(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 September 2011 (01.09.2011)

PCT

(10) International Publication Number
WO 2011/106404 A2

(51) International Patent Classification:
G06Q 20/00 (2006.01)

(21) International Application Number:
PCT/US2011/025899

(22) International Filing Date:
23 February 2011 (23.02.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/308,258 25 February 2010 (25.02.2010) US

(71) Applicant *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, M1-12SE, San Francisco, California 94128-8999 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MAKHOTIN, Oleg** [CA/CA]; 52 Woodlawn Ave., Mississauga, Ontario L5G 3K6 (CA).

(74) Agents: **BRITT, Juliene, P.** et al.; Kilpatrick Townsend and Stockton LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) Title: MULTIFACTOR AUTHENTICATION USING A DIRECTORY SERVER

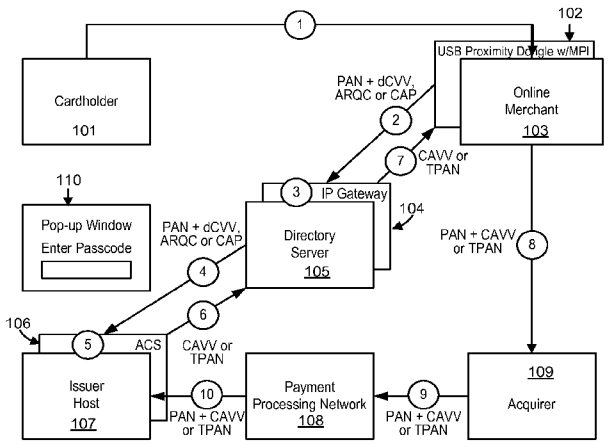

FIG. 1

(57) Abstract: A method and a server computer are provided for authenticating a cardholder account. The server computer implements the method, which includes obtaining a first identifier and a cryptogram from a first entity, identifying an issuer associated with the cardholder account, forwarding the first account identifier and the cryptogram to a second entity for validation, receiving a second identifier from the second entity, and sending the second identifier to the first entity. The first identifier can be associated with the cardholder account. The second identifier can be generated by the second entity and associated with a validated form of the first identifier.

WO 2011/106404 A2

MULTIFACTOR AUTHENTICATION USING A DIRECTORY SERVER

[0001] The present application is a non-provisional of and claims benefit under 35 U.S.C. § 119(e) of U.S. Provisional Patent Application No. 61/308,258, entitled "MultiFactor Authentication Using Directory Server", filed February 25, 2010, which is hereby incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Online transactions have increased in recent years as the use of the Internet has become common. Due to the abundance of hackers, many methods have been implemented to ensure a secure transaction. Some of these methods included requiring additional information about the cardholder (i.e., address, zip code, phone number), while recent methods require the additional entry of a card verification value (CVV). Such methods provide some security to cardholders, especially when preventing fraudulent charges by persons not in possession of the physical portable consumer device.

[0003] Additional security methods can also be performed unbeknownst to the user of the portable consumer device. Such methods may include protocols such as Visa's 3D Secure implemented in the Verified by Visa (VBV) service. The 3-D Secure method allows for the additional verification of the portable consumer device and the user of the device by prompting the user to enter password/code during a transaction. For example, when completing a transaction on a merchant website, an additional window can pop up and require entry of the password. This password is only known by the user and the issuer. The additional prompt and verification can be controlled by third parties.

[0004] However, some fraudsters are still able to obtain this information through phishing, especially when multiple third parties are controlling the communication between the merchant, user, and issuer during verification of the user and authorization of the transaction.

[0005] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0006] One embodiment provides a method for authenticating a cardholder account. The method includes obtaining a first identifier and a cryptogram from a first entity, identifying an issuer associated with the cardholder account, forwarding the first account identifier and the cryptogram to a second entity for validation, receiving a second identifier from the second entity, and sending the second identifier to the first entity. The first identifier can be associated with the cardholder account. The second identifier can be generated by the second entity and associated with a validated form of the first identifier.

[0007] The method can be performed on a directory server computer. The first identifier can include a primary account number (PAN) and/or any one or more of an electronic mail address, a telephone number, a card authentication program (CAP) token, a dynamic passcode authentication (DPA) token, or a one time passcode (OTP) cryptogram.

