(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 028 401 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
16.08.2000 Bulletin 2000/33

(51) Int. Cl.[7]: **G07F 19/00**, G07F 7/08

(21) Application number: **00200448.9**

(22) Date of filing: **10.02.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **12.02.1999 US 119818 P**
21.07.1999 US 144927 P

(71) Applicant: **CITIBANK, N.A.**
New York, New York 10043 (US)

(72) Inventors:
- **Schutzer, Dan**
  New York 10583 (US)
- **Slater, Alan**
  East Brunswick, New Jersey 08816 (US)
- **Cirillo, Thomas**
  Greenwich, Connecticut 06830 (US)
- **Derodes, Robert**
  Peachtree City, Georgia 30269 (US)
- **Dancanet, Lucien**
  Los Angeles, Califonia 90045 (US)

(74) Representative: **Hynell, Magnus**
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) Method and system for performing a bankcard transaction

(57) A method and system for performing a bankcard transaction provides a transaction card system for use, for example, on the Internet that allows a transaction card user to input authentication information to a transaction card issuer, which generates an anonymous or alternate card number and maintains a link between the anonymous or alternate card number and the transaction card user's transaction card number. An alternate aspect makes use, for example, of software on a local computing device, such as the transaction card user's personal computer or a point of sale terminal, which authenticates the transaction card user and generates the anonymous or alternate card number in sequence synchronization with the transaction card issuer's server.

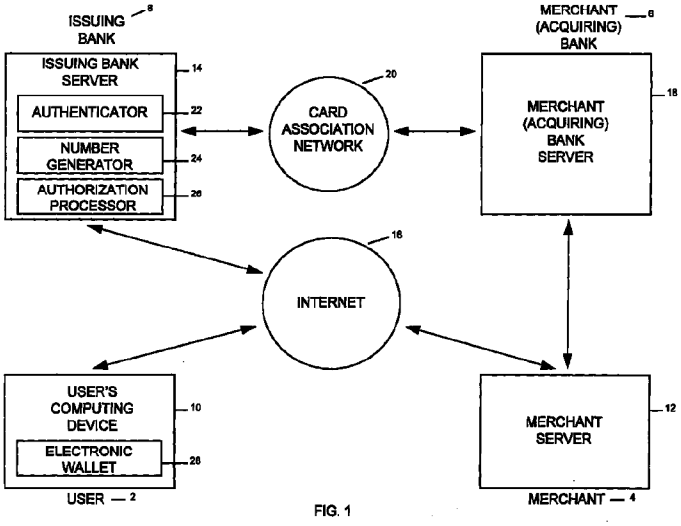

FIG. 1

EP 1 028 401 A2

Apple 1115

Description

Cross-Reference to Related Applications

[0001] This application claims priority to applicant's co-pending application having U.S. Serial No. 60/119,818 filed February 12, 1999 and applicant's co-pending application having U.S. Serial No. 60/144,927 filed July 21, 1999.

Field of the Invention:

[0002] The present invention relates generally to the field of bankcard transactions and more particularly to a method and system for securely performing a bankcard transaction utilizing an anonymous or alternate card number.

Background of the Invention

[0003] Transaction card transactions that occur over the Internet today utilizing the transaction card infrastructure are most commonly performed, for example, by a cardholder transmitting his or her credit or debit card number over an encrypted link, using a standard universally available web browser and server capability such as Secure Sockets Layer (SSL) to the merchant server. The link between the cardholder and the merchant must be encrypted to prevent the card number from being intercepted and fraudulently read by an unauthorized third party. This type of fraud is sometimes referred to as the man-in-the-middle attack. The link is encrypted so that no eavesdropper can listen in and steal the card number. However, this method has a number of disadvantages.

