(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: **US 2010/0306113 A1**

Gray et al. (43) **Pub. Date: Dec. 2, 2010**

(54) **SMARTCARD INTERNET AUTHORIZATION SYSTEM**

(75) Inventors: **William J. Gray**, Salt Lake City, UT (US); **William G. Hohle**, Lehi, UT (US); **Carl Larkin**, West Sussex (GB); **Lee J. Peart**, Skioiju (GB)

Correspondence Address:
Snell & Wilmer L.L.P. (AMEX)
ONE ARIZONA CENTER, 400 E. VAN BUREN STREET
PHOENIX, AZ 85004-2202 (US)

(73) Assignee: **American Express Travel Related Services Company, Inc.**, New York, NY (US)

(21) Appl. No.: **12/857,393**

(22) Filed: **Aug. 16, 2010**

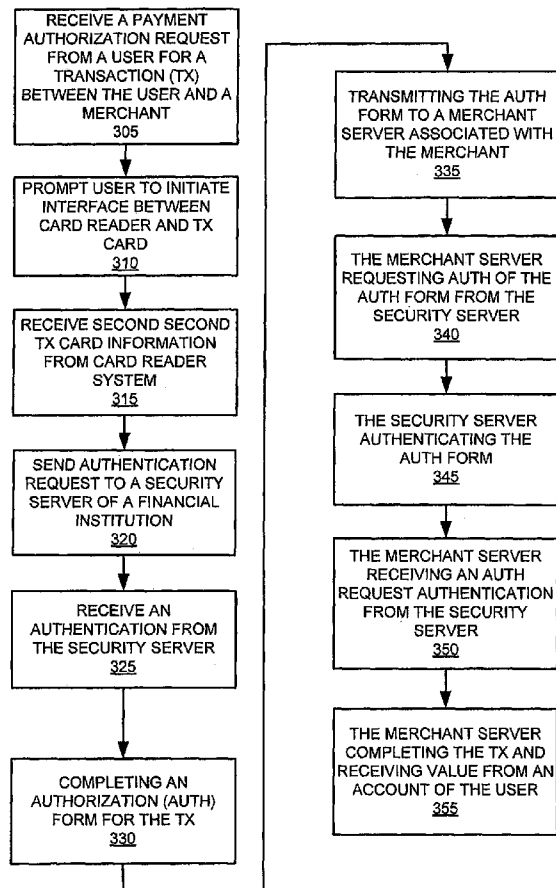**Related U.S. Application Data**

(63) Continuation of application No. 11/954,668, filed on Dec. 12, 2007, now Pat. No. 7,801,829, which is a continuation of application No. 09/754,465, filed on Jan. 4, 2001, now Pat. No. 7,366,703.

(60) Provisional application No. 60/174,564, filed on Jan. 5, 2000.

Publication Classification

(51) **Int. Cl.**
G06Q 20/00	(2006.01)
G06Q 99/00	(2006.01)

