These computer program products are means for providing software to the computer system. The computer readable medium allows the computer system to read data, instructions, messages or message packets, and other computer readable information from the computer readable medium. The computer readable medium, for example, may include non-volatile memory, such as a floppy disk, ROM, flash memory, disk drive memory, a CD-ROM, and other permanent storage. It is useful, for example, for transporting information, such as data and computer instructions, between computer systems. Computer program instructions may be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0076] Computer program instructions representing the block diagram and/or flowcharts herein may be loaded onto a computer, programmable data processing apparatus, or processing devices to cause a series of operations performed thereon to produce a computer implemented process. Computer programs (i.e., computer control logic) are stored in main memory and/or secondary memory. Computer programs may also be received via a communications interface. Such computer programs, when executed, enable the computer system to perform the features of one or more embodiments as discussed herein. In particular, the computer programs, when executed, enable the processor and/or multi-core processor to perform the features of the computer system. Such computer programs represent controllers of the computer system. A computer program product comprises a tangible storage medium readable by a computer system and storing instructions for execution by the computer system for performing a method of one or more embodiments.

[0077] Though the embodiments have been described with reference to certain versions thereof; however, other versions are possible. Therefore, the spirit and scope of the appended claims should not be limited to the description of the preferred versions contained herein.

What is claimed is:

1. A method for mobile payment, comprising:

generating, by a financial institution, a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification;

storing, by the financial institution, the credential and media binding information in the form of authentication code in a memory used by an electronic device;

accessing the stored credential and media binding information using the user access information for a payment transaction;

generating a digital certificate using the credential and the media binding information;

presenting the digital certificate to the financial institution for the payment transaction; and

authenticating the memory and verifying binding of the credential to the memory prior to completing the payment transaction.

2. The method of claim **1**, wherein the credential is stored in an assigned protected area of the memory by the financial institution.

3. The method of claim **2**, further comprising:

selecting a payment method for the payment transaction by using an application to select a credit card from a stored list of one or more credit cards.

4. The method of claim **2**, wherein a separate credential is associated with a financial institution for each credit card available for selection, and each separate credential is stored in a unique assigned protected area of the memory.

5. The method of claim **1**, further comprising storing expiration information in the memory for limiting access time of the credential and for updating the credential periodically by the financial institution.

6. The method of claim **2**, wherein the financial institution comprises a local or remote host.

7. The method of claim 6, wherein presenting the digital certificate to the financial institution for the payment transaction comprises sending the digital certificate for payment processing from the electronic device to a payment method reader, wherein the payment method reader comprises a near field communication (NFC) reader, and the digital certificate is passed over an NFC interface of the electronic device to the NFC reader.

8. The method of claim 1, wherein the user access information comprises a username and password.

9. The method of claim 8, wherein the media information comprises an enhanced media identification (EMID) generated based on a unique code embedded in the memory at a time of manufacturing the memory, and the credential is reinstalled by the financial institution when the electronic device is lost or stolen.

10. The method of claim 8, wherein the financial institution generates an authorization key based on the username, password and enhanced media identification (EMID), and stores the authentication key on the memory.

11. The method of claim 9, wherein the electronic device uses the authentication key to decrypt the credential.

12. The method of claim 1, wherein the memory is one of a memory device embedded in the electronic device or a removable memory device.

13. The method of claim 1, wherein the electronic device comprises a mobile device.

14. A system for mobile payment, comprising:

a server that generates a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification, and stores the credential and media binding information in the form of authentication code in a memory used by an electronic device through a secure channel;

an electronic device that accesses the stored credential and media binding information from the memory using the user access information for a payment transaction, and generates a digital certificate using the credential and the media binding information; and

a near field communication (NFC) interface that passes the digital certificate to the server for the payment transaction,

wherein the server authenticates the memory and verifies binding of the credential to the memory prior to completing the payment transaction.

15. The system of claim 14, wherein a payment method is selected by the electronic device, wherein the payment method comprises selecting a digital credit card, and the NFC interface passes the digital certificate to an NFC reader for a point-of-service (POS) system for requesting payment using a selected credit card from a list of stored digital credit cards stored in the memory.

16. The system of claim 14, wherein the server comprises a local or remote financial entity server.

17. The system of claim 16, wherein the financial entity server stores the credential in an assigned protected area of the memory.

18. The system of claim 14, wherein the financial entity server stores expiration information in the memory for limiting access time of the credential and for updating the credential periodically.

19. The system of claim 14, wherein the user access information comprises a username and password.

20. The system of claim 19, wherein the media information comprises an enhanced media identification (EMID) generated by the server based on a unique code embedded in the memory at a time of manufacturing the memory.

21. The system of claim 20, wherein the server generates an authorization key based on the username, password and EMID, and stores the authentication key on the memory.

22. The system of claim 21, wherein the electronic device uses the authentication key to decrypt the credential, and the memory is one of a memory device embedded in the electronic device or a removable memory device.

23. The system of claim 14, wherein the electronic device comprises a mobile device.

24. A server for mobile payment, comprising:

a credential service that uses a processor to generate a unique credential based on user access information and media binding information that is cryptographically bound to media using a unique media identification, and stores the credential and media binding information in the form of authentication code in a memory used by an electronic device through a secure channel; and

an authorization service that authenticates the memory and verifies binding of the credential to the memory prior to completing a requested payment transaction based on a digital certificate generated by the electronic device using the credential and media binding information.

25. The server of claim 24, wherein the server comprises a remote or local financial entity server.

26. The server of claim 25, wherein the credential service stores the credential in an assigned protected area of the memory, and the memory is one of a memory device embedded in the electronic device or a removable memory device.

27. The server of claim 24, wherein the credential service stores expiration information in the memory for limiting access time of the credential and for updating the credential periodically.

28. The server of claim 24, wherein the user access information comprises a username and password.

29. The server of claim 28, wherein the media information comprises an enhanced media identification (EMID) generated by the credential service based on a unique code embedded in the memory at a time of manufacturing the memory, wherein the credential service generates an authorization key based on the username, password and EMID, and stores the authentication key on the memory, and the electronic device uses the authentication key to decrypt the credential.

30. The server of claim 24, wherein the electronic device comprises a mobile device.

* * * * *

(12) **United States Patent**
Grecia

(10) **Patent No.: US 8,887,308 B2**
(45) **Date of Patent: *Nov. 11, 2014**

(54) **DIGITAL CLOUD ACCESS (PDMAS PART III)**

(71) Applicant: **William Grecia**, Downingtown, PA (US)

(72) Inventor: **William Grecia**, Downingtown, PA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 75 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/888,051**

(22) Filed: **May 6, 2013**

(65) **Prior Publication Data**

US 2014/0304778 A1 Oct. 9, 2014

Related U.S. Application Data

(63) Continuation of application No. 13/740,086, filed on Jan. 11, 2013, now Pat. No. 8,533,860, which is a continuation of application No. 13/397,517, filed on Feb. 15, 2012, now Pat. No. 8,402,555, which is a continuation of application No. 12/985,351, filed on Jan. 6, 2011, now abandoned, which is a continuation of application No. 12/728,218, filed on Mar. 21, 2010, now abandoned.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/10*** (2013.01)
USPC **726/29**; 726/28; 713/185

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,254,235	B2	8/2007	Boudreault et al.	
7,343,014	B2	3/2008	Sovio et al.	
7,526,650	B1 *	4/2009	Wimmer	713/176
2005/0065891	A1	3/2005	Lee et al.	
2008/0010685	A1	1/2008	Holtzman et al.	
2009/0083541	A1	3/2009	Levine	
2010/0100899	A1	4/2010	Bradbury et al.	
2011/0288946	A1 *	11/2011	Baiya et al.	705/26.1

OTHER PUBLICATIONS

U.S. Appl. No. 13/397,517 Notice of Allowance.
U.S. Appl. No. 13/740,086 Notice of Allowance.

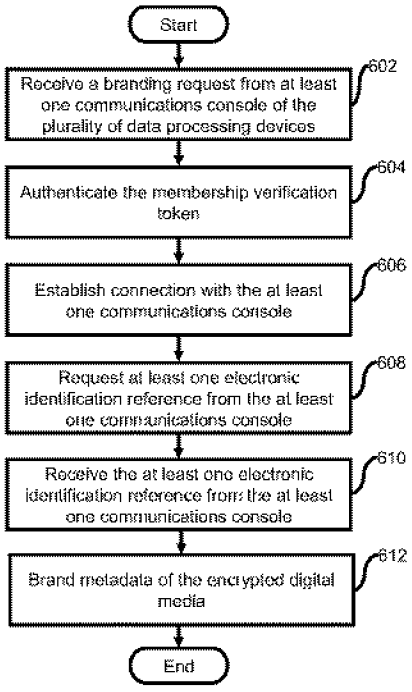
* cited by examiner

Primary Examiner — Jung Kim
Assistant Examiner — Tri Tran

(57) **ABSTRACT**

The invention is an apparatus that facilitates access to a data source to accept verification and authentication from an enabler using at least one token and at least one reference. The at least one reference could be a device serial number, a networking MAC address, or a membership ID reference from a web service. Access to the data source is also managed with a plurality of secondary enablers.

1 Claim, 7 Drawing Sheets



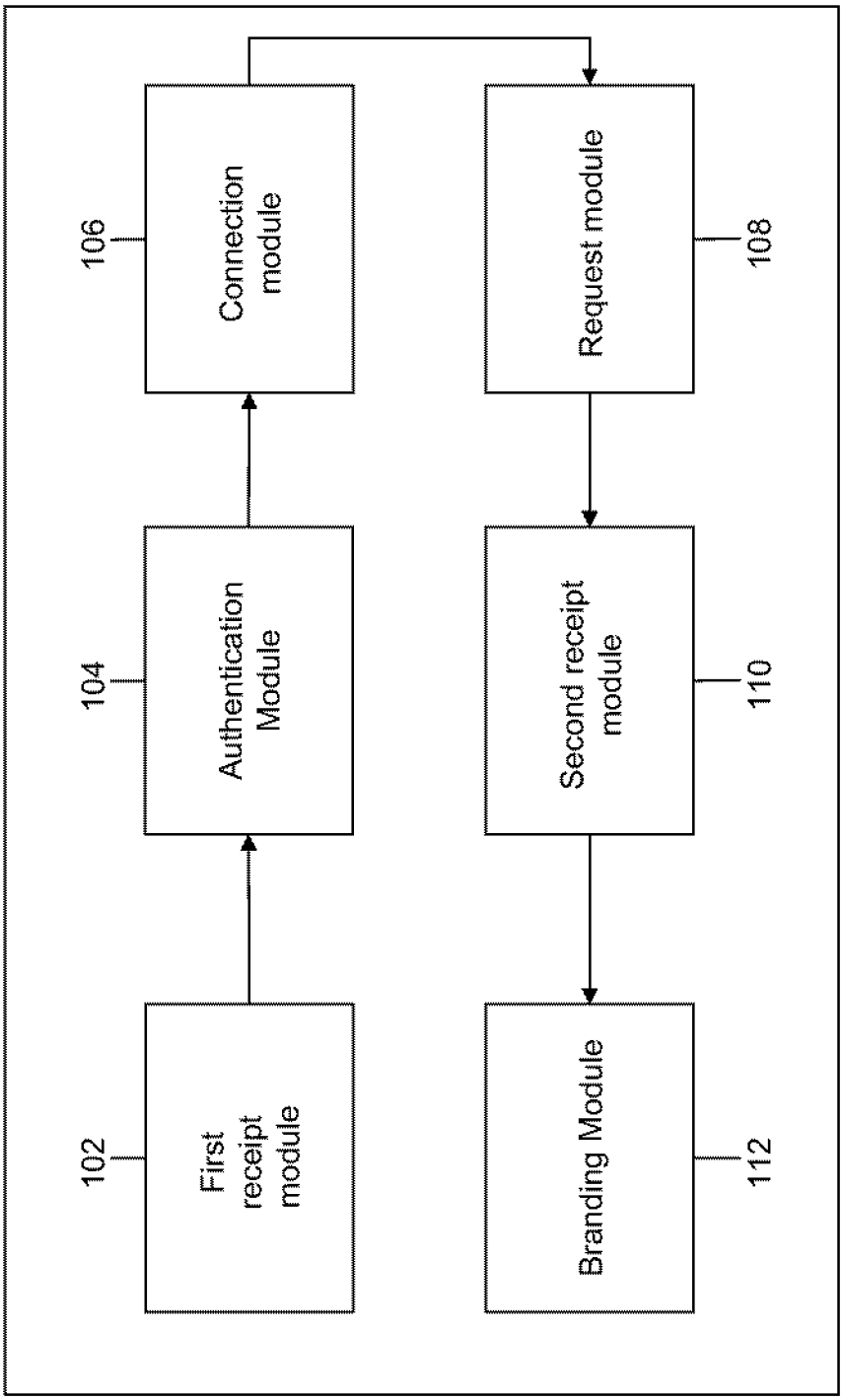

First receipt module
102
Authentication Module
104
Connection module
106
Request module
108
Second receipt module
110
Branding Module
112

FIG.1

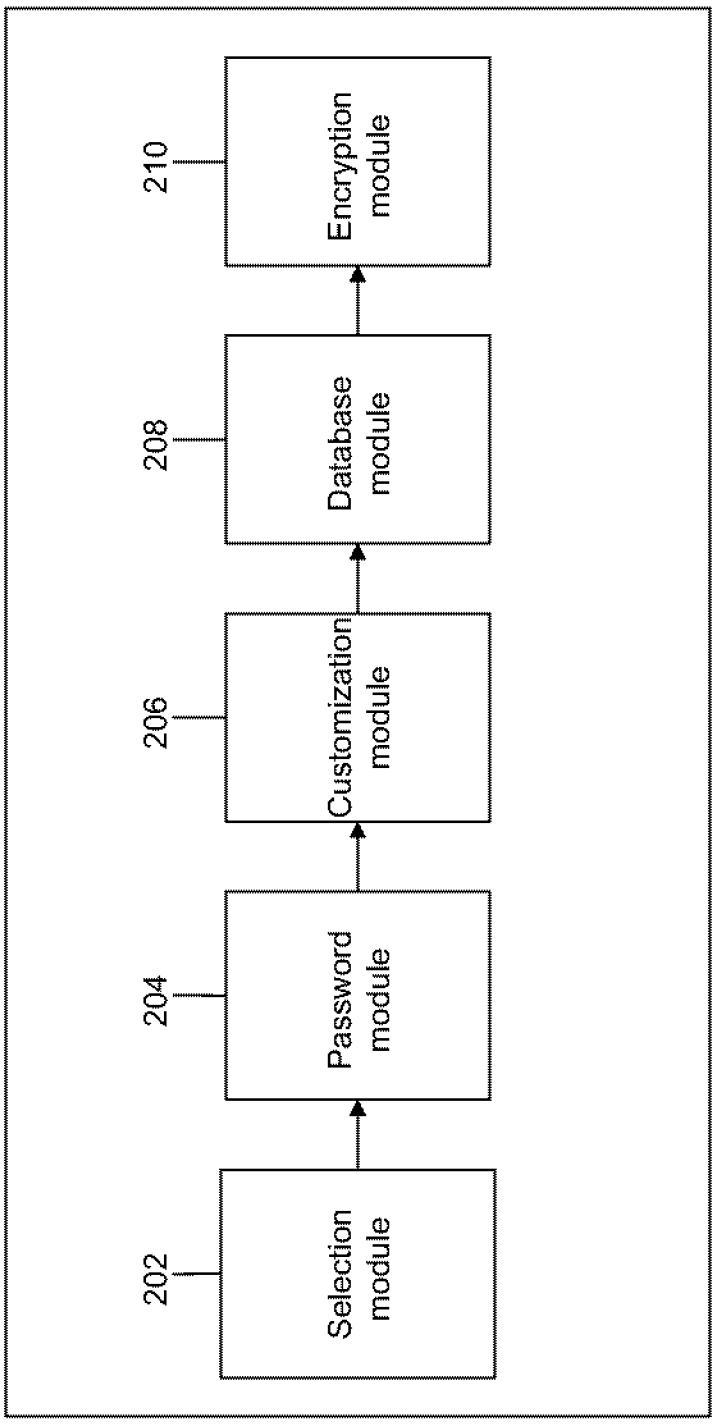

202
Selection module
204
Password module
206
Customization module
208
Database module
210
Encryption module

FIG.2

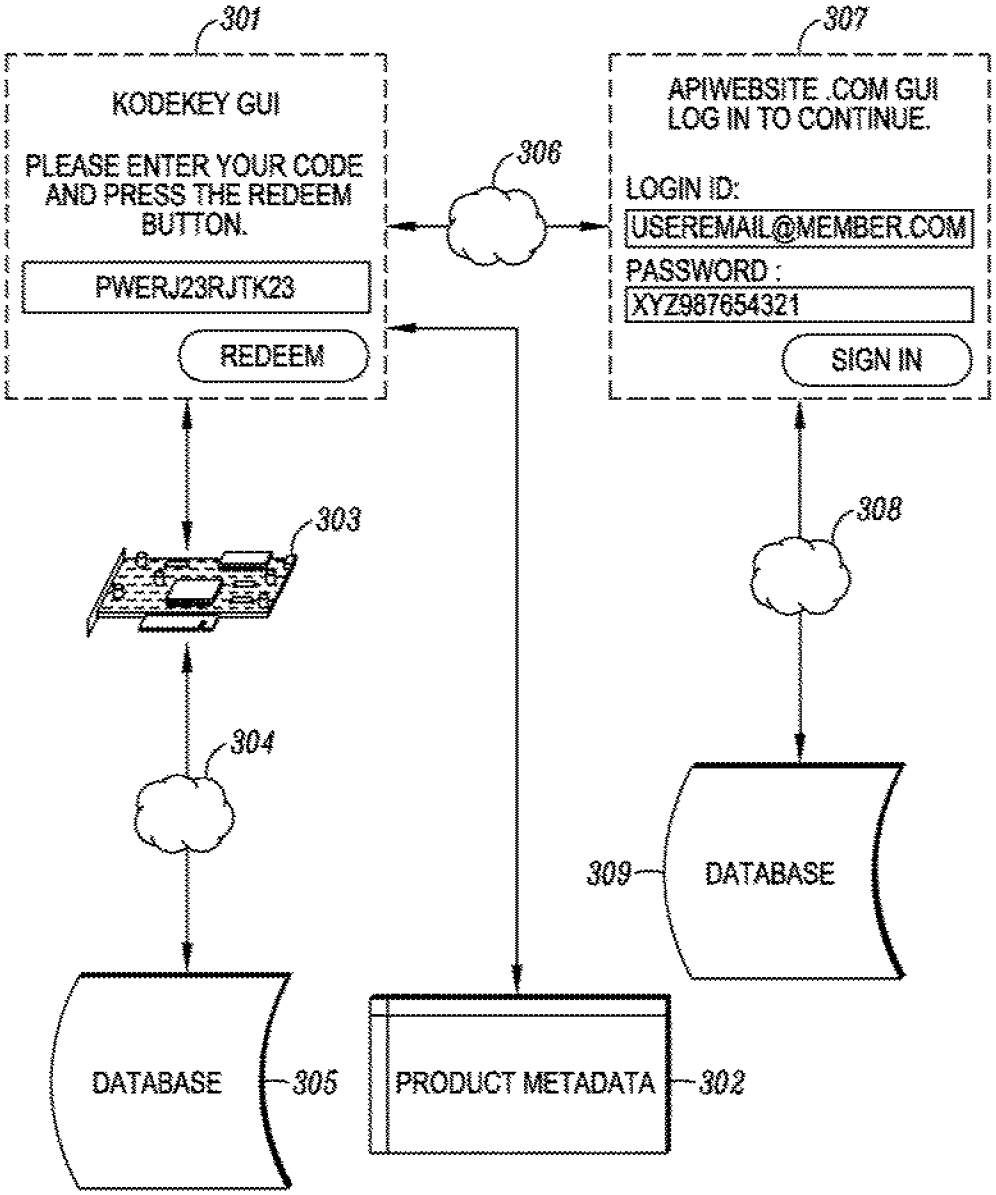

301
KODEKEY GUI
PLEASE ENTER YOUR CODE AND PRESS THE REDEEM BUTTON.
PWERJ23RJTK23
REDEEM
306
307
APIWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
SIGN IN
303
308
304
309
DATABASE
DATABASE
305
PRODUCT METADATA
302

FIG. 3

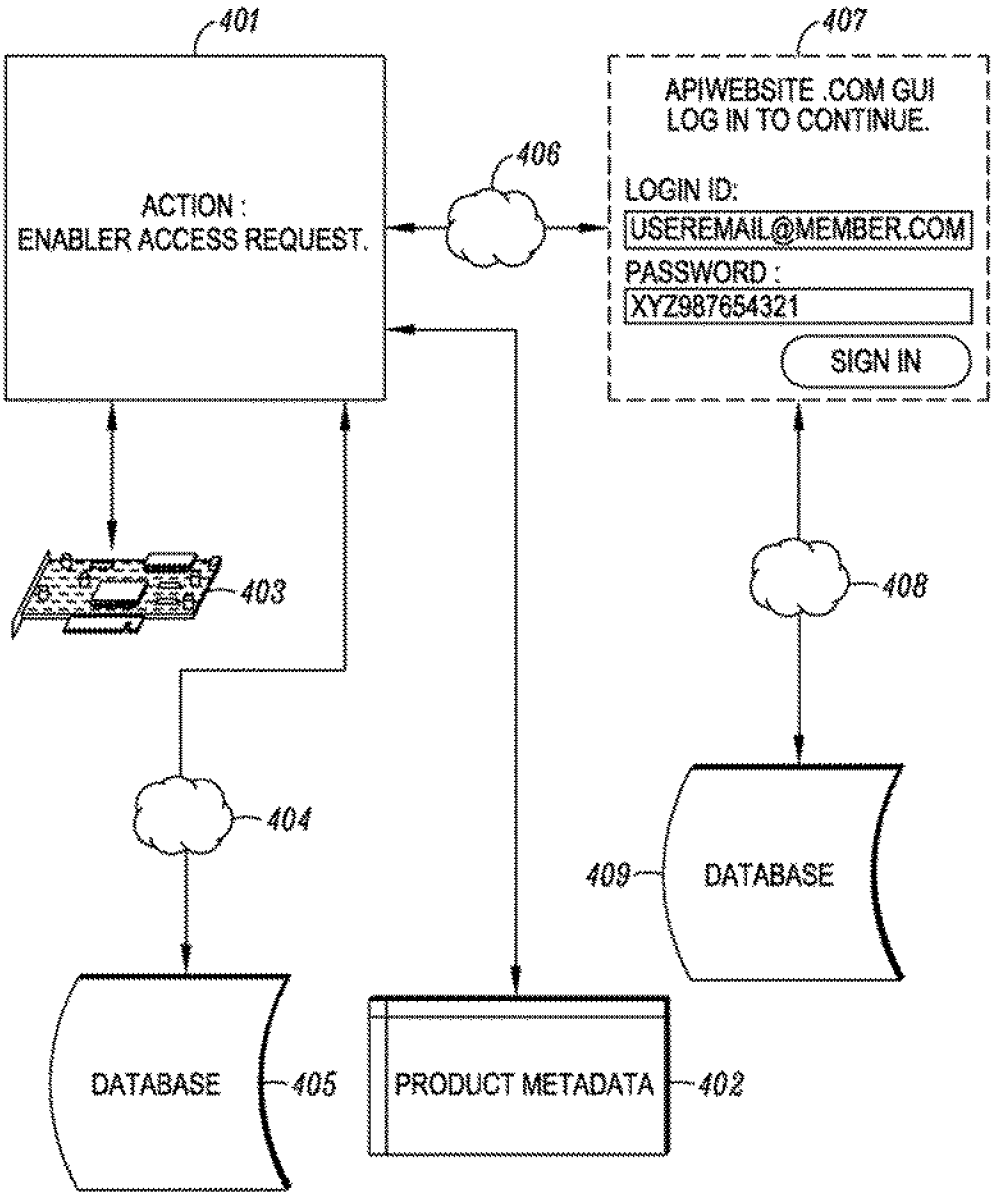

401
ACTION :
ENABLER ACCESS REQUEST.
406
407
APIWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
SIGN IN
403
408
404
409
DATABASE
DATABASE
405
PRODUCT METADATA
402