[0004] For example, the cardholder must trust the merchant with safeguarding the card number. This leaves the cardholder vulnerable to a risk of fraud by a merchant or its employees or a merchant who is honest but who is nevertheless negligent in maintaining the merchant's web site against break-ins. This risk is great enough to discourage customers from giving their card numbers to merchant web sites over the Internet whom they do not know or with whom they have no previous experience.

[0005] The particular risk is limited with credit cards and debit cards by consumer protection laws and association rules to a maximum exposure, such as $50 limit. Further, the cardholder has an opportunity, for example, with a credit card to dispute a charge before it is actually deducted from the cardholder's account. However, it is still a nuisance and a risk, and in the event of fraud, it may be necessary for the cardholder to be issued a new card and card number. The risk is greater with debit cards, because the limitation of liability is not as clear, and the charge is deducted from the cardholder's account before he or she is informed. Thus, with a debit card, the cardholder is placed in the position of having to dispute the deduction in order to regain his or her stolen funds.

[0006] Another disadvantage, for example, is that when a merchant accepts a card number from a customer over the Internet, the merchant has no way of authenticating that the customer making the purchase is the actual cardholder. The transaction is treated as a Mail Order/Telephone Order (MOTO) transaction, also known as a "card not present" transaction. In such a transaction, the merchant's transaction cost and exposure is much greater than when a customer is physically present at the point-of-sale. If the customer successfully disputes having made the transaction, the merchant payment is reversed by the card issuer.

[0007] These disadvantages provide incentives for a better approach to security for bankcard transactions from the standpoint of both cardholders and merchants, provided it is fast, simple and inexpensive. Many solutions have been proposed to address this need, most notably the Credit Card Association's standard specification, Secure Electronic Transaction (SET) protocol. A problem with solutions such as SET is that they impose a significant cost and performance penalty, requiring both cardholders and merchants to install special software and/or hardware that add significantly to transaction costs, in terms of both money and time.

Summary of the Invention

[0008] It is a feature and advantage of the present invention to provide method and system for securely performing a bankcard transaction which affords all of the account number of security of the SET protocol as well as the ability to authenticate the customer, while maintaining the simplicity of sending a transaction card number over an encrypted link, such as SSL.

[0009] It is another feature and advantage of the present invention to provide a method and system for securely performing a bankcard transaction which eliminates transmitting the customer's actual card number over the Internet to the merchant and likewise eliminates the need for a secure link between the customer and the merchant.

[0010] It is a further feature and advantage of the present invention to provide a method and system for securely performing a bankcard transaction, such as a credit card or debit card transaction, that is fast and easy to implement and that requires little, if any, modification to the existing Internet infrastructure.

[0011] To achieve the stated and other features, advantages and objects, an embodiment of the present invention provides a method and system for securely performing an bankcard transaction in which a transaction card user receives an alternate or anonymous card number tat is not the user's actual card number but tat is designed, for example, to pass any validity checks made by a merchant or the merchant's bank. The alternate or anonymous card number can be used only once

within a limited time period and cannot be copied and replayed. Upon receipt of the anonymous or alternate card number by the transaction card issuer, the anonymous card number can be associated by the card issuer with the proper cardholder and the cardholder's account can be authorized.

[0012] In an embodiment of the present invention, the transaction card user authenticates himself or herself, for example, to an authenticator of the transaction card issuer's server. The transaction card user can authenticate himself or herself, for example, by entering transaction card user information at a computing device, such as a personal computer, a personal digital assistant, or a smart card, coupled to the card issuer's server over a network, such as the Internet.

[0013] In addition, in an embodiment of the present invention, an electronic wallet application of the computing device can be utilized by the transaction card user for sending the transaction card user information to the transaction card issuer's server for user authentication. The transaction card user information includes, for example, one or more of a personal identification number, a password, a biometric sample, a digital signature or the transaction card number for the transaction card user, and the transaction card user information can be encrypted.