[0008] The method further can further include consulting a lookup table to retrieve a primary account number (PAN) associated with the first identifier. The first entity can be an access device. The access device can be coupled to a reader that reads the first identifier from a portable consumer device. The reader can include a merchant plug in (MPI). The second entity can be an access control server computer associated with the issuer.

[0009] The method can further include entering a third identifier associated with the portable consumer device. The third identifier can be received by the issuer in order to continue validation of the cardholder account. The second identifier can be any one of a temporary primary account number (TPAN) or cardholder authentication verification value (CAVV). The merchant plug in (MPI) can communicate with the reader to populate browser fields in a browser on the access device with a primary account number (PAN) and the card authentication verification value (CAVV) or the temporary primary account number (TPAN).

[0010] The method can further include sending the primary account number (PAN) and the card authentication verification value (CAVV) or the temporary primary account number (TPAN) to an acquirer. The acquirer can forward the

primary account number and the card authentication verification value (CAVV) to the issuer via a payment processing network for authorization of a transaction.

[0011] Another embodiment provides a server computer for use in an authenticated transaction. The server computer includes a processor and a computer readable medium coupled to the processor. The computer readable medium can include code which is executable by the processor to implement a method. The method can include receiving a first identifier and a cryptogram from an access device, identifying an issuer associated with the first identifier, sending the first identifier and the cryptogram to the issuer for validation, receiving a second identifier from the issuer, and providing the second identifier to the access device. The second identifier can be associated with a validated form of the first identifier. The access device can communicate the second identifier to a merchant to complete the authenticated transaction.

[0012] The access device can be coupled to a reader and can receive the first identifier and cryptogram from a portable consumer device through any one of a contact interface or a contactless interface. The reader can be a universal serial bus dongle capable of interfacing with a portable consumer device. The reader can further include a software module with a merchant plug in.

[0013] The server computer can further include a database having information used to identify an issuer associated with the first identifier. The first identifier can be a primary account number.

[0014] Yet another embodiment provides a computer readable medium having code executable by a processor for implementing a method. The method includes obtaining a first identifier and a cryptogram from a first entity, identifying an issuer associated with the cardholder account, forwarding the first account identifier and the cryptogram to a second entity for validation, receiving a second identifier from the second entity, and sending the second identifier to the first entity. The first identifier can be associated with the cardholder account. The second identifier can be generated by the second entity and associated with a validated form of the first identifier.

[0015] A further embodiment provides a method for authenticating a transaction on an access device. The method includes accessing a merchant

website, initiating a transaction on the merchant website, interfacing the access device with a reader, forwarding a first identifier and a cryptogram to a directory server through a merchant plug in, receiving a second identifier through the MPI, and communicating the second identifier to the reader from the MPI. The merchant can send a request for payment during the transaction. The reader can capture the first identifier stored on a portable consumer device and the cryptogram in response to the request for payment. The directory server can communicate the first identifier and the cryptogram to an issuer of the portable consumer device for validation. The second identifier can be associated with the validated first identifier.

[0016] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIG. 1 shows a transaction flow for authenticating a transaction in one embodiment.

[0018] FIG. 2 shows a system for implementing the transaction flow of FIG. 1.

[0019] FIG. 3 shows a flowchart of a method for authenticating a transaction on an access device.

[0020] FIG. 4 shows a flowchart of a method for authenticating a transaction on a directory server .

[0021] FIG. 5 shows a block diagram of an access device.

[0022] FIG. 6 shows a block diagram of a computer apparatus.

[0023] FIG. 7 shows a block diagram of a reader.

[0024] FIG. 8 shows a portable consumer device.

DETAILED DESCRIPTION

[0025] Systems and methods for providing multiple levels of authentication during an online transaction are disclosed. Using an access device, a user visits a merchant website that implements a merchant plug in (MPI) and completes a checkout process to make a purchase. At checkout, the user is prompted to wave his portable consumer device (e.g., a payment card) by a reader, coupled to an

access device (e.g., a portable computer, a phone, etc.). The reader reads information in the portable consumer device, which includes a cryptogram, and other information (e.g., a first identifier) such as an account number, expiration date, and a service code. The cryptogram can be generated by the portable consumer device. The captured portable consumer device information and cryptogram are forwarded from a first entity (i.e., an access device) to a directory server through the MPI. The directory server identifies a second entity (e.g., issuer)associated with the portable consumer device and forwards the portable consumer device information to the second entity. The second entity validates the portable consumer device information and the cryptogram. In addition, the second entity may require another form of validation, such as a passcode, from the user of the portable consumer device.