FIG. 4

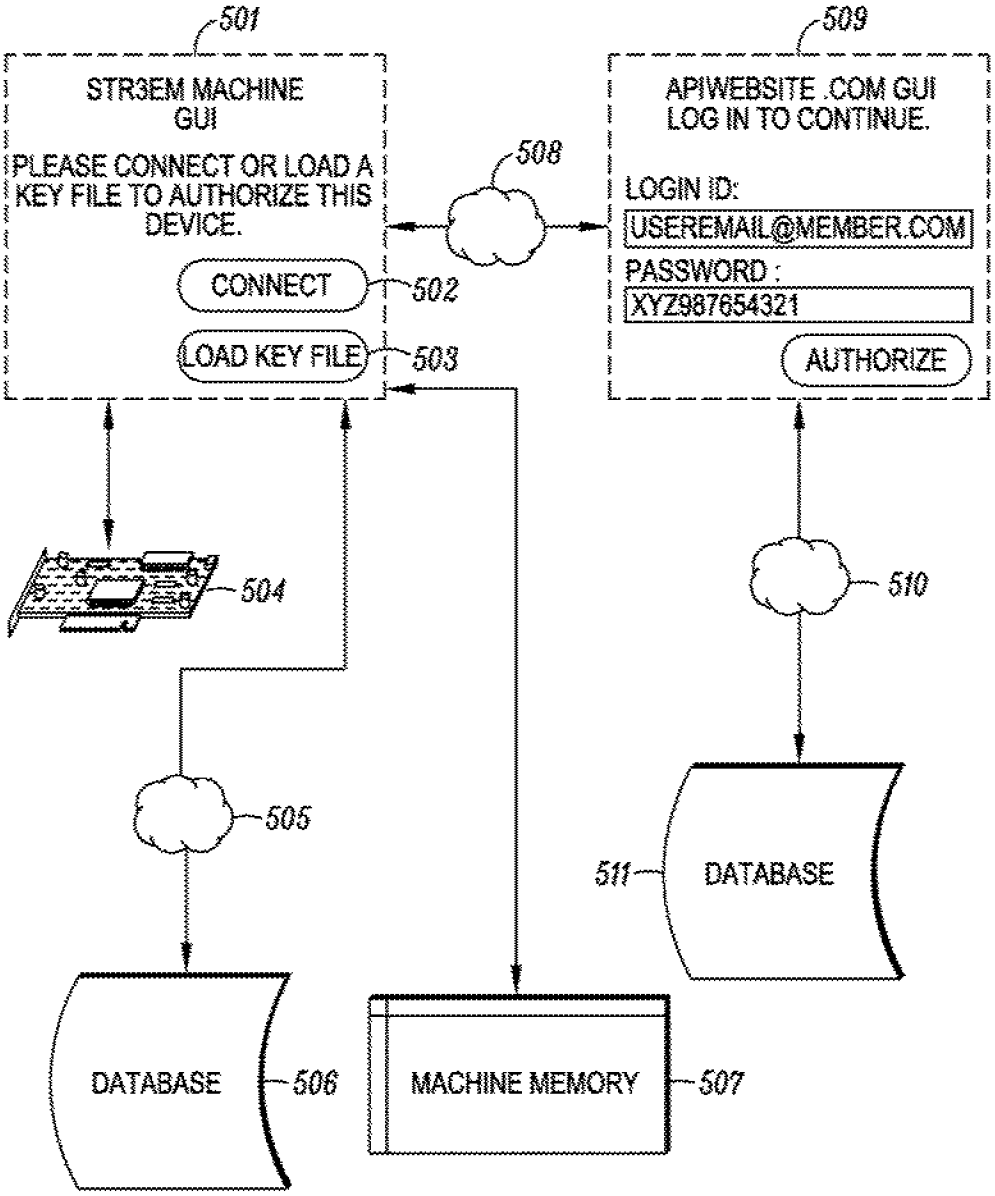

501
STR3EM MACHINE GUI
PLEASE CONNECT OR LOAD A KEY FILE TO AUTHORIZE THIS DEVICE.
CONNECT
502
LOAD KEY FILE
503
508
509
API.WEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
AUTHORIZE
504
505
510
511
DATABASE
DATABASE
506
MACHINE MEMORY
507

FIG. 5

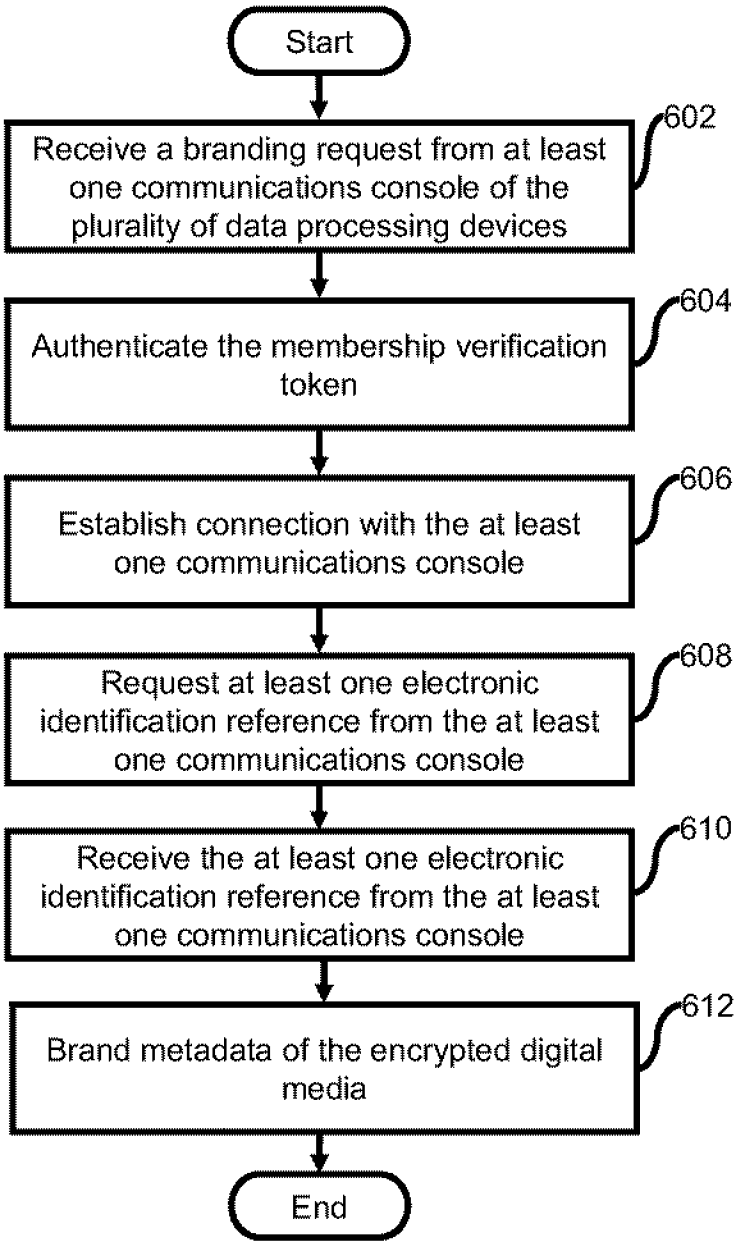

Start
Receive a branding request from at least one communications console of the plurality of data processing devices
602
Authenticate the membership verification token
604
Establish connection with the at least one communications console
606
Request at least one electronic identification reference from the at least one communications console
608
Receive the at least one electronic identification reference from the at least one communications console
610
Brand metadata of the encrypted digital media
612
End

FIG.6

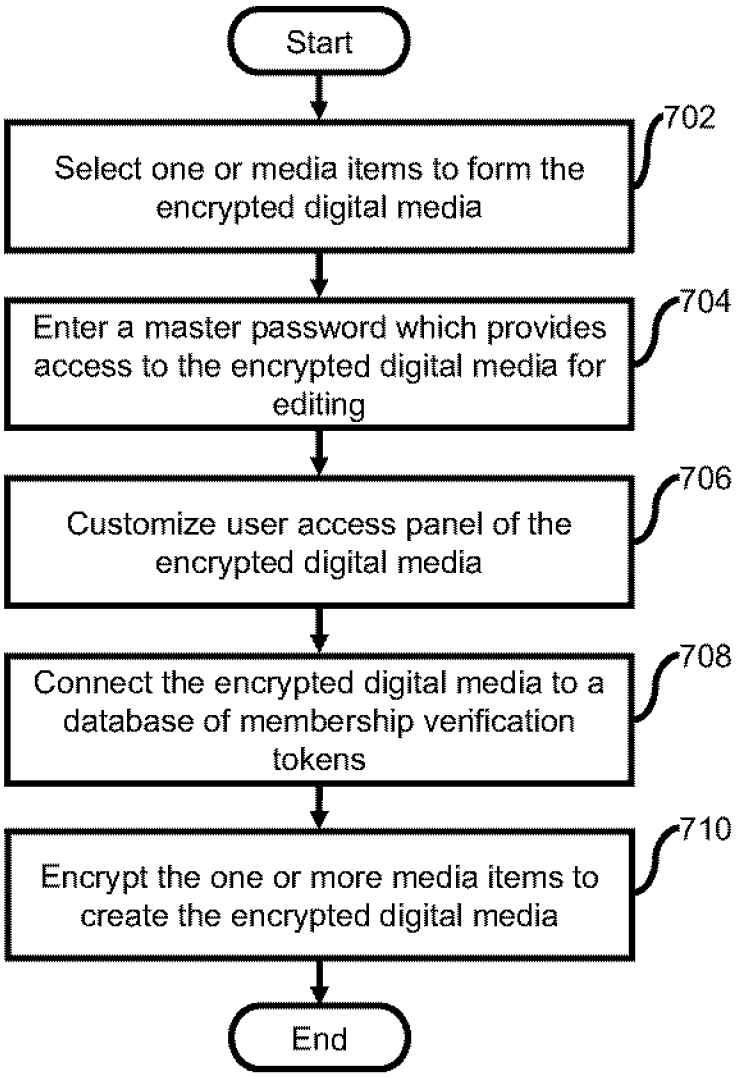

Start
Select one or media items to form the encrypted digital media
702
Enter a master password which provides access to the encrypted digital media for editing
704
Customize user access panel of the encrypted digital media
706
Connect the encrypted digital media to a database of membership verification tokens
708
Encrypt the one or more media items to create the encrypted digital media
710
End

FIG.7

DIGITAL CLOUD ACCESS (PDMAS PART III)

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of and claims the priority benefit of U.S. patent application Ser. No. 13/740,086 filed Jan. 11, 2013 which is a continuation of and claims the priority benefit of Ser. No. 13/397,517 filed Feb. 15, 2012 now issued as U.S. Pat. No. 8,402,555 on Mar. 19, 2013 which is a continuation of and claimed the priority benefit of Ser. No. 12/985,351 filed Jan. 6, 2011 which was a continuation of and claimed the priority benefit of U.S. patent application Ser. No. 12/728,218 filed Mar. 21, 2010, which are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of digital rights management schemes used by creators of electronic products to protect commercial intellectual property copyrights privy to illegal copying using computerized devices. More specifically, the present invention teaches a more personal system of digital rights management which employs electronic ID, as part of a web service membership, to manage access rights across a plurality of devices.

2. Description of the Prior Art

Digital rights management (DRM) is a generic term for access control technologies used by hardware manufactnrers, publishers, copyright holders and individuals to impose limitations on the usage of digital content across devices. DRM refers to any technology that inhibits undesirable or illegal uses of the digital content. The term generally doesn't refer to forms of copy protection that can be circumvented without modifying the file or device, such as serial numbers or key files. It can also refer to restrictions associated with specific instances of digital works or devices.

Traditional DRM schemes are defined as authentication components added to digital files that have been encrypted from public access. Encryption schemes are not DRM methods but DRM systems are implemented to use an additional layer of authentication in which permission is granted for access to the cipher key required to decrypt files for access. A computer server is established to host decryption keys and to accept authentication keys from Internet connected client computers running client software in which handles the encrypted files. The server can administer different authorization keys back to the client computer that can grant different sets of rules and a time frame granted before the client is required to connect with the server to reauthorize access permissions. In some cases content can terminate access after a set amount of time, or the process can break if the provider of the DRM server ever ceases to offer services.

In the present scenario, consumer entertainment industries are in the transition of delivering products on physical media such as CD and DVD to Internet delivered systems. The Compact Disc, introduced to the public in 1982, was initially designed as a proprietary system offering strict media to player compatibility. As the popularity of home computers and CD-ROM drives rose, so did the availability of CD ripping applications to make local copies of music to be enjoyed without the use of the disc. After a while, users found ways to share digital versions of music in the form of MP3 files that could be easily shared with family and friends over the Internet. The DVD format introduced in 1997 included a new apparatus for optical discs technology with embedded copy protection schemes also recognized as an early form of DRM. With internet delivered music and video files, DRM schemes has been developed to lock acquired media to specific machines and most times limiting playback rights to a single machine or among a limited number of multiple machines regardless of the model number. This was achieved by writing the machine device ID to the metadata of the media file, then cross referencing with a trusted clearinghouse according to pre-set rules. DRM systems employed by DVD and CD technologies consisted of scrambling (also known as encryption) disc sectors in a pattern to which hardware developed to unscramble (also known as decryption) the disc sectors are required for playback. DRM systems built into operating systems such as Microsoft Windows Vista block viewing of media when an unsigned software application is running to prevent unauthorized copying of a media asset during playback. DRM used in computer games such as SecuROM and Steam are used to limit the amount of times a user can install a game on a machine. DRM schemes for e-books include embedding credit card information and other personal information inside the metadata area of a delivered file format and restricting the compatibility of the file with a limited number of reader devices and computer applications.

In a typical DRM system, a product is encrypted using Symmetric block ciphers such as DES and AES to provide high levels of security. Ciphers known as asymmetric or public key/private key systems are used to manage access to encrypted products. In asymmetric systems the key used to encrypt a product is not the same as that used to decrypt it. If a product has been encrypted using one key of a pair it cannot be decrypted even by someone else who has that key. Only the matching key of the pair can be used for decryption. After receiving an authorization token from a first-use action are usually triggers to decrypt block ciphers in most DRM systems. User rights and restrictions are established during this first-use action with the corresponding hosting device of a DRM protected product.

Examples of such prior DRM art include Hurtado (U.S. Pat. No. 6,611,812) who described a digital rights management system, where upon request to access digital content, encryption and decryption keys are exchanged and managed via an authenticity clearing house. Other examples include Alve (U.S. Pat. No. 7,568,111) who teaches a DRM and Tuoriniemi (U.S. Pat. No. 20090164776) who described a management scheme to control access to electronic content by recording use across a plurality of trustworthy devices that has been granted permission to work within the scheme.

Recently, DRM schemes have proven unpopular with consumers and rights organizations that oppose the complications with compatibility across machines manufactured by different companies. Reasons given to DRM opposition range from limited device playback restrictions to the loss of fair-use which defines the freedom to share media products will family members.

Prior art DRM methods rely on content providers to maintain computer servers to receive and send session authorization keys to client computers with an Internet connection. Usually rights are given from the server for an amount of time or amount of access actions before a requirement to reconnect with the server is required for reauthorization. At times, content providers will discontinue servers or even go out of business some years after DRM encrypted content was sold to consumers causing the ability to access files to terminate.

In the light of the foregoing discussion, the current states of DRM measures are not satisfactory because unavoidable issues can arise such as hardware failure or property theft that could lead to a paying customer loosing the right to recover

purchased products. The current metadata writable DRM measures do not offer a way to provide unlimited interoperability between different machines. Therefore, a solution is needed to give consumers the unlimited interoperability between devices and "fair use" sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term return of investments.

SUMMARY OF THE INVENTION

An object of the present invention is to provide unlimited interoperability of digital media between unlimited machines with management of end-user access to the digital media.

In accordance with an embodiment of the present invention, the invention is a process of an apparatus which in accordance with an embodiment, another apparatus, tangible computer medium, or associated methods (herein referred to as The App) is used to: handle at least one branding action which could include post read and write requests of at least one writable metadata as part of at least one digital media asset to identify and manage requests from at least one excelsior enabler, and can further identify and manage requests from a plurality of connected second enablers; with at least one token and at least one electronic identification reference received from the at least one excelsior enabler utilizing at least one membership. Here, controlled by the at least one excelsior enabler, The App will proceed to receive the at least one token to verify the authenticity of the branding action and further requests; then establish at least one connection with at least one programmable communications console of the at least one membership to request and receive the at least one electronic identification reference; and could request and receive other data information from the at least one membership. The method then involves sending and receiving variable data information from The App to the at least one membership to verify a preexisting the at least one branding action of the at least one writable metadata as part of the at least one digital media asset; or to establish permission or denial to execute the at least one branding action or the post read and write requests of the at least one writable metadata. To do this, controlled by the at least one excelsior enabler. The App may establish at least one connection, which is usually through the Internet, with a programmable communications console, which is usually a combination of an API protocol and graphic user interface (GUI) as part of a web service. In addition, the at least one excelsior enabler provides reestablished credentials to the programmable communications console as part of the at least one membership, in which The App is facilitating and monitoring, to authenticate the data communications session used to send and receive data requests between the at least one membership and The App.

In accordance with another embodiment of the present invention, the present invention teaches a method for monitoring access to an encrypted digital media and facilitating unlimited interoperability between a plurality of data processing devices. The method comprises receiving a branding request from at least one communications console of the plurality of data processing devices, the branding request being a read and write request of metadata of the encrypted digital media, the request comprising a membership verification token corresponding to the encrypted digital media. Subsequently, the membership verification token is authenticated, the authentication being performed in connection with a token database. Thereafter, connection with the at least one communications console is established. Afterwards, at least one electronic identification reference is requested from the at least one communications console. Further, the at least one electronic identification reference is received from the at least one communications console. Finally, branding metadata of the encrypted digital media is performed by writing the membership verification token and the electronic identification reference into the metadata.

The present invention is particularly useful for giving users the freedom to use products outside of the device in which the product was acquired and extend unlimited interoperability with other compatible devices.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, the needs satisfied thereby, and the objects, features, and advantages thereof, reference now is made to the following description taken in connection with the accompanying drawings.

FIG. **1** shows a system for monitoring access to an encrypted digital media according to an embodiment of the present invention.

FIG. **2** shows a system for authoring an encrypted digital media according to an embodiment of the present invention.

FIG. **3** shows a flow chart giving an overview of the process of digital media personalization according to an embodiment of the present invention.

FIG. **4** shows a flow chart giving an overview of the process of an access request made by an enabler according to an embodiment of the present invention.

FIG. **5** shows personalized digital rights management component as part of a compatible machine with writable static memory.

FIG. **6** shows a flowchart for monitoring access to an encrypted digital media according to an embodiment of the present invention

FIG. **7** shows a flowchart showing authoring an encrypted digital media according to an embodiment of the present invention.

Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention

DETAILED DESCRIPTION OF THE DRAWINGS

Before describing in detail the particular system and method for personalised digital media access system in accordance with an embodiment of the present invention, it should be observed that the present invention resides primarily in combinations of system components related to the device of the present invention.

Accordingly, the system components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

In this document, relational terms such as 'first' and 'second', and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms 'comprises', 'comprising', or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method,

EWS-004428

article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element proceeded by 'comprises . . . a' does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises the element.

The present invention is directed at providing infinite access rights of legally acquired at least one encrypted digital media asset to the content acquirer, explained in this document as the excelsior enabler, and optionally to their recognized friends and family, explained in this document as a plurality of secondary enablers. To explain further, the excelsior enabler and secondary enablers defined comprises human beings or computerized mechanisms programmed to process steps of the invention as would normally be done manually by a human being. Additionally, an apparatus used alone or in accordance with an embodiment, another apparatus, tangible computer medium, or associated methods with a connection are needed (herein referred to as The App). To deliver the requirements of the invention, communicative and connected elements comprise: verification, authentication, electronic ID metadata branding, additional technical branding, and cross-referencing. The connection handling the communicative actions of the invention will usually be the Internet and can also be an internal apparatus cooperative. The App can further be defined as a Windows OS, Apple OS, Linux OS, and other operating systems hosting software running on a machine or device with a capable CPU, memory, and data storage. The App can be even further defined as a system on a chip (SOC), embedded silicon, flash memory, programmable circuits, cloud computing and runtimes, and other systems of automated processes.

The digital media assets used in this system are encrypted usually with an AES cipher and decryption keys are usually stored encoded, no encoded, encrypted, or no encrypted as part of the apparatus or as part of a connection usually an Internet server. As explained earlier, the system we will discuss will work as a front-end to encrypted files as an authorization agent for decrypted access.

FIG. **1** shows a system **100** for monitoring access to an encrypted digital media according to an embodiment of the present invention. The system **100** includes a first recipient module **102**, an authentication module **104**, a connection module **106**, a request module **108**, a second receipt module **110** and a branding module **112**. The first receipt module **102** receives a branding request from at least one communications console of the plurality of data processing devices. The branding request is a read and write request of metadata of the encrypted digital media and includes a membership verification token corresponding to the encrypted digital media. Examples of the encrypted digital media includes, and are not limited to, one or more of a video file, audio file, container format, document, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

Subsequently, the authentication module **104** authenticates the membership verification token. The authentication is performed in connection with a token database. Further, the connection module **106** establishes communication with the at least one communication console.

According to an embodiment of the present invention, the connection is established through one of internet, intranet, Bluetooth, VPN, Infrared and LAN.

According to another embodiment of the present invention, the communication console is a combination of an Application Programmable interface (API) protocol and graphic user interface (GUI) as a part of web service. The API is a set of routines, data structures, object classes, and/or protocols provided by libraries and/or operating system services. The API is either one of language dependent or language independent.

The request module **108** requests at least one electronic identification reference from the at least one communication console. The second receipt module **110** receives the at least one electronic identification reference from the least one communication console. The branding module **112** brands metadata of the encrypted digital media by writing the membership verification token and the electronic identification into the metadata.

FIG. **2** shows a system **200** for authoring an encrypted digital media according to an embodiment of the present invention. The figure includes a selection module **202**, a password module **204**, a customization module **206**, a database module **208** and an encryption module **210**. The selection module **202** facilitates selection of one or more media items to form the encrypted digital media. Examples of the one or media items include, and are not limited to, one or more of a video, an audio and a game.

According to an embodiment of the present invention, the one or more media items are one or more of remote URL links and local media files.

The password module **204** prompts the user to enter a master password which provides access to the encrypted digital media. Subsequently, the customization module **206** allows the user to customize the user access panel of the encrypted digital media.

According to an embodiment of the present invention, the customization module **206** facilitates adding one or more of a banner, a logo, an image, an advertisement, a tag line, a header message and textual information to the user access panel of the encrypted digital media.

Further, the database module **208** connects the encrypted digital media to a database of membership verification token required for decrypting the encrypted digital media.

According to an embodiment of the present invention, the membership verification token is a kodekey. The kodekey is a unique serial number assigned to the encrypted digital media.

The encryption module **210** encrypts the one or more media items to create the encrypted digital media.

According to an embodiment of the present invention, the system **200** further includes a watermark module. The watermark module watermarks information on the encrypted digital media, wherein the watermark is displayed during playback of the encrypted digital media.

According to another embodiment of the present invention, the system **200** further includes an access module. The access module allows the user to define access rights. Examples of the access rights include, but are not limited to, purchasing rights, rental rights and membership access rights.