[0014] In an alternative aspect for an embodiment of the present invention, the transaction card user authenticates himself or herself with the transaction card user information at a local computing device, such as a personal computer, a personal digital assistant, or a smart card of the transaction card user. In this aspect, the transaction card user authenticates himself or herself on an application of the transaction card user's local computing device, such as an electronic wallet application, by entering the transaction card user information on the application at the local computing device.

[0015] In an embodiment of the present invention, when the transaction card user is authenticated by the transaction card issuer, a number generator of the transaction card issuer's server generates an anonymous card number for the transaction card user. However, in the alternative aspect in which the transaction card user authenticates himself or herself on an application of the transaction card user's local computing device, the anonymous card number is likewise generated at the local computing device, for example, by a number generating application of the local computing device which is synchronized with the number generator of the transaction card issuer's server.

[0016] The anonymous card number for an embodiment of the present invention is generated according to a number generating scheme, such as a random number generating algorithm, a random sequence generator, and/or a secure-hashing algorithm. Further, the anonymous card number is generated according to predefined parameters limiting its use to the particular transaction and/or for a predetermined time period.

[0017] In an embodiment of the present invention, the anonymous card number generated by the transaction card issuer is associated with a transaction card number of the transaction card user, for example, by linking the anonymous card number with the transaction card number by either or both of the number generator or the authorization processor of the transaction card issuer's server.

[0018] However, in the alternative aspect in which the anonymous card number is generated at the transaction card user's local computing device, the anonymous card number is linked with the transaction card number according to a pre-defined sequence synchronization between the number generator of the local computing device and the transaction card issuer's server.

[0019] In an embodiment of the present invention, the anonymous or alternate card number is used in a transaction by the transaction card user in place of the transaction card user's transaction card number. For example, the transaction card user sends the anonymous card number to the merchant, which in turn sends it to the merchant' bank with a request for authorization. The merchant's bank sends the anonymous card number over the card association network to the transaction card issuer. The transaction card issuer's authorization processor receives the anonymous card number linked with the transaction card number and sends an authorization back to the merchant via the card association network and the merchant's bank.

[0020] In another embodiment of the present invention, the anonymous or alternate card number is used in a transaction by the transaction card issuer after authenticating the user. For example, the transaction card user authenticates himself to the issuing bank, and the issuing bank sends the anonymous card number directly to the merchant which, in turn, sends it to the merchant's bank with a request for authorization.

[0021] In another embodiment of the present invention, the transaction card user authenticates himself to the transaction card issuer, and the transaction card issuer sends the anonymous card number, along with an authorization, directly to the merchant which, in turn, sends both the anonymous card number and the authorization to the merchant's bank for verification and processing. The transaction card user uses the actual transaction card number and the alternate card number for billing and communicating to its transaction card user, and the alternate card number and authorization number for settlement with the merchant bank and card processing network.

[0022] Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention.

Brief Description of the Drawings

[0023]

Fig. 1 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous or alternate card number is sent to a cardholder by a card issuer for use in an on-line bankcard transaction;

Fig. 2 is a flow chart which illustrates an example of the process of the cardholder performing a bankcard transaction using the anonymous or alternate card number which was sent to the cardholder by the card issuer for an embodiment of the present invention;

Fig. 3 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous or alternate card number is generated at the cardholder's computing device for use in an on-line bankcard transaction;

Fig. 4 is a flow chart which illustrates an example of the process of the cardholder performing a bankcard transaction using the anonymous or alternate card number which was generated at the cardholder's computing device for an embodiment of the present invention;

Fig. 5 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous or alternate card number is generated a point of sale for the cardholder; and

Fig. 6 is a diagram which illustrates a sample of a Linear Feedback Shift Register used to generate anonymous or alternate card numbers for an embodiment of the present invention.

