UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2025-00075

U.S. Patent No. 9,679,289

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

TABLE OF EXHIBITS

Exhibit	Description
Ex-1001	U.S. Patent No. 9,679,289 to David L. Brown ("the '289 patent")
Ex-1002	Prosecution history of U.S. Patent No. 9,679,289
Ex-1003	Declaration of Andrew Wolfe, Ph.D., including his Curriculum Vitae
Ex-1004	U.S. Patent Application Publication No. 2006/0258289 to Dua ("Dua")
Ex-1005	European Patent Application Publication No. EP 1536306 to Buer et al. ("Buer")
Ex-1006	U.S. Patent Application Publication No. 2007/0245157 to Giobbi et al. ("Giobbi157")
Ex-1007	U.S. Patent Application Publication No. 2004/0255139 to Giobbi ("Giobbi139")
Ex-1008	PCT Application Publication No. WO 90/06633 to Lee et al. ("Lee")
Ex-1009	Order, *Proxense, LLC v. Samsung Elecs. Co., Ltd.,* No. 6:21-cv-00210-ADA (W.D. Tex. Jan. 18, 2022)
Ex-1010	Memorandum in Support of Claim Construction Order, *Proxense, LLC v. Samsung Elecs. Co., Ltd.,* No. 6:21-cv-00210-ADA (W.D. Tex. Dec. 28, 2022)
Ex-1011	Scheduling Order, *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320-ADA (W.D. Tex. March 18, 2024)

Ex-1012	U.S. Patent Application Publication No. 2005/0116050 to Jei et al. ("Jei")
Ex-1013	PCT Application Publication No. WO 2005/104584 to Bella et al. ("Bella")
Ex-1014	European Patent Application Publication No. EP 1600885 to Nishikawa et al. ("Nishikawa")
Ex-1015	Google's Proposed Constructions, *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320-ADA (W.D. Tex October 17, 2023)
Ex-1016	Proxense's Proposed Constructions, *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320-ADA (W.D. Tex October 17, 2023)
Ex-1017	U.S. Patent Application Publication No. 2004/0176032 to Kotola et al. ("Kotola")
Ex-1018	Preliminary Infringement Contentions Exhibit E, *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex)
Ex-1019	U.S. Patent Application Publication No. 2005/0151623 to Von Hoffmann ("Von Hoffmann")
Ex-1020	Claim Construction Order, *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320-ADA (W.D. Tex January 23, 2024)
Ex-1021	Bluetooth Specification, Profiles of the Bluetooth System, Version 1.0 B (December 1999)
Ex-1022	Comparison of District Courts (December 31, 2023)
Ex-1023 – Ex-1027	Reserved

Ex-1028	Complaint in *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex March 18, 2024)
Ex-1029	Plaintiff's Unopposed Motion for Leave to File Amended Complaint, *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex October 28, 2024)
Ex-1030	Scheduling Order, *Proxense, LLC v Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex), Dkt. 29
Ex-1031	U.S. District Courts—National Judicial Caseload Profile, available at: https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0630.2024.pdf (retrieved October 31, 2024)
Ex-1032	Docket Sheet in *Proxense LLC v. Apple Inc.*, W.D. Tex. (pulled November 1, 2024)
Ex-1033	Applications related to the '289 Patent.
Ex-1034	First Amended Complaint in *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex October 31, 2024)

LISTING OF CHALLENGED CLAIMS

Claim 1	
[1pre]	A hybrid device comprising:
[1a]	an integrated, secure memory storing local, secured information; and
[1b]	an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,
[1c]	the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,
[1d]	wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and service.
Claim 2	
[2]	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device.
Claim 3	
[3]	The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC.
Claim 4	
[4]	The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user.

Claim 5	
[5]	The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user.
Claim 6	
[6]	The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information.
Claim 7	
[7]	The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC.
Claim 8	
[8]	The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database.
Claim 9	
[9]	The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction.
Claim 10	
[10]	The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated,

	secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility.
Claim 11	
[11]	The hybrid device of claim 1, wherein the hybrid device is a cell phone.
Claim 12	
[12]	The hybrid device of claim 1, wherein the at least one external device is included in jewelry.
Claim 13	
[13]	The hybrid device of claim 1, wherein the at least one external device is a watch.
Claim 14	
[14pre]	A method comprising:
[14a]	creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,
[14b]	the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;
[14c]	receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and
[14d]	generating an enablement signal enabling one or more of an application, a function and a service.
Claim 15	
[15]	The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device.
Claim 16	
[16]	The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the

	application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC.
Claim 17	
[17]	The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user.
Claim 18	
[18]	The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction.
Claim 19	
[19]	The method of claim 14, wherein the hybrid device is a cell phone.
Claim 20	
[20]	The method of claim 14, wherein the external PDK is included in a watch.

I. Relief Requested

Apple Inc. (Petitioner) requests *inter partes* review of claims 1-20 of U.S. Patent No. 9,679,289 ("the '289 patent," Ex-1001) based on the following grounds:

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)
1	1-6, 8-11, and 14-19	103	Dua, Giobbi157
2	1-6, 8-11, and 14-19	103	Dua, Giobbi157, Kotola
3	1-7, 10-11, and 14-19	103	Buer
4	4, 8-10, 12, 13, 17, and 20	103	Buer, Giobbi157
5	4	103	Buer, Nishikawa

The '289 patent generally relates to keys and readers, such as RFID tags and RFID readers that interact with the RFID tags, Ex-1001, 1:45-2:10, and the claims recite a "hybrid device" (e.g., a cellular phone) that includes both an integrated, secure memory (PDK) and an RDC, which can respectively communicate with external RDCs and PDKs that are in proximity with the hybrid device. But devices having both an internal key and reader were known years before '289 patent's effective filing date.

Indeed, Dua discloses a cellular phone with an integrated RFID Tag-Reader Module that includes both an RFID tag (PDK) and an RFID reader (RDC) to automatically set up and establish a wireless connection in its proximity. Ex-1004,

[0011]-[0016]. Buer also teaches a cellular phone that includes both an internal authentication component (PDK) and a proximity reader (RDC) to secure access to various services using external RFID tokens (keys) and readers in its proximity. Ex-1005, [0010], [0014], [0130], [0163]. Numerous prior art patents teach using a digital key and reader to secure data or a service. *See, e.g.,* Exs. 1006-1008, 1012-1014. Thus, the challenged claims merely recite the well-known concept of enabling applications, functions, or services with digital keys and readers. The challenged claims should be held unpatentable.

II. The '289 Patent

A. Overview

The '289 patent is directed to a "hybrid device" (**red**) that includes both an integrated personal digital key (PDK) (**blue**) and an integrated receiver-decoder circuit (RDC) (**yellow**) that communicate with each other via a signal line. Ex-1001, 2:25-29. The hybrid device may be part of a cell phone.

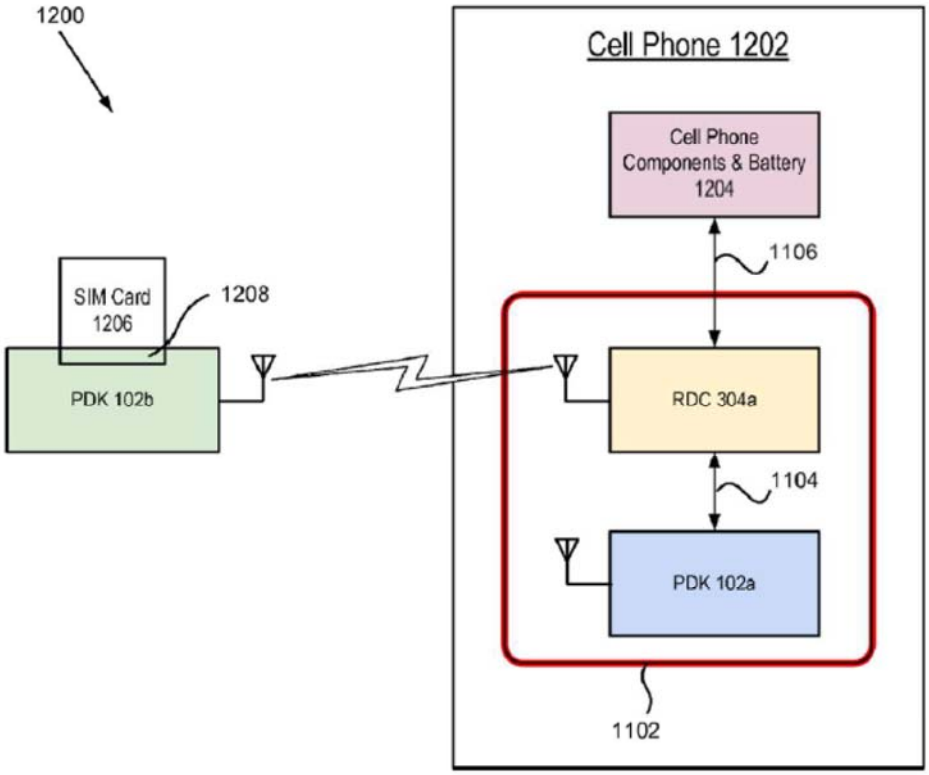


FIG. 12

Id., Fig. 12 (annotated). As shown, additional cell phone components and battery (pink) may be coupled to the integrated RDC by a signal line. *Id.*, 14:45-64. The integrated RDC may also communicate wirelessly with an external PDK. *Id.*, 14:59-61.

The hybrid device may interconnect with other external devices, so that the integrated PDK (**blue**) communicates wirelessly with an external RDC (**purple**), and the integrated RDC (**yellow**) communicates wirelessly with an external PDK (**green**) within its proximity zone:

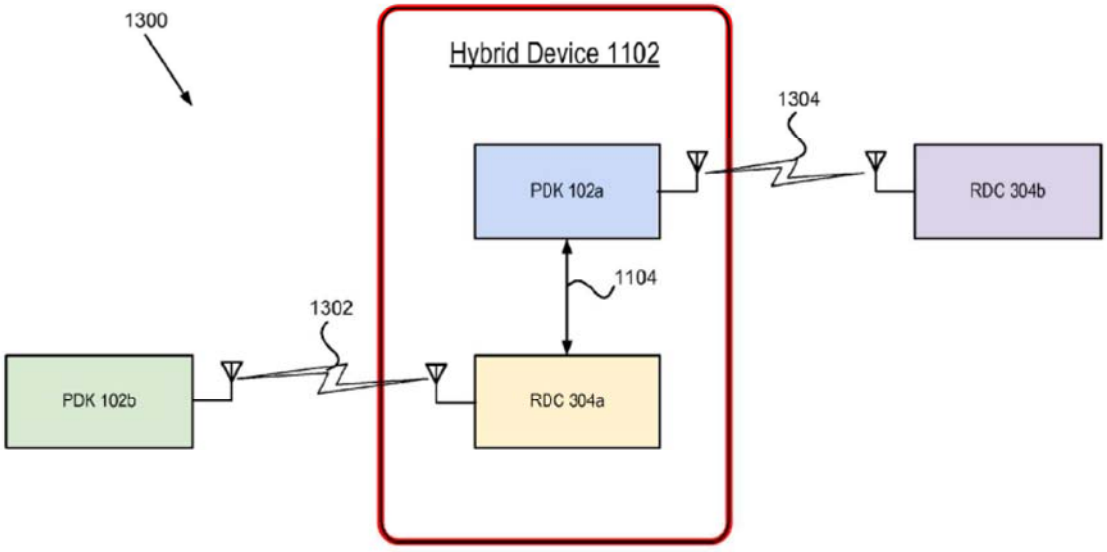


FIG. 13

Id., Fig. 13 (annotated), 16:47-63, 22:36-49.

The integrated PDK and RDC thus enables various applications, functions, or services, either on an external device or the hybrid device using information stored on the integrated or external PDKs (e.g., (1) financial information such as bank information, credit/debit card information, and account information; (2) biometric information such as a fingerprint, palm print, retinal scan; or (3) personal identification information such as a name, address, phone number). *Id.*, 4:37-47, 7:7-18, 16:64-17:4. When the hybrid device may be used to access or enable a Wi-Fi service, an external PDK 102b "provides ... information to the [integrated] RDC 304*a*," and the hybrid device "then communicates with the [external] RDC 304*b* to access the Wi-Fi service." *Id.*, 20:5-28. In this example, the hybrid device and the

external PDK may belong to different users, and the hybrid device may thus use another user's information stored on the external PDK. *Id.* As another example, the hybrid device may use the credit card information stored on the integrated PDK to provide authorization to the external RDC to make a purchase using the cell phone, and in this way, "to enable a service associated with the ... [external] RDC." *Id.*, 16:64-17:4. The purchase authorization may depend on the presence of an external PDK being in proximity to the hybrid device. *Id.*, 17:4-11, 17:18-43. The external PDK "authorizes the hybrid device," which "in turn authorizes" the external RDC, such that a user can only make a purchase when the external PDK is in proximity to the hybrid device. *Id.*, 17:4-11, 17:18-21. In other words, the external PDK may be "used to enable specific features in the hybrid device." *Id.*, 17:11-12.

B. Claim Construction[1]

The district court previously construed the following terms in family members of the '289 patent:

[1] The Board construed certain claim terms in *Microsoft Corporation v. Proxense, LLC*, IPR2024-00407, Paper 8.

Term	Construction
hybrid device	"[a] device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit."
personal digital key	"[a]n operably connected collection of elements including an antenna and a transceiver for communicating with a[n] RDC and a controller and memory for storing information particular to a user."
biometric information	"plain and ordinary meaning."
financial information	"plain and ordinary meaning."
receiver-decoder circuit	"[a] component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing."
inheritance information	"[i]nformation passed from a first device to a second device for use by the second device."
enablement signal	requires no construction

Ex-1009, 3-4; Ex-1010, 25, 27, 32, 34, 36, 38, 40.

In *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.) ("the Google litigation"),[2] the court adopted its prior constructions for "personal digital key" and "receiver-decoder circuit."[3] Ex-1020. Because the prior art in this Petition renders obvious all claims regardless of the construction, the Board need not construe terms to resolve unpatentability in this Petition.[4] *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019).

C. Level of Ordinary Skill

A person of ordinary skill in the art ("POSITA") at the time of the purported invention would have had a bachelor's degree in computer or electrical engineering

---

[2] Google agreed to certain constructions, Ex-1015, 1, and Proxense contends no other terms "beyond what the Court had previously construed in the *Samsung* case" need to be construed. Ex-1016, 1.

[3] Google proposed alternative constructions for "personal digital key" and "receiver-decoder circuit" in the Google litigation. Ex-1015, 1.

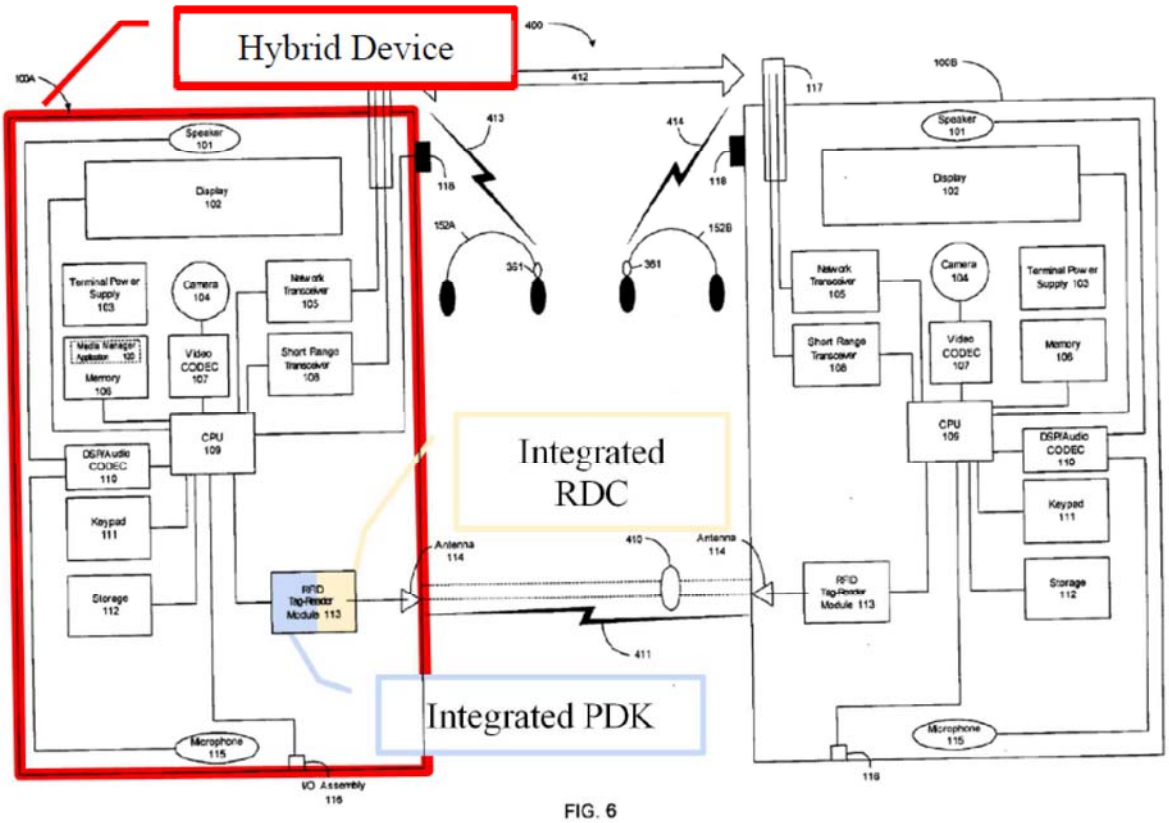
[4] The Board previously determined that only "personal digital key" warranted construction for the purposes of institution. *See e.g.*, *Samsung Elecs. Am., Inc. v. Proxense, LLC*, IPR2021-01438, Paper 12 at 16 (PTAB Feb. 28, 2022); *Samsung Elecs. Am., Inc. v. Proxense, LLC*, IPR2021-01439, Paper 11 at 16 (PTAB Feb. 28, 2022).

or an equivalent degree, and at least three years of experience in the field of encryption and security or equivalent experience. Additional education could substitute for professional experience, and significant work experience could substitute for formal education. Ex-1003 ¶38.

III. Overview of the Prior Art

A. Dua

Dua, U.S. Patent Application Publication No. 2006/0258289, published on November 16, 2006, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Dua teaches a hybrid device—a "cellular phone[]" containing "both an RFID tag and an RFID reader"—that establishes wireless connections with other external devices to enable functions and to exchange data. Ex-1004, [0015], [0070, [0089]. Dua's cellular phone includes an "RFID Tag-Reader Module," as shown below, to "rapidly exchange information with an electronic device that is in close proximity." *Id.*, [0070].



Id., Fig. 6 (annotated).

The RFID Tag-Reader Module, as shown below, includes specific circuit components for "RFID tag functionality" and circuit components for "RFID reader functionality." *Id.*, [0106].