According to yet another embodiment of the present invention, the system **200** further includes a name module. The name module allows the user to name the encrypted digital media.

FIG. **3** shows a flow chart giving an overview of the process of digital media personalization according to an embodiment of the present invention. The process is achieved by way of an enabler using an apparatus or otherwise known as an application in which facilitates digital media files. The apparatus interacts with all communicative parts required to fulfill the actions of the invention. The figure shows a Kodekey Graphical User Interface (GUI) **301**, a product metadata **302**, a networking card **303**, internet **304**, **306** and **308**, database **305** and **309** and an APIwebsite.com GUI **307**. A user posts a branding request via the Kodekey GUI interface **301**. The

EWS-004429

Kodekey GUI interface **301** is the GUI for entering token. The Kodekey GUI interface **301** prompts the user to enter the token and press the redeem button present on the Kodekey GUI interface **301**. The product metadata **302** is read/writable metadata associated with the digital media to be acquired. The networking card **303** facilitates querying of optional metadata branding process and referenced. The Kodekey GUI interface is connected to the database **305** via the internet **304** through the networking card **303**. The database **305** is the database used to read/write and store the tokens, also referred to as token database. The user is redirected to the APIwebsite.com GUI **307** through the internet **306**. The APIwebsite.com is the GUI to the membership API in which the electronic ID is collected and sent back to the Kodekey GUI interface **301**. The APIwebsite.com GUI **307** prompts the user to enter a login id and a password to access the digital media which is acquired from the database **309** through the internet **308**. The database **309** is the database connected to the web service membership in which the user's electronic ID is queried from.

Examples of the encrypted digital files include, and are not limited to, a video file, an audio file, container formats, documents, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

FIG. **4** shows a flow chart giving an overview of the process of an access request made by an enabler according to an embodiment of the present invention. Subsequently, the communicative parts to cross-reference information stored in the metadata of the digital media asset are checked which has been previously handled by the process of FIG. **1**. The figure shows an enabler access request **401**, a product metadata **402**, a networking card **403**, an internet **404**, **406** and **408**, a database **405** and **409** and an APIwebsite.com GUI **407**, The enabler access request **401** facilitates the user to make a request for the digital media. The product metadata **402** is read/writable metadata associated with the digital media to be acquired. The networking card **403** facilitates querying of optional metadata branding process and referenced. The database **405** is the database used to read/write and store the tokens. The APIwebsite.com GUI **407** is the GUI in which the electronic ID is collected and sent back to the Kodekey GUI interface **301**. The APIwebsite.com GUI **407** prompts the user to enter a login id and a password to access the digital media from the database **409** through the internet **408**. The database **409** is the database connected to the web service membership in which the user's electronic ID is queried from.

FIG. **5** shows personalized digital rights management component as part of a compatible machine with writable static memory. The figure represents an authorization sequence action in which a machine is authorized to accept a personalized digital media file. The figure includes STR3EM Machine GUI **501** including the connect icon **502**, a load key file icon **503**, a networking card **504**, an internet **505**, **508** and **510**, a database **506** and **511**, a machine memory **507** and a APIwebsite.com GUI **509**. The STR3EM Machine GUI **501** prompts the user to connect or load a key file to authorize the device through the connect icon **502** and the load key file icon **503**. The STR3EM Machine GUI **501** is connected to the networking card **504**. The networking card **504** facilitates querying of optional metadata branding process and referenced. Further, the STR3EM machine GUI **501** is connected to the database **506** via the internet **505**. The database **506** is the database used to read/write and store the tokens. Moreover, STR3EM Machine GUI **501** is connected to the machine memory **507**. The machine memory **507** represents the internal memory of the machine or device so authorizations can be saved for access of the digital media. The APIwebsite.com GUI **509** is connected to the STR3EM machine GUI through the internet **508**. Further, APIwebsite.com GUI **509** is connected to the database **511** through the internet **510**. The APIwebsite.com GUI **509** prompts the user to enter the login id and a password to authorize the access to digital media. The database **511** is the database connected to the web service membership in which the user's electronic ID is queried from.

FIG. **6** shows a flowchart for monitoring access to an encrypted digital media according to an embodiment of the present invention. At step **602**, a branding request is made by a user from at least at least one communications console of the plurality of data processing devices. The branding request is a read and write request of metadata of the encrypted digital media.

According to an embodiment of the present invention, the request includes a membership verification token corresponding to the encrypted digital media.

Subsequently, the membership verification token is authenticated at step **604**. The authentication is performed in connection with a token database. Further, connection with the at least communication console is established at step **606**. Afterwards, at least one electronic identification reference is requested from the at least one communications console at the step **608**. At step **610**, at least one electronic identification reference in received from the at least one communication console. Finally, metadata of the encrypted digital media is branded by writing the membership verification token and the electronic identification reference into the metadata at the step **612**.

FIG. **7** shows a flowchart showing authoring an encrypted digital media according to an embodiment of the present invention. At step **702**, one or more media items are selected by the user to form the encrypted digital media. Subsequently, a master password is entered for providing access to the encrypted digital media for editing at step **704**. Afterwards, the user customizes the user panel of the encrypted digital media at step **706**. Further, the encrypted digital media is connected to a database of membership verification tokens required for decrypting the encrypted digital media at the step **708**. Finally, the one or more media items are encrypted to create the encrypted digital media at the step **710**.

According to various embodiments of the present invention, the verification is facilitated by at least one token handled by at least one execlsior enabler. Examples of the token include, and are not limited to, a structured or random password, e-mail address associated with an e-commerce payment system used to make an authorization payment, or other redeemable instruments of trade for aeeess rights of digital media. Examples of e-eommerce systems are PayPal, Amazon Payments, and other credit card services.

According to an embodiment of the present invention, an identifier for the digital media is stored in a database with another database of a list of assoeiated tokens for eross-reference identification for verification.

According to an embodiment of the present invention, the database of a list of associated tokens includes Instant Payment Notification (IPN) received from successful financial e-eommerce transactions that ineludes the identifier for the digital media; import of CSV password lists, and manually created reference phrases.

For this discussion, the structured or random password example will be used as reference. The structured or random passwords can be devised in eneoded sehemes to flag the apparatus of permission type such as: 1) Purchases eau start a password sequence with "P" following a random number, so

further example would be "PSJD42349MFJDF". 2) Rentals can start or end a password sequence with "R" plus (+) the number of days a rental is allowed, for example "R7" included in "R7SJDHFG58473" flagging a seven day rental. 3) Memberships can start or end a password sequence with "M" plus (+) optionally the length of months valid for example "M11DFJGH34KF" would flag an eleven-month membership period.

According to an embodiment of the present invention, the tokens are stored in a relational database such as MySQL or Oracle. Cloud storage systems such as Amazon's Web Services Simple Storage Solution, or also known as S3, provides a highly available worldwide replicated infrastructure. In addition to S3, monetization offerings such as DevPay offer developers the opportunity to make money from applications developed to use the services.

The verification will reference to the S3 and DevPay services for example purposes only as many options such as FTP, SimpleDB, solid state storage and others can be used to host the token hosting needed for the verification element of this invention. The token represents permission from the content provider to grant access rights to the excelsior enabler and thereafter the plurality of secondary enablers. To set up the verification the content provider can manually or automatically generate a single or a plurality of structured or random password in which will represent the token. By using public or private access of S3 as part of an apparatus, the content provider can create empty text files giving each the name of the passwords generated. Because S3 is associated with a highly available worldwide infrastructure, to check this password token can be done my simply constructing a HTTP request from the apparatus and triggering follow up actions based on either a 200 HTTP response, which means OK at which point the next action can happen, or a 400 HTTP response which means ERROR at which point the verification process is voided. An additional token can be used to provide a flag to the apparatus that the verification element has been fulfilled for an initial verification token. Creating an alternate version of the first token by appending a reference to the end, for example, does this: "M11DFJGH34KF_user@str3em.com__01__01__11". In this example, it is defined that the eleven month authorized membership token was verified by a user@str3em.com on Jan. 1, 2011. By providing a second token, the first token becomes locked to ownership by the excelsior enabler preventing unauthorized users from reusing the first token without providing the authentication associated with the alternative referenced second token. In the interest of providers of the apparatus delivering this invention, this document will teach a method of a HTTP PUT calculation scheme for automatic royalty billing and administration for the token element used in the invention. Amazon's DevPay allow developers to attach monetary charges to data services of S3 offered as an embedded component of the apparatus. By using the "PUT" requests parameter, tokens generated by the apparatus are monitored, calculated, and charged to clients of the apparatus provider. For example: the default charge measure for DevPay is $0.05 for every 1000 PUT requests. By changing the amount to $100 for every 1000 PUT requests, the apparatus provider is paid a $0.10 royalty for each token created. Content providers using a connected apparatus like DevPay to deliver and manage digital media distribution do not need to have restrictions on the tokens created as with prior art DRM key providers as DevPay is charged on a pay-as-you-need model on a monthly basis. As a novelty to the apparatus provider, if a content provider fails to pay royalties due, the DevPay hosting will automatically deny token access to all related media products in distribution and restore this verification element when royalties are paid in full.

The authentication element of this invention is at least handled first by the at least one excelsior enabler with a connection to a membership. In the present discussion, the connection is equal to the Internet and the membership is equal to a web service. Further, the web service must be available for two way data exchange to complete the authentication process of this invention. Data exchange with a web service is usually facilitated with a programmable communications console, at most times, will be an Applications Programmable Interface (API). An API is a set of routines, data structures, object classes, and/or protocols provided by libraries and/or operating system services in order to support the building of applications. An API may be language-dependent: that is, available only in a particular programming language, using the particular syntax and elements of the programming language to make the API convenient to use in this particular context. Alternatively an API may be language-independent: that is, written in a way that means it can be called from several programming languages (typically an assembly/C-level interface). This is a desired feature for a service-style API that is not bound to a particular process or system and is available as a remote procedure call. A more detailed description of API that can be used for an apparatus can be found in the book, "Professional Web APIs with PHP: eBay, Google, Paypal, Amazon, FedEx plus Web Feeds", by Paul Reinheimer, Wrox publishers (2006). A program apparatus, scripts, often calls these APIs or sections of code residing on user computerized devices. For example, a web browser running on a user computer, cell phone, or other device can download a section of JavaScript or other code from a web server, and then use this code to in turn interact with the API of a remote Internet server system as desired. A Graphic User Interface (GUI) can be installed for human interaction or processes can be preprogrammed in a programmable script such as PHP, ASP.Net, Java, Ruby on Rails and others. The authentication element of the invention is usually embedded as a process of the apparatus but could be linked dynamically. In this document, the embedded version using a GUI will be used as reference. The web service equipped with the API is usually a well-known membership themed application in which the users must use an authentic identification. Some example includes Facebook in which as a rule, members are required to use their legal name identities. A reference number or name with the Facebook Platform API represents this information. Other verified web services in which real member names are required such as the LinkedIn API and the PayPal API and even others could be used, but for this discussion, Facebook will be used only as an example of how the authentication element of the invention is utilized. The Facebook API system, as well as others, operates based on an access authentication system called from a connected apparatus (which is usually an Internet powered desktop or browser based application) with an API Key, an Application Secret Key and could also include an Application ID. For example, the Facebook API Application Keys required to establish a data exchange session with the connected apparatus might look like:

API Key
37a925fc5ee9b4752af981b9a30e9a73gh
Application Secret
f2a2d92ef395cce88eb0261d4b4gsa782
Application ID
51920566446

The collective API keys are usually embedded in the source code of the apparatus, or stored on a remote Internet server, and could be included in the encrypted digital media metadata

and inserted on-the-fly into calls made to the API from the connected apparatus. This allows dynamic API connection of the apparatus using keys issued to individual content providers so in the event of a reprimand of a single the individual content provider by the API provider, the collective the individual content providers and the enablers of the connected apparatus are not affected.

Upon an access request of the digital media, the excelsior enabler interacts with the apparatus, usually software or web application, to enter membership credentials in a GUI front-end connected to the API. The membership credentials are usually comprised of a login element comprising a name, phrase, or e-mail address, and a secret password. The credentials can be generated by the enabler or automatically generated by the web service. Once the enabler authenticates their identity with the membership, the apparatus facilitating the data communication can request relevant information to fulfill the process chain of the invention. For example, Facebook API Platform defines members as ID numbers, so if a member's real name is John Doe, then Facebook API ID (also programmatically known as the FBID) would be 39485678. Once the enabler successfully sign in to the GUI element then the apparatus will query the API for at least one electronic identification reference, in this discussion is the FBID. The FBID is received to the permanent or temporary memory of the apparatus to sustain the branding and cross-referencing requirements of the invention. Additional information can be requested according to membership status or connected "friends" of the enabler. Additional information can be made required for successful authentication and includes: a minimum amount of total friends, a minimum amount of female friends, a minimum amount of male friends, a minimum amount of available pictures, a minimum age limit and other custom rules can be defined by the apparatus. An example of how this would work is a content provider can define a minimum of 32 Facebook friends are required to access an encrypted digital media asset offered for sale or promotion. This is achieved by the apparatus handling a access request in which the enabler has not yet acquired access rights by executing and parsing information returned by the Facebook "Friends.get" API command.

XML return example of the Facebook "Friends.get" API command where a plurality of FBID are returned to the apparatus for parsing additional information as may be required to satisfy successful authentication:

```
<?xml version="1.0" encoding="UTF-8"?>
<friends_get_response xmlns="http://api.facebook.com/1.0/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://api.facebook.com/1.0/
http://api.facebook.com/1.0/facebook.xsd" list="true">
<uid>222333</uid>
<uid>1240079</uid>
</friends_get_response>
```

When authenticating a compatible device or machine which may not have access to a connection for the authentication element, a key file or part of the metadata thereof could be made on another connected compatible device or machine and allow the enabler to execute Friends.get API command to collect and store the complete list of a plurality of FBID to the key file or the metadata thereof. The compatible device or machine which may not have access to a connection for the authentication element with an embedded interaction console, usually a user GUI, can request and load the key file or part of the metadata thereof to save the complete list of a plurality of electronic identification references, in this discussion is reference as the FBID, to storage or metadata as part of the compatible device or machine. This step ensures the cross-referencing element requirement of the invention can take place in the event the connection for the authentication element is not present in the compatible device or machine.

Another example is a content provider can allow shared access to friends of the excelsior enabler after a time period, like for example, 90 days. After the 90 day period, when media access is requested using the authentication element by a plurality of secondary enablers, which are usually friends and family of the excelsior enabler, the FBID of the excelsior enabler is cross-referenced with the FBID of the requesting secondary enabler by way of the apparatus ability to execute the Facebook "Friends.areFriends" API command.

XML return example of the Facebook "Friends.areFriends" API command where FBID 2223322 and 2222333 are friends and FBID 1240077 and 1240079 are not friends:

```
<?xml version="1.0" encoding="UTF-8"?>
<friends_areFriends_response
xmlns=http://api.facebook.com/1.0/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://api.facebook.com/1.0/
http://api.facebook.com/1.0/facebook.xsd" list="true">
<friend_info>
<uid1>222332</uid1><uid2>222333</uid2>
<are_friends>1</are_friends>
</friend_info>
<friend_info>
<uid1>1240077</uid1><uid2>1240079</uid2>
<are_friends>0</are_friends>
</friend_info>
</friends_areFriends_response>
```

Such usability can be important to sustain "fair use" rights of consumers of the digital media to emulate usability found with physical media products such as CD and DVD that can be loaned to friends and family after an inception grace period.

Once the information of the verification and authentication elements is acquired, the apparatus handles the next process of writing the information to the digital media metadata and can include additional information gathered from components of The App. Components of The App can include MAC address from a networking card, CRC checksum of an embedded file or circuit, SOC identifier, embedded serial number, OS version, web browser version, and many other identifiable components as part of The App. For this discussion, the MAC address from a networking card as part of The App will be used as reference of a secondary electronic identification reference. In computer networking, a Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification, and used in the Media Access Control protocol sub-layer. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number. It may also be known as an Ethernet Hardware Address (EHA), hardware address, adapter address, or physical address. The novelty of embedding the MAC address along with the FBID of the excelsior enabler is to provide a plurality of electronic identification references in which cross-referencing actions can allow more rapid access to be granted with less interaction from an enabler. For example, to retrieve the FBID from Facebook to cross-reference with the FBID stored in the digital media metadata requires the enabler to possibly physically need to enter their login and password credentials to the GUI connected to the apparatus. It may be possible that web browser

cookies allow automatic Facebook login by storing an active session key, but the session key is not guaranteed to be active at the time of an access request. While the enabler may not have an issue execnting another authentication command, several remote operations could exist to control authentication and access requests separately from each other. The apparatns can execnte a programmable retrieval command, nsually a GET command, to locate and retrieve the MAC address from an attached or connected networking card. After the FBID is acquired, the MAC address is also acquired to write the plurality of electronic identifications to the metadata of the at least one encrypted digital media asset by; obtaining the decryption key to decrypt the encrypted digital media asset which is usually stored encoded, no encoded, encrypted, or no encrypted as part of the apparatus or as part of a connected source, usually an Internet server with an encrypted HTTPS protocol. A plurality of MAC addresses can be stored along with the FBID of the excelsior enabler to manage access rights across a plurality of devices. To understand metadata and the uses, metadata is defined simply as to "describe other data". It provides information about certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the docnment is, who the author is, when the document was written, and a short summary of the document. Web pages often include metadata in the form of Meta tags. Description and keywords Meta tags are commonly used to describe the Web page's content. Most search engines use this data when adding pages to their search index. In the invention, the FBID and MAC addresses are written to the digital media asset metadata to prepare for the instant or delayed cross-referencing element of the invention. The same process of writing the information to the digital media metadata is true with secondary enablers allowing the same benefits of cross-referencing.

Cross-referencing, the last element of the invention is used to verify access rights of an enabler of a pre or post personalized encrypted digital media asset. Once an enabler execntes an action for access request, the apparatus will obtain the decryption key to first seek the MAC address record. If the MAC address is found, then a cross-reference process is executed by comparing the MAC address retrieved from the metadata of the digital media file with the MAC address retrieved from the networking card connected to the apparatus or The App. If the comparison action proves to be true, then access rights are granted to the enabler. If the comparison fails, then the apparatns can either ask the enabler to participate in communication with the authentication element of the invention, or conld deny further interactivity with the enabler. In this discussion, the apparatus requires the enabler to participate in communication with the authentication element to provide credentials to establish a cross-reference comparison with the FBID retrieved from the metadata and the FBID retrieved from the Facebook API. If the comparison action proves to be true, then access rights is granted to the excelsior enabler and the current MAC address of the networking card as part of The App is appended to the metadata of the encrypted digital media asset and access rights is granted to the excelsior enabler. If the FBID cross-reference fails, then the apparatus can either ask the potential secondary enabler to participate in communication with the authentication element of the invention, or could deny further interactivity with the potential secondary enabler. In this discussion, the apparatus requires the potential secondary enabler to participate in communication with the authentication element to provide credentials to establish a cross-reference comparison with the FBID retrieved from the metadata and the FBID retrieved from the Facebook "Friends.arelFriends" API command to determine if the potential secondary enabler identity is true or false. The determination is in accordance to any possible access grace periods set by the content provider of the encrypted digital media asset. If the comparison action proves to be true, then access rights is granted to the secondary enabler and the current MAC address of the networking card as part of The App and the FBID retrieved are appended to the established metadata information of the encrypted digital media asset and access rights can be granted to a plurality of secondary enablers; unlimited interoperability between devices and "fair use" sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term retnrn of investments is achieved.

While the present invention has been described in connection with preferred embodiments, it will be understood by those skilled in the art that variations and modifications of the preferred embodiments described above may be made without departing from the scope of the invention. Other embodiments will be apparent to those skilled in the art from a consideration of the specification or from a practice of the invention disclosed herein. It is intended that the specification and the described examples are considered exemplary only, with the true scope of the invention indicated by the following claims.

What is claimed is:

1. A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:

a) receiving an access request for cloud digital content throngh an apparatus in process with at least one CPU, the access request bcing a write request to a data store, wherein the data store is at least one of:

a memory connected to the at least one CPU;

a storage connected to the at least one CPU; and

a database connected to the at least one CPU through the Internet; wherein

the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then

b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then

c) establishing an API communication between the apparatus of (a) and a database apparatns, the database apparatus being a different database from the verification token database of (b) whcrein the API is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier;

then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of:

the received verification data of (a); and

the received query data of (e); wherein

the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content.

* * * * *

Electronic Acknowledgement Receipt

EFS ID:	20951711
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	12-DEC-2014
Filing Date:	06-MAY-2013
Time Stamp:	17:13:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	WalletTokenSOTAbreif.pdf	5204796 e2ec25a4883ffcc5f767d799204b0621607f29d2	no	320

Warnings:	
Information:	

Total Files Size (in bytes):	5204796

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/888,051	11/11/2014	8887308		2314

70984 7590 10/22/2014

The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 75 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

William Grecia, Brooklyn, NY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/888,051	05/06/2013	William Grecia	

CONFIRMATION NO. 2314

PUBLICATION NOTICE

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

OC000000071268268

Title:DIGITAL CLOUD ACCESS (PDMAS PART III)

Publication No.US-2014-0304778-A1
Publication Date:10/09/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/888,051	05/06/2013	2494	730		15	3

CONFIRMATION NO. 2314

CORRECTED FILING RECEIPT

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

OC000000071215887

Date Mailed: 10/08/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

William Grecia, Brooklyn, NY;

Applicant(s)

William Grecia, Brooklyn, NY;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 13/740,086 01/11/2013 PAT 8533860
which is a CON of 13/397,517 02/15/2012 PAT 8402555
which is a CON of 12/985,351 01/06/2011 ABN
which is a CON of 12/728,218 03/21/2010 ABN

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 06/05/2013
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/888,051**
Projected Publication Date: 10/09/2014
Non-Publication Request: No

Early Publication Request: Yes
Title

DIGITAL CLOUD ACCESS (PDMAS PART III)

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

70984 7590 09/19/2014

The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

EXAMINER
TRAN, TRI MINH

ART UNIT	PAPER NUMBER
2494	

DATE MAILED: 09/19/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/888,051	05/06/2013	William Grecia		2314

TITLE OF INVENTION: DIGITAL CLOUD ACCESS (PDMAS PART III)

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	12/19/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

70984 7590 09/19/2014
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/888,051	05/06/2013	William Grecia		2314

TITLE OF INVENTION: DIGITAL CLOUD ACCESS (PDMAS PART III)

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	12/19/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAN, TRI MINH	2494	726-029000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

EWS-004443

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/888,051	05/06/2013	William Grecia		2314

70984 7590 09/19/2014

The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

EXAMINER	
TRAN, TRI MINH	

ART UNIT	PAPER NUMBER
2494	

DATE MAILED: 09/19/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/888,051	Applicant(s) GRECIA, WILLIAM	
	Examiner TRI TRAN	Art Unit 2494	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6 May 2013*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *16*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 7/26/13
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/TRI TRAN/ Examiner, Art Unit 2494	/Jung Kim/ Supervisory Patent Examiner, Art Unit 2494

DETAILED ACTION

Claim 16 is allowed.

This communications is in response to the application filed on May 6th, 2013 which claimed priority to application 12/728218 filed on March 21st, 2010.

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interviews and emails with the Applicant/Inventor William Grecia on August 28th and September 3rd, 2014.