(52) **U.S. Cl.** **705/76**

(57) **ABSTRACT**

A system and method are disclosed for conducting electronic commerce such as a virtual purchase transaction with an on-line merchant. A user is provided with an intelligent token, such as a smart card containing a digital certificate. The intelligent token suitably authenticates with a wallet server on a network that conducts all or portions of the transaction on behalf of the user with out requiring changes to the merchant's server. The wallet server interacts with a security server of a selected financial service to provide authentication of the transaction. Upon authentication, the digital wallet pre-fills forms which are transmitted to the merchant who contacts the security server for validation of the forms and upon validation, completes the transaction with the user.
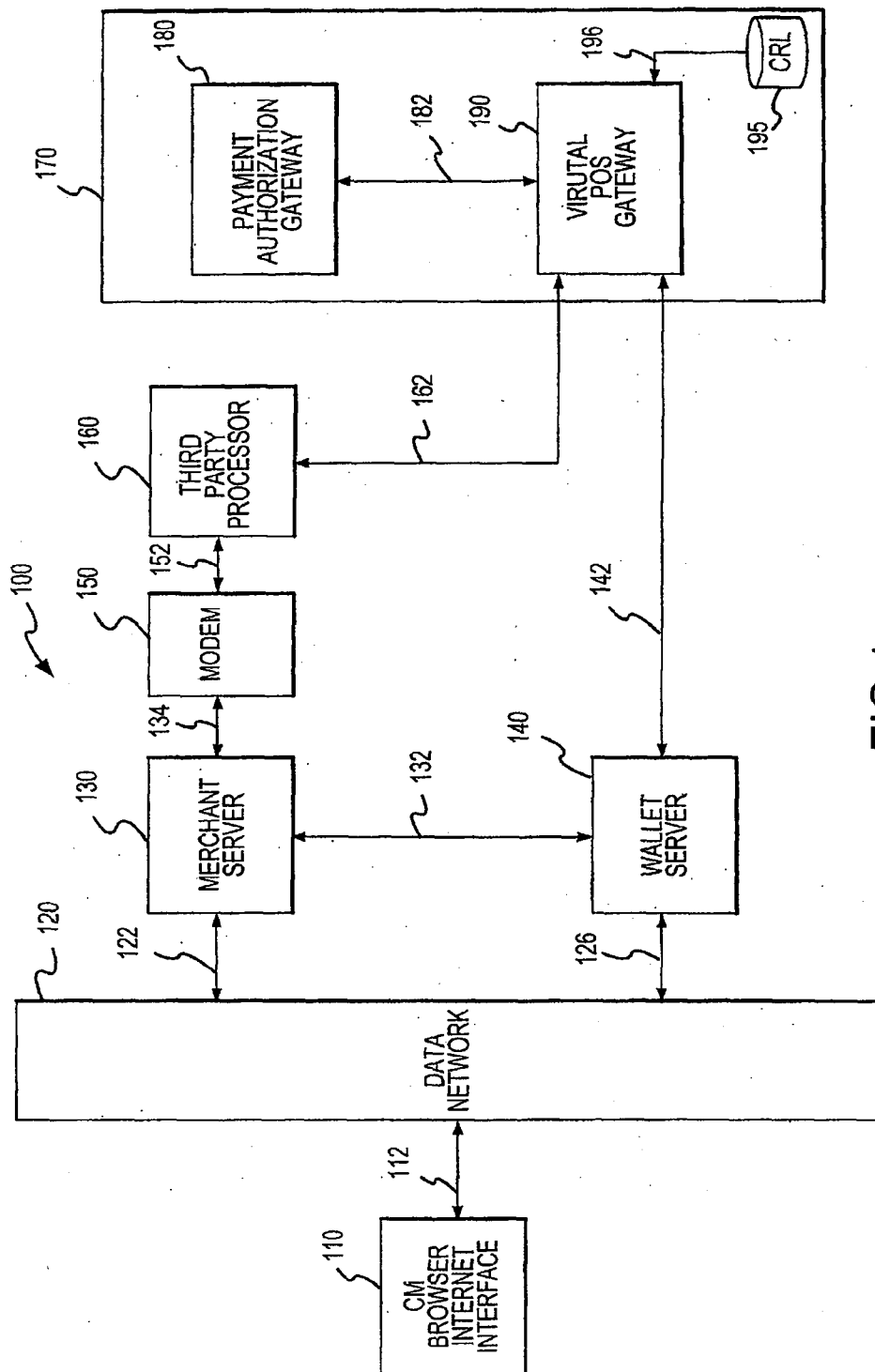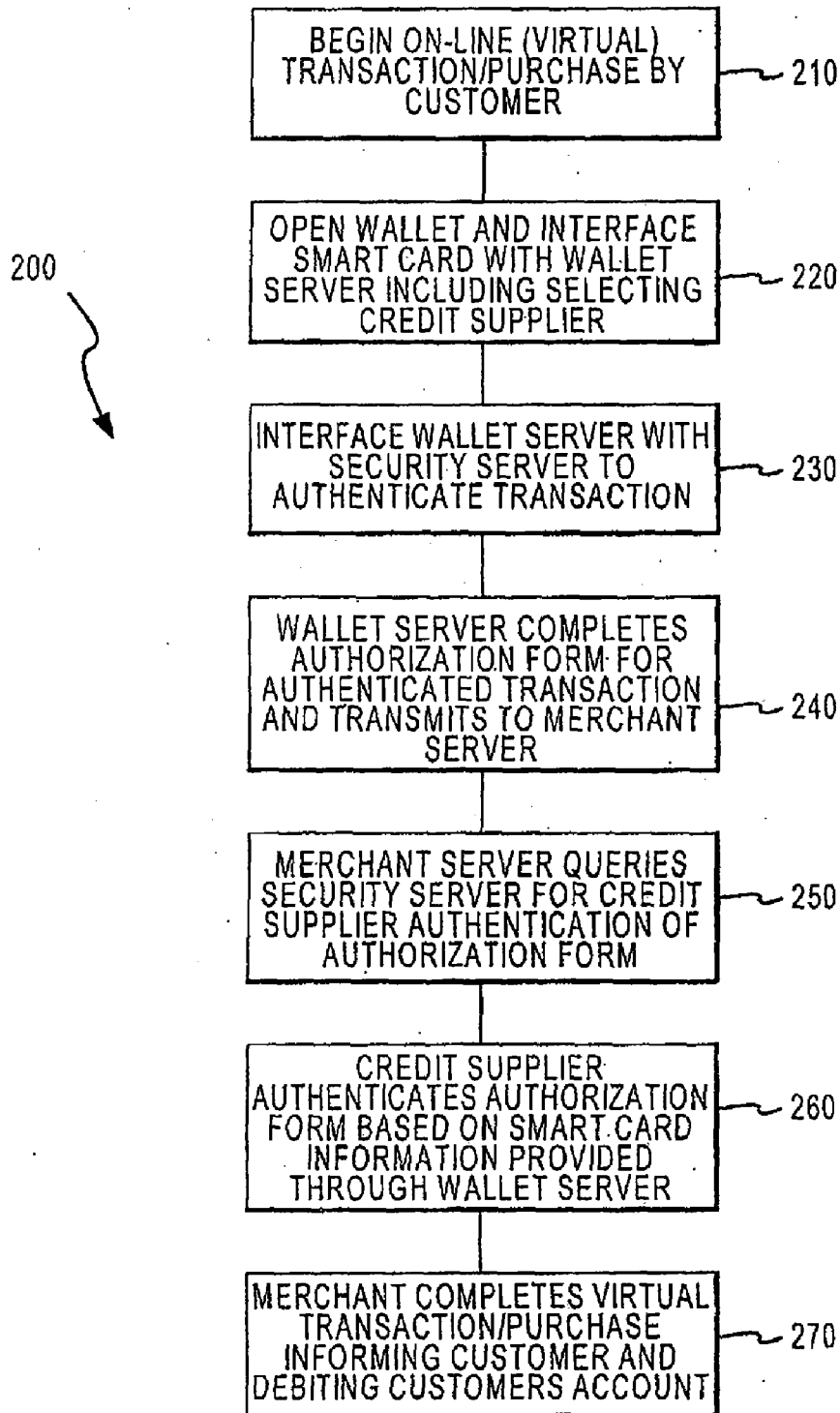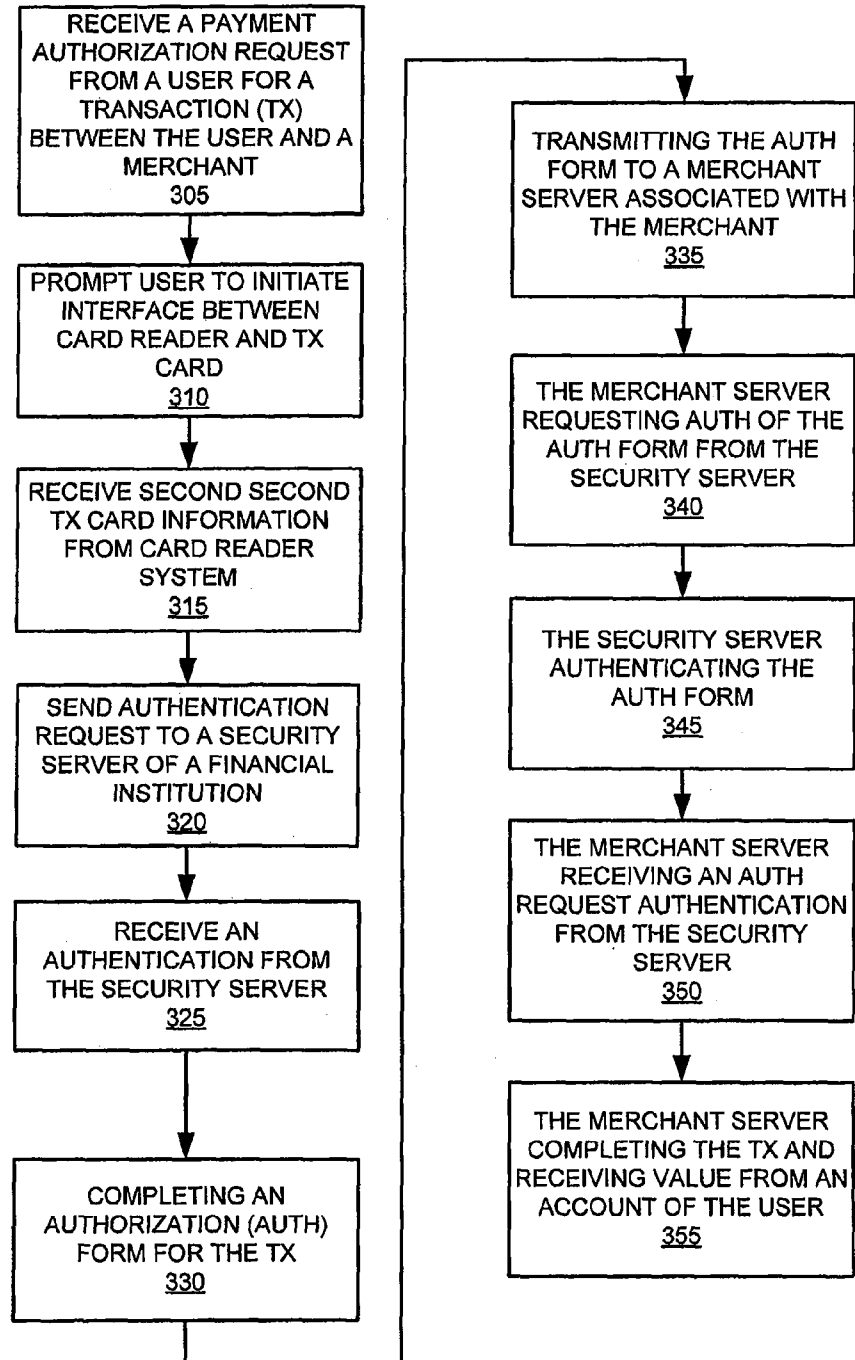
FIG.1