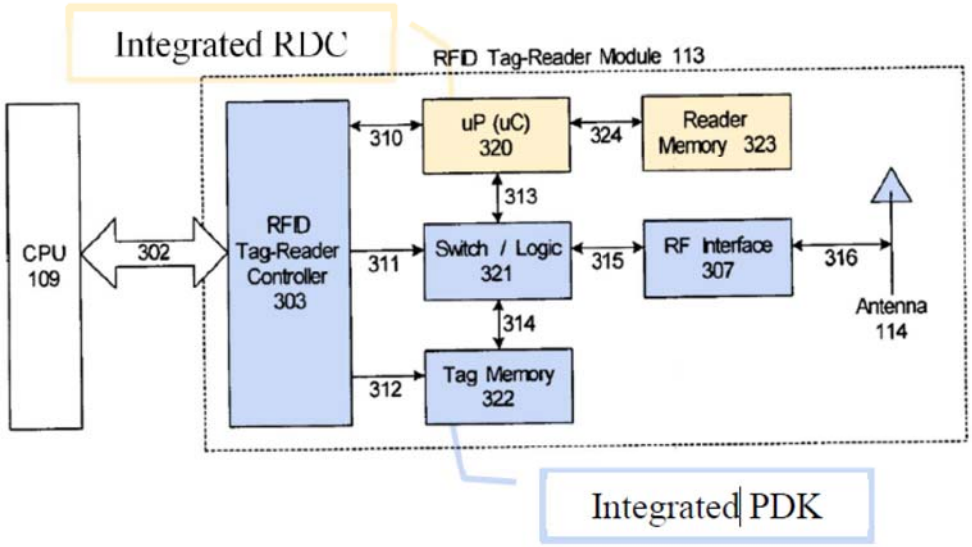


FIG. 4B

Id., Fig. 4B (annotated).

The components for "RFID tag functionality" (**blue**) store confidential information and encryption keys in "tamper resistant" internal tag memory for gaining access to an external device. *Id.*, [0108]-[0109]. This stored information may be encrypted. *Id.*, [0109], [0152]. Dua discloses transmitting this information to an external reader, which reads the information transmitted by the tag to establish a secure connection. *Id.*, [0092], [0100]-[0101], [0139]; Ex-1003 ¶¶53-55.

The components for "RFID reader functionality" (**yellow**) are capable of communicating with external RFID tags. Ex-1004, [0071]. When operating with enhanced security, the RFID reader may receive encrypted data and decode the encrypted data using an encryption key. *Id.*, [0152]; Ex-1003 ¶¶56-59. Dua discloses enabling services, such as "transmission of media assets to other devices in proximity via short-range RF," and other additional functionalities, including

"transacting at a point-of-sale location using a digital wallet application and the RFID capability." Ex-1004, [0058]; *see also id.*, [0070], [0089]. Ex-1003 ¶¶49-59.

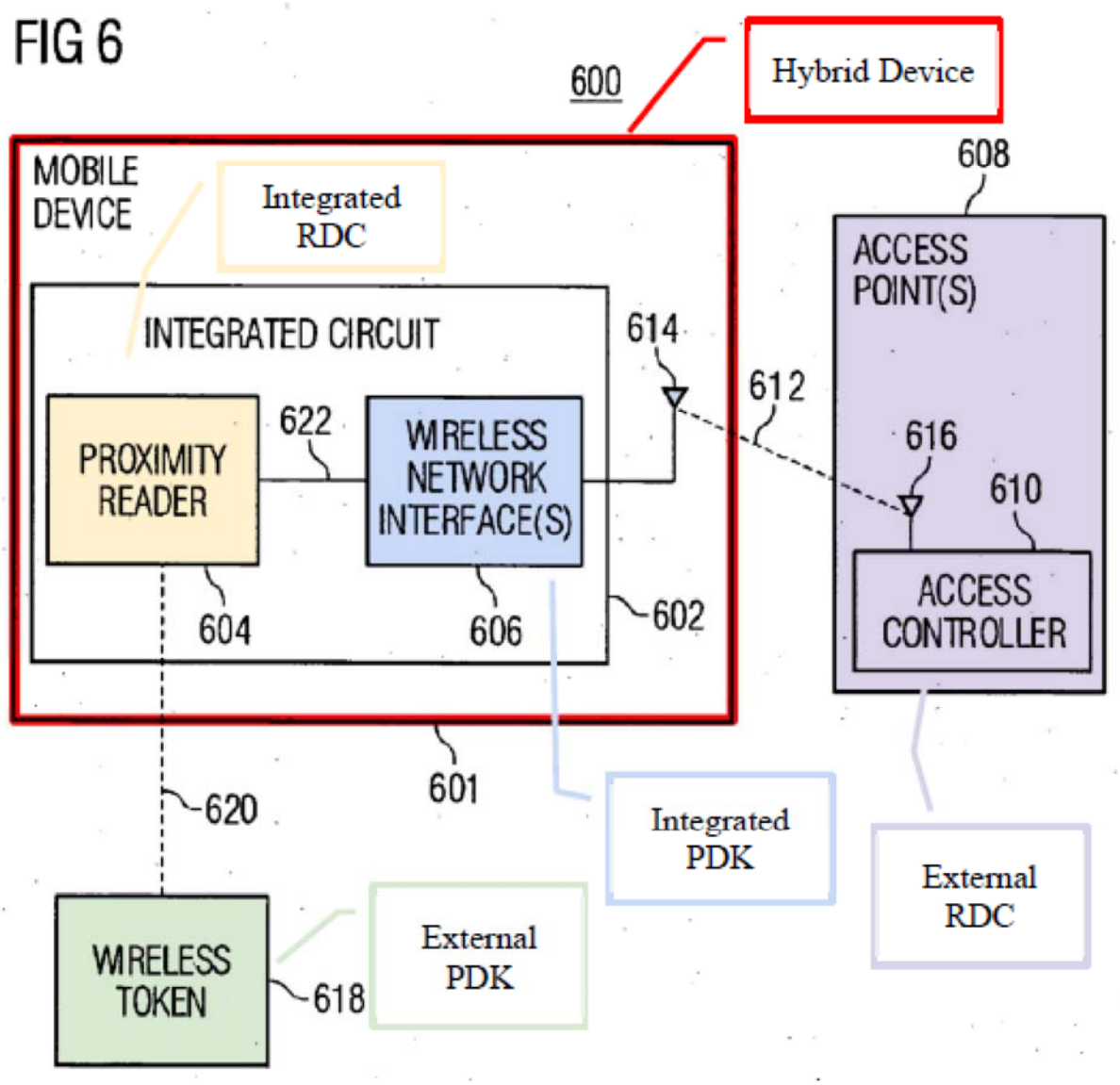
Dua incorporates by reference Kotola, U.S. Patent Application Publication No. 2004/0176032, for details concerning such "other RFID Tag-Reader Module designs." Ex-1004, [0114] (citing Ex-1017). Kotola published on September 9, 2004, and qualifies as prior art under pre-AIA 35 U.S.C. §102(b)

B. Buer

Buer, European Patent Application Publication No. EP 1536306, published on September 30, 2004, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Buer discloses that "[a]ccess to secured services may be controlled based on the proximity of a wireless token to a computing device through which access to the secured services is obtained." Ex-1005, Abstract. "An authorized user may be provided access to a service only when a wireless token assigned to the user is in the proximity of the computing device." *Id.* The computing device (e.g., access device) may be implemented as a cellular phone. *Id.*, [0163], [0195]. Buer's access device could be used to enable various applications, functions, or services, including the following two embodiments: (1) "embodiments of a wireless proximity and authentication system that controls access to one or more data networks," as disclosed in Figures 5-7, and (2) "embodiments of security processing systems (i.e., key management

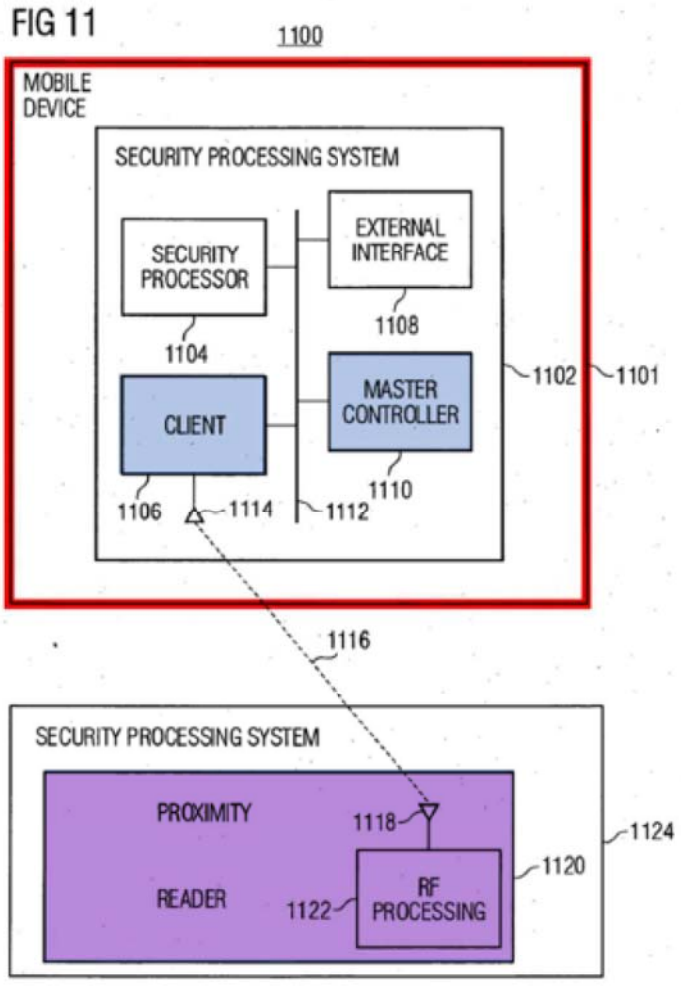
systems) that include wireless proximity and authentication," as disclosed in Figures 8-11. *Id.*, [0155], [0176].

First, the mobile device may be enabled "to access one or more wireless networks (e.g., a cellular network, an 802.11 network, a Bluetooth network, etc.)," as shown below.



Id., Fig. 6 (annotated), [0163]. The mobile device receives authentication information from the wireless token via RF signals 620 and communicates with the access points wirelessly via RF signals 612. *Id.*, [0164]-[0165].

Next, the mobile device (**red**) may also "be used to authenticate a user to another processing system," such as an external proximity reader 1120 or a computer that includes "point-of-sale components" (not shown) to "perform a sales transaction" (e.g., "credit card transactions"), as shown below.



Id., Fig. 11 (annotated), [0193]-[0196]. Ex-1003 ¶¶60-66.

C. Giobbi157

Giobbi157, U.S. Patent Application Publication No. 2007/0245157, published on October 18, 2007, qualifies as prior art under pre-AIA 35 U.S.C. §102(a). Giobbi157 "provide[s] efficient, secure, and highly reliable authentication for transaction processing and/or access control applications." Ex-1006, Abstract. In Giobbi157, a personal digital key (PDK) "stores one or more profiles (e.g., a biometric profile) in a tamperproof memory," *id.*, and may be integrated into a hybrid device, "such as a cell phone." *Id.*, [0035], [0011].

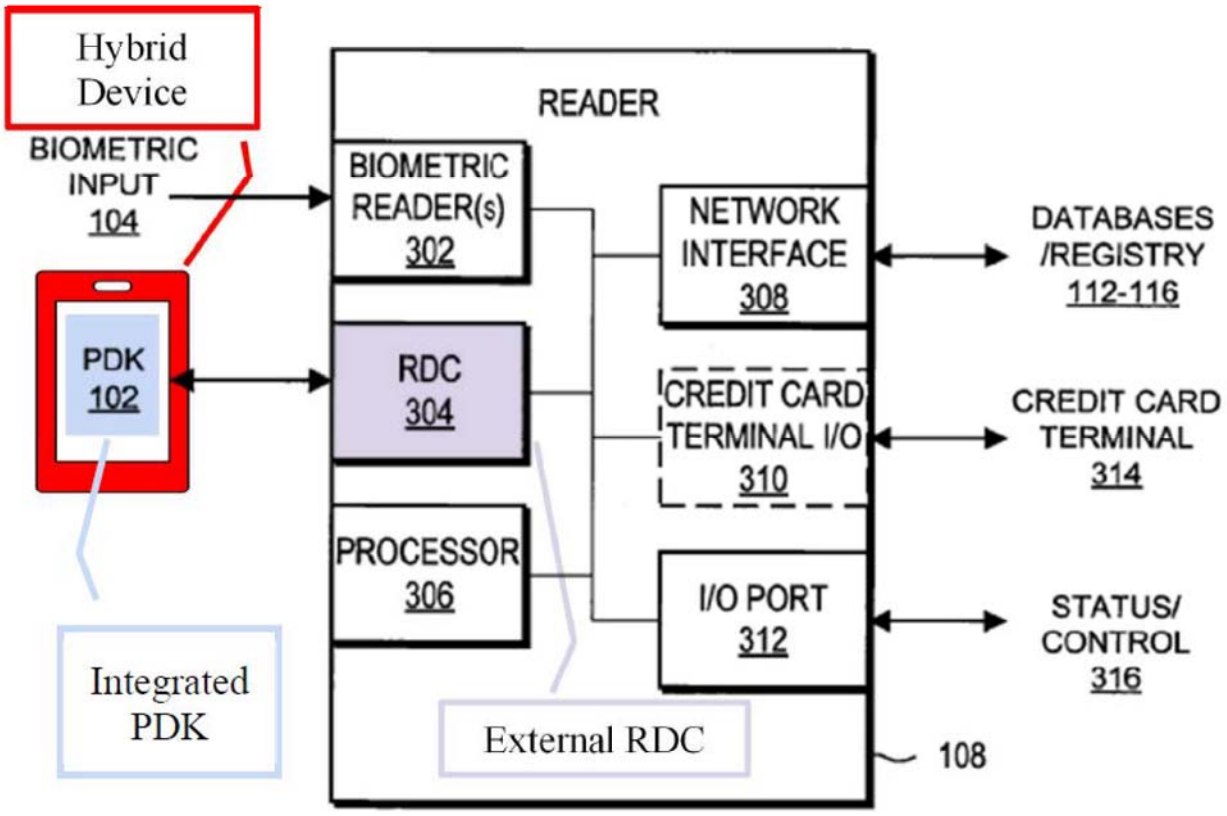


FIG. 3

Id., Fig. 3 (annotated). The integrated PDK wirelessly communicates with an external receiver-decoder circuit (RDC), such that information stored on the integrated PDK is transmitted to the external RDC located on a "Reader 108." *Id.*, [0012], [0026]. The external RDC is communicatively coupled to an external database that is used for enabling an application, function, or service:

> [I]n one type of authentication, information is received from the PDK 102 at the RDC 304, processed by the processor 306, and transmitted to an external database 112-116 through the network interface 308.

Id., [0053]. Giobbi157's hybrid device, which contains the PDK, enables an application, function, or service to take place by, for example, enabling a financial transaction, such as an ATM withdrawal:

> Additionally, the PDK can store other information such as credit/debit card information, bank information, or personal information in a memory for use in authorizing or completing a transaction.

Id., [0011], [0065]. Ex-1003 ¶¶67-73.

D. Nishikawa

Nishikawa, European Patent Application Publication No. EP 1600885, published on November 30, 2005, qualifies as prior art under pre-AIA 35 U.S.C. §102(b). Nishikawa discloses an improved e-token (e.g., "key holder type ID

module") that acts as "a SIM reader/writer ... having contact and noncontact interfaces." Ex-1014, [0001, [0017]. Nishikawa teaches "ways to improve the convenience of the key holder type ID module … to provide the reader/writer with a short-distance communication function and a fingerprint sensing function." *Id.*, [0017]. In Nishikawa, the SIM card is "loaded with multiple applications, such as electronic money, an electronic ticket, a fingerprint template, a fingerprint collating engine and a personnel ID card." *Id.*, [0111]. In doing so, Nishikawa provides the key holder type ID module with a "noncontact communication function and the short-distance communication means" for use "as an electronic ticket and as electronic money for various noncontact transactions," and with a "fingerprint sensor" for authentication "on the basis of biometric data." *Id.*, [0113]-[0114]. Ex-1003 ¶¶79-85.

IV. Grounds 1 and 2: Dua and Giobbi157 or Dua, Giobbi157 and Kotola Render Obvious Claims 1-6, 8-11, And 14-19

A. Independent Claims

1. Claim 14

Dua alone, or in view of Giobbi157 renders obvious independent claim 14. Ex-1003, ¶¶101-104.

a. [14pre]: "A method comprising:"

To the extent the preamble is limiting, Dua discloses it because Dua discloses a method to automatically set up and establish a wireless connection between two devices based on the proximity of the devices. Ex-1004, [0013]; Ex-1003 ¶105.

b. [14a]: "creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,"

Dua discloses [14a].

(1) A hybrid device:

Dua discloses the hybrid device in [14a] because it discloses a media player (e.g., cellular phone) that includes an RFID Tag-Reader Module that is integrated into the device, as shown below. Ex-1004, [0057], [0070]; Ex-1003 ¶¶106-124.

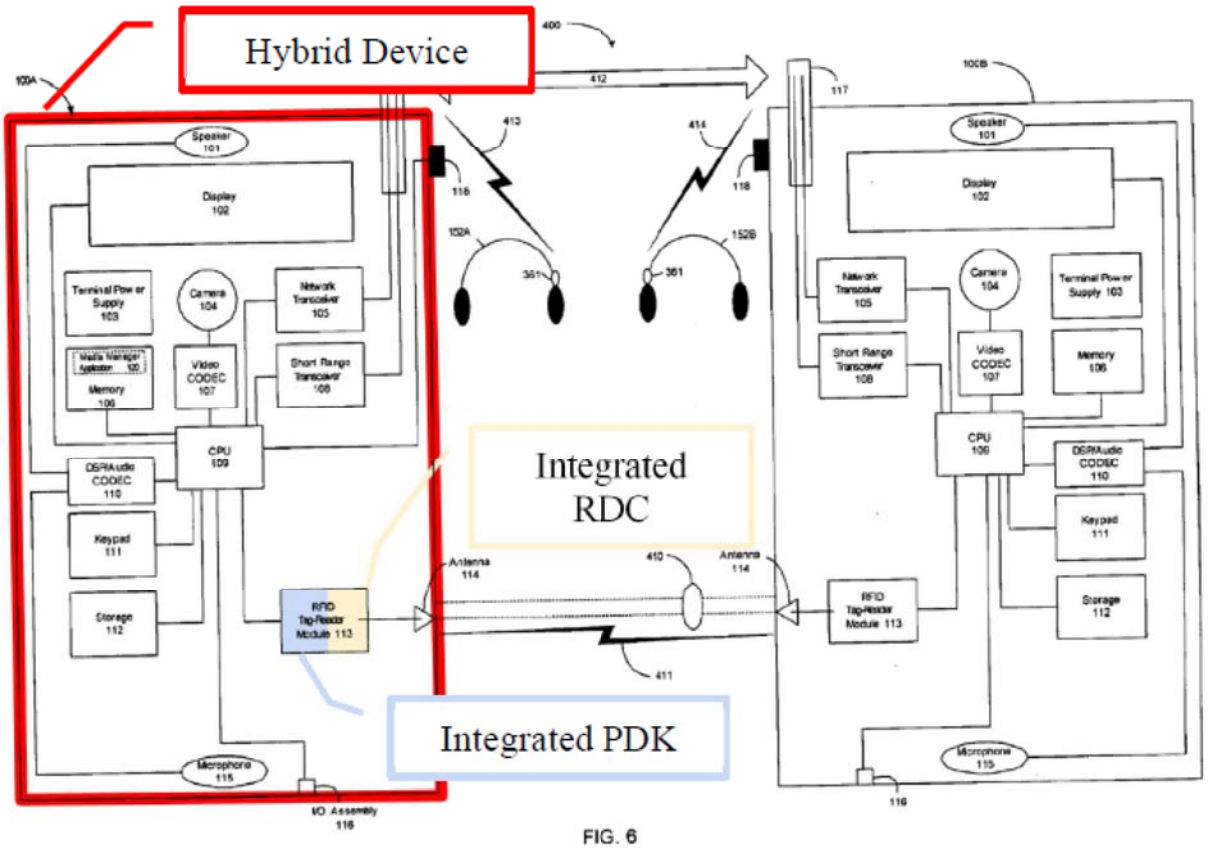


FIG. 6

Ex-1004, Fig. 6 (annotated). Dua's media player ("hybrid device," **red**) includes an RFID Tag-Reader Module 113 (e.g., "integrated PDK," **blue**; "integrated RDC," **yellow**) that enables the device to "rapidly exchange information with an electronic device that is in close proximity and which also has integrated RFID technology." Ex-1004, [0057], [0070], Figs. 1, 6. Dua's RFID Tag-Reader Module, as shown below, includes "both an RFID tag [(the claimed 'integrated PDK,' **blue**)] and an RFID reader [(the claimed 'integrated RDC,' **yellow**)]." *Id.*, [0089].