Amended Claims

1-15. (previously cancelled)

16. (Currently amended) A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:

a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of:

a memory connected to the at least one CPU;

a storage connected to the at least one CPU; and

a database connected to the at least one CPU through the Internet; wherein

the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then

b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then

c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b) wherein the API is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier; ~~comprises at least one of:~~

~~a reference;~~

~~an ID; and~~

~~an identifier;~~ then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); and

f) creating a computer readable authorization object by writing into the data store of (a) at least one of:

the received verification ~~token~~ data of (a); and

the received query data of (e); wherein

the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, ~~wherein the computer readable authorization object is available for processing by a plurality of CPUs using across-referencing action to determine a user access permission to the associated cloud digital content~~ wherein the computer readable authorization object is processed by the apparatus of (a) using a cross-referencing action during subsequent user access requests to determine one or more of a user access permission for the cloud digital content.

Allowable Subject Matter

1. The following is an examiner's statement of reasons for allowance:

The following prior art are the closest materials to the subject matter of claim 1 and similarly claimed in claims 9, 11, and 21:

Prior Art: Baiya et al. PG Pub 20110288946 - Method and System of Managing Digital Multimedia Content (herein after Baiya). Baiya discloses a process of "the management of digital multimedia content comprises a computer-implemented digital multimedia content management system comprising the following computer executable components: an upload component that uploads digital media content …a catalog component that allows a first user to tag the digital media content with one or more attributes… a grouping component that groups the digital media content according to the one or more attributes; a licensing component that attaches one or more keys to the digital media content; a security component that encrypts the digital media content; and a sharing component that allows one or more second users to access the digital media content (Fig. 3-4 and paragraphs [0008]). The user can access the copyrighted digital media for access by using an interface called Content Manager (paragraph [0022]) wherein the Content Manager is using Application Program Interface protocol for access control authentication and authorization information (paragraph [0064]).

Prior Art: Chris Wimmer US Patent 7526650 - Personal Identifiers for Protecting Video Content (herein after Wimmer), Wimmer discloses "techniques for branding video content with an end user's personal identity information ("personal identifier," "mark," or "brand") as a deterrent against unauthorized redistribution of the video content by the

user. A "user" is a person or personal entity that receives the video content to be protected or the owner of a client device that receives the video content to be protected" (column 2, lines 9-15). The method aims " to prevent redistribution of content before it happens rather than provide a tool for tracking down a user after an unauthorized redistribution of video content has already been made" (Fig. 1-5, 7 and column 2, line 25-29).

However, neither Baiya nor Wimmer either singly or in combination implicitly or explicitly suggests *a process for transforming a user access request for cloud digital content into a computer readable authorization object* with the steps of*:*

c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b) wherein the API is related to a verified web service, wherein the verified web service is a part of the database apparatus, wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus to complete the verification process, wherein the data exchange session is also capable of an exchange of query data, wherein the query data comprises at least one verified web service account identifier; then

d) requesting the query data, from the apparatus of (a), from the API communication data exchange session of (c), wherein the query data request is a request for the at least one verified web service identifier;

Since no prior art teaches or suggests any process with the above allowable limitations, claim 16 is allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

INQUIRY COMMUNICATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRI TRAN whose telephone number is (571)270-1994. The examiner can normally be reached on Monday-Friday 9:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jung (Jay) Kim can be reached on 571-272-3804. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/TRI TRAN/

Examiner, Art Unit 2494

/Jung Kim/

Supervisory Patent Examiner, Art Unit 2494

Notice of References Cited	Application/Control No. 13/888,051	Applicant(s)/Patent Under Reexamination GRECIA, WILLIAM	
	Examiner TRI TRAN	Art Unit 2494	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2011/0288946	11-2011	Baiya et al.	705/26.1
*	B	US-7,526,650	04-2009	Wimmer, Chris	713/176
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13888051	GRECIA, WILLIAM
	Examiner	**Art Unit**
	TRI TRAN	2494

CPC						
Symbol					**Type**	**Version**
H04L		63	/	10	F	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

/TRI TRAN/ Examiner.Art Unit 2494	09/04/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	1	
/Jung Kim/ Supervisory Patent Examiner, Art Unit 2494	9/8/14	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
13888051	GRECIA, WILLIAM
Examiner	**Art Unit**
TRI TRAN	2494

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
726	29	H 0 4 L 29 / 06 (2006.01.01)	

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	28				
713	185				

/TRI TRAN/ Examiner.Art Unit 2494	09/04/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	1	
/Jung Kim/ Supervisory Patent Examiner, Art Unit 2494	9/8/14	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13888051	GRECIA, WILLIAM
	Examiner	**Art Unit**
	TRI TRAN	2494

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1														
	2														
	3														
	4														
	5														
	6														
	7														
	8														
	9														
	10														
	11														
	12														
	13														
	14														
	15														
1	16														

/TRI TRAN/ Examiner.Art Unit 2494	09/04/2014	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	1	
/Jung Kim/ Supervisory Patent Examiner, Art Unit 2494	9/8/14	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13888051	GRECIA, WILLIAM
	Examiner	Art Unit
	TRI TRAN	2494

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/04/2014								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
1	16	=								

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13888051
Filing Date	2013-05-06
First Named Inventor	William Grecia
Art Unit	N/A 2494
Examiner Name	N/A Tri Tran
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.T./	1	7254235		2007-08-07	Boudreault et al.	
/T.T./	2	7343014		2008-03-11	Sovio et al.	
/T.T./	3	7526650		2009-04-28	Wimmer, Chris	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.T./	1	20110288946		2011-11-24	Baiya et al.	
/T.T./	2	20100100899		2010-04-22	Bradbury et al.	
/T.T./	3	20050065891		2005-03-24	Lee et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T./

Receipt date: 07/26/2013	Application Number	13888051	13888051 - GAU: 2494
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-05-06	
	First Named Inventor	William Grecia	
	Art Unit	N/A	
	Examiner Name	N/A	
	Attorney Docket Number		

/T.T./	4	20080010685		2008-01-10	Holtzman et al.	
/T.T./	5	20090083541		2009-03-26	Levine, Scott	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/T.T./	1	Copy of U.S. patent application #13/397,517 Notice of Allownce	☐
/T.T./	2	Copy of U.S. patent application #13/740,086 Notice of Allowance	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Tri Tran/ (09/04/2014)	Date Considered	09/04/2014

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T./

Receipt date: 07/26/2013	Application Number	13888051 13888051 - GAU: 2494
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-05-06
	First Named Inventor	William Grecia
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T./

Receipt date: 07/26/2013	Application Number	13888051	13888051 - GAU: 2494
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2013-05-06	
	First Named Inventor	William Grecia	
	Art Unit	N/A	
	Examiner Name	N/A	
	Attorney Docket Number		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/william grecia/	Date (YYYY-MM-DD)	2013-07-26
Name/Print	William Grecia	Registration Number	70984

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /T.T./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2314

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/888,051	05/06/2013	726	2494	

APPLICANTS

INVENTORS
William Grecia, Brooklyn, NY;

co-pending13/740086 with parent 13/397517 with parent 12/985351 with parent 12/728218

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
06/05/2013

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /TRI MINH TRAN/ Examiner's Signature	☐ Met after Allowance TT Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		NY	7	15	3

ADDRESS

The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418
UNITED STATES

TITLE

DIGITAL CLOUD ACCESS (PDMAS PART III)

FILING FEE RECEIVED		
730	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13888051	GRECIA, WILLIAM
	Examiner	Art Unit
	TRI TRAN	2494

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor Search (PALM)	8/27/14	TT
IP.com & Google	9/4/14	TT
EAST (relied on searches performed on parent applications 13/397517 & 13/740086 which are granted as patents).	8/28/14 - 8/29/14	TT
Consutled with Jay (Jung) Kim (SPE)	8/29/14, 9/4/14	TT
EAST combined with CPC classes (H04L9/3234 OR H04L63/0853 OR H04L2209/603 OR H04L63/126 OR H04L67/02 OR H04L63/083 OR H04L9/0866 OR H04L9/321 OR H04L2463/101)	9/4/14	TT

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
	claim search	9/4/14	TT

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	346	(((writ$3 request modif$3 add$3 attach$3 read$3 includ$3) with (verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 17:31
L2	78	l1 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 17:34
L3	34	l1 and 713/155-159,168,172-176,182,189.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 17:34
L4	46	l1 and 726/7-32.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 17:35
L5	21	l1 and (726/28-29 713/185).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/04 17:35
S1	0	"13397517"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/06 22:07
S3	124	(("7266839") or ("7567987") or ("20070266095") or ("20090100060") or ("20070010334") or ("20060036554") or ("7634734") or ("20080111052") or ("20030018491") or ("7610630") or ("7689823") or ("7702592") or ("7515710") or ("6799165") or	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 13:55

		("6385596") or ("5907617") or ("5903647") or ("5887060") or ("5883955") or ("5870543") or ("5883954") or ("7290699") or ("7340769") or ("7343014") or ("7386513") or ("7571328") or ("7624417") or ("20020010759") or ("20020157002") or ("20040024670") or ("20040062400") or ("20040162786") or ("20040220878") or ("20050066353") or ("20050182727") or ("20060173787") or ("20060173789") or ("20060259652") or ("20060259982") or ("20070055887") or ("20070156719") or ("20070179854") or ("20070180485") or ("20070250445") or ("20080027869") or ("20080091606") or ("20080109911") or ("20080165956") or ("20090012805") or ("20090049556") or ("20090083541") or ("20090183010") or ("20090217036") or ("20090254930") or ("20090257591") or ("20090265278") or ("20090299963") or ("20090307078") or ("20090327702") or ("20090328228")).PN.				
S4	60	(("7266839") or ("7567987") or ("20070266095") or ("20090100060") or ("20070010334") or ("20060036554") or ("7634734") or ("20080111052") or ("20030018491") or ("7610630") or ("7689823") or ("7702592") or ("7515710") or ("6799165") or ("6385596") or ("5907617") or ("5903647") or ("5887060") or ("5883955") or ("5870543") or ("5883954") or ("7290699") or ("7340769") or ("7343014") or ("7386513") or ("7571328") or ("7624417") or ("20020010759") or ("20020157002") or ("20040024670") or ("20040062400") or ("20040162786") or ("20040220878") or ("20050066353") or ("20050182727") or ("20060173787") or ("20060173789") or	US-PGPUB; USPAT	OR	OFF	2012/05/07 13:55

		("20060259652") or ("20060259982") or ("20070055887") or ("20070156719") or ("20070179854") or ("20070180485") or ("20070250445") or ("20080027869") or ("20080091606") or ("20080109911") or ("20080165956") or ("20090012805") or ("20090049556") or ("20090083541") or ("20090183010") or ("20090217036") or ("20090254930") or ("20090257591") or ("20090265278") or ("20090299963") or ("20090307078") or ("20090327702") or ("20090328228")).PN.				
S5	0	(("1505530A1") or ("1564621A1")).PN.	EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 13:56
S6	11	(("1505530") or ("1564621")).PN.	EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 13:56
S7	60	(("7266839") or ("7567987") or ("20070266095") or ("20090100060") or ("20070010334") or ("20060036554") or ("7634734") or ("20080111052") or ("20030018491") or ("7610630") or ("7689823") or ("7702592") or ("7515710") or ("6799165") or ("6385596") or ("5907617") or ("5903647") or ("5887060") or ("5883955") or ("5870543") or ("5883954") or ("7290699") or ("7340769") or ("7343014") or ("7386513") or ("7571328") or ("7624417") or ("20020010759") or ("20020157002") or ("20040024670") or ("20040062400") or ("20040162786") or ("20040220878") or ("20050066353") or ("20050182727") or ("20060173787") or ("20060173789") or ("20060259652") or ("20060259982") or ("20070055887") or ("20070156719") or ("20070179854") or ("20070180485") or ("20070250445") or ("20080027869") or ("20080091606") or	US-PGPUB; USPAT	OR	OFF	2012/05/07 15:06

		("20080109911") or ("20080165956") or ("20090012805") or ("20090049556") or ("20090083541") or ("20090183010") or ("20090217036") or ("20090254930") or ("20090257591") or ("20090265278") or ("20090299963") or ("20090307078") or ("20090327702") or ("20090328228")).PN.				
S8	0	S7 and ((DRM same ((many multi) near4 devices)) same (email$3 with authenticat$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 15:06
S9	0	S7 and ((DRM same ((many multi) near4 devices)) same (token))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 15:07
S10	3	S7 and ((DRM same ((many multi) near4 devices)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 15:07
S11	2	"20090210346"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 16:01
S12	8	(brand$3 near2 request) with (token meta ajd data) same encrypted	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 16:44
S13	243	media with (interoperability inter-operability inter adj operability) and ((devices networks friends famil$3) with (sharing share$1))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 16:49
S14	35	S13 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2012/05/07 16:50

			IBM_TDB			
S15	0	((drm digital adj right) with ((different various many multi$3) near3 (users clients pc hardware devices)) same (authenticat$3 with (mac device adj (identification id))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 21:52
S16	0	((drm digital adj right encrypted adj (media content)) with ((different various many multi$3) near3 (users clients pc hardware devices)) same (authenticat$3 with (mac device adj (identification id))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 21:53
S17	0	((drm digital adj right encrypted adj (media content)) same ((different various many multi$3) near3 (users clients pc hardware devices)) same (authenticat$3 with (mac device adj (identification id))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 21:53
S18	1	((drm digital adj right encrypted adj (media content)) same ((different various many multi$3 shar$3) with (users clients pc hardware devices)) same (authenticat$3 with (mac device adj (identification id))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/07 21:54
S19	11	((drm digital adj right encrypted adj (media content)) and (brand$3 near3 request$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 10:05
S20	0	(((control$4 access$3 monitor$3) with (encrypted adj (media content))) same ((different various many multi$3 shar$3) with (users clients pc hardware devices)) same (authenticat$3 with (mac device adj (identification id)))).ab,bsum.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 10:52
S21	80	(((control$4 access$3 monitor$3) with (encrypted adj (media content))) same ((different various many multi$3 shar$3) with (users clients pc hardware devices))).ab,bsum.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 10:53
S22	3	S21 and (authenticat$3 with (mac device adj (identification id)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 10:53
S23	5	S21 and (authenticat$3 with (token mac device adj (identification id)))	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2012/05/08 10:53

			EPO; JPO; DERWENT; IBM_TDB			
S24	33	S21 and (authenticat$3 same (token mac device adj (identification id)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 10:54
S25	11	(((control$4 access$3 monitor$3) with (encrypted adj (media content))) same ((different various many multi$3 shar$3) with (users clients pc hardware devices))).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 10:54
S26	5622	(((control$4 access$3 monitor$3) with ((media content))) same ((different various many multi$3 shar$3) with (users clients pc hardware devices))) and (smart adj card smartcard token)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 12:11
S27	2	(request$3 submit$4 receiv$3) same ((read$3 writ$3) with (meta$4) with encrypt$3 near3 (media content)) and ((digital adj right drm) same (shar$3 interoperable interoperability inter adj operable inter adj operability))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 13:24
S28	14	(request$3 submit$4 receiv$3) same ((read$3 writ$3) with (meta$4) with (media content)) and ((digital adj right drm) same (shar$3 interoperable interoperability inter adj operable inter adj operability))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 13:25
S29	2	S28 and (token smartcard smart adj card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 13:25
S30	60	(("7266839") or ("7567987") or ("20070266095") or ("20090100060") or ("20070010334") or ("20060036554") or ("7634734") or ("20080111052") or ("20030018491") or ("7610630") or ("7689823") or ("7702592") or ("7515710") or ("6799165") or ("6385596") or ("5907617") or ("5903647") or ("5887060") or ("5883955") or ("5870543") or ("5883954") or ("7290699") or ("7340769") or ("7343014") or ("7386513") or ("7571328") or ("7624417") or ("20020010759") or ("20020157002") or	US-PGPUB; USPAT	OR	OFF	2012/05/08 15:27

		("20040024670") or ("20040062400") or ("20040162786") or ("20040220878") or ("20050066353") or ("20050182727") or ("20060173787") or ("20060173789") or ("20060259652") or ("20060259982") or ("20070055887") or ("20070156719") or ("20070179854") or ("20070180485") or ("20070250445") or ("20080027869") or ("20080091606") or ("20080109911") or ("20080165956") or ("20090012805") or ("20090049556") or ("20090083541") or ("20090183010") or ("20090217036") or ("20090254930") or ("20090257591") or ("20090265278") or ("20090299963") or ("20090307078") or ("20090327702") or ("20090328228")).PN.				
S31	41	S30 and (token smartcard smart adj card sim subscriber adj identity adj module)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 15:27
S32	15	S31 and meta$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 15:28
S33	0	S32 and (writ$3 overwrit$3 wrote) with meta$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 15:51
S34	1488	(drm rights management digital adj (media content)) same (writ$3 overwrit$3 wrote) with meta$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 15:52
S35	127	S34 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR;	OR	OFF	2012/05/08 15:53

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S36	41	S35 and (token smartcard smart adj card sim subscriber adj identity adj module)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 15:53
S37	2	"20100131346"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/08 16:46
S38	5	"2005065891"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:13
S39	2	"20050065891"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:13
S40	3	"20060277598"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:25
S41	60	(("7266839") or ("7567987") or ("20070266095") or ("20090100060") or ("20070010334") or ("20060036554") or ("7634734") or ("20080111052") or ("20030018491") or ("7610630") or ("7689823") or ("7702592") or ("7515710") or ("6799165") or ("6385596") or ("5907617") or ("5903647") or ("5887060") or ("5883955") or ("5870543") or ("5883954") or ("7290699") or ("7340769") or ("7343014") or ("7386513") or ("7571328") or ("7624417") or ("20020010759") or ("20020157002") or ("20040024670") or ("20040062400") or ("20040162786") or ("20040220878") or ("20050066353") or ("20050182727") or	US-PGPUB; USPAT	OR	OFF	2012/05/09 10:53

		("20060173787") or ("20060173789") or ("20060259652") or ("20060259982") or ("20070055887") or ("20070156719") or ("20070179854") or ("20070180485") or ("20070250445") or ("20080027869") or ("20080091606") or ("20080109911") or ("20080165956") or ("20090012805") or ("20090049556") or ("20090083541") or ("20090183010") or ("20090217036") or ("20090254930") or ("20090257591") or ("20090265278") or ("20090299963") or ("20090307078") or ("20090327702") or ("20090328228")).PN.				
S42	41	S41 and (key adj fob token smartcard smart adj card sim subscriber adj identity adj module)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:53
S43	1491	(drm rights management (encrypt$3 digital) adj (media content)) same (writ$3 overwrit$3 wrote) with meta$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:54
S44	282	S43 and (request$3 log$4) with (key fob token smart adj card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:54
S45	57	S44 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:55
S46	1713	(drm digital ajd right$1 rights adj management (encrypt$3 digital) adj (media content)) same (writ$3 overwrit$3 wrote) with meta$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:58
S47	186	S46 and (request$3 log$4) with (key fob token smart adj card)	US-PGPUB; USPAT;	OR	OFF	2012/05/09 10:58

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S48	44	S47 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:58
S49	178	(drm digital adj right$1 rights adj management (encrypt$3 digital) adj (media content)) same (writ$3 overwrit$3 wrote) with meta$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:59
S50	91	S49 and (request$3 log$4) with (key fob token smart adj card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:59
S51	28	S50 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 10:59
S52	14884	(drm digital adj right$1 rights adj management (encrypt$3 digital) adj (media content)) same (key fob token smart adj card)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:08
S53	4816	S52 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:08
S54	1872	S52 and 713/155-159,168,172-176,182,189.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:10
S55	424	S54 and ((all various every plural$4 many multi$3 diffferent) adj2 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:11

S56	74	S55 and (application adj interface api)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:11
S57	1198	S53 and ((all various every plural$4 many multi$3 diffferent) adj2 devices)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:41
S58	66	S57 and ((read$3 writ$3 updat$) with meta$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 11:42
S59	43	((request$3 permission ask$3 query$3) with (read writ$3 updat$3 modif$3) with meta$4) same (drm digital adj right$1 media adj content encrypted adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 12:42
S60	0	S59 and (authenticat$3 verif$3 verification) with (token smart adj card fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 12:43
S61	2	S59 and (token smart adj card fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 12:44
S62	2	S59 and 713/155-159,168,172-176,182,189.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 12:46
S63	92781	26and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 12:49
S64	5	S59 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2012/05/09 12:49

			DERWENT; IBM_TDB			
S65	2	S59 and (user adj key token smart adj card fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 13:01
S66	66	((request$3 permission ask$3 query$3 permit$4 allow$3) with (read writ$3 updat$3 modif$3) with meta$4) same (drm digital adj right$1 media adj content encrypted adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 13:02
S67	70235	"36" and (user adj key token smart adj card fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 13:03
S68	4	S66 and (user adj key token smart adj card fob)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 13:03
S69	0	((web near3 account) same ((two adj way) exchange) with authenticat$3) same (drm digital adj right$1 media adj content encrypted adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 17:11
S70	8731	((web near3 account) same (((two adj way) exchange) with authenticat$3) key ajd exchange ake) same (drm digital adj right$1 media adj content encrypted adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 17:15
S71	185	((web near3 account) same (((two adj way) exchange) with authenticat$3) key adj exchange ake) same (drm digital adj right$1 media adj content encrypted adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 17:15
S72	62	S71 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 17:16
S73	5	S72 and (api application adj interface)	US-PGPUB; USPAT; USOCR;	OR	OFF	2012/05/09 17:17

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S74	12	(web adj (service account) with (key data) near2 exchange) and (DRm digital adj right$1 encrypted adj (media content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 17:34
S75	2	(web adj (service account) with (key data) near2 exchange) same (verifi$3 verification) and (DRm digital adj right$1 encrypted adj (media content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 18:26
S76	2	(web adj (service account) same (key data) near2 exchange) same (verifi$3 verification) and (DRm digital adj right$1 encrypted adj (media content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 18:26
S77	44	(web adj (service account) same (key data) near2 exchange) same (verifi$3 verification authenticat$3 authentication)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 22:27
S78	14	S77 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/09 22:27
S79	2139	(id identificaTION identif$3) with (account$1) and (drm digital adj right$1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:15
S80	479	S79 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:15
S81	134	S80 and (ike ake key adj exchang$3 data adj exchang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:16
S82	58	S80 and (ike ake key adj	US-PGPUB;	OR	OFF	2012/05/13

		exchang$3)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			20:16
S83	3285241	(user client) near4 customiz$3 modif$3 (display screen panel) same (encrypted adj2 (digital media))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:18
S84	2	(user client) near4 (customiz$3 modif$3) with (display screen panel) same (encrypted adj2 (digital media))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:19
S85	36294	(user client) near4 (customiz$3 modif$3) same (display screen panel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:20
S86	17102	(user client) near4 (customiz$3 modif$3) with (display screen panel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:20
S87	622	S86 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:21
S88	16	S87 and (drm digital adj right)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:21
S89	114	S87 and 713/155-159,168,172-176,182,189.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 20:56
S90	11	S89 and (encrypted adj2 (digital media))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	OFF	2012/05/13 20:57

			IBM_TDB			
S91	140	S87 and 726/22-32.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 21:19
S92	12	S91 and (encrypted adj2 (digital media))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 21:19
S93	250	S87 and 726/7-32.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 21:22
S94	15	S93 and (encrypted adj2 (digital media))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 21:23
S95	3	S94 not S92	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 21:23
S96	2	"20100100899"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/13 21:46
S97	17102	(user client) near4 (customiz$3 modif$3) with (display screen panel)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/14 11:29
S98	622	S97 and ("713" "726").clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/14 11:29
S99	250	S98 and 726/7-32.ccls.	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2012/05/14 11:29