200

BEGIN ON-LINE (VIRTUAL)
TRANSACTION/PURCHASE BY
CUSTOMER   — 210

OPEN WALLET AND INTERFACE
SMART CARD WITH WALLET
SERVER INCLUDING SELECTING   — 220
CREDIT SUPPLIER

INTERFACE WALLET SERVER WITH
SECURITY SERVER TO   — 230
AUTHENTICATE TRANSACTION

WALLET SERVER COMPLETES
AUTHORIZATION FORM FOR
AUTHENTICATED TRANSACTION   — 240
AND TRANSMITS TO MERCHANT
SERVER

MERCHANT SERVER QUERIES
SECURITY SERVER FOR CREDIT
SUPPLIER AUTHENTICATION OF   — 250
AUTHORIZATION FORM

CREDIT SUPPLIER
AUTHENTICATES AUTHORIZATION
FORM BASED ON SMART CARD   — 260
INFORMATION PROVIDED
THROUGH WALLET SERVER

MERCHANT COMPLETES VIRTUAL
TRANSACTION/PURCHASE
INFORMING CUSTOMER AND   — 270
DEBITING CUSTOMERS ACCOUNT

FIG.2

300

RECEIVE A PAYMENT
AUTHORIZATION REQUEST
FROM A USER FOR A
TRANSACTION (TX)
BETWEEN THE USER AND A
MERCHANT
305

PROMPT USER TO INITIATE
INTERFACE BETWEEN
CARD READER AND TX
CARD
310

RECEIVE SECOND SECOND
TX CARD INFORMATION
FROM CARD READER
SYSTEM
315

SEND AUTHENTICATION
REQUEST TO A SECURITY
SERVER OF A FINANCIAL
INSTITUTION
320

RECEIVE AN
AUTHENTICATION FROM
THE SECURITY SERVER
325

COMPLETING AN
AUTHORIZATION (AUTH)
FORM FOR THE TX
330

TRANSMITTING THE AUTH
FORM TO A MERCHANT
SERVER ASSOCIATED WITH
THE MERCHANT
335

THE MERCHANT SERVER
REQUESTING AUTH OF THE
AUTH FORM FROM THE
SECURITY SERVER
340

THE SECURITY SERVER
AUTHENTICATING THE
AUTH FORM
345

THE MERCHANT SERVER
RECEIVING AN AUTH
REQUEST AUTHENTICATION
FROM THE SECURITY
SERVER
350

THE MERCHANT SERVER
COMPLETING THE TX AND
RECEIVING VALUE FROM AN
ACCOUNT OF THE USER
355

Figure 3

SMARTCARD INTERNET AUTHORIZATION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001]　This application is a continuation of and claims the benefit of and priority to U.S. Ser. No. 11/954,668 entitled "SMARTCARD INTERNET AUTHORIZATION SYS-TEM" filed on Dec. 12, 2007. The '668 application is a continuation of and claims the benefit of and priority to U.S. Pat. No. 7,366,703 entitled "SMARTCARD INTERNET AUTHORIZATION SYSTEM" issued on Apr. 29, 2008 (aka U.S. Ser. No. 09/754,465 filed on Jan. 4, 2001). The '703 patent claims the benefit of and priority to U.S. Provisional Application No. 60/174,564, filed Jan. 5, 2000. All of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002]　The invention relates generally to methods and apparatus for conducting network transactions, and more particularly, to systems for authenticating and conducting business over data networks such as the Internet.

BACKGROUND OF THE INVENTION

[0003]　In recent years, many consumers have discovered the convenience and economy of purchasing goods and services electronically. A number of channels for electronic purchases (commonly called "e-purchases") are available, including shop-at-home television networks, call-in responses to television advertisements, and the like. Most recently, direct purchasing via the Internet has become extremely popular.