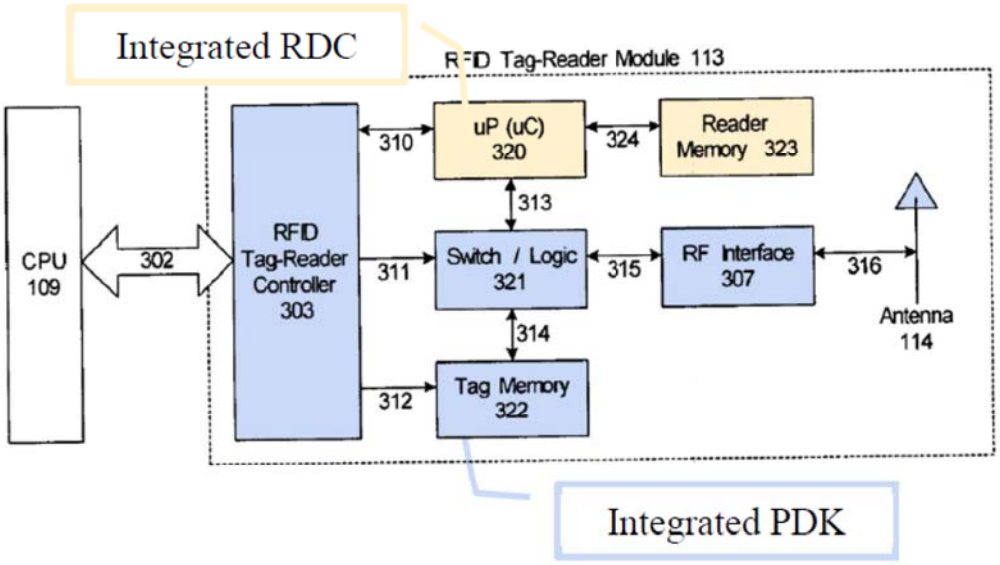


FIG. 4B

Id., Fig. 4B (annotated).

Dua's Tag-Reader Module (**blue**), as shown, includes a collection of circuit components that makes up a "personal digital key" under either the court's construction or Petitioner's proposed construction. Ex-1003 ¶110. This operably connected collection of components includes an antenna 114 and an RF Interface 307 (a transceiver) capable of modulating and demodulating RF signals for communications with an external tag reader (an RDC). Ex-1004, [0101], [0104], [0106]; Ex-1003 ¶111. Dua's RFID Tag-Reader Module (**blue**) includes "an integrated RFID Tag-Reader Controller 303 that manages all communication between CPU 109 and the functional components of RFID Tag-Reader Module 113," and "tag logic" 321. Ex-1004, [0106], [0108]. "Correspondingly, the tag memory 322 is connected to the switch/logic component 321" and "to the RFID Tag-Reader Controller 303 in order to receive configuration data." *Id.*, [0108]. The Tag

Memory 322 for storing tag data may be a "configurable tag memory," such as a "non-volatile configurable memory," and may be "tamper resistant as to prevent hackers from retrieving confidential information and encryption keys" stored therein. *Id.*, [0105], [0109]. The stored information may include a "user identifier" or "other attributes (e.g., a complete calling card containing the contact information for the device owner such as f[u]ll name, title, company, mailing address, E.164 number, e-mail address, etc.)." *Id.*, [0133], Fig. 7. The RFID tag component may also store information to enable services with an external device, including "electronic payments at the point-of-sale and secure key access to buildings, cars, etc." *Id.*, [0070], [0089]. Tag-Reader Controller 303 and Tag Memory 322 thus store information particular to a user. Ex-1003 ¶¶112-113.

Dua's Tag-Reader Module (yellow), as shown, includes a collection of circuit components that makes up a "receiver-decoder circuit" under either the court's construction or Petitioner's proposed construction. Ex-1003 ¶¶114-116. These operably connected components include a reader logic 320 that is implemented as a microcontroller (µC) and a microprocessor (µP). Ex-1004, [0106]. "The reader logic operates the interface and protocol framework for communicating with RFID tags (passive communication mode) and in particular, when supporting active communication mode, for communicating with RFID tag reader devices." *Id.* The RFID "reader component" is used for "transmitting interrogation signals via its

antenna to an external electronic device's RFID tag when in close proximity, and receiving a response signal from the external device's RFID tag." *Id.*, [0071], [0100]. The response signal includes "RFID transmission data." *Id.*, [0130]-[0143]. A reader memory 323 may also be used as a buffer storage for communication with media player 100, as well as with an RFID tag or another RFID tag reader device. *Id.*, [0107].

In Dua, when "enhanced security is desired" for RFID transmission, encryption keys are used and shared between the external device and the hybrid device to facilitate the sharing of "sensitive" information between the devices. *Id.*, [0152]. A POSITA reading Dua would have understood that the encryption keys provide "enhanced security" by enabling the devices to stored encrypted , "sensitive" information. *Id.*; Ex-1003 ¶¶117-118. It would have been obvious to store encrypted "confidential information" in the external device's tag memory and transfer encrypted information to enhance security during the data transfer to the hybrid device. Ex-1004, [0109]; Ex-1003 ¶118. A POSITA would have been motivated to use an encryption key to improve RFID security so that "hackers" could not access the encrypted, confidential information during any data transfer from the external device to the hybrid device, as Dua suggests. Ex-1004, [0109], [0152]; Ex-1003 ¶119; *see also* Ex-1006, [0047] ("[T]he data can be encrypted by the transceiver ... and transmitted over a secure link."), [0050] ("Encrypting data transmitted between

the PDK 102 and Reader 108 minimizes the possibility of eavesdropping or other fraudulent activity."). A POSITA would have had a reasonable expectation of success in encrypting the RFID transmissions because Dua explains that the encryption key is stored in the external tag memory (external PDK), and the external tag could transfer the encryption key to an RFID reader (integrated RDC) for decrypting the encrypted data. Ex-1004, [0108], [0152]; Ex-1003 ¶120. The RFID reader (integrated RDC) thus would receive any confidential data in an encrypted format and decode the encrypted data using the encryption key. Ex-1003 ¶120.

To the extent that Proxense contends the claimed RDC requires separate wireless communication components (e.g., RF interface and antenna) different from the claimed PDK, it would have been obvious to include a separate RF interface and antenna, instead of common RF interface and antenna. Ex-1003 ¶121; Ex-1017, [0058] (The mobile terminal including a separate terminal RFID reader module 220 that communicates wirelessly using a separate antenna 219 in addition to the RFID tag 215); [0056]-[0057] (RFID tag 215 is connected to antenna 220), Fig. 4. A POSITA would have been motivated to use multiple antennas because doing so provides antenna diversity for mitigating fading and improving signal reception and enables simultaneous transmission and reception of signals. Ex-1003 ¶122. Adding an additional RF interface and antenna to Dua's RFID Tag-Reader Module would have been no more than duplicating prior art elements according to known methods

to yield predictable results because Dua's device already uses multiple antennas and transceivers for sending and receiving different signals. Ex-1004, [0062], [0084]; Ex-1003 ¶122. Moreover, Dua itself fully incorporated by reference details concerning such "other RFID Tag-Reader Module designs." Ex-1004, [0114] (citing Ex-1017); Ex-1017, Fig. 4, [0056]-[0058]. A POSITA would have had a reasonable expectation of success in duplicating the RF interface and antenna to include separate wireless communication components for the RFID tag and RFID reader. Ex-1003, ¶122.

Alternatively, Dua in view of Kotola (ground 2) renders obvious having separate wireless communication components (e.g., RF interface and antenna) for the claimed PDK and RDC. *Id.*, ¶¶123-125. Kotola discloses a mobile terminal having an integrated RFID tag and an integrated RFID reader. Ex-1017, Fig. 4, [0056]-[0058]. As Kotola explains, the RFID tag is connected to "[a]n antenna film or coil 220" and "analog circuit 223 for converting the RF signals … into digital signals," *id.*, [0057], and the separate RFID reader is connected to "antenna 219," *id.*, [0058]. it would have been obvious to implement separate antennas, as Kotola teaches, because Dua's citation to Kotola "provide[s] a justification for combining the references for obviousness purposes." *Commonwealth Sci. & Indus. Rsch. Org. v. Buffalo Tech. (USA), Inc.*, 542 F.3d 1363, 1372 (Fed. Cir. 2008); Ex-1004, [0114] (citing Ex-1017). Moreover, a POSITA would have been motivated to use multiple

antennas because doing so provides antenna diversity for mitigating fading and improving signal reception and enables simultaneous transmission and reception of signals. Ex-1003 ¶124. A POSITA would have had a reasonable expectation of success in using additional wireless communication components for RFID reader. Ex-1003 ¶125.

Accordingly, Dua discloses a hybrid device, as claimed. Ex-1003 ¶¶126.

(2) Creating a First Wireless Link between an Integrated RDC of the Hybrid Device and an External Device:

Dua discloses creating a first wireless link during an RFID discovery process as in [14a] because the RFID reader component generates and transmits interrogation signals to create an RFID link between the integrated RFID reader (integrated RDC) in the hybrid device and an external RFID tag in an external device, as shown below. Ex-1004, [0122]; Ex-1003 ¶¶127-130.

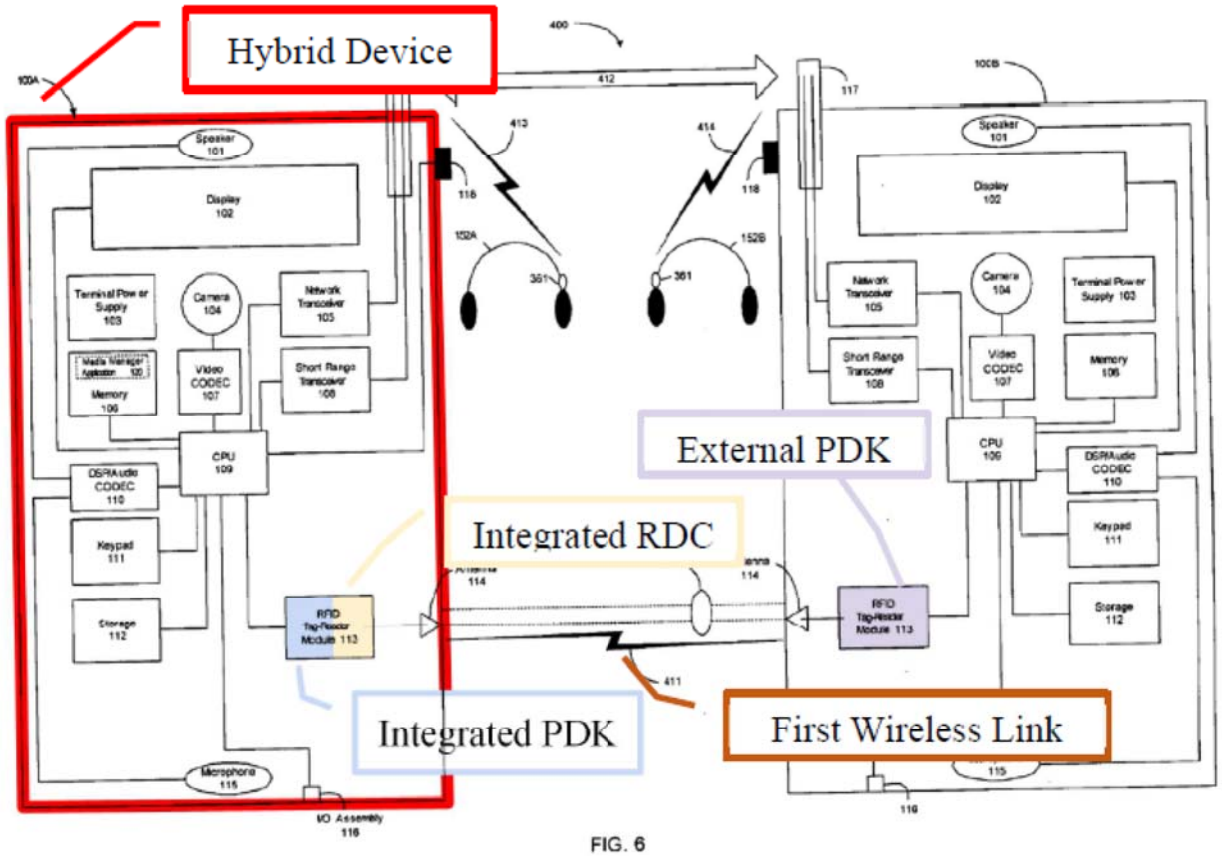


FIG. 6

Ex-1004, Fig. 6 (annotated). Because both components are labeled as "RFID Tag-Reader Module 113," they both include the circuit components required for the claimed "PDK" and "RDC," as addressed above. The "reader component" of the "RFID Tag-Reader Module 113" in device 100A (integrated RDC) then communicates with the "tag component" of the "RFID Tag-Reader Module 113" in

device 100B (external PDK).[5] *Id.*, [0071]-[0072], [0127]-[0128], Fig. 4. Moreover, as Dua explains, the "reader component" is used for transmitting interrogation signals to an external electronic device's RFID tag when in close proximity. *Id.*, [0071]-[0072], [0127].

c. [14b]: "the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;"

Dua discloses or renders obvious [14b].

As discussed in §IV.A.1.b, Dua's hybrid device includes an integrated PDK, which includes an integrated, secure memory, and an integrated RDC. Ex-1003 ¶¶131-138. Dua's RFID Tag-Reader Module (**blue**) also includes a Tag Memory 322 such as a "non-volatile configurable memory" that may be "tamper resistant as to prevent hackers from retrieving confidential information and encryption keys" stored therein. Ex-1004, [0105], [0109]. Thus, the integrated tag memory securely stores information therein. Ex-1003 ¶¶132-133.

[5] The "tag components" of the "RFID Tag-Reader Module 113" in device 100A (integrated PDK) also communicates with the "reader component" of the "RFID Tag-Reader Module 113" in device 100B (external RDC).

Dua explains that when "enhanced security is desired," encryption keys are used and shared between the hybrid device and external device to facilitate the sharing of "sensitive" information between the devices. Ex-1004, [0152]. A POSITA reading Dua would have understood that the encryption keys provide "enhanced security" by encrypting "sensitive" information using those keys. Ex-1004, [0152]; Ex-1003 ¶¶134-135.

To the extent this is disputed, a POSITA would have been motivated and found it obvious to encrypt the "confidential information" stored in the hybrid device's tag memory to enhance security. Ex-1004, [0109]; Ex-1003 ¶135. A POSITA would have been motivated to use an encryption key to improve RFID security so that "hackers" could not access the encrypted, confidential information during any data transfer from the hybrid device to the external device, as Dua suggests. Ex-1004, [0109], [0152]; Ex-1003 ¶136.

A POSITA would have had a reasonable expectation of success in using encryption to enhance security because Dua explains that the encryption key is stored in the integrated tag memory (integrated PDK), and the tag could transfer the encryption key to an external RFID reader for decrypting the encrypted data. Ex-1004, [0109], [0152]; Ex-1003 ¶137. Dua's integrated tag memory (integrated PDK) thus would store local, encrypted "confidential information" in an integrated, tamper-resistant memory. Ex-1003 ¶138.

d. [14c]: "receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and"

Dua discloses [14c] because it discloses receiving "RFID transmission data" (a first signal) at the hybrid device's reader component (the integrated RDC) via the first wireless link from the external RFID tag (the external PDK). Ex-1004, [0127]; Ex-1003 ¶¶139-141. As Dua explains, during the RFID discovery process, after the external device's RFID tag received the interrogation signals, the external device's RFID tag transmits RFID transmission data to the hybrid device. Ex-1004, [0127]-[0144]; Ex-1003 ¶141. The transmitted RFID transmission data (first signal) includes information such as "communication settings, media processing capabilities, and other parameters" for establishing a wireless connection with the external device. Ex-1004, [0128].

e. [14d]: "generating an enablement signal enabling one or more of an application, a function and a service."

Dua discloses [14d] because it discloses the hybrid device generating "a Bluetooth paging message" (an enablement signal) to enable an application, function, or service after receiving the RFID transmission data from an external device with an RFID tag-reader module. Ex-1004, [0123], [0128]; Ex-1003 ¶¶142-143. [14d] is recited as allowing "mixed operations." Ex-1001, Abstract, 16:39-46.

Because [14c] recites alternative events,[6] "the entire element is disclosed by the prior art if one alternative...is in the prior art." *Fresenius USA, Inc. v. Baxter Int'l, Inc.*, 582 F.3d 1288, 1298 (Fed. Cir. 2009).

To the extent that the enablement signal must be generated by the integrated RFID reader, Dua discloses this. As Dua explains, digital media may be playing on a hybrid device, and the user of the hybrid device may decide to transmit the digital media (e.g., music) to an external device. Ex-1004, [0126]. By bringing the external device into proximity with the hybrid device, the hybrid device's integrated RFID reader (RDC) wirelessly communicates interrogation signals to the external device's RFID tag, which in turn wirelessly communicates RFID transmission data to the integrated RFID reader (RDC). *Id.*, [0127]-[0142]. This RFID discovery/paging process causes the hybrid device to generate a Bluetooth paging message (enablement signal) to enable a service (e.g., wireless connection and transmission of media) on the external device. According to Dua, the Bluetooth paging message causes the external device to perform a wireless connection set up, and upon

[6] This is consistent with Proxense purported construction of "one or more of an application, a function and a service" as requiring only "application, function, **or** service." Ex-1018, 10 (Ex. E, Preliminary Infringement Contentions). Proxense served Final Infringement Contentions, and its position remains the same.

completion, the hybrid device "automatically transmits" media content to the external device. Ex-1004, [0123], [0128]. During the transmission of the media content, the media could be "automatically convert[ed] ... into a format that is supported by" the external device. *Id.*, [0161], [0172]. Accordingly, the Bluetooth paging message may be used to enable wireless transmission of media that would not have otherwise been supported by the external device. Ex-1003 ¶¶146-151.