Detailed Description of the Invention

[0024] Referring now in detail to an embodiment of the invention, an example of which is illustrated in the accompanying drawings, Fig. 1 is a schematic diagram which illustrates an overview of examples of key components and the flow of information between the key components for an embodiment of the present invention in which an anonymous card number is sent to a cardholder by a card issuer for use in an on-line bankcard transaction. An embodiment of the present invention involves a number of entities, such as a cardholder 2, a merchant 4, a merchant (acquiring) bank 6, and a card issuer 8. An embodiment of the present invention also makes use, for example, of computer hardware and software, such as a cardholder's computing device 10, a merchant's website server 12, and a card issuer's server 14, each coupled over a network, such as the Internet 16, as well as a merchant (acquiring) bank server 18 coupled to the merchant server 12 and also coupled to the issuing bank server 14 over a card association network 20. In addition, the card issuer's server comprises, for example, an authenticator 22, an alternate card number generator 24, and an authorization processor 26.

[0025] In an embodiment of the present invention, the cardholder 2 receives an alternate card number (referred to herein as either "anonymous card number" or "alternate card number") from the cardholder's issuing bank 8 that is not the cardholder's actual card number. The anonymous card number is issued after the cardholder 2 authenticates himself or herself directly to the cardholder's card issuer 8. The anonymous card number is utilized only once within a limited period of time. It is designed to pass any validity checks made by the merchant 4 and the merchant's bank 6 and cannot be copied and replayed. Upon receipt of the anonymous card number for authorization, the anonymous card number can be associated by the issuing bank 8 with the proper cardholder 2 and the cardholder's account and can be authorized.

[0026] Fig. 2 is a flow chart which illustrates an example of the process of the user 2 performing a bankcard transaction using the anonymous or alternate card number for an embodiment of the present invention in which the anonymous card number is sent to the cardholder 2 by the card issuer 8. At S1, the merchant's server 12 sends a request over the Internet 16 to the user 2 at the user's computing device 10 for a transaction card number in connection with an on-line transaction for the user 2. At S2, the user 2 receives the request at the user's computing device 10 and sends a request over the Internet 16 to the card issuer's server 14 for an alternate card number. At S3, the card issuer's authenticator 22 receives the request, authenticates the user 2 and obtains an alternate card number linked to the user's actual card number from the card issuer's number generator 24, and sends the alternate card number over the Internet 16 to the user 2 at the user's computing device 10. At S4, the user 2 at the user's computing device 10 sends the alternate card number over the Internet 16 to the merchant' server 12.

[0027] Referring further to Fig. 2, in an embodiment of the present invention, at S5, the merchant's server 12 receives and sends the alternate card number to the merchant (acquiring) bank's server 18 with a request for authorization. At S6, the merchant (acquiring) bank's server 18 receives the request for authorization and sends the request with the alternate card number over the card association network 20 to the card issuer's server 14. At S7, the card issuer's authorization processor 26 receives the request for authorization, links the alternate card number to the user's actual account for authorization, and sends an authorization for the alternate card number to the merchant (acquiring) bank's

server 18 over the card association network 20. At S8, the merchant (acquiring) bank's server 18 receives the authorization and sends it to the merchant's server 12. At S9, the merchant's server 12 receives the authorization and completes the transaction with the user 2.

[0028] Referring again to Fig. 2, in an embodiment of the present invention, the cardholder 2 authenticates himself or herself on-line over a secure (encrypted) line with the cardholder's issuing bank 8 at S2, utilizing, for example, an electronic wallet 28 as shown in Fig. 1. When the cardholder 2 is authenticated, he or she receives the anonymous card number over the same line at S3. Alternatively, at S3, the cardholder 2 can have the anonymous card number sent by the card issuer 8 directly to the merchant 4, in which case, it is not necessary for the cardholder 2 to send the anonymous card number to the merchant 4 at S4.