			EPO; JPO; DERWENT; IBM_TDB			
S100	30	S99 and (encrypted adj2 (digital media) digital adj (media content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/14 11:29
S101	53	S98 and (encrypted adj2 (digital media) digital adj (media content))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/14 11:35
S102	8	(updat$3 read$3 writ$3 modif$3) with brand$3 with (meta metadata meta-data).ab,clm,ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/17 10:54
S103	2	"7526650"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/05/21 13:47
S104	15144386	"20120030291" "20120124612" "20120124613" "20120124611" "20120124614" "20120124610" "7" "20120124678"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/01 12:55
S105	14	"20120030291" "20120124612" "20120124613" "20120124611" "20120124614" "20120124610" "20120124678"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/01 12:56
S106	17	(digital adj media with (sharing interoperability)) same (cloud vendors universal)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/01 15:21
S107	43	(digital adj media with (sharing interoperability)) same (metadata meta-data meta adj data)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/01 15:25
S108	154	(writ$3 request modif$3) with (metadata meta-data meta adj data)	US-PGPUB; USPAT;	OR	OFF	2012/10/01 15:45

		same (digital adj media)	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S109	2	S108 and ((digital adj media same(sharing interoperability)) same (cloud vendors universal))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/01 15:46
S110	8	(((writ$3 request modif$3 add$3 attach$3) near4 (membership identity right authorization authorized ID)) with (metadata meta-data meta adj data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/02 10:35
S111	79	(((writ$3 request modif$3 add$3 attach$3 read$3 includ$3) with (verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/02 11:07
S112	71	S111 not S110	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/02 11:07
S113	19	S112 and unlimit$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/02 11:31
S114	0	S112 and interoperabilty	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/02 11:56
S115	10	(((shar$3 device adj (id identification) address mac password serial key) with (token verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/02 15:34
S116	1	"12982378"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/10/03 17:05

S117	0	"20100100899" and (right$1 with meta)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/10/30 21:42
S118	1	"20100100899" and (right$1 with metadata)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/10/30 21:43
S120	1	"20110288946" and (key$1 with metadata)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/10/31 15:29
S121	1	"61307196"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/11/05 10:26
S122	154	(writ$3 request modif$3) with (metadata meta-data meta adj data) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/14 17:55
S123	82	(((writ$3 request modif$3 add$3 attach$3 read$3 includ$3) with (verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/14 17:57
S124	3	(identifier with (cross-referenc$3 cross) with token) and (digital adj (media content) DRM)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/15 15:56
S125	19452	((device$1 right$1 near object$1) with (identification identif$4)) same shar$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 12:33
S126	8704	((device$1 right$1 near object$1) with (identification identif$4)) with shar$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2013/01/16 12:34

			DERWENT; IBM_TDB			
S127	5292	((device$1 right$1 near object$1) near5 (identification identif$4)) with shar$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 12:34
S128	3921	((device$1 right$1 near object$1) near3 (identification identif$4)) with shar$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 12:34
S129	292	S128 and "726".clas.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 12:34
S130	174	S128 and 726/7-32.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 12:35
S131	19	(((shar$3 device adj (id identification) address mac password serial key) with (token verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/16 12:40
S132	10	(((shar$3 device adj (id identification) address mac password serial key) with (token verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data)) same (digital adj media)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 12:52
S133	9	S131 not S132	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/16 12:52
S134	3	"7526650"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/16 14:49
S135	31	(((shar$3 device adj (id identification) address mac password serial key) with (token verification	US-PGPUB; USPAT; USOCR;	OR	ON	2013/01/17 14:42

		verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data)) same (digital adj media right adj object)	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S136	3	"20060161635"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/17 14:43
S137	3	"20020107803"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2013/01/17 14:43
S143	18	(authenticat$3 with token) and (token adj database) and (API same token same database) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/08/28 14:01
S145	3	"8533860" .pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/29 11:55
S146	14	"8402555".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/08/29 12:27
S147	0	"13888051"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/09/01 22:08
S148	1	(authenticat$3 with token) and (token adj database) and ((API near5 session) with (id identificer key query data)) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/09/01 22:27
S149	0	(authenticat$3 with token) and (token adj database) and ((API near5 communication) with (id identificer key query data)) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/09/01 22:30

S150	12	(authenticat$3 with token) and (token adj database) and ((API near5 communication) same (id identificer key query data)) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2014/09/01 22:30
S152	36	"8402555"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/02 15:36
S153	3	"8533860".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2014/09/02 15:51

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L6	62	"l1" and (726/28-29 713/185).ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/09/04 17:35
L7	309	(((writ$3 request modif$3 add$3 attach$3 read$3 includ$3) with (verification verif$4 membership identity right authorization authorized ID)) with (metadata metadata meta adj data data)) same (digital adj media)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/09/04 17:35
L8	19	l7 and (726/28-29 713/185).ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/09/04 17:36
S2	0	"13397517"	US-PGPUB; USPAT; UPAD	OR	OFF	2012/05/06 22:08
S119	1	"13397517"	US-PGPUB; USPAT; UPAD	OR	OFF	2012/10/31 12:15
S138	0	((brand$3 read$3 writ$3) near3 (request$3 inquir$4) with (metadazta meta-data meta adj data) same (encrypted adj2 (media content) DRM digital adj right object adj right)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/01/22 11:59
S139	3	((brand$3 read$3 writ$3) near3 (request$3 inquir$4) with (metadata meta-data meta adj data) same (encrypted adj2 (media content) DRM digital adj right object adj right)).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/01/22 11:59
S140	224	((brand$3 read$3 writ$3) near3 (request$3 inquir$4) with (metadata meta-data meta adj data) same (encrypted adj2 (media content) DRM digital adj right object adj right data	US-PGPUB; USPAT; UPAD	OR	ON	2013/05/15 16:03

		srouce)).clm.				
S141	0	((brand$3 read$3 writ$3) near3 (request$3 inquir$4) with (metadata meta-data meta adj data) same (encrypted adj2 (media content) DRM digital adj right object adj right data srouce) and authentixat$3).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/05/15 16:05
S142	9	((brand$3 read$3 writ$3) near3 (request$3 inquir$4) with (metadata meta-data meta adj data) same (encrypted adj2 (media content) DRM digital adj right object adj right data srouce) and authenticat$3).clm.	US-PGPUB; USPAT; UPAD	OR	ON	2013/05/15 16:05
S144	18	(authenticat$3 with token) and (token adj database) and (API same token same database) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; UPAD	OR	ON	2014/08/28 14:51
S151	0	"13888051"	US-PGPUB; USPAT; UPAD	OR	ON	2014/09/01 22:08
S154	21	(authenticat$3 with (password identfier ID token)) and ((token authenticat$3) near2 database) and ((API near5 communication) same (id identificer key query data)) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; UPAD	OR	ON	2014/09/04 11:30
S155	13	S154 AND ((H04L9/3234 OR H04L63/0853 OR H04L2209/603 OR H04L63/126 OR H04L67/02 OR H04L63/083 OR H04L9/0866 OR H04L9/321 OR H04L2463/101).CPC.)	US-PGPUB; USPAT; UPAD	OR	ON	2014/09/04 11:49
S156	0	(authenticat$3 same ((facebook amazone tweeter paypal google) near3 API)) and (token adj database) and ((API near5 session) with (id identificer key query data)) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; UPAD	OR	ON	2014/09/04 11:55
S157	0	(authenticat$3 same ((facebook amazone tweeter paypal google) same API)) and (token adj database) and ((API near5 session) with (id identificer key query data)) and (authoriz$6 same token same (reference ID identifier))	US-PGPUB; USPAT; UPAD	OR	ON	2014/09/04 13:37

9/4/2014 5:37:09 PM
C:\Users\ttran14\Documents\EAST\Workspaces\13888051.wsp

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

70984 7590 09/19/2014
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/888,051	05/06/2013	William Grecia		2314

TITLE OF INVENTION: DIGITAL CLOUD ACCESS (PDMAS PART III)

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$960	$0	$0	$960	12/19/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAN, TRI MINH	2494	726-029000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /william grecia/ Date 9/19/2014
Typed or printed name William Grecia Registration No. 70984

EWS-004488

Electronic Patent Application Fee Transmittal

Application Number:	13888051
Filing Date:	06-May-2013
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Filer:	William Grecia
Attorney Docket Number:	

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	960	960
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**960**

Electronic Acknowledgement Receipt

EFS ID:	20184520
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	19-SEP-2014
Filing Date:	06-MAY-2013
Time Stamp:	00:25:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$960
RAM confirmation Number	7354
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Issue Fee Payment (PTO-85B)	13888051pay.pdf	1885264 927d1ed3b8744a26be7868187c46c1a2e4ac8467	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29969 d5461d786cd7939f884f7ec7a71f9cf0c2f5ac4f	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	1915233	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PLUS Search Results for S/N 13888051, Searched Wed Aug 06 15:14:24 EDT 2014

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5864155 99
8094825 99
8489509 99
8713316 99
20050265555 99
20070275740 99
20090116646 99
20120233019 99
20120260163 99
20130151851 99
20140143547 99
4275356 74
20070218837 74
20070299780 74
20080015888 74
20080065548 74
20080077612 74
20130007894 74
7477749 69
7509421 69
7509685 69
7512986 69
7567846 69
7580894 69
7590863 69
7716330 69
7756281 69
7885633 69
7920702 69
7987140 69
7991092 69
7996486 69
8082350 69
7885633 69
7920702 69
7987140 69
7991092 69
7996486 69
8082350 69
8095991 69
8105165 69
8140049 69
8165304 69
8180936 69
8185959 69
8194859 69
8201260 69
8214067 69
8218767 69

PLUS Search Results for S/N 13888051, Searched Wed Aug 06 15:14:24 EDT 2014

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5864155 99
8094825 99
8489509 99
8713316 99
20050265555 99
20070275740 99
20090116646 99
20120233019 99
20120260163 99
20130151851 99
20140143547 99
4275356 74
20070218837 74
20070299780 74
20080015888 74
20080065548 74
20080077612 74
20130007894 74
7477749 69
7509421 69
7509685 69
7512986 69
7567846 69
7580894 69
7590863 69
7716330 69
7756281 69
7885633 69
7920702 69
7987140 69
7991092 69
7996486 69
8082350 69
7885633 69
7920702 69
7987140 69
7991092 69
7996486 69
8082350 69
8095991 69
8105165 69
8140049 69
8165304 69
8180936 69
8185959 69
8194859 69
8201260 69
8214067 69
8218767 69

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	William		Grecia	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Downingtown	State/Province	PA	Country of Residence	US

Mailing Address of Inventor:

Address 1	2885 Sanford Ave SW #13208		
Address 2			
City	Grandville	**State/Province**	MI
Postal Code	49418	**Country**	USA

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	70984		
Email Address	sa.cs2cd@gmail.com	Add Email	Remove Email
Email Address	cs2cd@yahoo.com	Add Email	Remove Email

Application Information:

Title of the Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)		
Attorney Docket Number		**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	**Suggested Figure for Publication (if any)**	3

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☒ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	70984		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13740086	2013-05-06
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13740086	Continuation of	13397517	2013-01-11	8533860	2013-09-10

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13397517	Continuation of	12985351	2012-02-15	8402555	2013-03-19

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12985351	Continuation of	12728218	2011-01-06

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12728218			2010-03-21

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date o f filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Mailing Address Information For Applicant:			
Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City		**State/Province**	
Country		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications.					
Signature	/william grecia/			Date (YYYY-MM-DD)	2014-07-22
First Name	William	Last Name	Grecia	Registration Number	70984
Additional Signature may be generated within this form by selecting the Add button.					

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent C o o p eration Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	19747885
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	31-JUL-2014
Filing Date:	06-MAY-2013
Time Stamp:	20:02:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	aia0014correct2Uf.pdf	235903 cde2ed995175955ff686e412b618ab8933e8dbe0	no	7

Warnings:	
Information:	

This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	235903

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	13888051
Filing Date	06-May-2013
First Named Inventor	William Grecia
Attorney Docket Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
William Grecia	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8402555

8533860

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

○ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number _____

◉ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/william grecia/
Name	William Grecia

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	13888051
Filing Date:	06-May-2013
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Filer:	William Grecia
Attorney Docket Number:	

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or Terminal Disclaimer	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 13888051

Filing Date: 06-May-2013

Applicant/Patent under Reexamination: Grecia et al.

Electronic Terminal Disclaimer filed on July 31, 2014

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	19747907
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	31-JUL-2014
Filing Date:	06-MAY-2013
Time Stamp:	20:08:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$160
RAM confirmation Number	6262
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33295 2ed65edff9b0c985bbe6f33331fd91ca538d50e1	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	29753 36e4c052e106d4adc9d9595470f250bfaf4d7bef	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	63048	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

37 CFR 1.78 Application Data Sheet (Corrected)

Applicant submits a corrected Application Data Sheet.

Applicant requests a corrected filing receipt reflecting the continuation status of this application.

Respectfully Requested

/William Grecia/
William Grecia
Applicant Pro Se

Electronic Acknowledgement Receipt

EFS ID:	19646985
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	22-JUL-2014
Filing Date:	06-MAY-2013
Time Stamp:	14:35:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	aia0014corr888.pdf	1566168 6f4f33c1d2bb92949e02ce47abb6523fdc5f4578	no	7

Warnings:	
Information:	

2	Miscellaneous Incoming Letter	correctads.pdf	192445 849ff6ea811ba64fb425d7b8046a5537c3bbebfc	no	1

Warnings:	
Information:	
Total Files Size (in bytes):	1758613

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	William		Grecia	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Downingtown	State/Province	PA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	2885 Sanford Ave SW #13208		
Address 2			
City	Grandville	State/Province	MI
Postal Code	49418	Country i	

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	70984		
Email Address	sa.cs2cd@gmail.com	Add Email	Remove Email
Email Address	cs2cd@yahoo.com	Add Email	Remove Email

Application Information:

Title of the Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)		
Attorney Docket Number		Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	3

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	70984		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	13740086	2013-05-06
Prior Application Status	Patented		Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13740086	Continuation of	13397517	2013-01-11	8533860	2013-09-10

EWS-004515

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13397517	Continuation of	12985351	2012-02-15	8402555	2013-03-19

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12985351	Continuation of	12728218	2011-01-06

Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
12728218			2010-03-21

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code [i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◯ Assignee	◯ Legal Representative under 35 U.S.C. 117	◯ Joint Inventor
◯ Person to whom the inventor is obligated to assign.	◯ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Mailing Address Information:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/william grecia/			Date (YYYY-MM-DD)	2014-07-22
First Name	William	Last Name	Grecia	Registration Number	70984
Additional Signature may be generated within this form by selecting the Add button. Add					

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EWS-004520

Notification of Loss of Small Entity Status

Applicant on July 10, 2014 signed a licensing agreement with an entity that would not qualify for Small Entity Status, thus passing through the non-qualification as per PTO rules. Applicant will pay full entity fees from this said date of entity change.

Respectfully

/William Grecia/
William Grecia
Applicant Pro Se

Electronic Acknowledgement Receipt

EFS ID:	19591951
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	16-JUL-2014
Filing Date:	06-MAY-2013
Time Stamp:	10:43:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Notification of loss of entitlement to small entity status	lossentity.pdf	194206 d5b36f31cf5ca009e896c0755208cc8fc278ae0f	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	194206

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/888,051	05/06/2013	William Grecia	

CONFIRMATION NO. 2314

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

EARLY PUBLICATION REQUEST LETTER

OC000000069342989

Date Mailed: 07/02/2014

NOTICE REGARDING EARLY PUBLICATION REQUEST

The request for voluntary publication, amended publication, early publication, redacted publication, republication, corrected publication or revised publication has been received for this application. The request, including payment of any necessary fee(s), is in compliance with 37 CFR 1.215, 1.217, 1.219 or 1.221.

The projected publication date is 10/09/2014.

/byemane/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

37 C.F.R. 1.219 Early Publication Request

Applicant request early publication of this application. No fee is required to accompany this request.

Respectfully Requested

/William Grecia/
William Grecia
Applicant Pro Se

Electronic Acknowledgement Receipt

EFS ID:	19444570
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	28-JUN-2014
Filing Date:	06-MAY-2013
Time Stamp:	08:40:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Early Publication	earlypubrequest.pdf	192305 5e01c87041ffd57bf3d7023312568aada7e858fb	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	192305

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

William Grecia

Application No.: 13/888,051

Filed: May 6, 2013

For: DIGITAL CLOUD ACCESS

(PDMAS PART III)

Examiner: N/A

Art Unit: N/A

CNF# 2314

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents

P. O. Box 1450

Alexandria VA, 22313-1450

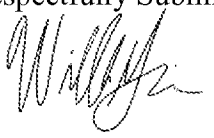
Sir:

This is a preliminary amendment to the claims. No further fees are required for this preliminary amendment as known to the applicant.

IN THE CLAIMS:

Please amend all claims as labeled. The submitted claim in this application shall replace all previously submitted versions.

Respectfully Submitted



William Grecia

Applicant Pro Se

CLAIMS

1-15 (CANCELED)

16. (NEW) A process for transforming a user access request for cloud digital content into a computer readable authorization object, the process for transforming comprising:

a) receiving an access request for cloud digital content through an apparatus in process with at least one CPU, the access request being a write request to a data store, wherein the data store is at least one of:

a memory connected to the at least one CPU;

a storage connected to the at least one CPU; and

a database connected to the at least one CPU through the Internet; wherein

the access request further comprises verification data provided by at least one user, wherein the verification data is recognized by the apparatus as a verification token; then

b) authenticating the verification token of (a) using a database recognized by the apparatus of (a) as a verification token database; then

c) establishing an API communication between the apparatus of (a) and a database apparatus, the database apparatus being a different database from the verification token database of (b), wherein establishing the API communication requires a credential assigned to the apparatus of (a), wherein the apparatus assigned credential is recognized as a permission to conduct a data exchange session between the apparatus of (a) and the database apparatus, the data exchange session capable of an exchange of query data; then

d) requesting the query data from the API communication data exchange session of (c), wherein the query data comprises at least one of:

a reference;

an ID; and

an identifier; then

e) receiving the query data requested in (d) from the API communication data exchange session of (c); then

f) creating a computer readable authorization object by writing into the data store of (a) at least one of:

the received verification token of (a); and

the received query data of (e); wherein

the created computer readable authorization object is recognized by the apparatus of (a) as user access rights associated to the cloud digital content, wherein the computer readable authorization object is available for processing by a plurality of CPUs using a cross-referencing action to determine a user access permission to the associated cloud digital content.

Electronic Acknowledgement Receipt

EFS ID:	19433961
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	27-JUN-2014
Filing Date:	06-MAY-2013
Time Stamp:	12:50:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	PDMASIII-prelimfinal.pdf	355118 f6d4c8b1de691ad1cdd9b28b11b42c964bd827d4	no	3

Warnings:	
Information:	

Total Files Size (in bytes):	355118

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/888,051	Filing Date 05/06/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **06/27/2014**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 1	Minus	** 20	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/CORALIA BETANCOURT/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
Mr.	William		Grecia	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Brooklyn	State/Province	NY	Country of Residence [i]	US

Citizenship under 37 CFR 1.41(b) [i] US

Mailing Address of Applicant:

Address 1	2885 Sanford Ave SW		
Address 2	#13208		
City	Grandville	State/Province	MI
Postal Code	49418	Country [i]	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	70984		
Email Address	sa.cs2cd@gmail.com	Add Email	Remove Email

Application Information:

Title of the Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)		
Attorney Docket Number		Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	**Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	70984		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13740086	Continuation of	13397517	2013-01-11	8533860	2013-09-10
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13397517	Continuation of	12985351	2012-02-15	8402555	2013-03-19
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12985351	Continuation of	12728218	2011-01-06		
Prior Application Status	Abandoned				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)		
12728218			2010-03-21		

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	
	Application Number	
Title of Invention	DIGITAL CLOUD ACCESS (PDMAS PART III)	

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			(•) Yes ( ) No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Remove

Assignee 1

If the Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/william grecia/			Date (YYYY-MM-DD)	2013-08-29
First Name	William	Last Name	Grecia	Registration Number	70984

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EWS-004537

Electronic Acknowledgement Receipt

EFS ID:	16727284
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	29-AUG-2013
Filing Date:	06-MAY-2013
Time Stamp:	19:06:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	SB0014-dca.pdf	1483246 285212fa8e8256fda2cd23a05ecacd45bfaa3f17	no	4

Warnings:	
Information:	

Total Files Size (in bytes):	1483246

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Examiner: N/A
William Grecia	Art Unit: N/A
Application No.: 13/888,051	CNF# 2314
Filed: January 11, 2013 For: DIGITAL CLOUD ACCESS	**PRELIMINARY AMENDMENT**
(PDMAS PART III)	

Assistant Commissioner for Patents

P. O. Box 1450

Alexandria VA, 22313-1450

Sir:

This is a preliminary amendment to the claims. No further fees are required for this preliminary amendment as known to the applicant.

IN THE CLAIMS:

Please amend all claims labeled as (Currently Amended).

Respectfully Submitted

William Grecia

Applicant Pro Se

Claims:

1. (Currently Amended) A method for authorizing a second user to access content using a cloud system, the method comprising:

receiving, at a front-end agent connected to the cloud system, a request from a first device of a first user, wherein the request comprises a permission to provide a second user with access to content authorized for access by the first user, the front-end agent comprising a network communication with the first device and recognized second devices operated by the first user, wherein the devices are configured for the network communication with a communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is obtained from a web service, the web service capable of facilitating a two way data exchange to complete a verification process wherein the data exchange session comprises at least one identification reference, wherein the identification reference comprises one or more of a verified web service account identifier, letter, number, rights token, e-mail, password, access time, serial number, address, manufacturer identification, checksum, operating system version, browser version, credential, cookie, or key;

requesting and receiving the at least one identification reference from the at least one communications console; and

writing the identification reference into a memory.

~~receiving, at the front-end agent from the second device, a communication that the second user is authorized to access the content;~~
~~determining, at the front-end agent, whether the second user is known to the front-end agent;~~

~~in response to determining that the second user is known, identifying credentials associated with the second user; and~~

~~associating the credentials of the second user with the content;~~

2. (Original) The method of claim 1, further comprising:

identifying the first user providing the request; and

determining whether the first user is authorized to grant access to the content.

3. (Original) The method of claim 1, wherein:

the request comprises identifying information for the second user.

4. (Original) The method of claim 3, wherein the identifying information comprises at least one of:

an email address; and

a number.

5. (Original) The method of claim 1, further comprising:

an automatically created credential.

6. (Original) The method of claim 1, further comprising:

an established credential.

7. (Original) The method of claim 1, wherein authorizing further comprises:

adding the credentials to a list associated with the content.

8. (Original) The method of claim 1, wherein providing accessing information further comprises: providing a network address.

9. (Original) The method of claim 8, wherein:

at least one source exist to access the content.

10. (Currently Amended) An electronic device for controlling access to content using a cloud system, comprising a processor operative to:

establish a connection with at least one communications console, wherein the communications console is a combination of a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is obtained from a verified web service, the web service capable of facilitating a two way data exchange to complete a verification process wherein the data exchange session comprises at least one identification reference;

- request the at least one identification reference from the at least one communications console, wherein the identification reference comprises one or more of a verified web service account identifier, letter, number, rights token, e-mail, password, access time, serial number, address, manufacturer identification, checksum, operating system version, browser version, credential, cookie, or key;

- receive the at least one identification reference from the at least one communications console; and

- write the identification reference into a memory.

~~recognize a plurality of devices owned by at least a first user;~~

~~define a front-end agent in connection with the plurality of devices recognized by the at least first user;~~

~~receive, at the front-end agent, a request from a first device of the first user to allow a second user access to content;~~

~~receive from a second device a communication that the second user is authorized to access the content;~~

~~determine whether the second user is known to the front-end agent;~~

~~identify credentials associated with the second user; and~~

~~associate the credentials of the second user with the content.~~

1 1. (Currently Amended) The electronic device of claim 10, wherein the processor is further operative to:

receive a request from the second user for content access.~~; and~~

~~provide identifying information for the front-end agent in response to receiving.~~

12. (Currently Amended) The electronic device of claim 10, wherein the processor is further operative to:

handling a manually created credential or an automatically created credential.[[;]]

13. (Original) The electronic device of claim 12, wherein the processor is further operative to:

associate the credentials with access to the content using a list.