Alternatively, the Bluetooth paging message is generated to enable a function (e.g., wireless connection) between the hybrid device and external device. Ex-1004, [0144]. As Dua explains, the hybrid device and target device may "conserve power by not always having their wireless interface turned on." *Id.*, [0144], [0137]. According to Dua, the RFID transmission data helps "facilitate the automatic activation of a radio transceiver with an appropriate communications protocol," such as exchanging Bluetooth paging messages, to enable wireless connectivity functions in the two devices. *Id.*, [0144]; Ex-1003 ¶152.

To the extent the enablement signal must be generated by the integrated RFID tag (integrated, secure memory), Dua also discloses this. Dua explains its integrated RFID tag can establish "wireless communication between a diverse set of [external] devices" for various purposes, including "for electronic payments" at point-of-sale or to "secure key access to buildings." Ex-1004, [0052], [0070]. According to Dua, "a credit card profile or other payment information" may be stored on the hybrid

device. *Id.*, [0224]. During electronic payments using RFID technology, the integrated RFID tag (integrated, secure memory) would generate RFID signal (enablement signal) to exchange financial information with the external point-of-sale device that is in close proximity to enable electronic payments. 1004, [0070]. Ex-1003 ¶¶153-155.

While Dua does not expressly disclose where the credit card profile or other payment information is stored, a POSITA would have been motivated and found it obvious to securely store the financial information in its tamper-resistant tag memory "to prevent hackers from retrieving confidential information." *Id.*, [0105], [0109]. Indeed, as Giobbi157 teaches, "credit/debit card information" used to complete financial transactions (e.g., "charging a credit card for a purchase") would be stored in a "profile memory field 232" in the "physical access secured and tamperproof" memory. Ex-1006, [0036], [0042], [0063].

A POSITA would reasonably expected to succeed in storing the "credit card profile or other payment information" in Dua's tamper-resistant tag memory because storing the "credit card profile or other payment information" in tag memory would require minimal modification without undue experimentation. Ex-1003 ¶156-158. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003 ¶158; *see Friskit, Inc. v. Real Networks, Inc.*, 306 F. App'x 610, 616 (Fed. Cir. 2009).

2. Claim 1

a. [1pre]: "A hybrid device comprising:"

To the extent the preamble is limiting, Dua discloses a hybrid device because it discloses a media player (e.g., cellular phone) that includes an RFID Tag-Reader Module (hybrid device). Ex-1004, [0057], [0070]; §IV.A.1.b; Ex-1003 ¶¶159-160.

b. [1a]: "an integrated, secure memory storing local, secured information; and"

Dua discloses or renders obvious [1a] for reasons articulated in [14b]. Ex-1004, [0105], [0109], [0152]; Ex-1003 ¶¶161-162; §IV.A.1.c.

c. [1b]: "an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,"

Dua discloses [1b] because its RFID reader component (RDC) communicates wirelessly with at least one external RFID tag when within a proximity zone, as explained in [14a]. Ex-1004, [0071]-[0072], [0122], [0127]; Ex-1003 ¶¶163-164; §IV.A.1.b.

d. [1c]: "the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,"

Dua discloses [1c] because its RFID reader component (RDC) is communicatively coupled to the integrated, secure tag memory for communication with the integrated, secure tag memory (PDK), as shown below. Ex-1003 ¶¶165-168.

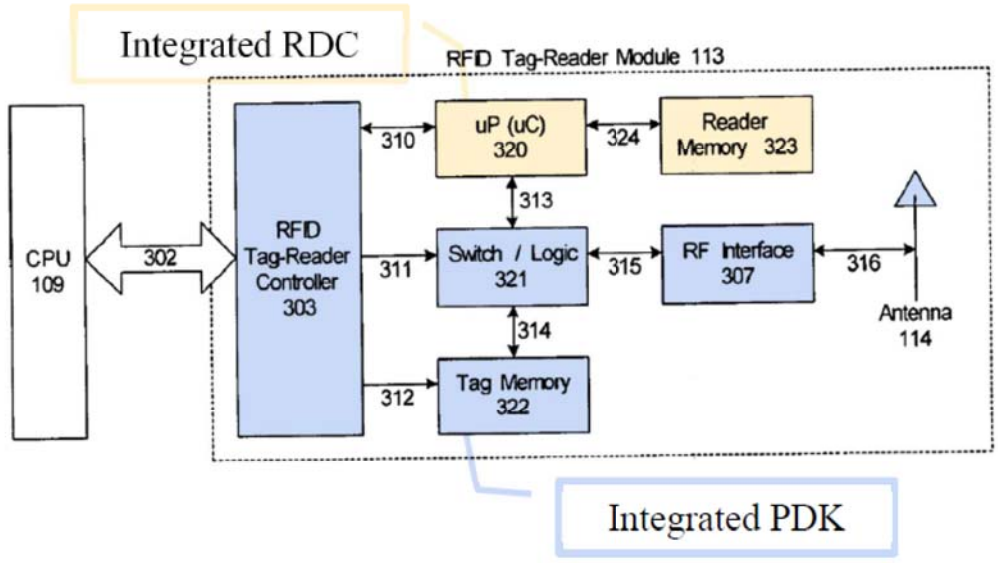


FIG. 4B

Ex-1004, Fig. 4B (annotated).

Dua's RFID Tag-Reader Module includes "an integrated RFID Tag-Reader Controller 303 that manages all communication between CPU 109 and the functional components of RFID Tag-Reader Module 113," and "tag logic" (e.g., switch/logic component 321). *Id.*, [0106], [0108]. During cross-discovery, an RFID tag can be written with data received by an RFID reader. *Id.*, [0152]. Accordingly, the integrated RDC is communicatively coupled to the integrated, secure memory to update the information stored in the RFID tag memory. *Id.*, [0151]-[0154].

e. [1d]: "wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and service."

As discussed in §IV.A.1.e, Dua discloses [1d] that either the integrated RDC or the local, secured information stored by the integrated, secure memory (PDK) enables an application, function, or service. Ex-1003 ¶¶169-170.

(a) Integrated RDC Communicating Wirelessly with the External Device Within the Proximity Zone Enables an Application, Function, or Service:

As discussed in §IV.A.1.e, Dua discloses that, when an external device is within a proximity zone of its integrated RFID reader (RDC), the integrated RFID reader (RDC) communicates wirelessly with the external device's RFID tag. Ex-1003 ¶170. Data received by the RFID reader is sent to the hybrid device's CPU for use by applications operating on the hybrid device to generate a Bluetooth paging message to enable a wireless connection and transmission of media to the external device, as in [1d](a). Ex-1004, [0103], [0123], [0128], [0161], [0172]; Ex-1003 ¶171.

(b) The Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

As discussed in §V.A.1.e, Buer teaches that the local, encrypted financial information stored in the integrated, tamper-resistant memory enables "electronic payments" at point-of-sale, as in [1d](b). Ex-1004, [0052], [0070], [0109]; Ex-1003 ¶172.

B. Dependent Claims

1. [2]: "The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device."

Dua discloses claim 2 because its application, service, or function that is enabled runs on the hybrid device itself. *See* [14d]; Ex-1003 ¶¶173-174. Dua explains that the hybrid device may "conserve power by not always having their wireless interface turned on." Ex-1004, [0144], [0137]. Dua explains that the hybrid device uses the RFID discovery/paging process to help "facilitate the automatic activation of a radio transceiver" in the hybrid device. *Id.*, [0144]; Ex-1003 ¶¶174.

2. [3]: "The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC."

Dua discloses claim 3 that an application, function, or service that is enabled runs externally to the hybrid device using an external RDC. *See* [1d], [14d]; Ex-1003 ¶¶175-179. Dua explains that its integrated RFID tag could establish "wireless communication between a diverse set of [external] devices" for various purposes, including "for electronic payments" at point-of-sale or to "secure key access to buildings." Ex-1004, [0052], [0070]. According to Dua, the hybrid device uses RFID to wirelessly communicate with the external RF 13.56 MHz readers. *Id.*, [0089]. Credit card information stored in the hybrid device is sent via the integrated RFID Tag-Reader Module to the external RFID reader at the point-of-sale device for enabling electronic payments. *Id.*, [0070], [0224].

A POSITA reading Dua would have desired to stored encrypted credit card information in the hybrid device to provide enhanced security. *Id.*, [0152]; Ex-1003 ¶177. A POSITA would have been motivated to improve RFID security so that the credit card information that is transferred between a tag and a reader could be encrypted so that "hackers" could not access the sensitive information, as Dua suggests. Ex-1004, [0109], [0152]; Ex-1003 ¶178; *see also* Ex-1006, [0047] ("[T]he

data can be encrypted by the transceiver … and transmitted over a secure link."), [0050] ("Encrypting data transmitted between the PDK 102 and Reader 108 minimizes the possibility of eavesdropping or other fraudulent activity"). A POSITA would have had a reasonable expectation of success in using encryption to enhance security because Dua explains that the encryption key is stored in the tag memory, and the tag could transfer the encryption key to an RFID reader for decrypting the encrypted data. Ex-1004, [0108]-[0109], [0152]; Ex-1003 ¶179. The reader thus would receive the credit card information in an encrypted format and decode the encrypted credit card information using the encryption key. Ex-1003 ¶179. Accordingly, the external RFID reader would be an external RPC because the external RFID reader would decrypt the encrypted credit card information. Ex-1003 ¶179.

3. [4]: "The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user."

Dua in view of Giobbi157 renders obvious claim 4 because the information stored locally on its integrated tag is secured biometric information for authenticating a user. Dua discloses that its hybrid device may include "an integrated biometric fingerprint reader [to] provide[] enhanced security for protecting ... against unauthorized use." Ex-1004, [0058]. Giobbi157 teaches storing "biometric profile" in a local, secured memory, so that a user would use "a matching biometric input"

obtained from the hybrid device to "unlock" the tag memory. Ex-1006, [0043]. Giobbi157 teaches that the biometric input would be used to compare "stored biometric information" to authenticate the user (e.g., fingerprint authentication). *Id.*, [0028], [0037]-[0038], [0048]. A POSITA would have been motivated to include biometric information for authenticating a user in Dua's local, tamper-resistant tag memory because doing so would promote Dua's purpose of "enhanc[ing] security for protecting ... against unauthorized use." Ex-1004, [0058]; Ex-1003 ¶183. A POSITA would have been capable of storing "biometric information for authenticating a user" in Dua's tag memory, as Giobbi157 teaches, because Dua's hybrid device has an integrated biometric fingerprint reader, Ex-1004, [0058], and it would have required minimal modification without undue experimentation to store the "biometric fingerprint" information in Dua's tag memory. Ex-1003 ¶184. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003 ¶184; *see Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in storing "biometric information for authenticating a user" in Dua's tamper-resistant tag memory. Ex-1003 ¶184.

4. [5]: "The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user."

As discussed in §IV.B.3, Dua in view of Giobbi157 renders obvious claim 5 because the biometric information is based on a biometric scan of a finger. Ex-1006, [0037]; Ex-1003 ¶185. Giobbi157 explains that in the "case of fingerprint authentication," "the biometric profile sample may represent only [a] small portion area of the full fingerprint image," "the fingerprint profile sample … [may] describe[] an arc of one or more lines of the fingerprint," or "the fingerprint profile sample can be data representing color information of the fingerprint." Ex-1006, [0038]; Ex-1003 ¶¶186-187.

5. [6]: "The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information."

As discussed in §IV.A.1.e, Dua in view of Giobbi157 renders obvious claim 6 because the local, secure information may be "credit card profile or other payment information" used to complete financial transactions (e.g., "electronic payments" at point-of-sale). Ex-1004, [0052], [0070], [0224]. As explained in §IV.A.1.e, Dua does not expressly discloses where the credit card profile or other payment information is stored, but Dua in view of Giobbi157 renders obvious that the credit

card profile or other payment information would have been stored in its tamper-resistant tag memory. *Id.*, [0105], [0109]; Ex-1003 ¶¶188-190.

6. [8]: "The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database."

Dua in view of Giobbi157 renders obvious claim 8. Giobbi157 discloses that its external reader is communicatively coupled "to receive and/or transmit information to remote databases for remote authentication." Ex-1006, [0031], [0053]. The remote databases include a "validation database ... for authorizing a transaction to be processed." *Id.*, [0033]. In Giobbi157, "the process involves transmitting credit card (or other purchasing information) to a validation database 112 to authorize the purchase and receive the status of the card." *Id.*, [0074]. A POSITA would have been motivated to use an external validation database, as Giobbi157 teaches, because the validation database would provide protection to ensure that "the card is active and not reported lost or stolen and that sufficient funds are present to execute the purchase," *id.*, when Dua's RFID Tag-Reader Module is used for "electronic payments at the point-of-sale." *Id.*, [0070]. A POSITA would have been motivated to use an external validation database, as Giobbi157 teaches, because doing so would require minimal modification without undue

experimentation. Ex-1003 ¶¶191-193. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003 ¶194; *see Friskit*, 306 F. App'x at 616. A POSITA would have had a reasonable expectation of success in using a validation database to complement the financial transaction. Ex-1003 ¶194.

7. [9]: "The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction."

Dua in view of Giobbi157 renders obvious claim 9. Ex-1003 ¶¶195-196. As discussed with respect to claim 8, Giobbi157 discloses an external validation database. Giobbi157 discloses that "in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale." Ex-1006, [0033].

8. [10]: "The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility."

Dua in view of Giobbi157 renders obvious claim 10. Dua discloses its integrated RFID tag could establish "wireless communication between a diverse set

of devices," including "for electronic payments" at point-of-sale or to "secure key access to buildings." Ex-1004, [0052], [0070].

As the '289 patent explains, a device may have two applications, each of which can access a different local, secured information stored on an integrated, secure memory. Ex-1001, 9:41-47. For example, a first application (e.g., "auto login/logoff") may be "enabled" based on a first local, secured information (e.g., "username and password"), *id.*, 9:47-50, while a second application (e.g., "credit card transaction") uses a second local, secured information (e.g., biometric information" or "credit card information," etc.), *id.*, 9:50-55, 9:13-19. It would have been obvious that the information for "electronic payments" is different from information for "secure key access to buildings." Ex-1003 ¶¶197-199. Indeed, Giobbi157 discloses storing multiple user profiles, such as biometric profile, PIN profile, picture profile, registry profile, credit cards, and personal information, in its secured and tamperproof memories. Ex-1006, [0037]-[0042], [0058]. Each of the profiles provides a different accessibility to certain application, function, or service. For example, one profile may be used to enable "access to secure physical or digital assets," and another may be used for completing a purchase transaction. *Id.*, [0063]. A POSITA would have been motivated to store multiple subsets of local, secured information, as Giobbi157 teaches, so the hybrid device can access different applications, functions, or services. A POSITA would have been motivated to store

a credit card information in one subset of local, secured information for credit card processing, and a biometric profile or PIN profile in another subset of local, secured information for accessing physical assets, such as gaining access to buildings. Ex-1003 ¶200. A POSITA would have been motivated to use multiple profiles, as Giobbi157 teaches, because doing so would require minimal modification without undue experimentation. Ex-1003 ¶201. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003 ¶201; *see Friskit*, *306* F. App'x at 616. A POSITA would have had a reasonable expectation of success in using multiple profiles. Ex-1003 ¶201.

9. [11]: "The hybrid device of claim 1, wherein the hybrid device is a cell phone."

Dua discloses claim 11 because the hybrid device may be a portable electronic device such as a cell phone. Ex-1004, [0057], [0070], [0174]; *see* claims 1, 14; Ex-1003, ¶¶202-203.

10. [15]: "The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device."

See [2]; Ex-1003, ¶204.

11. **[16]: "The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC."**

See [3]; Ex-1003, ¶205.

12. **[17]: "The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user."**

See [4]; Ex-1003, ¶206.

13. **[18]: "The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction."**

See [6]; Ex-1003, ¶207.

14. **[19]: "The method of claim 14, wherein the hybrid device is a cell phone."**

See [11]; Ex-1003, ¶208.

V. Grounds 3 and 4: Buer Renders Obvious Claims 1-7, 10-11, and 14-19 (Ground 3); Buer and Giobbi157 Render Obvious Claims 4, 8-10, 12, 13, 17, and 20 (Ground 4).

A. Independent Claims

Buer renders obvious each of independent claims 1 and 14. Ex-1003 ¶209. Independent claim 14 is representative.

1. Claim 14

a. [14pre]: "A method comprising:"

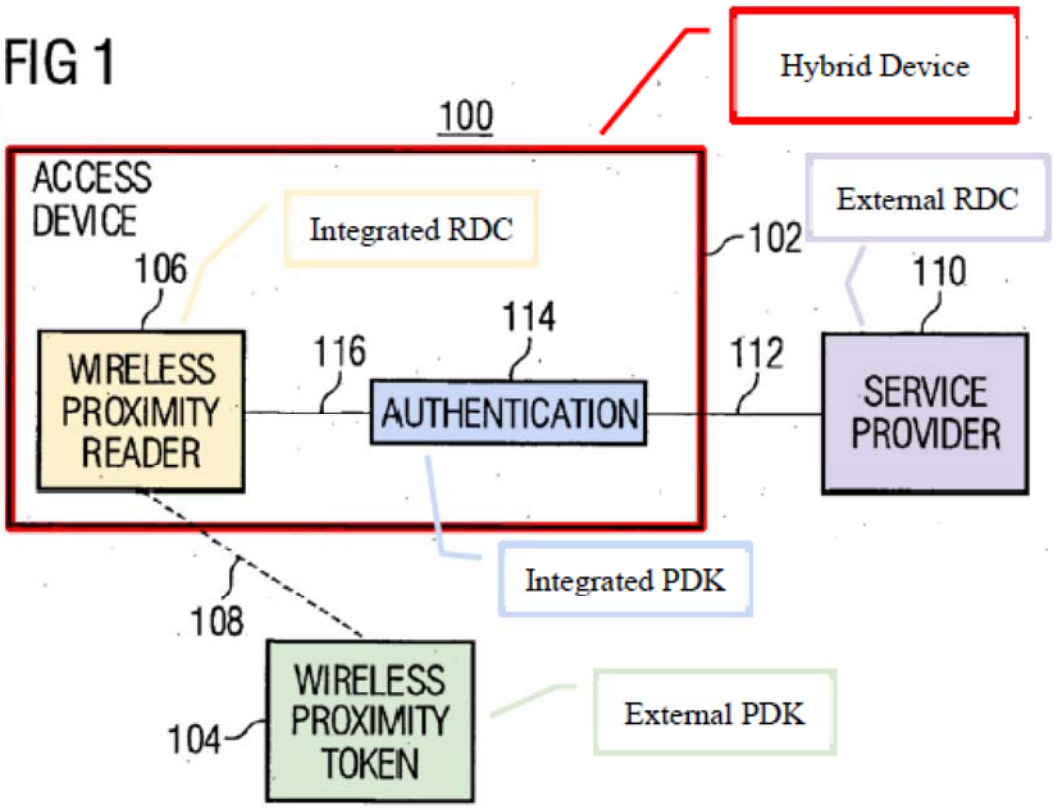
To the extent the preamble is limiting, Buer discloses it because Buer discloses a method for an access device to access a secured service. Ex-1003 ¶210.

b. [14a]: "creating a first wireless link between an integrated receiver-decoder circuit (RDC) of a hybrid device and an external device,"

Buer discloses [14a].