[0029] Referring once more to Fig. 2, in an embodiment of the present invention, the cardholder 2 authenticates himself or herself to the cardholder's issuing bank 8 by typing in his or her card number and a secret PIN or password or hash of a PIN or password at the user's computing device 10 and sending it over an encrypted link to the issuing bank 8 at S2. The encrypted link ensures that no third party can eavesdrop and steal the card number and PIN. The cardholder 2 can feel secure that the card number, PIN or password or hashed PIN or password are safe with the issuing bank 8, as the issuing bank 8 already knows and safeguards this information. Because the cardholder 2 authenticates himself or herself with a PIN or password, the issuing bank 8 can authenticate the cardholder 2 to the merchant 12. If the transaction or the customer's history warrants, the issuing bank 8 can require more secure authentication, such as additional secrets, matching biometrics, and/or digital signatures.

[0030] In an alternative aspect of an embodiment of the present invention, the issuing bank 8 can install software on the cardholder's PC or information appliance 10, such as a smart card or personal digital assistant (PDA) type computing device, that can generate the anonymous card number after the cardholder 2 identifies himself or herself to the software and/or appliance 10. Fig. 3 is a schematic diagram which illustrates an overview of an example key components and the flow of information between the key components for an alternate aspect of an embodiment of the present invention in which an anonymous card number is generated at the cardholder's computing device 10 in an on-line transaction. In this aspect, the card issuer 8 can install software 30 on the cardholder's computing device 10, which can be a personal computer (PC) or hardware token, such as a smartcard, that generates the anonymous card number locally upon authentication of the cardholder 2.

[0031] Fig. 4 is a flow chart which illustrates an example of the process of the user 2 performing a bankcard transaction for an embodiment of the present invention in which the anonymous card number is generated at the cardholder's computing device 10. Referring to Fig. 4, at S10 , the merchant server 12 sends a request for a transaction card number over the Internet 16 to the cardholder 2 at the cardholder's computing device 10. At S11, the cardholder 2 receives the request at the cardholder's computing device 10, and the number generating software 30 at the cardholder's computing device 10 generates and sends an alternate card number to the merchant's server 12. At S12, the merchant's server 12 receives the alternate card number and sends a request for authorization with the alternate card number to the merchant (acquiring) bank's server 18.

[0032] Referring further to Fig. 4, in an embodiment of the present invention, at S13, the merchant (acquiring) bank's server 18 receives the request and sends the request over the card association network 20 to the card issuer's server 14. At S14, the card issuer's alternate card number generator 24 receives the request, generates the next number in sequence synchronized to the cardholder's software 30, links the alternate card number to the cardholder's actual card number, and sends the cardholder's actual card number to the card issuer's authorization processor 26. At S15, the card issuer's authorization processor 26 receives the cardholder's actual card number and sends an authorization over the card association network 20 to the merchant (acquiring) bank's server 18. At S16, the merchant (acquiring) bank's server 18 receives the authorization and sends it to the merchant's server 12. At S17, the merchant's server 12 receives the authorization and completes the transaction with the user 2.

[0033] In another aspect of an embodiment of the present invention, the card issuer 8, such as a bank, provides an electronic wallet system, including, for example, an electronic wallet server. In this aspect, the issuing bank 8 matches the anonymous card number with the actual user account. If the electronic wallet generates an anonymous card number for the cardholder 2 for which the wallet server is not the issuing bank, then the anonymous card number is sent back to the wallet server for matching the anonymous card number with the actual user card number and for sending it to the issuing bank 8 for authorization. In this situation, the electronic wallet, in effect, performs an acquiring bank function.

[0034] Another aspect of an embodiment of the present invention enables the cardholder 2 to perform a transaction, such as a purchase, at a physical point-of-sale without revealing the cardholder's true card number. Fig. 5 is a schematic diagram which illustrates an example of key components and the flow of information between the key components for an aspect of an embodiment of the present invention in which an alternate card number is generated at a point-of sale for a bankcard transaction. This aspect makes use, for example, of a card 32 with no embossed number but with an input device 34, such as a keypad, a display 36, such as

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.