14. (Currently Amended) Non-transitory computer readable media for authorizing a second user to access content using a cloud system, comprising computer readable code recorded thereon for:

receiving, at a front-end agent connected to the cloud system, a request from a first device of a first user, wherein the request comprises a permission to provide a second user with access to content authorized for access by the first user, the front-end agent comprising a network communication with the first device and recognized second devices operated by the first user, wherein the devices are configured with a graphic user interface (GUI) and an Application Programmable Interface (API) wherein the API is obtained from a web service, the web service capable of facilitating a two way data exchange to complete a verification process wherein the data exchange session comprises at least one identification reference, wherein the identification reference comprises one or more of a verified web service account identifier, letter, number, rights token, e-mail, password, access time, serial number, address, manufacturer identification, checksum, operating system version, browser version, credential, cookie, or key;

~~receiving, at the front-end agent from the second device, a communication that the second user is authorized to access the content;~~

requesting and receiving the at least one identification reference from at least one of the GUI or the API;

determining, at the front-end agent, whether the second user is known to the front-end agent; and

~~in response to determining that the second user is known, identifying credentials associated with the second user; and~~

associating the credentials of the second user with the content by writing the at least one identification reference into a memory.

15. (Original) The non-transitory computer-readable media of claim 14, further comprising computer
readable code recorded thereon for:

handling a manually created credential or an automatically created credential.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13888051
Filing Date	2013-05-06
First Named Inventor	William Grecia
Art Unit	N/A
Examiner Name	N/A
Attorney Docket Number	

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7254235		2007-08-07	Boudreault et al.	
	2	7343014		2008-03-11	Sovio et al.	
	3	7526650		2009-04-28	Wimmer, Chris	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110288946		2011-11-24	Baiya et al.	
	2	20100100899		2010-04-22	Bradbury et al.	
	3	20050065891		2005-03-24	Lee et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13888051
	Filing Date	2013-05-06
	First Named Inventor	William Grecia
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	

	4	20080010685		2008-01-10	Holtzman et al.	
	5	20090083541		2009-03-26	Levine, Scott	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Copy of U.S. patent application #13/397,517 Notice of Allownce	☐
	2	Copy of U.S. patent application #13/740,086 Notice of Allowance	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13888051
	Filing Date	2013-05-06
	First Named Inventor	William Grecia
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13888051
	Filing Date	2013-05-06
	First Named Inventor	William Grecia
	Art Unit	N/A
	Examiner Name	N/A
	Attorney Docket Number	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/william grecia/	Date (YYYY-MM-DD)	2013-07-26
Name/Print	William Grecia	Registration Number	70984

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Attention To The Commissioner Of Patents:

INFORMATION DISCLOSURE STATEMENTS (IDS) IN ACCORDANCE WITH MPEP 609.02

This application is a continuation of 13/397,517 and subject to the complete IDS, NPL, and Examiner's prosecution history of record within 13/397,517.

/William grecia/
William Grecia
Applicant Pro Se

Electronic Acknowledgement Receipt

EFS ID:	16423943
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	26-JUL-2013
Filing Date:	06-MAY-2013
Time Stamp:	10:32:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	PDMASIII-prelimac.pdf	87324 690f1dbe6e3f94ef7df132a1b5e2e7dfbefcb b1d	no	5

Warnings:	
Information:	

2	Non Patent Literature	13740086-noa.pdf	959726 7fb14b810876381188d8247dc472fbd492bbc979	no	21
Warnings:					
Information:					
3	Non Patent Literature	13397517-noa.pdf	520026 c69c4d513b5087356cbeffa71a3ce2bde8169c0a	no	15
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	13888051_IDS.pdf	612535 d948175b57ffa497c2218276449c8110cd7c5a31	no	5
Warnings:					
Information:					
5	Transmittal Letter	ids-transmac.pdf	50498 2f7c78a397cdff4ccd32200a5791f62564696cc1	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	2230109		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/888,051

APPLICATION AS FILED - PART I

	(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE($)	FEE($)		RATE($)	FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	15 minus 20 =	*	x 40 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	730		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)					
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/888,051	05/06/2013	2447	730		15	3

CONFIRMATION NO. 2314

70984
The STR3EM Team
2885 Sanford Ave SW #13208
Grandville, MI 49418

FILING RECEIPT

Date Mailed: 06/12/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

William Grecia, Brooklyn, NY;

Applicant(s)

William Grecia, Brooklyn, NY;

Power of Attorney: None

Domestic Applications for which benefit is claimed - None.
A proper domestic benefit claim must be provided in an Application Data Sheet in order to constitute a claim for domestic benefit. See 37 CFR 1.76 and 1.78.

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 06/05/2013
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/888,051**
Projected Publication Date: 11/06/2014
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****

Title

DIGITAL CLOUD ACCESS (PDMAS PART III)

Preliminary Class

709

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 06/05/2013

MTEKLEMI RF #30127675 Mailroom Dt: 06/05/2013 13888051

Credit Card Refund Total: $70.00

Master Card XXXXXXXXXXXX5807

PTO/SB/01 (09-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☒ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	
First Named Inventor	William Grecia
COMPLETE IF KNOWN	
Application Number	
Filing Date	5/6/2013
Art Unit	2494
Examiner Name	Tran, Tri

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

DIGITAL CLOUD ACCESS – PDMAS PART III

(Title of the Invention)

the application of which was made or was authorized to be made by me and

☒ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application Number or PCT International Application Number _____ and was amended on (MM/DD/YYYY) _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☒ If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

PTO/SB/01 (09-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☒	The address associated with Customer Number:	70984	OR ☐	Correspondence address below

Name		
Address		
City	State	Zip
Country	Telephone	Email

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

NAME OF SOLE OR FIRST INVENTOR:	☐ A petition has been filed for this unsigned inventor
Given Name (first and middle [if any])	Family Name or Surname
William	Grecia
Inventor's Signature	Date
/william grecia/	5/6/2013

Residence: City	State	Country	Citizenship
Brooklyn	NY	USA	USA

Mailing Address			
2885 Sanford Ave SW #13208			
City	State	Zip	Country
Grandville	MI	49418	USA

☐ Additional inventors or a legal representative are being named on the _____ supplemental sheet(s) PTO/SB/02A or 02LR attached hereto

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/05 (08-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	
First Inventor	William Grecia
Title	DIGITAL CLOUD ACCESS – PDMAS PART
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☑ **Fee Transmittal Form** (e.g., PTO/SB/17)
2. ☑ **Applicant claims small entity status.** See 37 CFR 1.27.
3. ☑ **Specification** [*Total Pages* 29]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. ☑ **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 7]
5. **Oath or Declaration** [*Total Sheets* _____]
   a. ☑ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. – c. are required)
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. ☐ **Assignment Papers** (cover sheet & document(s))
   Name of Assignee _____
10. ☐ **37 CFR 3.73(b) Statement** *(when there is an assignee)* ☐ **Power of Attorney**
11. ☐ **English Translation Document** *(if applicable)*
12. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
13. ☐ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
    (*Should be specifically itemized)*
15. ☐ **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. ☐ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☐ Other: _____

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☑ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: 13/740,086

Prior application information: *Examiner* Tran, Tri *Art Unit:* 2494

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 70984 ***OR*** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/william grecia/	Date	5/6/2013
Name (Print/Type)	William Grecia	Registration No. (Attorney/Agent)	

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Filer:	William Grecia
Attorney Docket Number:	

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Miscellaneous-Filing:				
Processing Fee, Except for Provis. Apps	2053	1	70	70
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**800**

Electronic Acknowledgement Receipt

EFS ID:	15703806
Application Number:	13888051
International Application Number:	
Confirmation Number:	2314
Title of Invention:	DIGITAL CLOUD ACCESS (PDMAS PART III)
First Named Inventor/Applicant Name:	William Grecia
Customer Number:	70984
Filer:	William Grecia
Filer Authorized By:	
Attorney Docket Number:	
Receipt Date:	06-MAY-2013
Filing Date:	
Time Stamp:	17:34:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$800
RAM confirmation Number	5562
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

EWS-004566

1		PDMAS-III-revb.pdf	173307 eba5bdb1b52a603831129e892ffb6b898fcae198	yes	29

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Specification	1	25
Specification	26	28
Specification	29	29

Warnings:					
Information:					
2	Drawings-only black and white line drawings	drawings.pdf	128103 a03db35d6454a9c9e1e059a3dd2115d80afdf9a0	no	7
Warnings:					
Information:					
3	Oath or Declaration filed	PDMAS-III-oath.pdf	128764 5eeeec34e401374d5e2e55d9074de41a47f3e33b	no	4
Warnings:					
Information:					
4	Transmittal Letter	PDMAS-III-trans.pdf	279840 c9430fe7ff36511ddd5ea6dbe0cdd9f67214d112	no	2
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	36207 dc2027f0fb22edd884dd80b722d5bc1792382f34	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	746221		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

TITLE

DIGITAL CLOUD ACCESS (PDMAS PART III)

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of and claims the priority benefit of US patent application co-pending serial number 13/740,086 filed January 11, 2013 which is a continuation of and claims the priority benefit of 13/397,517 filed February 15, 2012 now issued as U.S. patent 8,402,555 on March 19, 2013 which is a continuation of and claimed the priority benefit of 12/985,351 filed January 6, 2011 which was a continuation of and claimed the priority benefit of US patent application serial number 12/728,218 filed March 21, 2010, which are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to the field of digital rights management schemes used by creators of electronic products to protect commercial intellectual property copyrights privy to illegal copying using computerized devices. More specifically, the present invention teaches a more personal system of digital rights management which employs electronic ID, as part of a web service membership, to manage access rights across a plurality of devices.

[0004] 2. Description of the Prior Art

[0005] Digital rights management (DRM) is a generic term for access control technologies used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content across devices. DRM refers to any technology that inhibits undesirable or illegal uses of the digital content. The term generally doesn't refer to forms of copy protection that can be circumvented without modifying the file or device, such as serial numbers or key files. It can also refer to restrictions associated with specific instances of digital works or devices.

[0006] Traditional DRM schemes are defined as authentication components added to digital files that have been encrypted from public access. Encryption schemes are not DRM methods but DRM systems are implemented to use an additional layer of authentication in which permission is granted for access to the cipher key required to decrypt files for access. A computer server is established to host decryption keys and to accept authentication keys from Internet connected client computers running client software in which handles the encrypted files. The server can administer different authorization keys back to the client computer that can grant different sets of rules and a time frame granted before the client is required to connect with the server to reauthorize access permissions. In some cases content can terminate access after a set amount of time, or the process can break if the provider of the DRM server ever ceases to offer services.

[0007] In the present scenario, consumer entertainment industries are in the transition of delivering products on physical media such as CD and DVD to Internet delivered systems. The Compact Disc, introduced to the public in 1982, was initially designed as a proprietary system offering strict media to player compatibility. As the popularity of home computers and CD-ROM drives rose, so did the availability of CD ripping applications to make local copies of music to be enjoyed without the use of the disc. After a while, users found ways to share digital versions of music in the form of MP3 files that could be easily shared with family and friends over the Internet. The DVD format introduced in 1997 included a new apparatus for optical discs technology with embedded copy protection schemes also recognized as an early form of DRM. With internet delivered music and video files, DRM schemes has been developed to lock acquired media to specific machines and most times limiting playback rights to a single machine or among a limited number of multiple machines regardless of the model number. This was achieved by writing the machine device ID to the metadata of the media file, then cross referencing with a trusted clearinghouse according to

pre-set rules. DRM systems employed by DVD and CD technologies consisted of scrambling (also known as encryption) disc sectors in a pattern to which hardware developed to unscramble (also known as decryption) the disc sectors are required for playback. DRM systems built into operating systems such as Microsoft Windows Vista block viewing of media when an unsigned software application is running to prevent unauthorized copying of a media asset during playback. DRM used in computer games such as SecuROM and Steam are used to limit the amount of times a user can install a game on a machine. DRM schemes for e-books include embedding credit card information and other personal information inside the metadata area of a delivered file format and restricting the compatibility of the file with a limited number of reader devices and computer applications.

[0008] In a typical DRM system, a product is encrypted using Symmetric block ciphers such as DES and AES to provide high levels of security. Ciphers known as asymmetric or public key/private key systems are used to manage access to encrypted products. In asymmetric systems the key used to encrypt a product is not the same as that used to decrypt it. If a product has been encrypted using one key of a pair it cannot be decrypted even by someone else who has that key. Only the matching key of the pair can be used for decryption. After receiving an authorization token from a first-use action are usually triggers to decrypt block ciphers in most DRM systems. User rights and restrictions are established during this first-use action with the corresponding hosting device of a DRM protected product.

[0009] Examples of such prior DRM art include Hurtado (U.S. Pat. No. 6,611,812) who described a digital rights management system, where upon request to access digital content, encryption and decryption keys are exchanged and managed via an authenticity clearing house. Other examples include Alve (U.S. Pat. No. 7,568,111) who teaches a DRM and Tuoriniemi (U.S. Pat. No. 20090164776) who described a management scheme to control

access to electronic content by recording use across a plurality of trustworthy devices that has been granted permission to work within the scheme.

[00010] Recently, DRM schemes have proven unpopular with consumers and rights organizations that oppose the complications with compatibility across machines manufactured by different companies. Reasons given to DRM opposition range from limited device playback restrictions to the loss of fair-use which defines the freedom to share media products will family members.

[00011] Prior art DRM methods rely on content providers to maintain computer servers to receive and send session authorization keys to client computers with an Internet connection. Usually rights are given from the server for an amount of time or amount of access actions before a requirement to reconnect with the server is required for reauthorization. At times, content providers will discontinue servers or even go out of business some years after DRM encrypted content was sold to consumers causing the ability to access files to terminate.

[00012] In the light of the foregoing discussion, the current states of DRM measures are not satisfactory because unavoidable issues can arise such as hardware failure or property theft that could lead to a paying customer loosing the right to recover purchased products. The current metadata writable DRM measures do not offer a way to provide unlimited interoperability between different machines. Therefore, a solution is needed to give consumers the unlimited interoperability between devices and "fair use" sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term return of investments.

SUMMARY OF THE INVENTION

[00013] An object of the present invention is to provide unlimited interoperability of digital media between unlimited machines with management of end-user access to the digital media.

[00014] In accordance with an embodiment of the present invention, the invention is a process of an apparatus which in accordance with an embodiment, another apparatus, tangible computer medium, or associated methods (herein referred to as The App) is used to: handle at least one branding action which could include post read and write requests of at least one writable metadata as part of at least one digital media asset to identify and manage requests from at least one excelsior enabler, and can further identify and manage requests from a plurality of connected second enablers; with at least one token and at least one electronic identification reference received from the at least one excelsior enabler utilizing at least one membership. Here, controlled by the at least one excelsior enabler, The App will proceed to receive the at least one token to verify the authenticity of the branding action and further requests; then establish at least one connection with at least one programmable communications console of the at least one membership to request and receive the at least one electronic identification reference; and could request and receive other data information from the at least one membership. The method then involves sending and receiving variable data information from The App to the at least one membership to verify a preexisting the at least one branding action of the at least one writable metadata as part of the at least one digital media asset; or to establish permission or denial to execute the at least one branding action or the post read and write requests of the at least one writable metadata. To do this, controlled by the at least one excelsior enabler. The App may establish at least one connection, which is usually through the Internet, with a programmable communications console, which is usually a combination of an API protocol and graphic user interface (GUI) as part of a web service. In addition, the at least one excelsior enabler provides reestablished

credentials to the programmable communications console as part of the at least one membership, in which The App is facilitating and monitoring, to authenticate the data communications session used to send and receive data requests between the at least one membership and The App.

[00015] In accordance with another embodiment of the present invention, the present invention teaches a method for monitoring access to an encrypted digital media and facilitating unlimited interoperability between a plurality of data processing devices. The method comprises receiving a branding request from at least one communications console of the plurality of data processing devices, the branding request being a read and write request of metadata of the encrypted digital media, the request comprising a membership verification token corresponding to the encrypted digital media. Subsequently, the membership verification token is authenticated, the authentication being performed in connection with a token database. Thereafter, connection with the at least one communications console is established. Afterwards, at least one electronic identification reference is requested from the at least one communications console. Further, the at least one electronic identification reference is received from the at least one communications console. Finally, branding metadata of the encrypted digital media is performed by writing the membership verification token and the electronic identification reference into the metadata.

[00016] The present invention is particularly useful for giving users the freedom to use products outside of the device in which the product was acquired and extend unlimited interoperability with other compatible devices.

BRIEF DESCRIPTION OF THE DRAWINGS

[00017] For a more complete understanding of the present invention, the needs satisfied thereby, and the objects, features, and advantages thereof, reference now is made to the following description taken in connection with the accompanying drawings.

[00018] FIG. 1 shows a system for monitoring access to an encrypted digital media according to an embodiment of the present invention.

[00019] FIG. 2 shows a system for authoring an encrypted digital media according to an embodiment of the present invention.

[00020] FIG. 3 shows a flow chart giving an overview of the process of digital media personalization according to an embodiment of the present invention.

[00021] FIG. 4 shows a flow chart giving an overview of the process of an access request made by an enabler according to an embodiment of the present invention.

[00022] FIG. 5 shows personalized digital rights management component as part of a compatible machine with writable static memory.

[00023] FIG.6 shows a flowchart for monitoring access to an encrypted digital media according to an embodiment of the present invention

[00024] FIG.7 shows a flowchart showing authoring an encrypted digital media according to an embodiment of the present invention.

[00025] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention

DETAILED DESCRIPTION OF THE DRAWINGS

[00026] Before describing in detail the particular system and method for personalised digital media access system in accordance with an embodiment of the present invention, it should be observed that the present invention resides primarily in combinations of system components related to the device of the present invention.

[00027] Accordingly, the system components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent

to understanding the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[00028] In this document, relational terms such as `first` and `second`, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms `comprises`, `comprising`, or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element proceeded by `comprises . . . a` does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises the element.

The present invention is directed at providing infinite access rights of legally acquired at least one encrypted digital media asset to the content acquirer, explained in this document as the excelsior enabler, and optionally to their recognized friends and family, explained in this document as a plurality of secondary enablers. To explain further, the excelsior enabler and secondary enablers defined comprises human beings or computerized mechanisms programmed to process steps of the invention as would normally be done manually by a human being. Additionally,, an apparatus used alone or in accordance with an embodiment, another apparatus, tangible computer medium, or associated methods with a connection are needed (herein referred to as The App). To deliver the requirements of the invention, communicative and connected elements comprise: verification, authentication, electronic ID metadata branding, additional technical branding, and cross-referencing. The connection handling the communicative actions of the invention will usually be the Internet

and can also be an internal apparatus cooperative. The App can further be defined as a Windows OS, Apple OS, Linux OS, and other operating systems hosting software running on a machine or device with a capable CPU, memory, and data storage. The App can be even further defined as a system on a chip (SOC), embedded silicon, flash memory, programmable circuits, cloud computing and runtimes, and other systems of automated processes.

[00029] The digital media assets used in this system are encrypted usually with an AES cipher and decryption keys are usually stored encoded, no encoded, encrypted, or no encrypted as part of the apparatus or as part of a connection usually an Internet server. As explained earlier, the system we will discuss will work as a front-end to encrypted files as an authorization agent for decrypted access.

[00030] FIG. 1 shows a system **100** for monitoring access to an encrypted digital media according to an embodiment of the present invention. The system **100** includes a first recipient module **102**, an authentication module **104**, a connection module **106**, a request module **108**, a second receipt module **110** and a branding module **112**. The first receipt module **102** receives a branding request from at least one communications console of the plurality of data processing devices. The branding request is a read and write request of metadata of the encrypted digital media and includes a membership verification token corresponding to the encrypted digital media. Examples of the encrypted digital media includes, and are not limited to, one or more of a video file, audio file, container format, document, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

[00031] Subsequently, the authentication module **104** authenticates the membership verification token. The authentication is performed in connection with a token database. Further, the connection module **106** establishes communication with the at least one communication console.

[00032] According to an embodiment of the present invention, the connection is established through one of internet, intranet, Bluetooth, VPN, Infrared and LAN.

[00033] According to another embodiment of the present invention, the communication console is a combination of an Application Programmable interface (API) protocol and graphic user interface (GUI) as a part of web service. The API is a set of routines, data structures, object classes, and /or protocols provided by libraries and / or operating system services. The API is either one of language dependent or language independent.

[00034] The request module **108** requests at least one electronic identification reference from the at least one communication console. The second receipt module **110** receives the at least one electronic identification reference from the least one communication console. The branding module **112** brands metadata of the encrypted digital media by writing the membership verification token and the electronic identification into the metadata.

[00035] **FIG. 2** shows a system **200** for authoring an encrypted digital media according to an embodiment of the present invention. The figure includes a selection module **202**, a password module **204**, a customization module **206**, a database module **208** and an encryption module **210**. The selection module **202** facilitates selection of one or more media items to form the encrypted digital media. Examples of the one or media items include, and are not limited to, one or more of a video, an audio and a game.

[00036] According to an embodiment of the present invention, the one or more media items are one or more of remote URL links and local media files.

[00037] The password module **204** prompts the user to enter a master password which provides access to the encrypted digital media. Subsequently, the customization module **206** allows the user to customize the user access panel of the encrypted digital media.

[00038] According to an embodiment of the present invention, the customization module **206** facilitates adding one or more of a banner, a logo, an image, an advertisement, a tag line, a

header message and textual information to the user access panel of the encrypted digital media.

[00039] Further, the database module **208** connects the encrypted digital media to a database of membership verification token required for decrypting the encrypted digital media.

[00040] According to an embodiment of the present invention, the membership verification token is a kodekey. The kodekey is a unique serial number assigned to the encrypted digital media.

[00041] The encryption module **210** encrypts the one or more media items to create the encrypted digital media.

[00042] According to an embodiment of the present invention, the system **200** further includes a watermark module. The watermark module watermarks information on the encrypted digital media, wherein the watermark is displayed during playback of the encrypted digital media.

[00043] According to another embodiment of the present invention, the system **200** further includes an access module. The access module allows the user to define access rights. Examples of the access rights include, but are not limited to, purchasing rights, rental rights and membership access rights.

[00044] According to yet another embodiment of the present invention, the system **200** further includes a name module. The name module allows the user to name the encrypted digital media.

[00045] **FIG. 3** shows a flow chart giving an overview of the process of digital media personalization according to an embodiment of the present invention. The process is achieved by way of an enabler using an apparatus or otherwise known as an application in which facilitates digital media files. The apparatus interacts with all communicative parts required

to fulfill the actions of the invention. The figure shows a Kodekey Graphical User Interface (GUI) **301**, a product metadata **302**, a networking card **303**, internet **304**, **306** and **308**, database **305** and **309** and an APIwebsite.com GUI **307**. A user posts a branding request via the Kodekey GUI interface **301**. The Kodekey GUI interface **301** is the GUI for entering token. The Kodekey GUI interface **301** prompts the user to enter the token and press the redeem button present on the Kodekey GUI interface **301**. The product metadata **302** is read / writable metadata associated with the digital media to be acquired. The networking card **303** facilitates querying of optional metadata branding process and referenced. The Kodekey GUI interface is connected to the database **305** via the internet **304** through the networking card **303**. The database **305** is the database used to read/write and store the tokens, also referred to as token database. The user is redirected to the APIwebsite.com GUI **307** through the internet **306**. The APIwebsite.com is the GUI to the membership API in which the electronic ID is collected and sent back to the Kodekey GUI interface **301**. The APIwebsite.com GUI **307** prompts the user to enter a login id and a password to access the digital media which is acquired from the database **309** through the internet **308**. The database **309** is the database connected to the web service membership in which the user's electronic ID is queried from.

[00046] Examples of the encrypted digital files include, and are not limited to, a video file, an audio file, container formats, documents, metadata as part of video game software and other computer based apparatus in which processed data is facilitated.