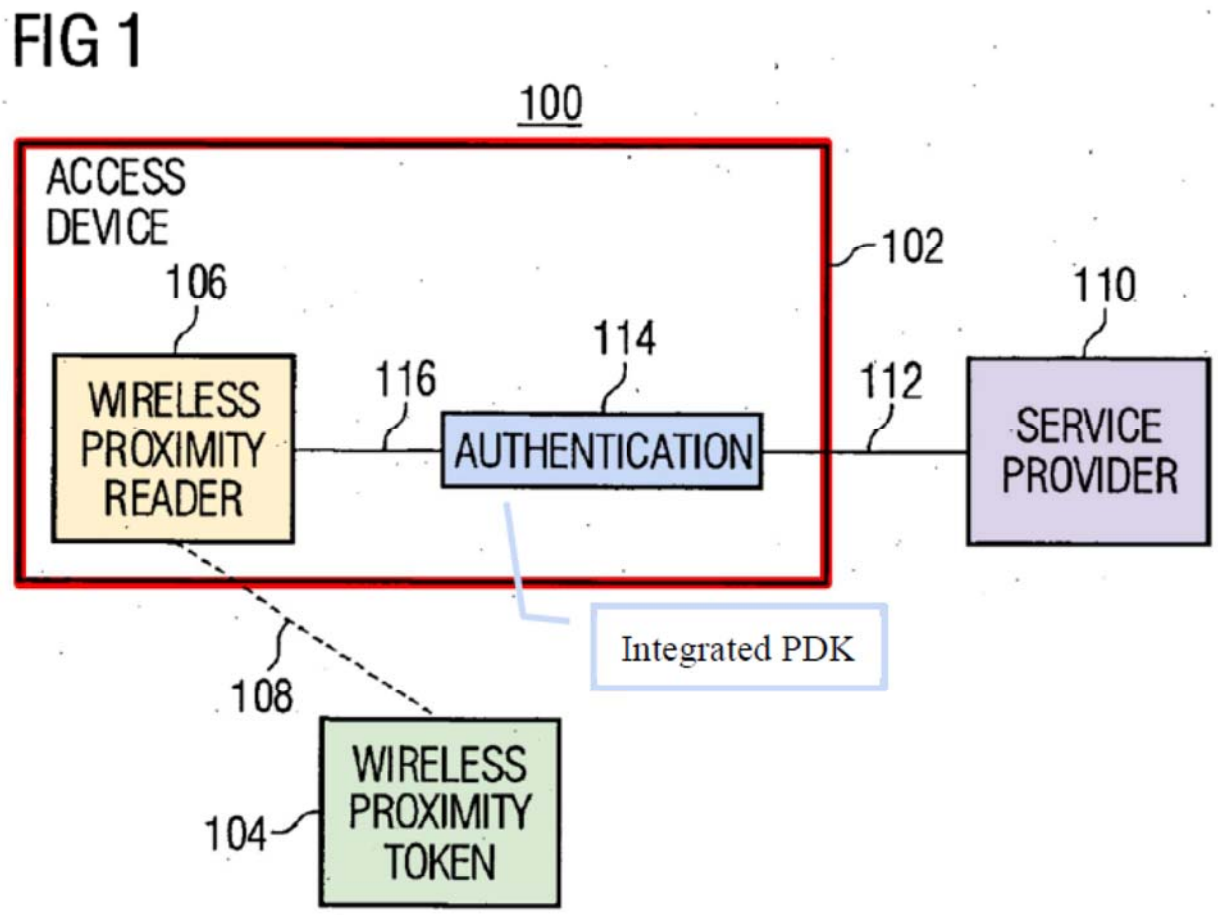
(1) A hybrid device:

Buer discloses the hybrid device in [14a] because it discloses an access device that combines an authentication circuitry (an integrated PDK) and a wireless proximity reader (an integrated RDC) to provide a hybrid device, as shown below. Ex-1003 ¶¶211-226.



Ex-1005, Fig. 1 (annotated). Buer's authentication system provides access to a secured service, where the access is controlled based on the proximity of a wireless token to an access device. Ex-1003, ¶213. In Figure 1, Buer's access device 102 ("hybrid device," **red**) includes two components: an authentication component 114 ("integrated PDK," **blue**) and a wireless proximity reader 106 ("integrated RDC," **yellow**). Ex-1005, Fig. 1. The authentication component 114 is configured to process (e.g., encrypt or sign) the information before sending it to the service provider 110 (**purple**). *Id.*, [0118], Fig. 1. The wireless proximity reader 106 is configured to receive information from a wireless proximity token 104 ("external PDK," **green**) when the token is proximate to the access device. *Id.*, [0111]-[0112], Fig. 1.

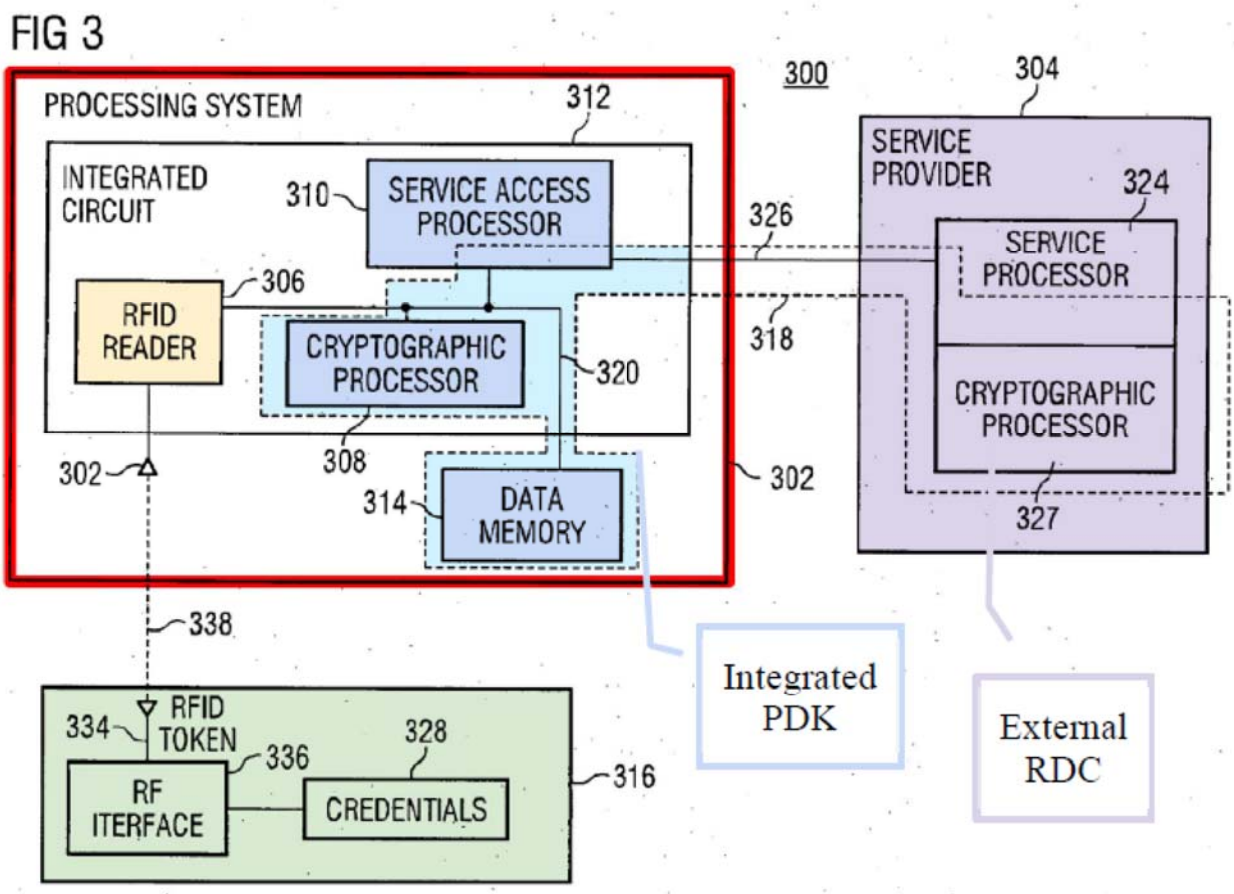
In Buer's access device, as shown below, the authentication component discloses the integrated PDK. Ex-1003, ¶¶214-221.



Ex-1005, Fig. 1 (annotated). In Buer, the authentication component is implemented as a cryptographic processing system, *id.*, Figs. 3, 6, and is a "personal digital key" under either the court's construction or Petitioner's proposed construction.

The authentication component (e.g., cryptographic processing system), as shown below, is an operably connected collection of circuit components (**blue**) that include a service access processor for communicating with an external service provider ("an antenna and a transceiver for communicating with a[n] RDC") and

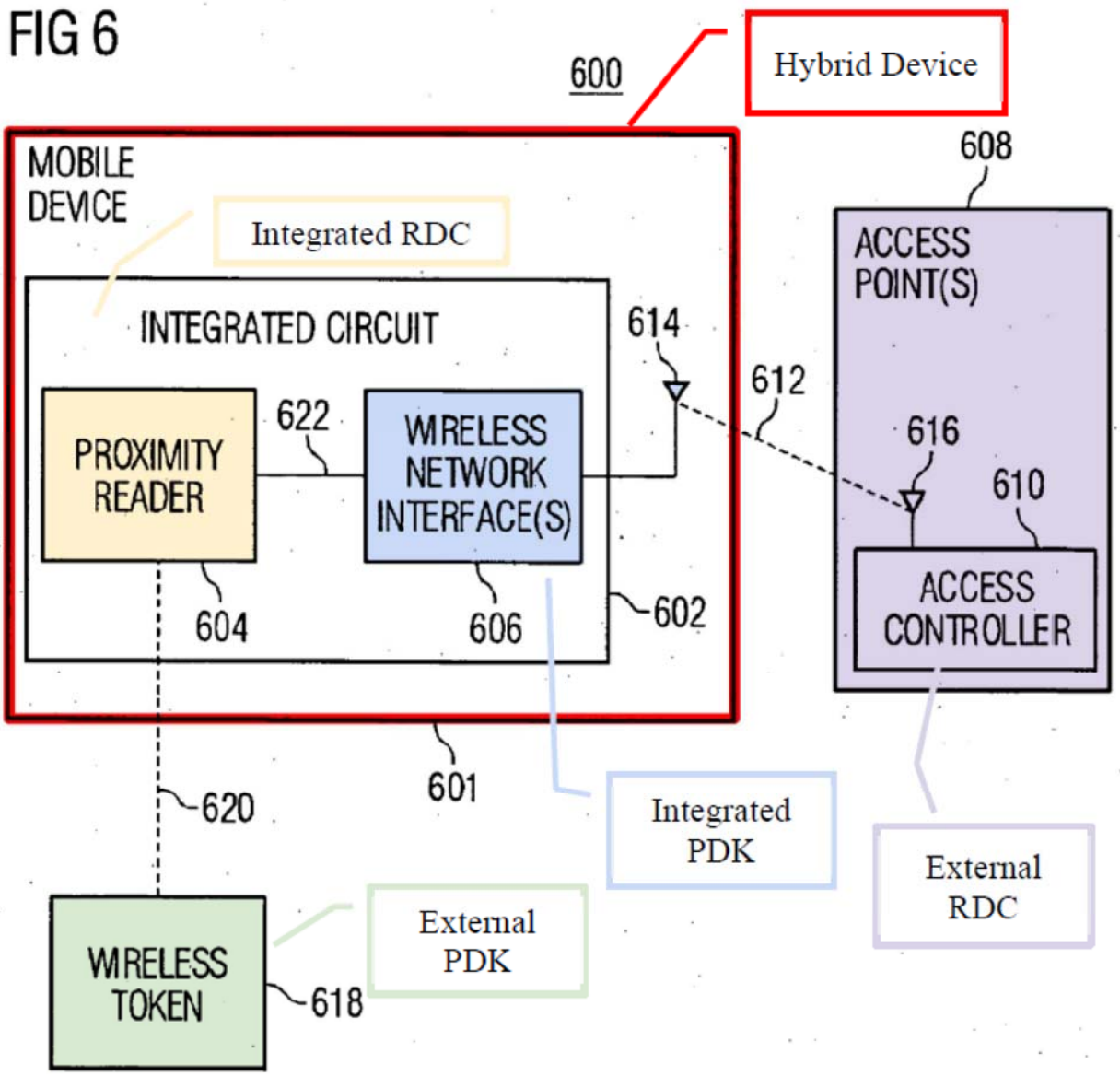
cryptographic processor and data memory ("controller and memory for storing information particular to a user"). *Id.*, [0137].



Id., Fig. 3 (annotated). Buer's cryptographic processor 308 acts as a controller for encrypting any important information, such as a user's credentials ("information particular to a user"), received from the external token. *Id.*, [0119], [0135]-[0137], [0141], [0150]. The encrypted information (and credentials) is stored in data memory 314 within the cryptographic boundary 318 (**light blue**). *Id.*, [0135], [0137].

The service access processor 310 then sends encrypted information via a communication link 326 to an external cryptographic processor 322, 327[7] (**purple**) for decryption and/or authentication processing, as necessary. *Id.*, [0138], [0152]-[0153]. While Buer does not expressly disclose whether communication link 326 is a wireless communication link, a POSITA would have understood the disclosure of "lead lines in the drawings may comprise a data network, for example, a local network and/or a wide area network (e.g., the Internet)," *Id.*, [0199]-[0201], to suggest that the encrypted information would be transmitted wirelessly via an antenna and a transceiver. Ex-1003, ¶219. Indeed, when implemented in Buer's mobile device (**red**), the cryptographic processing system (while not shown) is used to "cryptographically encrypt/sign the information" before the mobile device "sends the signed Information" via a wireless a network interface (**blue**) "to the network access provider (e.g., access point 608)" (**purple**). *Id.*, [0165], [0170], [0174]. As shown in Figure 6, the mobile device (**red**) includes an antenna 614 and wireless network interface(s) 606 (**blue**) that are used to send the encrypted (or signed) information over a wireless network (e.g., a cellular network, an 802.11 network, a Bluetooth network, etc.) via RF signals 612 to the network access provider. *Id.*, [0163], [0165], [0174].

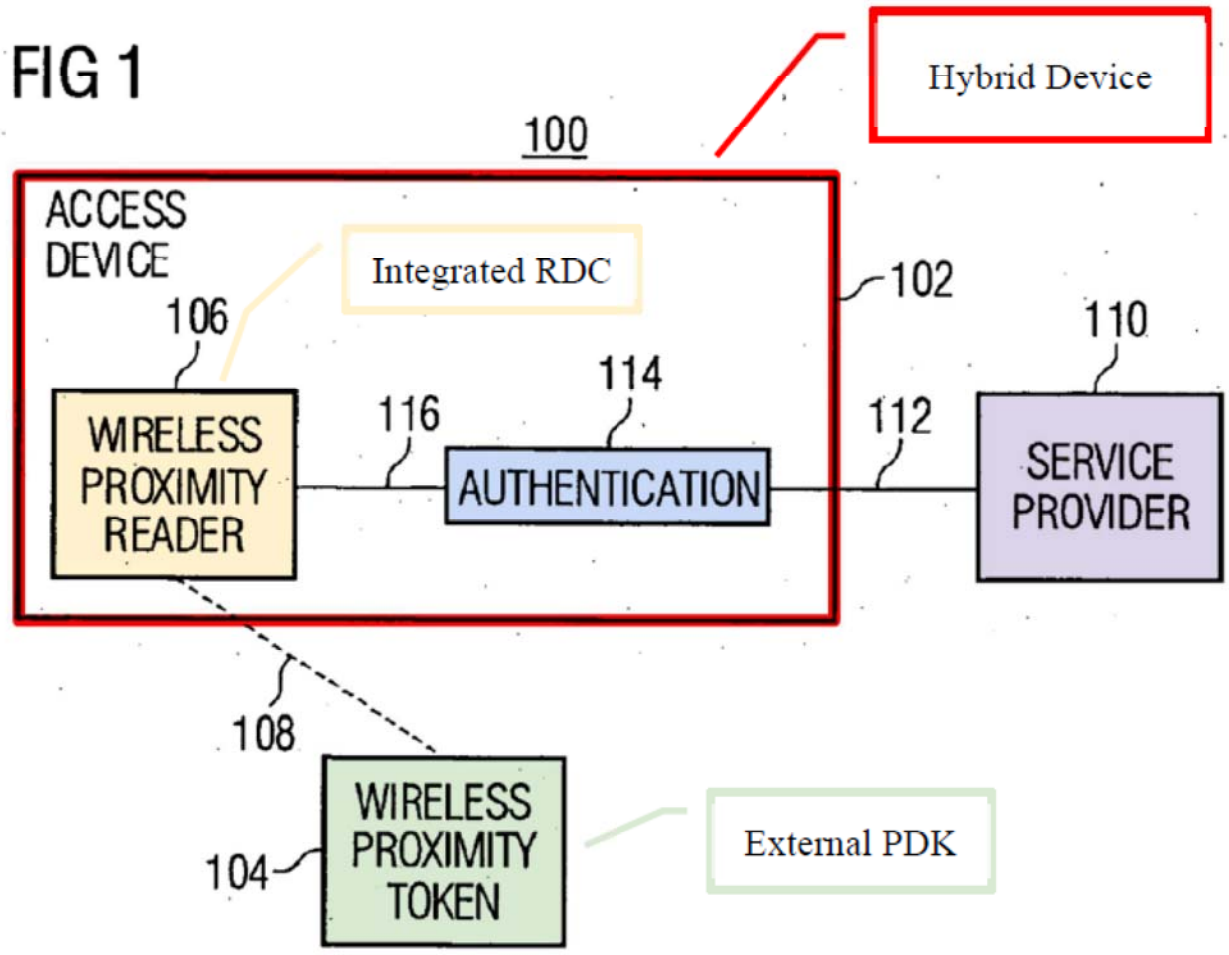
[7] Figure 3 appears to include a typographical error.