[0004]　In a typical Internet transaction, a consumer generally identifies goods and/or services for purchase by viewing an online advertisement such as a hypertext markup language (HTML) document provided via a World Wide Web (WWW) browser. Payment typically occurs in various ways. One such way is via a charge card number that is provided via a secure channel such as a secure sockets layer (SSL) connection that is established between the consumer and the merchant.

[0005]　While millions of such transactions take place every day via the Internet, these conventional SSL transactions often exhibit a number of marked disadvantages. Although SSL typically provides a secure end-to-end connection that prevents unscrupulous third parties from eavesdropping (e.g., "sniffing") or otherwise obtaining a purchaser's charge card number, the protocol does not provide any means for ensuring that the charge card number itself is valid, or that the person providing the card number is legally authorized to do so. Because of the high incidence of fraud in Internet transactions, most charge card issuers consider network transactions to be "Card Not Present" transactions subject to a higher discount rate. Stated another way, because of the increased risk from "Card Not Present" transactions, most charge card issuers charge the merchant a higher rate for accepting card numbers via electronic means than would be charged if the card were physically presented to the merchant.

[0006]　To improve the security deficiencies inherent in transporting charge card numbers over unsecure networks, many have suggested the use of "smart cards". Smartcards typically include an integrated circuit chip having a micro-processor and memory for storing data directly on the card. The data can correspond to a cryptographic key, for example,

or to an electronic purse that maintains an electronic value of currency. Many smart card schemes have been suggested in the prior art, but these typically exhibit a marked disadvantage in that they are non-standard and typically require the merchants to obtain new, proprietary software for their Web storefronts to accept the smart card transactions. Moreover, the administration costs involved with assigning and maintaining the cryptographic information associated with smart cards have been excessive to date.

[0007]　Another standard, the Secure Electronic Transaction (SET) standard has been suggested to improve the security of Internet transactions through the use of various cryptographic techniques. Although SET does provide improved security over standard SSL transactions, the administration involved with the various public and private keys required to conduct transactions has limited SET's widespread acceptance. SET also requires special software for those merchants wishing to support SET transactions.

[0008]　Additionally, existing digital wallet technology, such as the digital wallet technology provided by, for example, GlobeSet, Inc., 1250 Capital of Texas Highway South, Building One, Suite 300, Austin, Tex., 78746, is being more frequently used to provide a means for users to utilize transaction card products (e.g., credit, charge, debit, smart cards, account numbers and the like) to pay for products and services on-line. In general, digital wallets are tools which store personal information (name, address, chargecard number, credit card number, etc.) in order to facilitate electronic commerce or other network interactions. The personal information can be stored on a general server or at a client location (PC or Smartcard) or on a hybrid of both a general server and a client server. Presently, the digital wallet general server is comprised of a Web server and a database server which centrally houses the user's personal and credit card information, shopping preferences and profiles of on-line merchants.

[0009]　A digital wallet preferably performs functions such as single sign on/one password, automatic form filling of check out pages, one or two click purchasing, personalization of Websites, on-line order and delivery tracking, itemized electronic receipts, and customized offers and promotions based upon spending patterns and opt-ins. More particularly, a one-click purchase activates the wallet and confirms the purchase at the same time. A two-click check out first activates the wallet, then the second click confirms the purchase. In use, the wallet bookmark is typically clicked by the user and an SSL session is established with the Wallet server. A browser plug-in is executed and the user supplies an ID/password or smart card for authentication in order to gain access to the wallet data. When shopping at an on-line merchant, the appropriate wallet data is transferred from the wallet server to the merchant's Web server.

[0010]　Existing systems, however, generally require that a merchant initiate changes to accommodate each different smart card or wallet. Accordingly, a new system of conducting electronic transactions is desired which would provide improved security with minimal overhead for users and merchants. Moreover, such a new system should integrate well with various smart cards and Internet wallets and other services provided by various merchants without requiring the merchant to make substantial changes to permit use of different systems.

SUMMARY OF THE INVENTION

[0011]　In an exemplary embodiment of the invention, a user is provided with a smart card having a standardized protocol

to make credit and debit transactions, such as, for example, the Blue™ from American Express™ smart card or the Europay MasterCard™ Visa™ (EMV) smart card. The user, also known as the cardmember (CM), utilizes the EMV Smartcard to interface with a wallet server to authenticate the user with a merchant server on a network through communications with a security server provided by a financial institution or credit provider such as, for example, American Express (AMEX). The CM purchaser conducts a virtual purchase transaction via the internet through a wallet server interacting with the security server to provide enhanced reliability and confidence in the transaction.