[00047] FIG. 4 shows a flow chart giving an overview of the process of an access request made by an enabler according to an embodiment of the present invention. Subsequently, the communicative parts to cross-reference information stored in the metadata of the digital media asset are checked which has been previously handled by the process of FIG. 1. The figure shows an enabler access request **401**, a product metadata **402**, a networking card **403**, an internet **404**, **406** and **408**, a database **405** and **409** and an APIwebsite.com GUI **407**, The

enabler access request **401** facilitates the user to make a request for the digital media. The product metadata **402** is read / writable metadata associated with the digital media to be acquired. The networking card **403** facilitates querying of optional metadata branding process and referenced. The database **405** is the database used to read/write and store the tokens. The APIwebsite.com GUI **407** is the GUI in which the electronic ID is collected and sent back to the Kodekey GUI interface **301.** The APIwebsite.com GUI **407** prompts the user to enter a login id and a password to access the digital media from the database **409** through the internet **408**. The database **409** is the database connected to the web service membership in which the user's electronic ID is queried from.

[00048] FIG. 5 shows personalized digital rights management component as part of a compatible machine with writable static memory. The figure represents an authorization sequence action in which a machine is authorized to accept a personalized digital media file. The figure includes STR3EM Machine GUI **501** including the connect icon **502**, a load key file icon **503**, a networking card **504**, an internet **505**, **508** and **510**, a database **506** and **511**, a machine memory **507** and a APIwebsite.com GUI **509**. The STR3EM Machine GUI **501** prompts the user to connect or load a key file to authorize the device through the connect icon **502** and the load key file icon **503**. The STR3EM Machine GUI **501** is connected to the networking card **504**. The networking card **504** facilitates querying of optional metadata branding process and referenced. Further, the STR3EM machine GUI **501** is connected to the database **506** via the internet **505**. The database **506** is the database used to read/write and store the tokens. Moreover, STR3EM Machine GUI **501** is connected to the machine memory **507**. The machine memory **507** represents the internal memory of the machine or device so authorizations can be saved for access of the digital media. The APIwebsite.com GUI **509** is connected to the STR3EM machine GUI through the internet **508**. Further, APIwebsite.com GUI **509** is connected to the database **511** through the internet **510**. The APIwebsite.com GUI

509 prompts the user to enter the login id and a password to authorize the access to digital media. The database **511** is the database connected to the web service membership in which the user's electronic ID is queried from.

[00049] FIG.6 shows a flowchart for monitoring access to an encrypted digital media according to an embodiment of the present invention. At step **602**, a branding request is made by a user from at least at least one communications console of the plurality of data processing devices. The branding request is a read and write request of metadata of the encrypted digital media.

[00050] According to an embodiment of the present invention, the request includes a membership verification token corresponding to the encrypted digital media.

[00051] Subsequently, the membership verification token is authenticated at step **604**. The authentication is performed in connection with a token database. Further, connection with the at least communication console is established at step **606**. Afterwards, at least one electronic identification reference is requested from the at least one communications console at the step **608**. At step **610**, at least one electronic identification reference in received from the at least one communication console. Finally, metadata of the encrypted digital media is branded by writing the membership verification token and the electronic identification reference into the metadata at the step **612**.

[00052] FIG.7 shows a flowchart showing authoring an encrypted digital media according to an embodiment of the present invention. At step **702**, one or more media items are selected by the user to form the encrypted digital media. Subsequently, a master password is entered for providing access to the encrypted digital media for editing at step **704**. Afterwards, the user customizes the user panel of the encrypted digital media at step **706**. Further, the encrypted digital media is connected to a database of membership verification tokens

required for decrypting the encrypted digital media at the step **708**. Finally, the one or more media items are encrypted to create the encrypted digital media at the step **710.**

[00053] According to various embodiments of the present invention, the verification is facilitated by at least one token handled by at least one excelsior enabler. Examples of the token include, and are not limited to, a structured or random password, e-mail address associated with an e-commerce payment system used to make an authorization payment, or other redeemable instruments of trade for access rights of digital media. Examples of e-commerice systems are PayPal, Amazon Payments, and other credit card services.

[00054] According to an embodiment of the present invention, an identifier for the digital media is stored in a database with another database of a list of associated tokens for cross-reference identification for verification.

[00055] According to an embodiment of the present invention, the database of a list of associated tokens includes Instant Payment Notification (IPN) received from successful financial e-commerce transactions that includes the identifier for the digital media; import of CSV password lists, and manually created reference phrases.

[00056] For this discussion, the structured or random password example will be used as reference. The structured or random passwords can be devised in encoded schemes to flag the apparatus of permission type such as: 1) Purchases can start a password sequence with "P" following a random number, so further example would be "PSJD42349MFJDF". 2) Rentals can start or end a password sequence with "R" plus (+) the number of days a rental is allowed, for example "R7" included in "R7SJDHFG58473" flagging a seven day rental. 3) Memberships can start or end a password sequence with "M" plus (+) optionally the length of months valid for example "M11DFJGH34KF" would flag an eleven-month membership period.

[00057] According to an embodiment of the present invention, the tokens are stored in a relational database such as MySQL or Oracle.. Cloud storage systems such as Amazon's Web Services Simple Storage Solution, or also known as S3, provides a highly available worldwide replicated infrastructure. In addition to S3, monetization offerings such as DevPay offer developers the opportunity to make money from applications developed to use the services.

[00058] The verification will reference to the S3 and DevPay services for example purposes only as many options such as FTP, SimpleDB, solid state storage and others can be used to host the token hosting needed for the verification element of this invention. The token represents permission from the content provider to grant access rights to the excelsior enabler and thereafter the plurality of secondary enablers. To set up the verification the content provider can manually or automatically generate a single or a plurality of structured or random password in which will represent the token. By using public or private access of S3 as part of an apparatus, the content provider can create empty text files giving each the name of the passwords generated. Because S3 is associated with a highly available worldwide infrastructure, to check this password token can be done my simply constructing a HTTP request from the apparatus and triggering follow up actions based on either a 200 HTTP response, which means OK at which point the next action can happen, or a 400 HTTP response which means ERROR at which point the verification process is voided. An additional token can be used to provide a flag to the apparatus that the verification element has been fulfilled for an initial verification token. Creating an alternate version of the first token by appending a reference to the end, for example, does this: "M11DFJGH34KF_user@str3em.com_01_01_11". In this example, it is defined that the eleven month authorized membership token was verified by a user@str3em.com on January 1, 2011. By providing a second token, the first token becomes locked to ownership by the

excelsior enabler preventing unauthorized users from reusing the first token without providing the authentication associated with the alternative referenced second token. In the interest of providers of the apparatus delivering this invention, this document will teach a method of a HTTP PUT calculation scheme for automatic royalty billing and administration for the token element used in the invention. Amazon's DevPay allow developers to attach monetary charges to data services of S3 offered as an embedded component of the apparatus. By using the "PUT" requests parameter, tokens generated by the apparatus are monitored, calculated, and charged to clients of the apparatus provider. For example: the default charge measure for DevPay is $0.05 for every 1000 PUT requests. By changing the amount to $100 for every 1000 PUT requests, the apparatus provider is paid a $0.10 royalty for each token created. Content providers using a connected apparatus like DevPay to deliver and manage digital media distribution do not need to have restrictions on the tokens created as with prior art DRM key providers as DevPay is charged on a pay-as-you-need model on a monthly basis. As a novelty to the apparatus provider, if a content provider fails to pay royalties due, the DevPay hosting will automatically deny token access to all related media products in distribution and restore this verification element when royalties are paid in full.

[00059] The authentication element of this invention is at least handled first by the at least one excelsior enabler with a connection to a membership. In the present discussion, the connection is equal to the Internet and the membership is equal to a web service. Further, the web service must be available for two way data exchange to complete the authentication process of this invention. Data exchange with a web service is usually facilitated with a programmable communications console, at most times, will be an Applications Programmable Interface (API). An API is a set of routines, data structures, object classes, and/or protocols provided by libraries and/or operating system services in order to support the building of applications. An API may be language-dependent: that is, available only in a

particular programming language, using the particular syntax and elements of the programming language to make the API convenient to use in this particular context. Alternatively an API may be language-independent: that is, written in a way that means it can be called from several programming languages (typically an assembly/C-level interface). This is a desired feature for a service-style API that is not bound to a particular process or system and is available as a remote procedure call. A more detailed description of API that can be used for an apparatus can be found in the book, "Professional Web APIs with PHP: eBay, Google, Paypal, Amazon, FedEx plus Web Feeds", by Paul Reinheimer, Wrox publishers (2006). A program apparatus, scripts, often calls these APIs or sections of code residing on user computerized devices. For example, a web browser running on a user computer, cell phone, or other device can download a section of JavaScript or other code from a web server, and then use this code to in turn interact with the API of a remote Internet server system as desired. A Graphic User Interface (GUI) can be installed for human interaction or processes can be preprogrammed in a programmable script such as PHP, ASP.Net, Java, Ruby on Rails and others. The authentication element of the invention is usually embedded as a process of the apparatus but could be linked dynamically. In this document, the embedded version using a GUI will be used as reference. The web service equipped with the API is usually a well-known membership themed application in which the users must use an authentic identification. Some example includes Facebook in which as a rule, members are required to use their legal name identities. A reference number or name with the Facebook Platform API represents this information. Other verified web services in which real member names are required such as the LinkedIn API and the PayPal API and even others could be used, but for this discussion, Facebook will be used only as an example of how the authentication element of the invention is utilized. The Facebook API system, as well as others, operates based on an access authentication system called from a connected

apparatus (which is usually an Internet powered desktop or browser based application) with an API Key, an Application Secret Key and could also include an Application ID. For example, the Facebook API Application Keys required to establish a data exchange session with the connected apparatus might look like:

API Key

37a925fc5ee9b4752af981b9a30e9a73gh

Application Secret

f2a2d92ef395cce88eb0261d4b4gsa782

Application ID

51920566446

[00060] The collective API keys are usually embedded in the source code of the apparatus, or stored on a remote Internet server, and could be included in the encrypted digital media metadata and inserted on-the-fly into calls made to the API from the connected apparatus. This allows dynamic API connection of the apparatus using keys issued to individual content providers so in the event of a reprimand of a single the individual content provider by the API provider, the collective the individual content providers and the enablers of the connected apparatus are not affected.

[00061] Upon an access request of the digital media, the excelsior enabler interacts with the apparatus, usually software or web application, to enter membership credentials in a GUI front-end connected to the API. The membership credentials are usually comprised of a login element comprising a name, phrase, or e-mail address, and a secret password. The credentials can be generated by the enabler or automatically generated by the web service. Once the enabler authenticates their identity with the membership, the apparatus facilitating the data communication can request relevant information to fulfill the process chain of the invention. For example, Facebook API Platform defines members as ID numbers, so if a member's real

name is John Doe, then Facebook API ID (also programmatically known as the FBID) would be 39485678. Once the enabler successfully sign in to the GUI element then the apparatus will query the API for at least one electronic identification reference, in this discussion is the FBID. The FBID is received to the permanent or temporary memory of the apparatus to sustain the branding and cross-referencing requirements of the invention. Additional information can be requested according to membership status or connected "friends" of the enabler. Additional information can be made required for successful authentication and includes: a minimum amount of total friends, a minimum amount of female friends, a minimum amount of male friends, a minimum amount of available pictures, a minimum age limit and other custom rules can be defined by the apparatus. An example of how this would work is a content provider can define a minimum of 32 Facebook friends are required to access an encrypted digital media asset offered for sale or promotion. This is achieved by the apparatus handling a access request in which the enabler has not yet acquired access rights by executing and parsing information returned by the Facebook "Friends.get" API command.

[00062] XML return example of the Facebook "Friends.get" API command where a plurality of FBID are returned to the apparatus for parsing additional information as may be required to satisfy successful authentication:

<?xml version="1.0" encoding="UTF-8"?>

<friends_get_response xmlns="http://api.facebook.com/1.0/"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://api.facebook.com/1.0/ http://api.facebook.com/1.0/facebook.xsd"

list="true">

<uid>222333</uid>

<uid>1240079</uid>

</friends_get_response>

[00063] When authenticating a compatible device or machine which may not have access to a connection for the authentication element, a key file or part of the metadata thereof could be made on another connected compatible device or machine and allow the enabler to execute Friends.get API command to collect and store the complete list of a plurality of FBID to the key file or the metadata thereof. The compatible device or machine which may not have access to a connection for the authentication element with an embedded interaction console, usually a user GUI, can request and load the key file or part of the metadata thereof to save the complete list of a plurality of electronic identification references, in this discussion is reference as the FBID, to storage or metadata as part of the compatible device or machine. This step ensures the cross-referencing element requirement of the invention can take place in the event the connection for the authentication element is not present in the compatible device or machine.

[00064] Another example is a content provider can allow shared access to friends of the excelsior enabler after a time period, like for example, 90 days. After the 90 day period, when media access is requested using the authentication element by a plurality of secondary enablers, which are usually friends and family of the excelsior enabler, the FBID of the excelsior enabler is cross-referenced with the FBID of the requesting secondary enabler by way of the apparatus ability to execute the Facbeook "Friends.areFriends" API command.

[00065] XML return example of the Facebeook "Friends.areFriends" API command where FBID 2223322 and 2222333 are friends and FBID 1240077 and 1240079 are not friends:

<?xml version="1.0" encoding="UTF-8"?>

<friends_areFriends_response

xmlns=http://api.facebook.com/1.0/

xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

xsi:schemaLocation="http://api.facebook.com/1.0/ http://api.facebook.com/1.0/facebook.xsd"

list="true">

<friend_info>

<uid1>222332</uid1><uid2>222333</uid2>

<are_friends>1</are_friends>

</friend_info>

<friend_info>

<uid1>1240077</uid1><uid2>1240079</uid2>

<are_friends>0</are_friends>

</friend_info>

</friends_areFriends_response>

[00066] Such usability can be important to sustain "fair use" rights of consumers of the digital media to emulate usability found with physical media products such as CD and DVD that can be loaned to friends and family after an inception grace period.

[00067] Once the information of the verification and authentication elements is acquired, the apparatus handles the next process of writing the information to the digital media metadata and can include additional information gathered from components of The App. Components of The App can include MAC address from a networking card, CRC checksum of an embedded file or circuit, SOC identifier, embedded serial number, OS version, web browser version, and many other identifiable components as part of The App. For this discussion, the MAC address from a networking card as part of The App will be used as reference of a secondary electronic identification reference. In computer networking, a Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification, and used in the Media Access Control protocol sub-layer. If assigned by the manufacturer, a MAC address usually

encodes the manufacturer's registered identification number. It may also be known as an Ethernet Hardware Address (EHA), hardware address, adapter address, or physical address. The novelty of embedding the MAC address along with the FBID of the excelsior enabler is to provide a plurality of electronic identification references in which cross-referencing actions can allow more rapid access to be granted with less interaction from an enabler. For example, to retrieve the FBID from Facebook to cross-reference with the FBID stored in the digital media metadata requires the enabler to possibly physically need to enter their login and password credentials to the GUI connected to the apparatus. It may be possible that web browser cookies allow automatic Facebook login by storing an active session key, but the session key is not guaranteed to be active at the time of an access request. While the enabler may not have an issue executing another authentication command, several remote operations could exist to control authentication and access requests separately from each other. The apparatus can execute a programmable retrieval command, usually a GET command, to locate and retrieve the MAC address from an attached or connected networking card. After the FBID is acquired, the MAC address is also acquired to write the plurality of electronic identifications to the metadata of the at least one encrypted digital media asset by; obtaining the decryption key to decrypt the encrypted digital media asset which is usually stored encoded, no encoded, encrypted, or no encrypted as part of the apparatus or as part of a connected source, usually an Internet server with an encrypted HTTPS protocol. A plurality of MAC addresses can be stored along with the FBID of the excelsior enabler to manage access rights across a plurality of devices. To understand metadata and the uses, metadata is defined simply as to "describe other data". It provides information about certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the

author is, when the document was written, and a short summary of the document. Web pages often include metadata in the form of Meta tags. Description and keywords Meta tags are commonly used to describe the Web page's content. Most search engines use this data when adding pages to their search index. In the invention, the FBID and MAC addresses are written to the digital media asset metadata to prepare for the instant or delayed cross-referencing element of the invention. The same process of writing the information to the digital media metadata is true with secondary enablers allowing the same benefits of cross-referencing.

[00068] Cross-referencing, the last element of the invention is used to verify access rights of an enabler of a pre or post personalized encrypted digital media asset. Once an enabler executes an action for access request, the apparatus will obtain the decryption key to first seek the MAC address record. If the MAC address is found, then a cross-reference process is executed by comparing the MAC address retrieved from the metadata of the digital media file with the MAC address retrieved from the networking card connected to the apparatus or The App. If the comparison action proves to be true, then access rights are granted to the enabler. If the comparison fails, then the apparatus can either ask the enabler to participate in communication with the authentication element of the invention, or could deny further interactivity with the enabler. In this discussion, the apparatus requires the enabler to participate in communication with the authentication element to provide credentials to establish a cross-reference comparison with the FBID retrieved from the metadata and the FBID retrieved from the Facebook API. If the comparison action proves to be true, then access rights is granted to the excelsior enabler and the current MAC address of the networking card as part of The App is appended to the metadata of the encrypted digital media asset and access rights is granted to the excelsior enabler. If the FBID cross-reference fails, then the apparatus can either ask the potential secondary enabler to participate in communication with the authentication element of the invention, or could deny further

interactivity with the potential secondary enabler. In this discussion, the apparatus requires the potential secondary enabler to participate in communication with the authentication element to provide credentials to establish a cross-reference comparison with the FBID retrieved from the metadata and the FBID retrieved from the Facebook "Friends.areFriends" API command to determine if the potential secondary enabler identity is true or false. The determination is in accordance to any possible access grace periods set by the content provider of the encrypted digital media asset. If the comparison action proves to be true, then access rights is granted to the secondary enabler and the current MAC address of the networking card as part of The App and the FBID retrieved are appended to the established metadata information of the encrypted digital media asset and access rights can be granted to a plurality of secondary enablers; unlimited interoperability between devices and "fair use" sharing partners for an infinite time frame while protecting commercial digital media from unlicensed distribution to sustain long-term return of investments is achieved.

[00069] While the present invention has been described in connection with preferred embodiments, it will be understood by those skilled in the art that variations and modifications of the preferred embodiments described above may be made without departing from the scope of the invention. Other embodiments will be apparent to those skilled in the art from a consideration of the specification or from a practice of the invention disclosed herein. It is intended that the specification and the described examples are considered exemplary only, with the true scope of the invention indicated by the following claims.

[00070] CLAIMS

What is claimed is:

1. A method for authorizing a second user to access content using a cloud system, the method comprising:

receiving, at a front-end agent connected to the cloud system, a request from a first device of a first user, wherein the request comprises a permission to provide a second user with access to content authorized for access by the first user, the front-end agent comprising a network communication with the first device and recognized second devices operated by the first user;

receiving, at the front-end agent from the second device, a communication that the second user is authorized to access the content;

determining, at the front-end agent, whether the second user is known to the front-end agent;

in response to determining that the second user is known, identifying credentials associated with the second user; and

associating the credentials of the second user with the content;

2. The method of claim 1, further comprising:

identifying the first user providing the request; and

determining whether the first user is authorized to grant access to the content.

3. The method of claim 1, wherein:

the request comprises identifying information for the second user.

4. The method of claim 3, wherein the identifying information

comprises at least one of:

an email address; and

a number.

5. The method of claim 1, further comprising:

an automatically created credential.

6. The method of claim 1, further comprising:

an established credential.

7. The method of claim 1, wherein authorizing further comprises:

adding the credentials to a list associated with the content.

8. The method of claim 1, wherein providing accessing information further comprises:

providing a network address.

9. The method of claim 8, wherein:

at least one source exist to access the content.

10. An electronic device for controlling access to content using a cloud system, comprising a processor operative to:

recognize a plurality of devices owned by at least a first user;

define a front-end agent in connection with the plurality of devices recognized by the at least first user;

receive, at the front-end agent, a request from a first device of the first user to allow a second user access to content;

receive from a second device a communication that the second user is authorized to access the content;

determine whether the second user is known to the front-end agent;

identify credentials associated with the second user; and

associate the credentials of the second user with the content.

11. The electronic device of claim 10, wherein the processor is further operative to:

receive a request from the second user for content access; and

provide identifying information for the front-end agent in response to receiving.

12. The electronic device of claim 10, wherein the processor is further operative to:

handling a manually created credential or an automatically created credential;

13. The electronic device of claim 12, wherein the processor is further operative to:

associate the credentials with access to the content using a list.

14. Non-transitory computer readable media for authorizing a second user to access content using a cloud system, comprising computer readable code recorded thereon for:

receiving, at a front-end agent connected to the cloud system, a request from a first device of a first user, wherein the request comprises a permission to provide a second user with access to content authorized for access by the first user, the front-end agent comprising a network communication with the first device and recognized second devices operated by the first user;

receiving, at the front-end agent from the second device, a communication that the second user is authorized to access the content;

determining, at the front-end agent, whether the second user is known to the front-end agent;

in response to determining that the second user is known, identifying credentials associated with the second user; and

associating the credentials of the second user with the content.

15. The non-transitory computer-readable media of claim 14, further comprising computer readable code recorded thereon for:

handling a manually created credential or an automatically created credential.

ABSTRACT

The invention is an apparatus that facilitates access to a data source to accept verification and authentication from an enabler using at least one token and at least one reference. The at least one reference could be a device serial number, a networking MAC address, or a membership ID reference from a web service. Access to the data source is also managed with a plurality of secondary enablers.