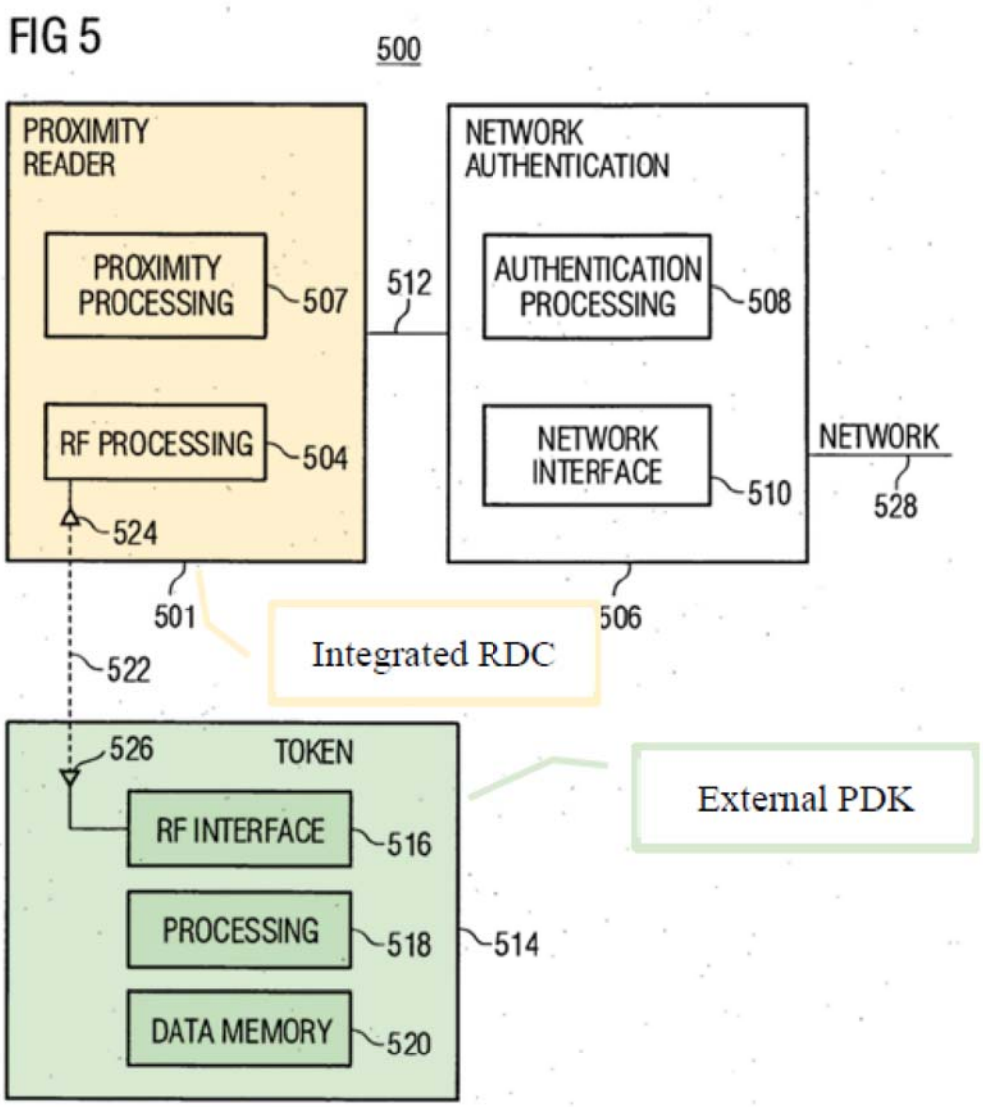
Id., Fig. 6 (annotated). Accordingly, Buer's cryptographic processing system, including its cryptographic processor, service access processor, and data memory, is an integrated PDK.

Buer's wireless proximity reader discloses the integrated RDC in [14a] and is a "receiver-decoder circuit" under either the court's construction or Petitioner's proposed construction. Buer's wireless proximity reader 106 ("integrated RDC,"

yellow), as shown below, is a component that is "configured to receive signals 108 (e.g., RF signals)" from at least one wireless proximity token 104 ("external PDK," green) when the token 104 is "proximate to the access device 102." *Id.*, [0111]; Ex-1003, ¶¶222-225.



Id., Fig. 1 (annotated). Buer's proximity reader 501 may include a collection of circuit components, including an antenna 524, an RF processing component 504, and a proximity processing component 502, 507,[8] as shown below. *Id.*, [0157].



[8] There appears to be a typographical error in Figure 5 because the proximity processing component should be labeled 502. *See* Ex-1005, [0157].

Id., Fig. 5 (annotated).

In Buer, the "wireless proximity reader and token may be implemented using one or more of a wide variety of wireless proximity techniques." *Id.*, [0128]. As Buer explains, the proximity reader and the external token communicate via RF signals when they are within proximity to one another. *Id.*, [0112], [0146], [0157], [0173]. In particular, the token stores encrypted authentication information that is provided to the proximity reader. *Id.*, [0130], [0158]. The reader receives the encrypted data and extracts any embedded information. *Id.*, [0097], [0184]. Accordingly, the proximity reader necessary decodes the encrypted information for later processing (including for extracting the embedded information, as disclosed). Ex-1003, ¶225.

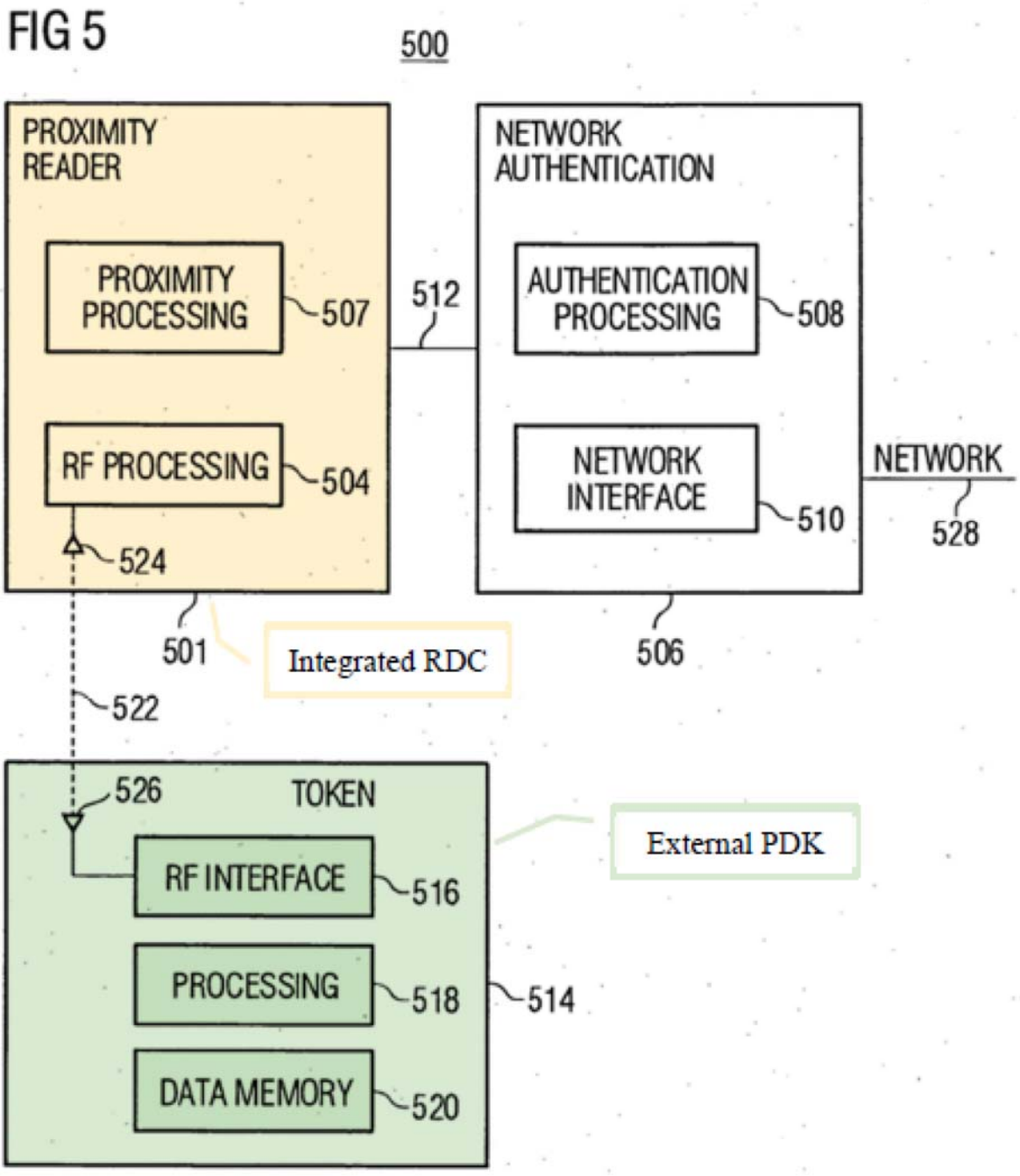
Because Buer's access device includes an integrated authentication component and a wireless reader, Buer discloses a hybrid device that includes both an integrated PDK and an integrated RDC, as recited in [14a]. Ex-1003, ¶226.

(2) Creating a First Wireless Link between an Integrated RDC of the Hybrid Device and an External Device:

Buer discloses creating a first wireless link between the wireless proximity reader (integrated RDC) and a wireless proximity token (external device) as in [14a]. Ex-1003, ¶¶227-228. As Buer explains, "an RFID signaling sequence" between the reader and the token includes creating a first set of RF signals that are "used to power

and activate the token" before the token can send its information to the reader. Ex-1005, [0146]-[0149].

In Buer, the wireless token is an "external PDK" that acts as a physical authentication/verification mechanism (e.g., "what the user possesses"). *Id.*, [0114]. If the request was made without the token, access may be denied. *Id.*, [0011]. On the other hand, "after the system verifies that the user (e.g., the user's token) is relatively close to the device," access to various services, applications, or functions (e.g., access to data networks, application, or financial transactions) may be enabled. *See id.*, [0120]-[0122], [0155]. Buer's external token discloses the external PDK because, similar to Buer's integrated PDK, it is also an operably connected collection of circuit elements including antenna 526, an RF interface 516 (transceiver), processing component 518, and data memory 520 for storing user information, as shown in Figure 5. *Id.*, [0157]-[0159].



Id., Fig. 5 (annotated). In Figure 5, Buer's RF interface 516 with antenna 526 is used to transmit/receive RF signals via line 522 to/from the proximity reader (integrated RDC). *Id.*, [0157]. Buer's processing component 518 acts as a controller for

"control[ling] communication with the proximity reader 501," "enabl[ing] the token 514 to be programmed with the authentication information," "process[ing] RF signals received from the proximity reader 501," and "control[ling] the generation of appropriate signals to send the authentication information." *Id.*, [0159]. And Buer's processing component 518 and data memory 520 are used to store the "authentication information such as network authentication credentials, passwords and/or certificates" (e.g., "information particular to a user"). *Id.*, [0158]-[0159]. Thus, Buer's external token discloses an external PDK, consistent with the court's and Petitioner's constructions. Ex-1003, ¶¶229-231.

c. [14b]: "the hybrid device including an integrated, secure memory and the integrated RDC, wherein the integrated, secure memory stores local, secured information;"

As discussed in §V.A.1.b, Buer's hybrid device includes an integrated PDK, which includes an integrated, secure memory and the wireless proximity reader (integrated RDC). Ex-1003, ¶232. As Buer explains, the integrated PDK may use "tamper resistant and/or tamper evident hardware." Ex-1005, [0013], [0134]. The information is encrypted when stored in data memory 314 within the cryptographic boundary. *Id.*, [0135], [0137]. Thus, Buer discloses an integrated, tamper-resistant memory storing local, encrypted information. Ex-1003, ¶233.

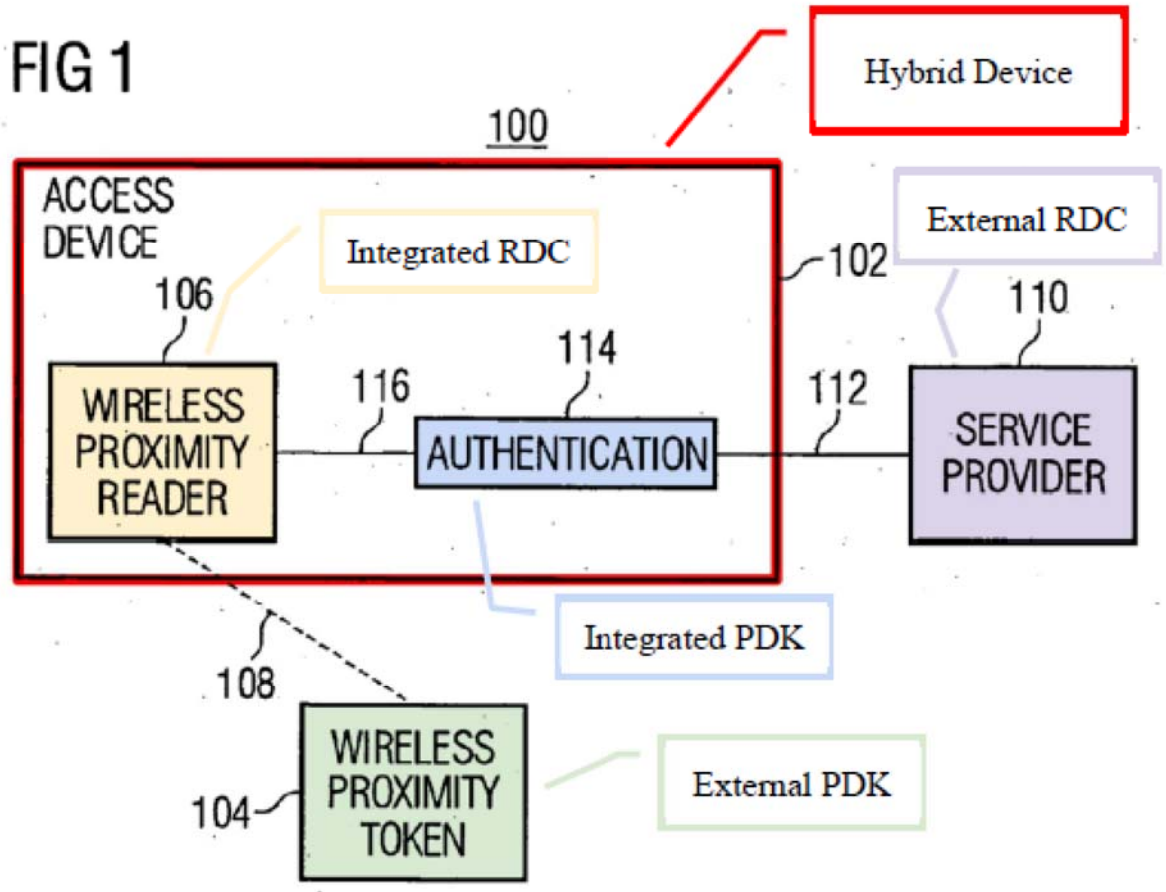
d. [14c]: "receiving a first signal, at the integrated RDC, via the first wireless link, from the external device; and"

Buer discloses receiving RF signals at the integrated RDC from the external PDK as in [14c] because the integrated reader receives RFID signals, including proximity signaling and authentication information, during the RFID signaling from the external token. Ex-1003, ¶¶234-235. In particular, during the initial RFID signaling sequence, the token may perform proximity signaling by sending RF signals to the proximity reader for the proximity reader to verify that a particular token is within range. Ex-1005, [0157]-[0158]. The token generates additional RF signals to send the encrypted authentication information that is stored in the token to the proximity reader. *Id.*, [0148]-[0150]; *see also id.*, [0097], [0130], [0158]-[0159], [0184]. The integrated reader receives the RFID signals that are broadcasted from the wireless token and extracts the encrypted authentication information (e.g., credentials) from the RFID signals. *Id.*, [0148]-[0150], Fig. 4; *see also id.*, Figs. 7, 9; Ex-1003, ¶236.

e. [14d]: "generating an enablement signal enabling one or more of an application, a function and a service."

Buer discloses the authentication component generating an enablement signal enabling a wide variety of applications, functions, or services, as in [14d] because it

provides encrypted or signed credentials to a service provider to enable access to secured services, as shown below. Ex-1003, ¶¶237-239.



Ex-1005, Fig. 1 (annotated); *see also id.*, [0113] ("[T]he communication media 112 may comprise, for example, electric wires, optical cables or air."). [14d] is recited as allowing "mixed operations," Ex-1001, Abstract, 16:39-46, "the entire element is disclosed by the prior art if one alternative ... is in the prior art." *Fresenius*, 582 F.3d at 1298.

Proximity Reader Communicating Wirelessly with an External Token Enables an Application, Function, or Service:

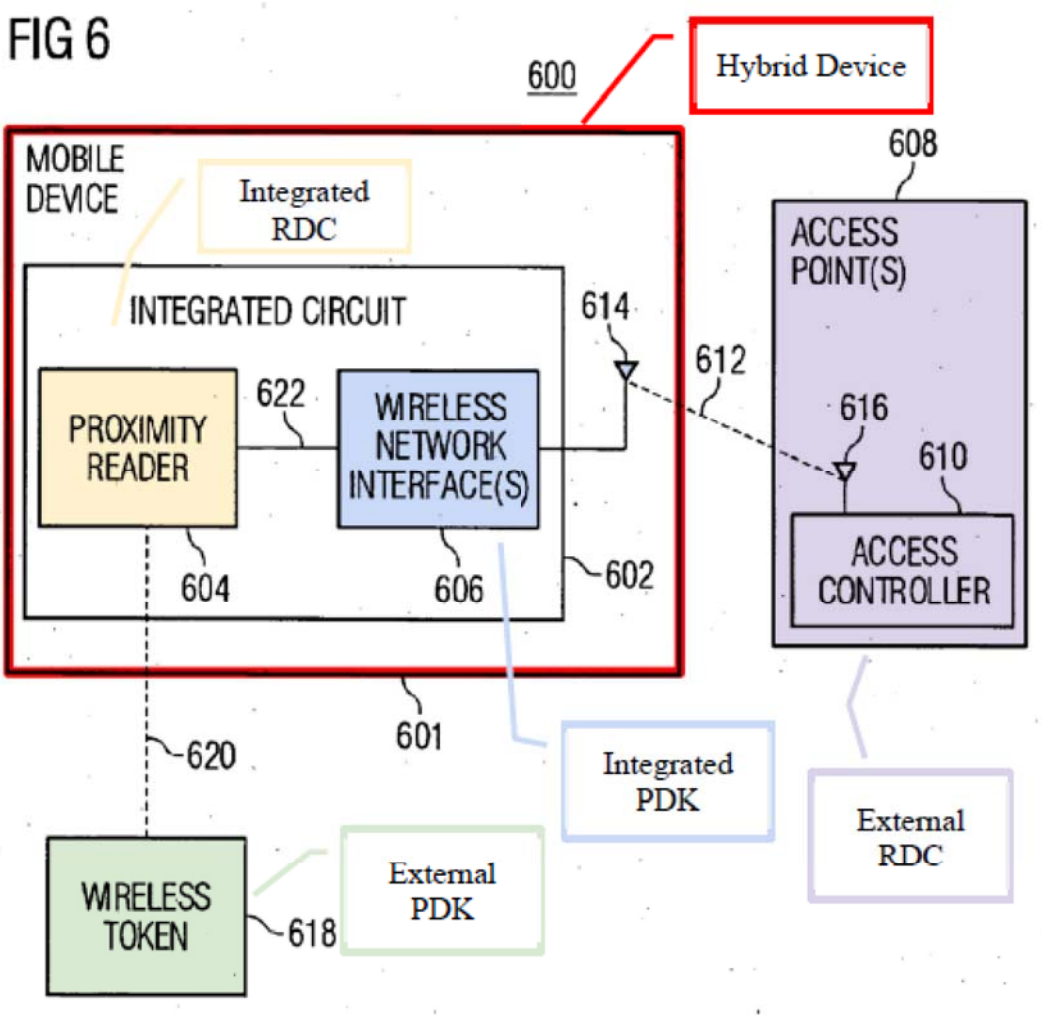
Buer discloses that information received wirelessly by the integrated proximity reader from the external token enables the application, service, or function on the hybrid device itself. Ex-1003, ¶¶240-245. In Buer, after a proximity reader verifies a user (via an external token), the authentication component generates an enablement signal (e.g., RF signal) providing the necessary authentication information (e.g., signed information) via its cryptographic processing system to a service provider to enable a wide variety of applications, functions, or services on the hybrid device. Ex-1005, [0152], [0174]. The service provide may enable access to the following requested service:

> [S]ervice may include, for example, access to data and/or a data processing service. Thus, a service may enable an access device to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to cryptographic material such as security associations and keys, access a web page, access a data network or access a processing application.