[0012] The user logs onto the internet via a browser and selects a wallet, causing the establishment of a secure sockets layer link to the wallet server and, at about the same time, activates the client window. The wallet server requests the user to insert the smartcard for authentication to the server wallet account. With an encrypted identity certificate being set, the user then selects the credit provider/financial institution, such as AMEX, who will be providing guarantee of the payment, from the provider available in the wallet. The user then logs onto the merchant server, completes shopping, goes to the checkout screen and clicks secure checkout. Again, the interfaces are over a secure sockets layer.

[0013] Next, the wallet server completes the form and transmits it to the merchant server, which uses telephone connections via a modem, direct link to a third party processor or directly to the security processor of the credit provider. The credit provider security processor uses the wallet interface to the user card to access smartcard functionality and generates a signed transaction. Alternatively, the connection can also be used to securely update functionality as required. The AMEX security processor authorizes the transaction on a "card press" basis. The merchant server then integrates the authorization with the wallet server completed form received from the wallet server and successfully completes the transaction, informing the user that the transaction has been successfully completed.

[0014] Thus, electronic transactions, such as purchase transactions, are conducted by receiving a transaction request from a user at a wallet server, issuing a challenge to the user from the wallet server, receiving a response from the user based upon the challenge, processing the response to verify the transaction instrument, assembling credentials (including authorization for the electronic transaction), and interfacing with a security server to authenticate the transaction. The system provides the benefits of protecting the market and the credit provider from fraud, transaction non-imputation, an ability to modify parameters on-line, and providing the user with better service at a lower cost by reducing the costs to the merchant because the entire process is transparent to the merchant.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The above and other features and advantages of the present invention are hereinafter described in the following detailed description of exemplary embodiments to be read in conjunction with the accompanying drawing figures, wherein like reference numerals are used to identify the same or similar parts or steps in the similar views, and:

[0016] FIG. 1 is a block diagram of an exemplary embodiment of the transaction system of the present invention;

[0017] FIG. 2 is a diagram of an exemplary process executed by the exemplary transaction system of FIG. 1; and

[0018] FIG. 3. is a diagram of an exemplary process for authorizing a transaction.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0019] The present invention may be described herein in terms of functional block components and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit (I.C.) components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, or the like, with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the invention could be used to detect or prevent security issues with a scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography, please review a text written by Bruce Schneider which is entitled "Applied Cryptography: Protocols, Algorithms, And Source Code In C," published by John Wiley & Sons (second edition, 1996), which is hereby incorporated by reference.

[0020] It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical electronic transaction system.

[0021] To simplify the description of the exemplary embodiment, the invention is described as pertaining to a system of electronic commerce, i.e., transactions, running over the Internet. It will be appreciated, however, that many applications of the present invention could be formulated. For example, the system could be used to authenticate users of a computer system, or to activate a passcode system, or any other purpose. One skilled in the art will appreciate that the network may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. Communication between the parties to the transaction and the system of the present invention is accomplished through any suitable communication means, such as, for example, a telephone network, Intranet, Internet, point of interaction device (point of sale device, personal digital assistant, cellular phone, kiosk, etc.), online communications, off-line communications, wireless communications, and/or the like. The users may interact with the system via any input

device such as a keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, or the like. Moreover, although the invention is frequently described herein as being implemented with TCP/IP communications protocols, it will be readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols.

[0022] Furthermore, the user and merchant may represent individual people, entities, or business and while reference is made to AMEX, this is by way of example and the financial authorization entity may represent various types of card issuing institutions, such as banks, credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. The payment network includes existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards.

[0023] Additionally, other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown. Each participant is equipped with a computing system to facilitate transactions. The user has a personal computer, the merchant has a computer/server, and the financial authorization entity has a main frame computer; however, any of the computers may be a minicomputer, a PC server, a network set of computers, laptops, notebooks, hand held computers, set-top boxes, and the like.

[0024] The customer and merchant may represent individual people, entities, or business. Although labeled as a "bank," the bank may represent other types of card issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown.

[0025] Each participant is equipped with a computing system to facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, and the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are possible. The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a minicomputer, a PC server, a network set of computers, and the like.

[0026] The computing units are connected with each other via a data communication network. The network is a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network is embodied as the internet. In this context, the computers may or may not be connected to the internet at all times. For instance, the customer computer may employ a modem to occasionally connect to the internet, whereas the bank computing center might maintain a permanent connection to the internet. It is

noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network.

[0027] The merchant computer and the bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network.

[0028] The electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

[0029] A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer.

[0030] Referring now to FIG. 1, a transaction system 100 typically includes at least one user or cardmember (CM) having a computer incorporating an internet browser 110 adapted to interface with a data network. In an exemplary embodiment, transaction system 100 is used in electronic commerce to conduct purchase transactions. It will be appreciated that although the transaction system described herein is an electronic commerce system, the present invention is equally applicable to various other electronic transaction systems. Specifically, the user system 110 is a purchaser or user which interfaces with a computer having an interface through data network 120 to a merchant server 130 and also to a digital wallet server 140.