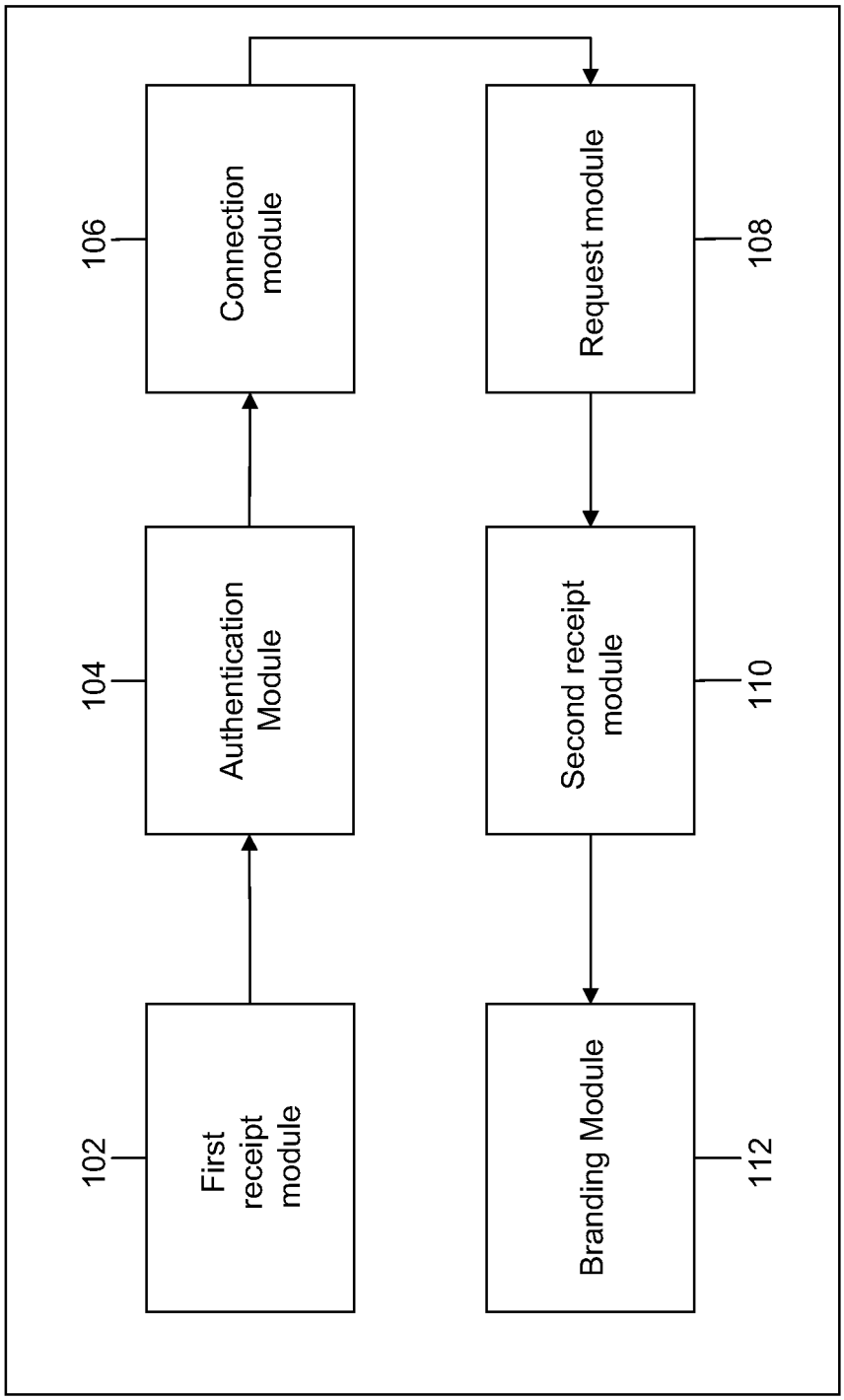

First receipt module
102
Authentication Module
104
Connection module
106
Request module
108
Second receipt module
110
Branding Module
112

FIG.1

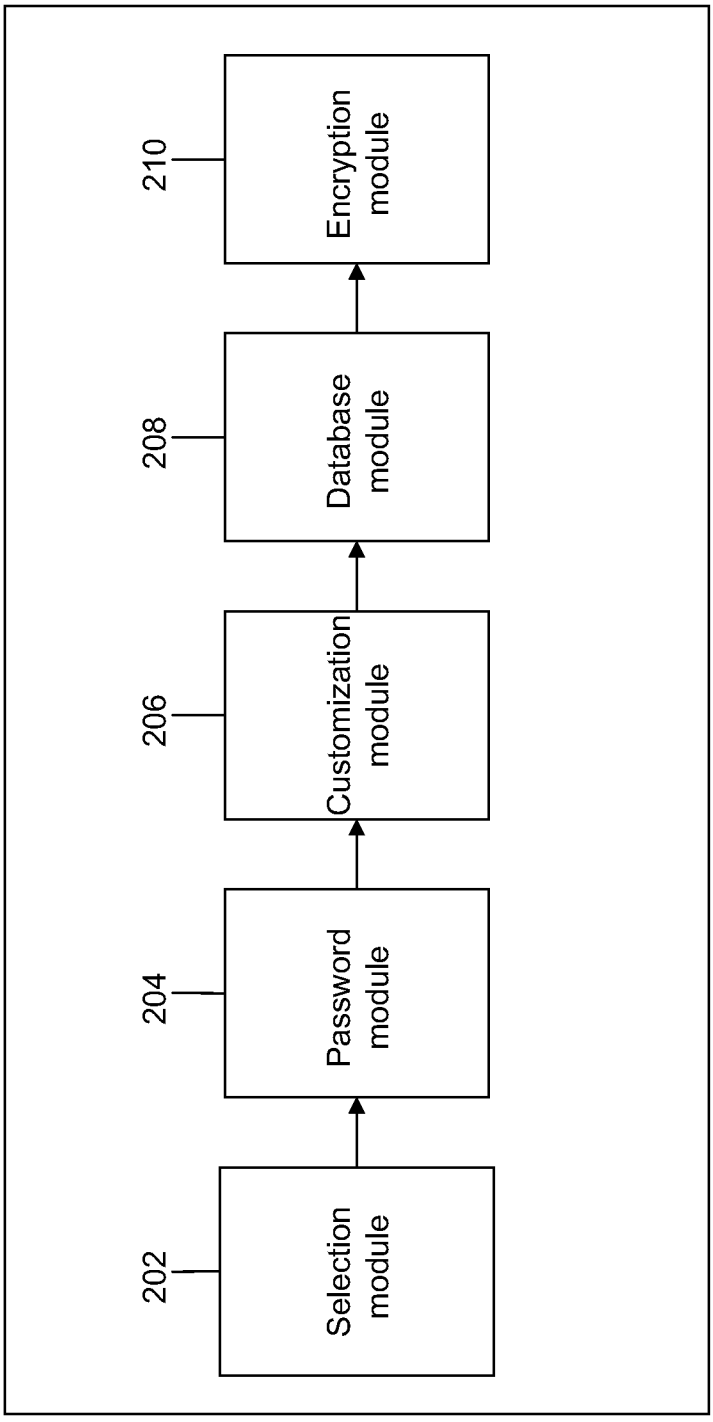

202
Selection module
204
Password module
206
Customization module
208
Database module
210
Encryption module

FIG.2

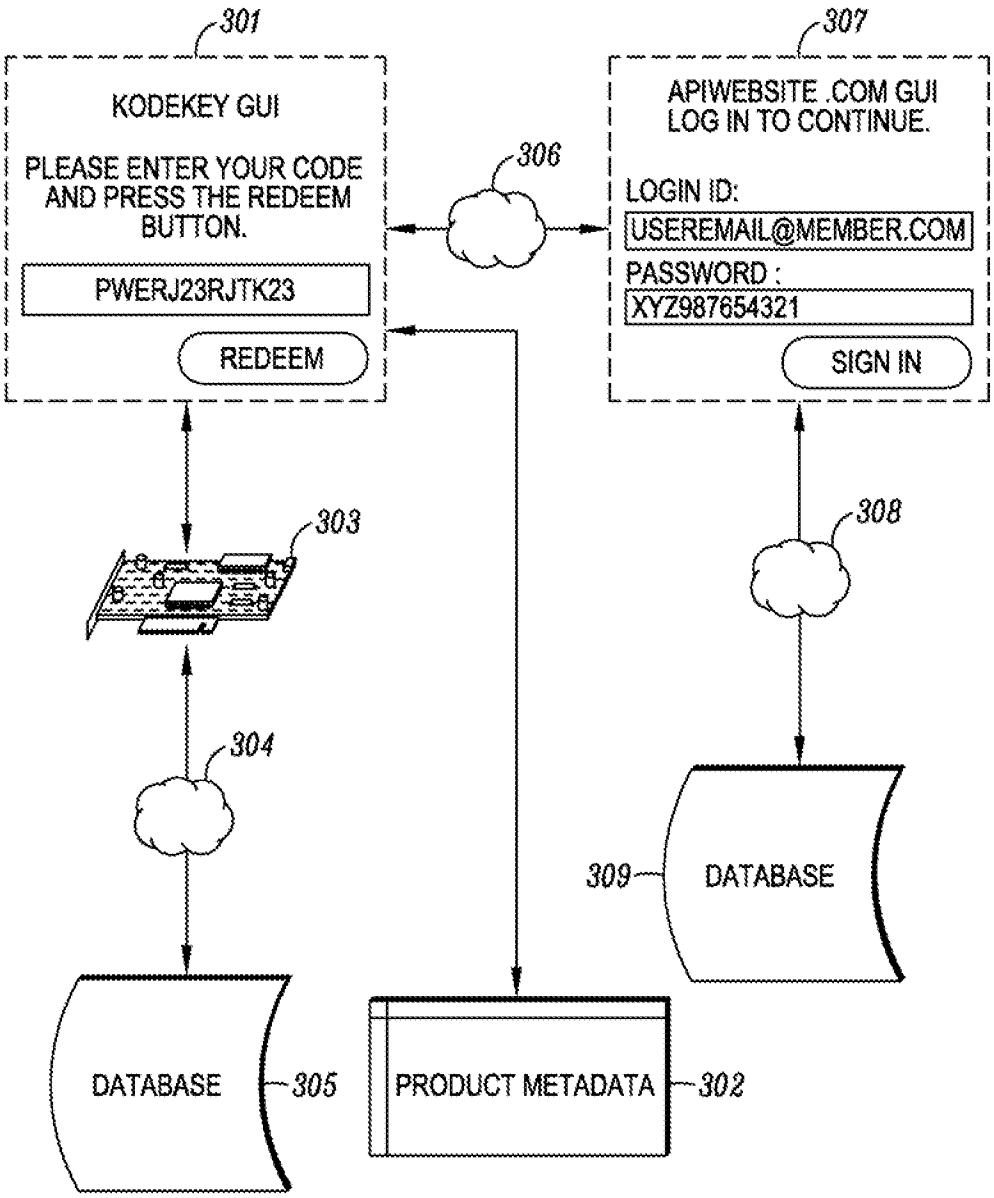

301
KODEKEY GUI
PLEASE ENTER YOUR CODE AND PRESS THE REDEEM BUTTON.
PWERJ23RJTK23
REDEEM
306
307
APIWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
SIGN IN
303
304
308
309
DATABASE
DATABASE
305
PRODUCT METADATA
302

FIG. 3

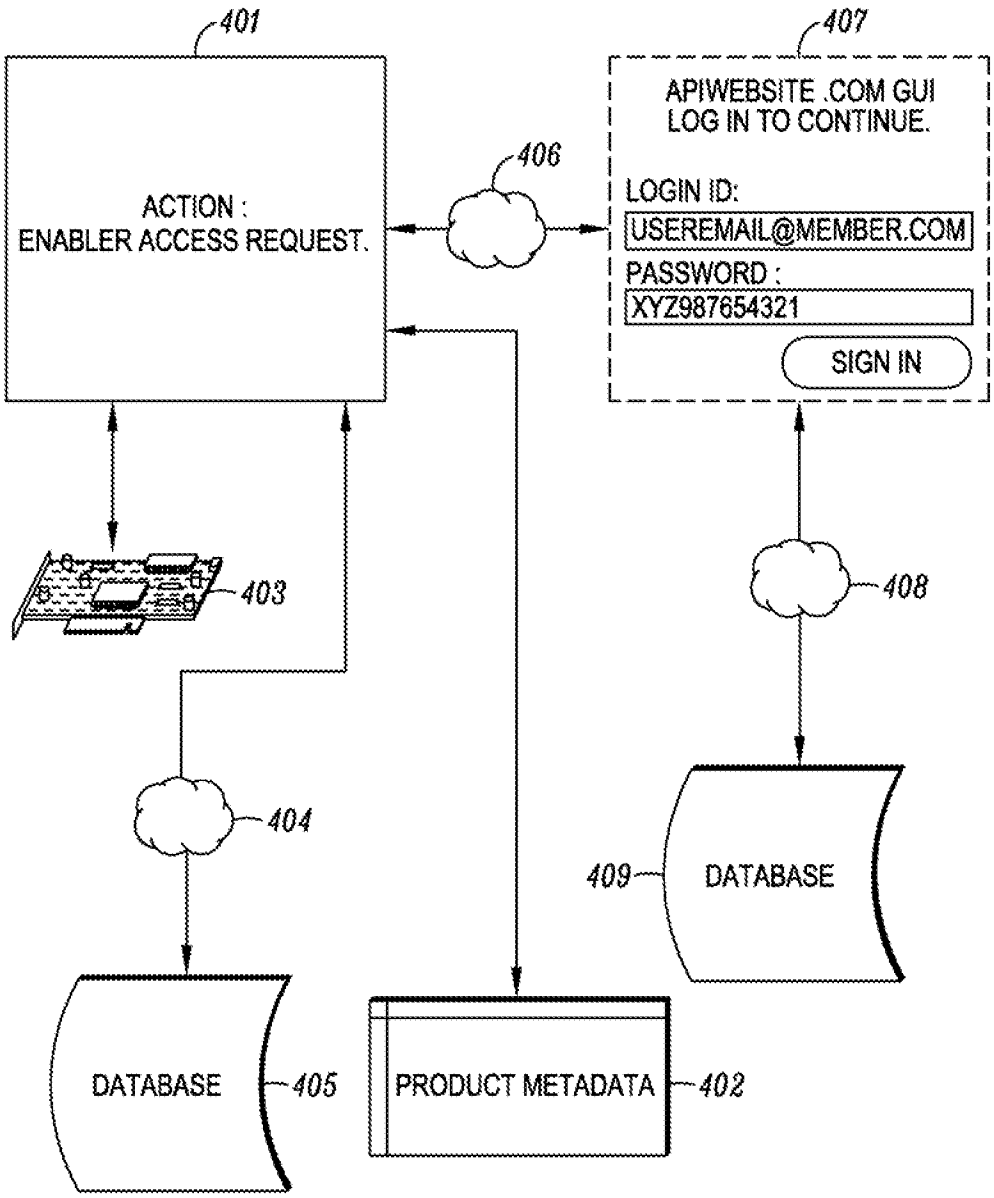

401
ACTION :
ENABLER ACCESS REQUEST.
406
407
APIWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
SIGN IN
403
408
404
409
DATABASE
DATABASE
405
PRODUCT METADATA
402

FIG. 4

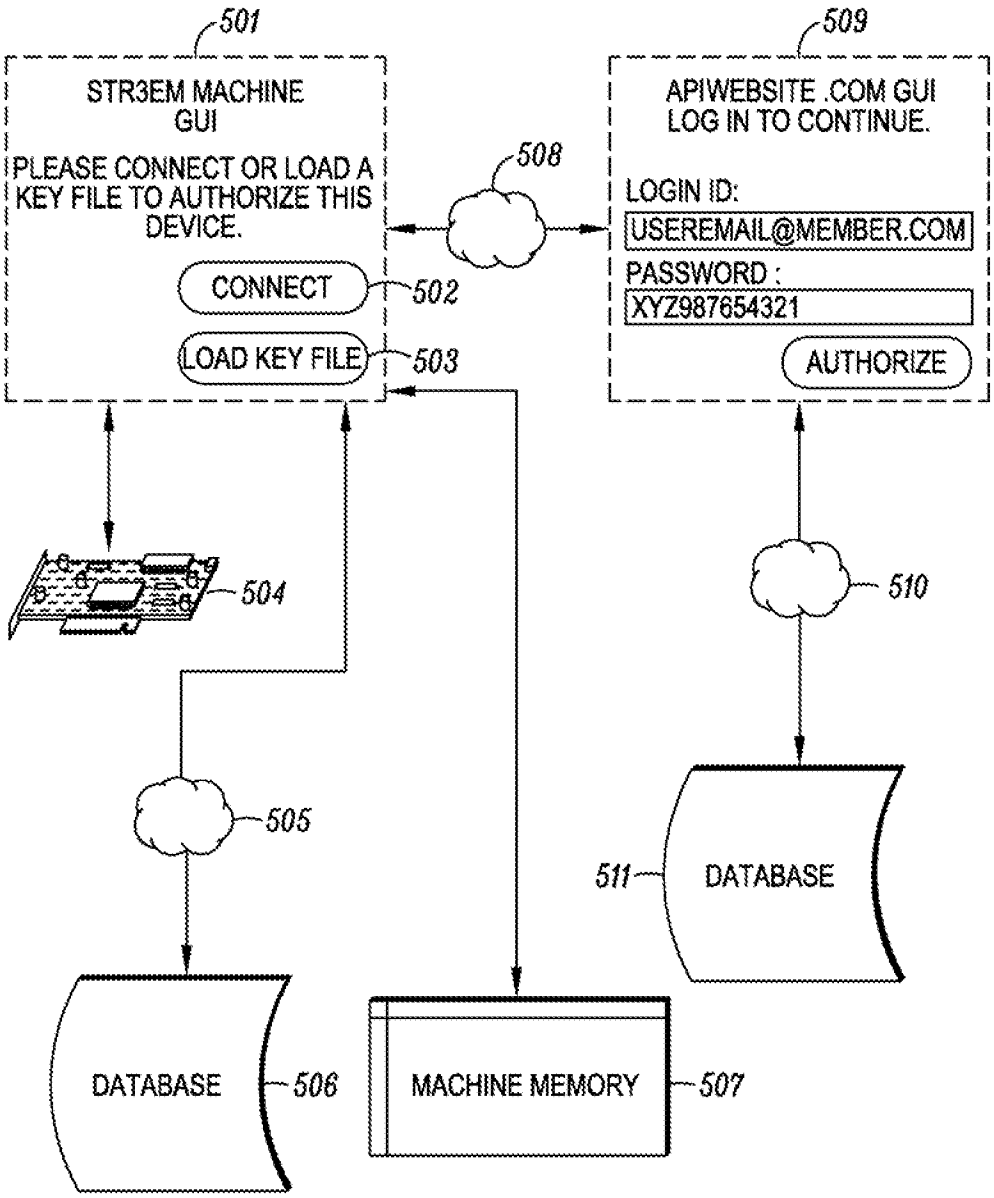

501
STR3EM MACHINE GUI
PLEASE CONNECT OR LOAD A KEY FILE TO AUTHORIZE THIS DEVICE.
CONNECT
502
LOAD KEY FILE
503
508
509
APIWEBSITE .COM GUI
LOG IN TO CONTINUE.
LOGIN ID:
USEREMAIL@MEMBER.COM
PASSWORD :
XYZ987654321
AUTHORIZE
504
505
506
DATABASE
MACHINE MEMORY
507
510
511
DATABASE

FIG. 5

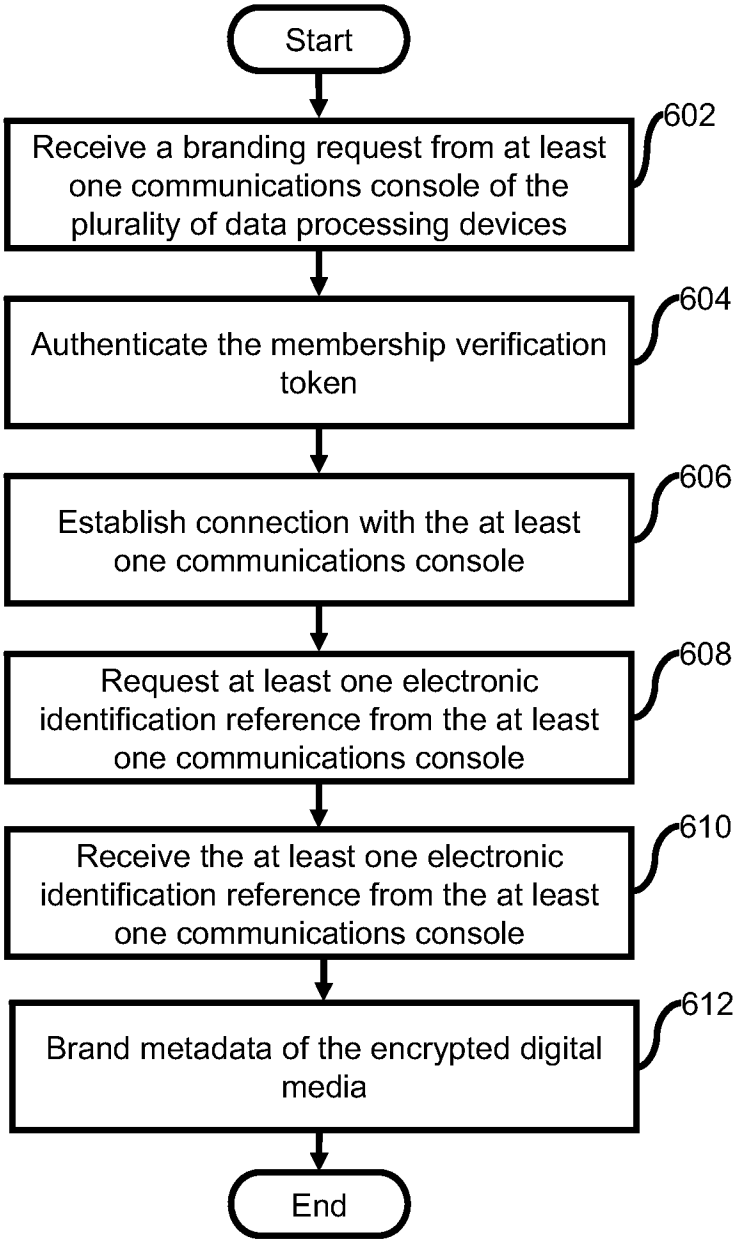

Start
Receive a branding request from at least one communications console of the plurality of data processing devices
602
Authenticate the membership verification token
604
Establish connection with the at least one communications console
606
Request at least one electronic identification reference from the at least one communications console
608
Receive the at least one electronic identification reference from the at least one communications console
610
Brand metadata of the encrypted digital media
612
End

FIG.6

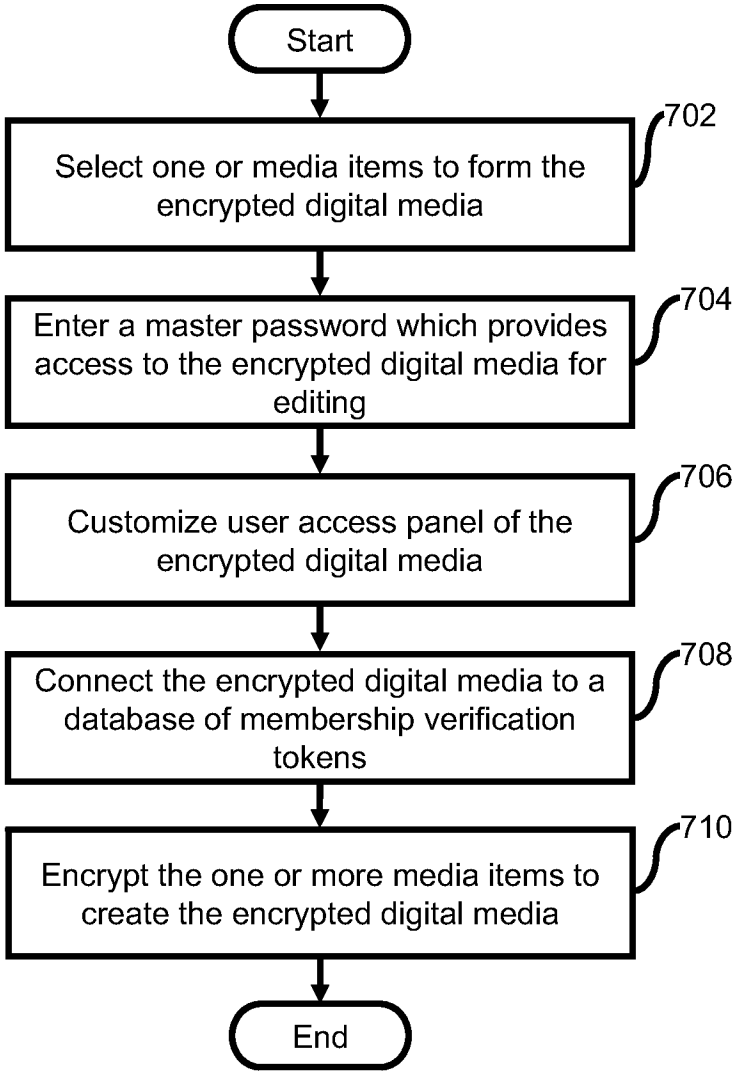

Start
Select one or media items to form the encrypted digital media
702
Enter a master password which provides access to the encrypted digital media for editing
704
Customize user access panel of the encrypted digital media
706
Connect the encrypted digital media to a database of membership verification tokens
708
Encrypt the one or more media items to create the encrypted digital media
710
End

FIG.7

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 06/05/2013

MTEKLEMI ADJ #00000008 Mailroom Dt: 05/06/2013
Seq No: 5562 Sales Acctg Dt: 05/07/2013 13888051
04 FC : 2053 -70.00 OP