Id., [0120]; *see also, e.g., id.*, [0122], [0155], [0162], [0195]-[0196]. According to Buer, application access may include "invoking, interacting with or using the

application or loading the application onto the access device." *Id.*, [0122]. Data network access may include "sending and/or receiving data over the network." *Id.*

Like the '289 patent, Buer discloses enabling network access on a hybrid device. Buer discloses that the network interface 606 performs "network authentication and connection processing" by "communicating with a respective access controller 610 in one or more access point(s) 608 via RF signals 612" transmitted via antennas 614. *Id.*, [0165]. The RF signals generated by the wireless network interface are enablement signals that contain the encrypted or signed information that is sent to the "network access provider (e.g., access point 608)." *Id.*, [0165], [0174].



Id., Fig. 6 (annotated). The network provider then verifies the credentials and provides access to the requested wireless network. *Id.*, [0175]. Thus, the service provider may "enable an access device to … access a data network." Ex-1005, [0120], [0122], Fig. 7.

The Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

Buer discloses that information stored by the integrated, secure memory, such as credit card information, may "be used to authenticate a user to another processing system" (external device) associated with an external proximity reader 1120 (external RDC) that includes "point-of-sale components" to "perform a sales transaction," such as "credit card transactions." *Id.*, [0193]-[0196]. As Buer explains, the mobile device may include a trusted platform module (TPM), which includes a proximity reader that is used to extract any user credential from a token. *Id.*, [0184], [0190]-[0191], [0194]. The extracted credential would be stored in its integrated PDK via the local data memory 824. *Id.*, [0185]; Ex-1003, ¶246. As Buer explains, the mobile device's TPM may include an RFID client, which generates an enablement signal (e.g., RF signal containing credit card information) that is transmitted to another processing system, such as a computer with a point-of-sale device. Ex-1005, [0192]-[0195]. Thus, similar to the '289 patent, "data services" may be enabled on the external security processing system. Ex-1005, [0195]; Ex-1003, ¶¶246-247.

2. Claim 1

a. [1pre]: "A hybrid device comprising:"

To the extent the preamble is limiting, as discussed in §V.A.1.b, Buer discloses the preamble because it discloses an access device that combines an authentication circuitry and a wireless proximity reader to provide a hybrid device. *See* claim 14; Ex-1003, ¶248.

b. [1a]: "an integrated, secure memory storing local, secured information; and"

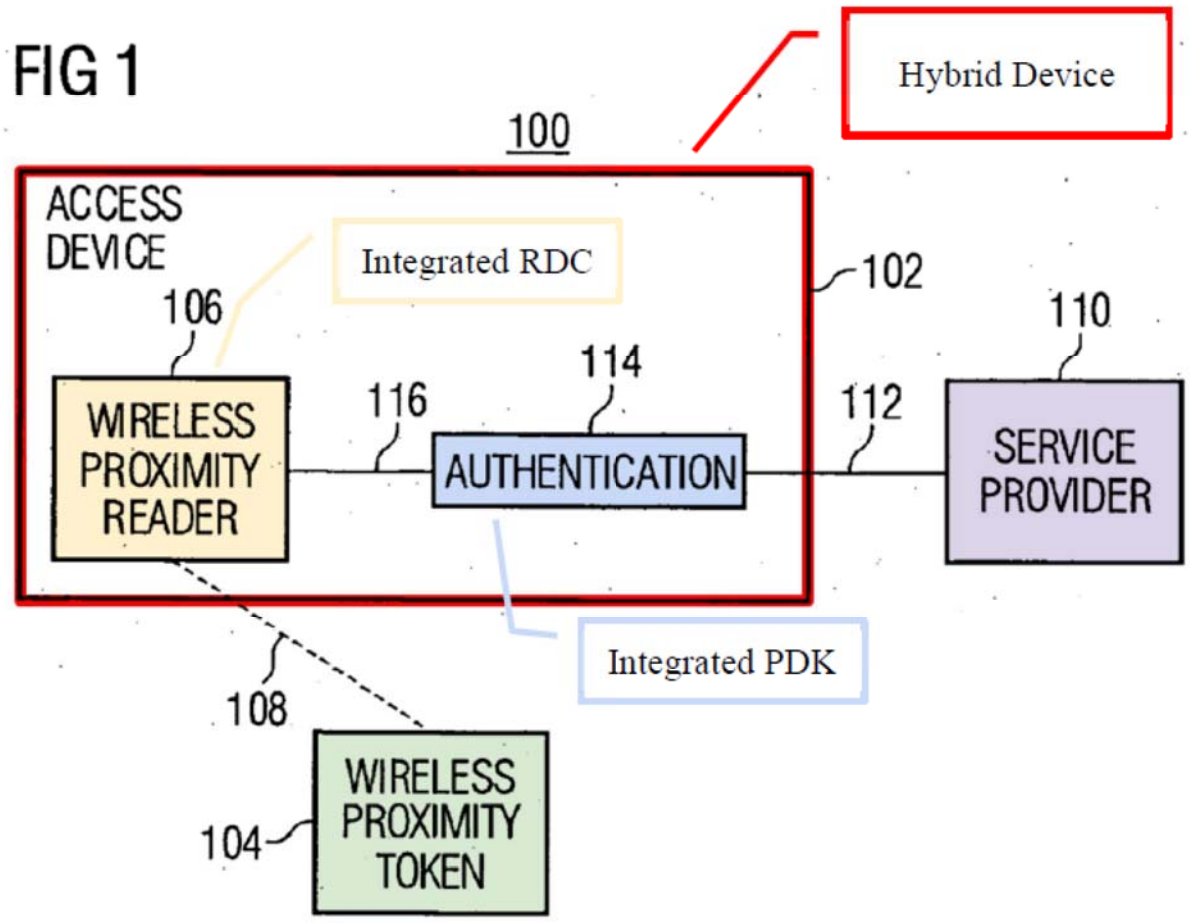
As discussed in §V.A.1.c, Buer's hybrid device includes an integrated PDK, which includes an integrated, tamper-resistant memory storing local, encrypted information. Ex-1005, [0013], [0134]-[0137]; Ex-1003, ¶¶249-250.

c. [1b]: "an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone,"

As discussed in §V.A.1.b, Buer discloses the integrated wireless proximity reader (RDC) communicates "wirelessly with at least" an external token "within a proximity zone." Ex-1003, ¶251. Buer's wireless proximity reader (RDC) is configured to receive RF signals when the token is "proximate to the access device," such as "when they are within a predefined distance of each other." Ex-1005, [0111], [0146]; Ex-1003, ¶251.

d. [1c]: "the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,"

Buer discloses that the integrated "[wireless proximity] reader 106" is communicatively coupled to the integrated, secure memory in the "authentication component 114" "via a connection 116 within a common integrated circuit" as in [1c], as shown below. Ex-1005, [0116]; Ex-1003, ¶¶252-254.



Ex-1005, Fig. 1 (annotated). As discussed above for [1a], when Buer's authentication component is implemented as a cryptographic processing system, it

is coupled to the reader via a first data bus 320 in Figure 3 or via a first internal lead 622 in Figure 6. *Id.*, [0137], [0167], Figs. 3, 6.

e. [1d]: "wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and service."

As discussed in §V.A.1.e, Buer discloses the authentication component enabling a wide variety of applications, functions, or services as in [1d]. *See* [14d]; Ex-1003, ¶¶255-257. [1d] is recited as allowing "mixed operations" involving several alternatives: (1) what component is used to enable the application, function, or service (e.g., "either or both RDC and PDK functionality"), (2) what is being enabled (e.g., application, function, or service), and (3) which device is being enabled (e.g., hybrid device or external RDC). Ex-1001, Abstract, 16:39-46. Because [1d] recites alternative events, "the entire element is disclosed by the prior art if one alternative ... is in the prior art." *Fresenius*, 582 F.3d at 1298.

(a) Integrated RDC Communicating Wirelessly with an External Device Within the Proximity Zone Enables an Application, Function, or Service:

As discussed in §V.A.1.e, Buer discloses that its integrated proximity reader (RDC), communicating wirelessly with an external token within a proximity zone,

enables network access on a hybrid device, as in [1d](a). Ex-1005, [0120], [0122], [0165], [0174]-[0175], Figs. 6-7; Ex-1003, ¶¶258-260.

(b) The Information Stored by the Integrated, Secure Memory Enables an Application, Function, or Service:

As discussed in §V.A.1.e, Buer also discloses that the local, encrypted information stored by the integrated, tamper-resistant memory enables network access by sending encrypted or signed information to the "network access provider (e.g., access point 608)," as in [1d](b). Ex-1005, [0013], [0134], [0165], [0174]; Ex-1003, ¶¶261-262. Alternatively, Buer discloses that credit card information stored in its trusted platform module (TPM) is used to enable another processing system, such as a computer with a point-of-sale device. Ex-1005, [0192]-[0195]. Thus, similar to the '289 patent, "data services" may be enabled on the external security processing system. *Id.*, [0195]; Ex-1003, ¶263.

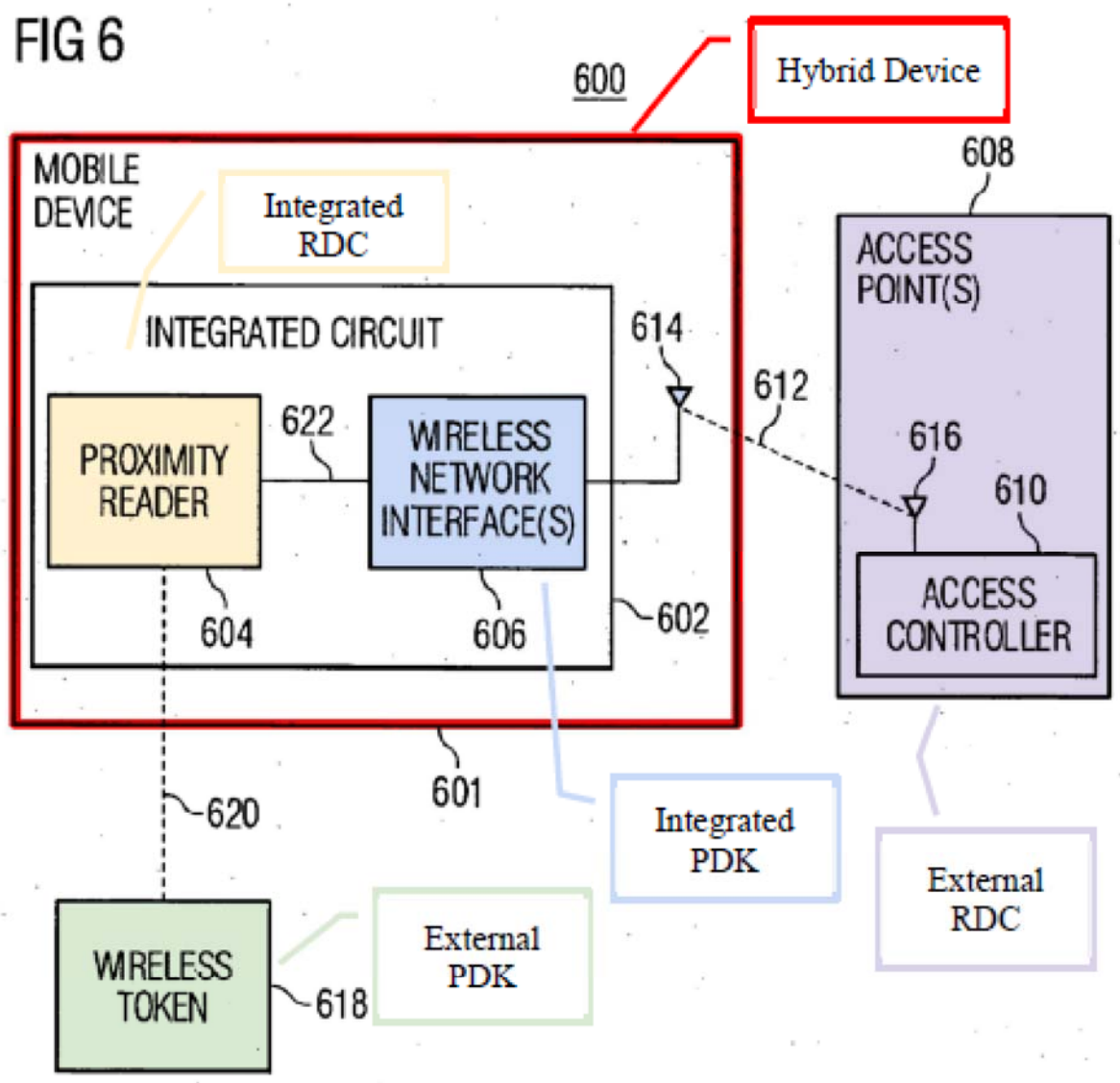
B. Dependent Claims

1. [2]: "The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, on the hybrid device."

Buer discloses claim 2 because a network access is enabled on the hybrid device. *See* [1d](a); Ex-1003, ¶264.

2. **[3]: "The hybrid device of claim 1, wherein at least one of the one or more of the application, the function, and the service is enabled, at least in part, external to the hybrid device using an external RDC, the hybrid device communicatively coupled to wirelessly communicate with the external RDC."**

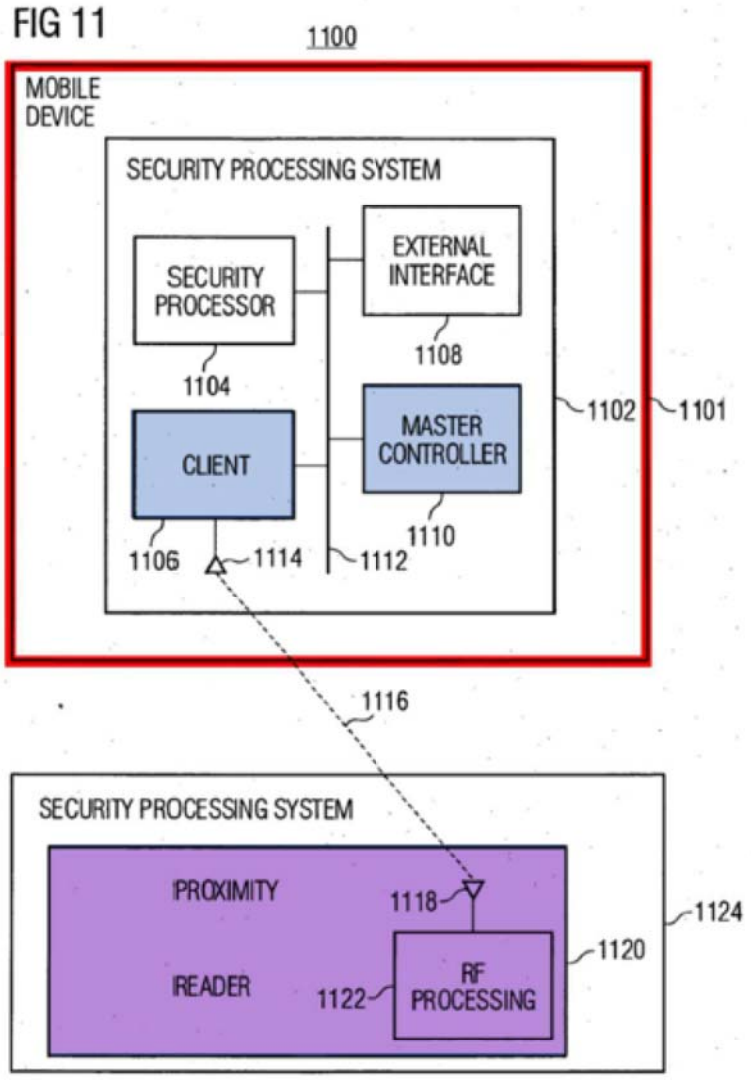
Buer discloses claim 3 because encrypted information stored on the integrated, secure memory is wirelessly communicated to an external RDC to enable an application, function, or service, as shown below. *See* [1d](b); Ex-1003, ¶265.



Ex-1005, Fig. 6 (annotated). Buer's service provider, *id.*, Figs. 1, 3, 6, as a whole, or the internal cryptographic processor 322, 327, or access controller 610 individually, is an external RDC because they are "capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing," as the court has construed., or Petitioner's proposed construction. *Id.*, [0153], [0165]. In Figure 3, Buer's external cryptographic processor 322, 327 (**purple**) is capable of receiving encrypted information and "decrypti[ng] and/or authenticati[ng] operations necessary to … receive the encrypted information and provide the information in the clear for internal processing." *Id.*, [0138]. In Figure 6, the access controller 610 is capable of wirelessly receiving data over a given wireless network. *Id.*, [0165]. According to Buer, the access controller 610 receives encrypted or "signed Information." *Id.*, [0174]-[0175]. A POSITA reading Buer would have understood that the access controller 610, or the service provider (e.g., access point 608), would decode the encrypted or signed information for verification of the credentials, similar to the cryptographic processing disclosed in Figure 3. Ex-1003, ¶¶266-269. Like the '289 patent, Buer discloses enabling network access by sending encrypted or signed information to the "network access provider (e.g., access point 608)." Ex-1005, [0165], [0174].

Alternatively, Buer discloses that credit card information stored by the integrated, secure memory may "be used to authenticate a user to another processing

system" (external device) associated with an external proximity reader 1120 (external RDC) that includes "point-of-sale components" to "perform a sales transaction," such as "credit card transactions," as shown below. *Id.*, [0195]-[0196].



Id., Fig. 11 (annotated). Ex-1003, ¶271.

3. [4]: "The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user."

Buer discloses claim 4 because the various authorization data for authenticating a user includes "password" and biometric information. Ex-1005, [0181], [0114]. A POSITA reading Buer would have understood that when a token transfers its stored information (such as biometric information), *Id.*, [0149], that information is encrypted using Buer's cryptographic processing and stored in the local, secured memory in the hybrid device. *Id.*, [0135]. Ex-1003, ¶¶272-274.

To the extent this is disputed or the Board determines otherwise, Buer in view of Giobbi157 renders obvious claim 4.

Giobbi157 teaches storing "biometric profile" in a local, secured memory, so that a user would use "a matching biometric input" obtained from the hybrid device to "unlock" the tag memory. Ex-1006, [0043]. Giobbi157 teaches that the biometric input would be used to compare "stored biometric information" to authenticate the user (e.g., fingerprint authentication). *Id.*, [0028], [0037]-[0038], [0048].

A POSITA would have been motivated and found it obvious to include biometric information for authenticating a user in Buer's local, tamper-resistant memory because doing so would promote Buer's purpose of further restricting access to service until the user satisfies additional verification queries. Ex-1005, [0114], [0013], [0134]; Ex-1003, ¶¶289-292.

A POSITA would have had a reasonable expectation of success in storing "biometric information for authenticating a user" in Buer's tamper-resistant memory, as Giobbi157 teaches, because storing "biometric information for authenticating a user" in memory would require minimal modification without undue experimentation. Ex-1003, ¶293. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003, ¶293; *see Friskit*, 306 F. App'x at 616.

4. [5]: "The hybrid device of claim 1, wherein the local, secured information includes biometric information based on a biometric scan of a finger, the biometric information for authenticating a user."

Buer discloses claim 5 because the biometric information may be "a fingerprint" used to verify the authenticity of the user. Ex-1005, [0114], [0130], [0196]. Ex-1003, ¶¶275-276.

5. [6]: "The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on the financial information."

Buer discloses claim 6 because the local, secure information may be "credit card information," and the information is used to "perform a sales transaction." Ex-1005, [0195]. Ex-1003, ¶277.