[0031] The various computer systems and servers are interconnected as appropriate by data network 120, which is any data network, such as the internet or other public or private data network. Other suitable networks 120 include the public switch telephone network (PSTN), wireless networks, corporate or university intranets, and the like. Additionally, merchant server 130 is coupled to a modem 150 which is in communication with a third party processor (TPP) 160 which may be, but is not necessarily included, in the financial authorization entity secure processor 170. TPP 160 is further coupled to a virtual point of sale (POS) gateway processor 190 which is in the financial authorization entity secure processor 170. Also in the secure processor 170, and coupled to POS gateway processor 190, is payment authorization gateway 180. Further, wallet server 140 is coupled to merchant server 130 and to virtual point of sale (VPOS) gateway processor 190.

[0032] While an exemplary embodiment has been illustrated in FIG. 1, it will be appreciated that other embodiments

are possible. Thus, as also described above, components (e.g., user **110**, merchant **130**, and wallet server **140**) may be individual computers or network groups of computers acting with similar purpose to fulfill the functions described herein. Functionality attributed to a single component may be distributed among one or more individual computers in order to fulfill the described functionality. For example, the wallet server **140** may in fact be a collection of web servers, application servers, data base servers, and other types of servers. Also, in various embodiments, data bases (not shown) and/or profile servers (not shown) may be connected to wallet server **140**. For further information related to smart cards, browser functions, digital wallets and e-commerce transactions, see U.S. patents "Transaction Card", U.S. Pat. No. 6,581,839 issued on Jun. 24, 2003; "Method and Apparatus for Conducting Electronic Transactions", U.S. Pat. No. 7,343,351 issued on Mar. 11, 2008; "System and Method For Authenticating A Web Page", U.S. Pat. No. 7,203,838 issued on Apr. 10, 2007; and U.S. patent application "System and Method For Profiling A Web Site", U.S. Ser. No. 09/656,061, filed on Sep. 6, 2000, all of which are herein incorporated by reference.

[0033] To conduct a transaction, user **110** suitably establishes a connection through network **120** with a merchant **130**. When a purchase is to be consummated, user **110** accesses wallet server **140**. User **110** is then directed by wallet server **140** to insert a Smart Card into a Smart Card reader of the system to verify that a Smart Card is in the user's **110** possession. At the same time, a graphical representation of a digital wallet included within wallet server **140** appears to the user **110** and user **110** is directed to select a transaction authorization entity, such as American Express (AMEX). The Smart Card preferably includes a digital certificate that uniquely identifies the card such that digital credentials relating to the transaction may be created as described hereinafter. Upon receipt of the Smart Card information, wallet server **140** communicates with virtual POS gateway **190**. Virtual POS gateway **190** queries payment authorization gateway **180** to obtain authorization for the payment. Upon obtaining such authorization, virtual POS gateway **190** transmits the information to wallet server **140**. Wallet server **140** then completes an authorization form and transmits the form to merchant server **130**.

[0034] Upon receipt of the authorization form, merchant server via modem **150** communicates with third party processor **160**, which in turn communicates with virtual POS gateway **190**, again querying payment authorization gateway **180**. Again, virtual POS gateway **190** communicates through third party processor **160** via modem **150** to merchant server **130**, authenticating the completed form. Once completed, merchant server **130** authorizes the transaction and the transaction is completed, and the user **110** is notified.

[0035] Referring also to FIG. **2**, the flowchart shows an exemplary sequence of events involved in the on-line virtual transaction. As shown at step (**210**), a virtual transaction purchase by a customer is begun on-line, with a customer communicating with a vendor. At the completion of shopping, the customer or user **110** initiates a secure checkout procedure as shown in step (**220**), opening the wallet and interfacing a Smart Card with the wallet server **140**, including selecting the credit supplier. The wallet server **140** interfaces at step (**220**) with a security server to authenticate the transaction. In step (**240**), the wallet server **140** receives transactional authentication, completes an authorization form for the transaction and transmits the form to the merchant server **130**.

In step (**250**), the merchant server queries the security server for credit supplier authentication of the authorization form. Based on the information supplied by the credit supplier, and in conjunction with the authentication above discussed in the previous steps, the credit supplier authenticates the authorization form based on the information from the Smart Card provided through the wallet server and transmits an authentication to the merchant server **130**. Upon receipt of the authorization form, the merchant completes the virtual transaction/purchase, informing the customer and debiting the customer's account.