6. [7]: "The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on a signal received from the at least one external device by the integrated RDC."

As discussed in §V.B.2, Buer discloses claim 7 because the integrated PDK sends financial information to the external RF processing component for use by the RF processing component. Ex-1005, [0194]-[0195]. Buer explains that its external token may also be equipped "with smart card functionality" (e.g., "credit cards") so that a user's "credit card information" may be provided to an integrated proximity reader in an access device. *Id.*, [0129]-[0130], [0193], Fig. 8. It would have been obvious to implement Buer's "key management functions" to "back[]up" or store the external token's credit card information on the user's cellular phone for point-of-sale transactions. *Id.*, [0177], [0195]. A POSITA would have been motivated to use the token to transfer the credit card Information in a secure manner to the cellular phone without the user having to directly enter the information into the device. Ex-1005, [0007]; Ex-1003, ¶¶278-280. Moreover, a POSITA would have been motivated to provide financial transactions "only when a wireless token assigned to the user is in the proximity of" the cellular phone to further protect against unauthorized use of the credit card information, Ex-1005, [0011], or to utilize the

cellular phone's "biometric reader to further verify the authenticity of the user," *id.*, [0114].

7. [8]: "The hybrid device of claim 1, wherein the local, secure information includes financial information and at least one of the one or more of the application, the function, and the service enabled completes a financial transaction based on an authorization of the financial information using an external authentication database, the financial information transmitted to the external authentication database."

Buer and Giobbi157 render obvious claim 8 because a financial transaction is completed based on an authorization of the financial information using an external authentication database.

Giobbi157 teaches that its external reader is communicatively coupled "to receive and/or transmit information to remote databases for remote authentication." Ex-1006, [0031], [0053]. The remote databases include a "validation database … for authorizing a transaction to be processed." *Id.*, [0033]. In Giobbi157, "the process involves transmitting credit card (or other purchasing information) to a validation database 112 to authorize the purchase and receive the status of the card." *Id.*, [0074].

A POSITA would have been motivated to implement Giobbi157's validation database in Buer's security processing system 1124 with the point-of-sale components because doing so would enhance Buer's "credit card transactions," (Ex-1005, [0195]-[0196]), to provide status information concerning whether "the card is active and not reported lost or stolen and that sufficient funds are present to execute

the purchase," Ex-1006, [0074], which can only be verified using an external database. Ex-1003, ¶¶294-296. Accordingly, a POSITA would have been motivated to implement Buer's external processing system with access to validation database to authorize the purchase and to "display[] status to a user." Ex-1006, [0026], [0074]. A POSITA would have been motivated to implement Buer's external processing system with Giobbi157's validation database, at least, because Buer and Giobbi157 are in the same field of endeavor—the field of incorporating RDC/PDK technology into hybrid devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1006, [0026]. Likewise, a POSITA would recognize that Buer and Giobbi157 use similar techniques to solve the same problem. Ex-1003, ¶297.

A POSITA would have had a reasonable expectation of success in coupling one or more external databases to Buer's external processing system because Buer and Giobbi157 use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0114], [0125], [0163]; Ex-1006, [0030], [0035]; Ex-1003, ¶298. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003, ¶298; *see Friskit*, 306 F. App'x at 616.

8. [9]: "The hybrid device of claim 8, wherein the external authentication database is separate from a merchant providing a sale in the financial transaction."

Buer in view of Giobbi157 renders obvious claim 9 because Giobbi157 discloses that "in purchase transactions, the validation database 112 is a credit card validation database that is separate from the merchant providing the sale." Ex-1006, [0033]. Ex-1003, ¶¶299-300.

9. [10]: "The hybrid device of claim 1, wherein the one or more of the application, the function and the service enabled based on the local, secured information stored by the integrated, secure memory includes a first application, function or service based on a first subsets of local, secured information stored by the integrated, secure memory and a second application, function or service based on a second subset of local, secured information, the first and second subset of local, secured information having different accessibility."

Buer discloses that its access device can secure access to multiples applications, functions, or services. *Id.*, [0120]-[122], [0193]-[0195]. Buer provides different examples of services the access device may have access, including "data and/or a data processing service," "a web page," "processing application," and "sales transactions." *Id.* Buer explains that "multiple sets of information (e.g., credentials) may be included on a single token to enable a user to access different services." *Id.*, [0127], [0177].

A POSITA would have found obvious that the different services would have had "different accessibility" based on the "key" or "credential" that may be "linked to a particular" service. Ex-1003, ¶¶281-282. A POSITA reading Buer would have understood that each of the keys or credentials stored in the access device would enable different applications, functions, or services, such that a first "key" or "credential" would be used to access, for example, data services, while a second "key" or "credential" would be used to access, for example, sales transactions. Ex-1003, ¶282.

To the extent this is disputed or the Board determines otherwise, Buer in view of Giobbi157 renders obvious claim 10.

Giobbi157 teaches storing multiple user profiles, such as biometric profile, PIN profile, picture profile, registry profile, credit cards, and personal information, in its secured and tamperproof memories. Ex-1006, [0037]-[0042], [0058]. Each of the profiles provides a different accessibility to certain application, function, or service. For example, one profile may be used to enable "access to secure physical or digital assets," and another may be used for completing a purchase transaction. *Id.*, [0063].

A POSITA would have been motivated and found it obvious to implement Buer's database to store multiple profiles, as Giobbi157 teaches, because doing so would allow Buer to securely store information from multiple tokens to enable

different accessibility of applications based on the linked tokens. Ex-1005, [0115], [0143]; Ex-1006, [0037]-[0042], [0058]; Ex-1003, ¶¶301-303. A POSITA would have been motivated to implement Buer's database to store multiple profiles, at least, because Buer and Giobbi157 are in the same field of endeavor—the field of incorporating RDC/PDK technology into hybrid devices to allow secure data sharing and services. Ex-1005, Abstract; Ex-1006, [0026]. Likewise, a POSITA would recognize that Buer and Giobbi157 use similar techniques to solve the same problem. Ex-1003, ¶304.

A POSITA would have had a reasonable expectation of success in storing multiple profiles in Buer's database because Buer and Giobbi157 use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1003, ¶306. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003, ¶306; *see Friskit*, 306 F. App'x at 616.

10. [11]: "The hybrid device of claim 1, wherein the hybrid device is a cell phone."

Buer discloses claim 11 because the access device may be "a cellular phone." Ex-1005, [0163]; §V.A.1; Ex-1003, ¶283.

11. [12]: "The hybrid device of claim 1, wherein the at least one external device is included in jewelry."

Buer at least suggests claim 12 because it teaches that its external token (PDK) may be included in "smart cards, credit cards, dongles, badges, biometric devices such as fingerprint readers, mobile devices such as cellular telephones, PDAs, etc." Ex-1005, [0130].

Giobbi157 teaches that a PDK "can be integrated into commonly carried items," such as "jewelry items such as watches, rings, necklaces or bracelets." Ex-1006, [0035]. It would have been obvious in view of Buer's disclosure of including a PDK in a wearable, such as a badge, to include the external PDK in other wearables, like jewelry, as Giobbi157 teaches. Ex-1003, ¶307-308. A POSITA would also be motivated to combine these references at least because Giobbi157 and Buer are in the same field of endeavor as the '289 patent—the field of incorporating RDC/PDK technology into hybrid devices. Likewise, a POSITA would recognize that Giobbi157 and Buer use similar techniques to solve the same problem as the '289 patent—as discussed throughout this Petition, the Giobbi157 and Buer references integrate PDKs and RDCs into hybrid devices in the same manner claimed by the '289 patent.

A POSITA would have had a reasonable expectation of success in including the external device in jewelry because Giobbi157 already teaches that a PDK can be

incorporated into jewelries such as watches and necklaces, and Buer already contemplates including its PDK in a wearable. Ex-1003, ¶309.

12. **[13]: "The hybrid device of claim 1, wherein the at least one external device is a watch."**

See [12]; Ex-1003, ¶310.

13. **[15]: "The method of claim 14, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on the hybrid device."**

See [2]; Ex-1003, ¶284.

14. **[16]: "The method of claim 14 further comprising: sending the enablement signal, wherein at least one of the one or more of the application, the function, and the service is enabled at least in part on a device external to the hybrid device and communicatively coupled to an external RDC."**

See [3]; Ex-1003, ¶285.

15. **[17]: "The method of claim 14, wherein the local, secured information includes biometric information for authenticating a user."**

See [4]; Ex-1003, ¶286.

16. **[18]: "The method of claim 14, wherein the local, secured information includes financial information and wherein the one or more of the application, the function and the service completes a financial transaction."**

See [6]; Ex-1003, ¶287.

17. **[19]: "The method of claim 14, wherein the hybrid device is a cell phone."**

See [11]; Ex-1003, ¶288.

18. [20]: "The method of claim 14, wherein the external PDK is included in a watch."

See [12]; Ex-1003, ¶311.

VI. Ground 5: Buer and Nishikawa Render Obvious claim 4

A. [4]: "The hybrid device of claim 1, wherein the local, secured information includes biometric information for authenticating a user."

Buer in view of Nishikawa renders obvious claim 4 because the local, secured information includes biometric information for authenticating a user. Ex-1003, ¶¶312-313. Nishikawa discloses improving "cellular phone" with a SIM card that is capable of "be[ing] loaded with multiple applications, such as electronic money, an electronic ticket, a fingerprint template, a fingerprint collating engine and a personnel ID card." Ex-1014, [0111], [0001], 0036]. Nishikawa explains that "[f]ingerprint data (biometric data) on the finger print of a special user ... is stored in the SIM [card]" to authenticate the user "on the basis of biometric data." Ex-1014, [0073], [0114].

A POSITA would have been motivated to adapt Buer's cellular phone to load multiple applications on a SIM card, as Nishikawa teaches, to improve the convenience of Buer's cellular phone and to add additional capability, including the ability to store biometric information in addition to credit card information, and, as prior art teaches, to use the "standard size and shape" of a conventional SIM card to

introduce additional features. *Id.*; Ex-1013, 3:34-4:4, 11:15-27; Ex-1003, ¶¶314-315. A POSITA would have also been motivated to improve authentication of the user of the cellular phone, which furthers Buer's express teaching on using a biometric to add an additional layer of authentication. Ex-1014, [0111], [0073]; Ex-1005, [0114]. A POSITA would have recognized that Buer and Nishikawa are in the same field of endeavor and use similar techniques to solve the same problem. Ex-1003, ¶316.

A POSITA would have had a reasonable expectation of success in adapting Buer's cellular phone to store biometric information on its SIM card, because Buer and Nishikawa use similar hardware, and the combination would require minimal modification without undue experimentation. Ex-1005, [0114], [0125], [0163]; Ex-1014, [0004]-[0013]; Ex-1003 ¶317. Such a combination would have been no more than combining prior art elements according to known methods to yield predictable results. Ex-1003 ¶317; *see Friskit*, 306 F. App'x at 616.

VII. Discretionary Denial Is Not Warranted

A. Discretionary Denial Not Warranted Under *General Plastic*

In *General Plastic*, the Board set forth a series of factors that may be analyzed for follow-on petitions to help conserve its finite resources. IPR2016-01357, Paper 19.

Petitioner is concurrently filing a Motion for Joinder seeking to join this Petition to IPR2024-00783 (the "Google IPR"). A joinder petition in these circumstances is not the type of serial petition to which *General Plastic* applies, especially as Petitioner has not previously filed an IPR against the '289 Patent. Petitioner does not present any new grounds. If joined, Petitioner would be taking an understudy role and the Board's finite resources would not be impacted. Indeed, the PTAB has previously stated that a joinder petition "effectively neutralizes" a *General Plastic* analysis. *See Apple Inc. v. Uniloc 2017 LLC*, IPR2018-00580, Paper 13 at 10; *see also Celltrion, Inc. v. Genentech, Inc.,* IPR2018-01019, Paper 11 at 10.

Moreover, the *General Plastic* factors do not favor denial. The parties challenging the '289 patent (Microsoft[9], Google, and Apple) have no significant relationship but rather are direct market competitors. While there is some overlap between Google and Microsoft IPRs, this Petition is substantively identical to the Google IPR Petition and addresses different prior art references and arguments than the Microsoft IPR Petition. There are also no concerns of road-mapping based on patent owner's preliminary response because Google could not have taken advantage of such later-filed response in preparing its petition that Apple now seeks to join. The filing of multiple petitions here is the result of Proxense filing serial district

[9] Microsoft filed a petition challenging claims of the '289 patent in IPR2024-00407.

court actions. There is no risk that the Petition would undermine the Office's ability to complete the proceedings in a timely manner. Moreover, the Board has authority to consolidate proceedings to achieve efficiency. *See* 35 U.S.C. §315(d); 37 C.F.R. §42.122(a).

B. Discretionary Denial Not Warranted Under *Fintiv*

While Apple and Proxense are involved in the litigation *Proxense, LLC v. Apple Inc.*, Case No. 6-24-cv-00143 (W.D. Tex) (filed March 18, 2024) ("the Apple Litigation"), Proxense only recently asserted the '289 Patent in the Apple Litigation. *See* Ex-1034 (entered October 31, 2024).

In any case, the Board should not exercise its § 314(a) discretion to deny institution. While the trial is currently tentatively scheduled for January 2026 (Ex-1032, 8), the case schedule is subject to change, as Proxense admits. *See* Ex-1029, 3. Moreover, the median time from filing to trial in the Western District of Texas is 32.7 months (Ex-1031, 37), which would set trial for December 2026, well after the approximate November, 2025 final written decision deadline in the Google IPR, which this Petition seeks to join. In addition, Petitioner has a pending motion to transfer (Dkt. 30) in the Apple Litigation. If the motion is granted, the case will be transferred to the Northern District of California where a new case schedule will be entered. Finally, Petitioner stipulates that if the present proceeding is instituted, Petitioner will not pursue the grounds raised in this Petition in the Apple Litigation

with respect to the claims for which trial is instituted. *See Sand Revolution*, IPR2019-01393, Paper 24 at 7. The stipulation reduces any overlap and mitigates concerns of duplicative efforts or potentially conflicting decisions.

C. Discretionary Denial Not Warranted Under §325(d)

Advanced Bionics strongly favors institution. IPR2019-01469, Paper 6. None of the references presented herein were considered by the Examiner during prosecution or previously considered. *See generally* Ex-1002. Accordingly, Petitioner submits that the first part of the *Advanced Bionics* framework is not satisfied because this Petition includes grounds based on combinations of prior art not previously considered by the Office. Because the first part is not satisfied, the Board need not consider the second part. To the extent the Board determines an analysis under the second part of *Advanced Bionics* is warranted, Petitioner submits that the asserted Grounds demonstrate that the Examiner erred in the evaluation of the prior art. Thus, Petitioner submits that the evidence and facts presented in the Petition warrant reconsideration of the prior art, and respectfully requests the Board decline exercising its discretion to deny institution under 35 U.S.C. §325(d).

VIII. Mandatory Notices

A. Real Parties-in-Interest Under 37 C.F.R. §42.8(b)(1)

Apple Inc. is the real party-in-interest.

B. Related Matters Under 37 C.F.R. §42.8(b)(2)

The '289 patent is assigned to Proxense, LLC, which has recently moved the district court in *Proxense, LLC v. Apple Inc.*, No. 6:24-cv-00143 (W.D. Tex.) to assert the '289 patent against Apple. To the best of Petitioner's knowledge, the '289 patent is/was involved in the following district court litigations/proceedings:

Name	Number	Court	Filed
Proxense, LLC v. Microsoft Corp.	6:23-cv-00319	WDTX	May 2, 2023
Proxense, LLC v. Google LLC	6:23-cv-00320	WDTX	May 2, 2023
Proxense, LLC v. Apple Inc.	6:24-cv-00143	WDTX	Mar. 18, 2024
Microsoft Corp. v. Proxense, LLC	IPR2024-00407	PTAB	Jan. 16, 2024
Google LLC v. Proxense, LLC	IPR2024-00783	PTAB	Apr. 19, 2024
Google LLC v. Proxense, LLC	IPR2024-01319[10]	PTAB	Aug. 22, 2024

[10] In IPR2024-01319, Google seeks joinder with Microsoft's challenge in IPR2024-00407.

Petitioner is not aware of any disclaimers or reexamination certificates addressing the '289 Patent. Exhibit Ex-1033 lists the applications and patents related to the '289 Patent according to Patent Center.

C. Counsel and Service Information Under 37 C.F.R. §42.8(b)(3)

Lead Counsel	Back-Up Counsel
PHILIP W. WOO USPTO Reg. No. 39,880 DUANE MORRIS LLP, 260 Homer Avenue #202 Palo Alto, CA 94301 P: (650) 847-4145 F: (650) 644-0150 PWWoo@duanemorris.com	MONTÉ T. SQUIRE USPTO Reg. No. 80,123 DUANE MORRIS LLP 1201 North Market Street, Suite 501, Wilmington, DE 19801 P: (302) 657-4918 F: (302) 397-2543 MTSquire@duanemorris.com
	D. STUART BARTOW USPTO Reg. No. 56,505 DUANE MORRIS LLP 1201 North Market Street, Suite 501, Wilmington, DE 19801 P: (650) 847-4158 F: (650) 618-8505 DSBartow@duanemorris.com
	PAUL BELNAP USPTO Reg. No. 73,106 DUANE MORRIS LLP 901 New York Ave. NW, Suite 700 East, Washington, D.C. 20001 P: (202) 776-7879 F: (202) 776-7801 PHBelnap@duanemorris.com

D. Service Information Under 37 C.F.R. §42.8(b)(4)

Please address correspondence to lead and back-up counsel at the addresses above. Petitioner consents to electronic service by e-mail at the addresses above.

IX. Standing

Petitioner certifies that the '289 patent is available for IPR, and Petitioner is not barred or estopped from requesting IPR on the grounds identified in this Petition.

X. Conclusion

Petitioner has established that the challenged claims are unpatentable and requests the Board institute and cancel each challenged claim as unpatentable.

Dated: November 4, 2024

Respectfully submitted,

DUANE MORRIS LLP

BY: /Philip W. Woo/
Philip W. Woo
USPTO Reg. No. 39,880
Duane Morris LLP
260 Homer Avenue #202
Palo Alto, CA 94301

ATTORNEY FOR PETITIONER

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that the foregoing **PETITION FOR *INTER PARTES* REVIEW** contains 13,941 words, excluding those portions exempted under 37 C.F.R. § 42.24(a), as measured by the word-processing system used to prepare this paper.

Date: November 4, 2024

BY: /Philip W. Woo/

Philip W. Woo
USPTO Reg. No. 39,880
Duane Morris LLP
260 Homer Avenue #202
Palo Alto, CA 94301

ATTORNEY FOR PETITIONER

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on November 4, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

PATENT LAW WORKS/PROXENSE
Greg Sueoka
4516 South 700 East, Suite 290
Salt Lake City, UT 84107

Additionally, a courtesy copy of the IPR and all supporting exhibits were emailed to counsel of record for the Patent Owner in the litigation before the United States District Court for the Western District of Texas:

Brian D. Melton
Susman Godfrey, LLP
1000 Louisiana St.
Suite 5100
Houston, TX 77002

Dated: November 4, 2024

BY: /Philip W. Woo/

Philip W. Woo
USPTO Reg. No. 39,880
Duane Morris LLP
260 Homer Avenue #202
Palo Alto, CA 94301

ATTORNEY FOR PETITIONER