[0036] Because the Smart Card as above-described contains identifying information that is unique to a particular card, the purchase transaction conducted with the Smart Card is more secure than a transaction conducted with an ordinary charge or credit card. Accordingly, a discount rate may be justified for the secure transaction, which may be processed by the card issuer as a "card present" transaction. Additionally, if the transaction is a "card present" transaction, risk of fraud may be transferred from the merchant to the card issuer.

[0037] Thus, the present invention is directed to a system and method for permitting the authentication of a virtual on-line transaction where a user, by the use of a Smart Card and a wallet server, may have on-line virtual transactions authenticated to a merchant using various Smart Cards and credit providers while minimizing changes to the merchant's server to accommodate a number of different types of systems.

[0038] Accordingly, corresponding structures, acts, and equivalents of all elements in the claims below are intended to include any structural material or acts for performing the functions in combination with other elements as specifically claimed. The scope of the invention should be determined by the allowed claims and their legal equivalents, rather than by the examples given above.

   1. A method comprising:

   receiving, at a wallet server for authorizing a transaction between a merchant and a user using a transaction account, a payment authorization request, wherein said payment authorization request is associated with said transaction, and wherein said payment authorization request includes first transaction account information;

   receiving, by said wallet server, said second transaction account information including a digital certificate uniquely identifying said transaction account;

   sending, by said wallet server, an authentication request for said transaction to a security server of a financial institution, wherein said authentication request includes said second transaction account information;

   receiving, by said wallet server, an authentication for said transaction from said security server;

   completing, by said wallet server, an authorization form for said transaction; and

   transmitting, by said wallet server, said authorization form to a merchant server, wherein said merchant server is associated with said merchant,

   wherein said merchant server requests authorization of said authorization form from said security server,

   wherein said security server authenticates said authorization form using said second transaction account information,

   wherein said merchant server receives an authorization request authentication from said security server, and

5

wherein said merchant server completes said transaction and receives value from an account of said user.

2. The method of claim 1, wherein said request includes purchase information, charge information and transaction account identifying information.

3. The method of claim 1, wherein said wallet server further comprises a digital wallet server.

4. The method of claim 1, wherein said account reader system is a smart card reader system.

5. The method of claim 1, wherein said wallet server comprises a hardware server.

6. The method of claim 1, wherein said payment authorization request further includes a selection of a financial institution.

7. The method of claim 1, wherein said payment authorization request is received via a network.

8. The method of claim 1, further comprising prompting, by said wallet server, said user to initiate an interface between an account reader system and a transaction account device.

9. The method of claim 8, wherein said account reader system reads said transaction account to acquire said second transaction account information and sends said second transaction account information to said wallet server.

10. A system comprising:

a tangible, non-transitory memory communicating with a wallet server,

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

receiving, at a wallet server for authorizing a transaction between a merchant and a user using a transaction account, a payment authorization request, wherein said payment authorization request is associated with said transaction, and wherein said payment authorization request includes first transaction account information;

receiving, by said wallet server, said second transaction account information including a digital certificate uniquely identifying said transaction account;

sending, by said wallet server, an authentication request for said transaction to a security server of a financial institution, wherein said authentication request includes said second transaction account information;

receiving, by said wallet server, an authentication for said transaction from said security server;

completing, by said wallet server, an authorization form for said transaction; and

transmitting, by said wallet server, said authorization form to a merchant server, wherein said merchant server is associated with said merchant,

wherein said merchant server requests authorization of said authorization form from said security server,

wherein said security server authenticates said authorization form using said second transaction account information,

wherein said merchant server receives an authorization request authentication from said security server, and

wherein said merchant server completes said transaction and receives value from an account of said user.

11. A non-transitory tangible computer-readable medium having computer-executable instructions stored thereon that, if executed by at least one of a wallet server, a card reader system, a merchant server, or a security server, cause at least one of said wallet server, said card reader system, said merchant server, or said security server to perform operations comprising:

receiving, at a wallet server for authorizing a transaction between a merchant and a user using a transaction account, a payment authorization request, wherein said payment authorization request is associated with said transaction, and wherein said payment authorization request includes first transaction account information;

receiving, by said wallet server, said second transaction account information including a digital certificate uniquely identifying said transaction account;

sending, by said wallet server, an authentication request for said transaction to a security server of a financial institution, wherein said authentication request includes said second transaction account information;

receiving, by said wallet server, an authentication for said transaction from said security server;

completing, by said wallet server, an authorization form for said transaction; and

transmitting, by said wallet server, said authorization form to a merchant server, wherein said merchant server is associated with said merchant,

wherein said merchant server requests authorization of said authorization form from said security server,

wherein said security server authenticates said authorization form using said second transaction account information,

wherein said merchant server receives an authorization request authentication from said security server, and

wherein said merchant server completes said transaction and receives value from an account of said user.

* * * * *