[0026] After validation, the second entity generates a temporary identifier (e.g., a second identifier) corresponding to the validated portable consumer device information. This temporary identifier is sent to the directory server, which securely forwards the temporary identifier to the MPI. The MPI communicates the temporary identifier to the access device. The access device then provides the information associated with the temporary identifier and the temporary identifier to the merchant at the online checkout.

[0027] A usual transaction flow then commences: the merchant sends the transaction information including the temporary identifier to an acquirer, the acquirer submits the transaction information to a payment processing server, the payment processing server in a payment processing network determines the issuer associated with the portable consumer device and forwards the transaction information to the issuer. Finally, the issuer validates the transaction information, including the temporary identifier, and authorizes the transaction if the transaction is to be authorized (e.g., there is sufficient credit or funds to conduct the transaction).

[0028] An enhancement from offering the aforementioned multifactor authentication is that a user can use an alias, or first identifier, such as an electronic mail (email) address, telephone number, username, or a similar type of known user information, to access their primary account number (PAN). Accordingly, the user does not need to remember their full PAN or other card information in order to use the card during a transaction, but can still be assured the same level of security

during an online transactions. Accordingly, this can improve cardholder experience during live online transactions.

[0029] A second enhancement of the multifactor authentication is the cryptogram, which offers added security during on online transaction. For each transaction, a unique cryptogram is generated. The cryptogram can be generated on the portable consumer device or, alternatively, on the access device. Accordingly, if the portable consumer device information, the first identifier of the user, or any other information regarding the account is remotely stolen during an online transaction, a fraudster is unable to complete any future transaction if the card is not present. In another embodiment, the cryptogram can be passed through the network by special access device, such as a chip reader to the user's computer, or can manually be entered if no access device is available to the user.

[0030] The multi-factor authentication system can be implemented on a known platform, such as Visa's 3-D Secure platform, allowing the embodiments the system to be more acceptable to users. Additionally, utilizing the multifactor authentication system not only allows for added protection against counterfeit and lost/stolen online fraud, but also shifts liability of possible fraud to the issuers and away from the merchants both in face-to-face transactions and in on-line transactions. This is because the same validation mechanisms (dCVV, ARQC or CAP/DPA validation) can be implemented in both face-to-face and online environments.

[0031] Exemplary systems and methods using this process for authenticating an online transaction are provided below.

[0032] **I. Exemplary Systems**

[0033] A system according to an embodiment of the invention is shown in FIGS. 1-2.

[0034] FIG. 1 illustrates a transaction flow in a system for authenticating a transaction. The transaction flow includes steps 1-10 which show the steps of authentication during an online transaction. As described within embodiments below, Visa's 3-D Secure technology is implemented in conjunction with the present invention. However, it should be understood that the present invention can be implemented in other transactional security systems that do not utilize Visa's 3-D Secure technology.

[0035] In step (1), a user, can browse an online merchant website and can purchase a good or service. A proximity reader, such as a contact chip USB dongle (e.g., a payWave or other card reader able to capture a dCVV or ARQC or a CAP/DPA token cryptogram), is interfaced with an access device, such as a client computer or a cardholder's personal computer (PC) or handheld computer (e.g., SmartPhone). The user can then install software on the reader or on the access device with a merchant plug in (MPI). The MPI allows the user to securely connect to an IP gateway (e.g. using session keys) with his/her access device.

[0036] In step (2), when initiating a transaction (i.e., completing a purchase through check-out), the cardholder is prompted to wave their portable consumer device, or payment card (e.g., a Visa payWave card or other type of portable consumer device such as a phone, key fob, etc.) across the proximity reader, (e.g., USB payWave or EMV chip reader), which captures the PAN and a cryptogram (dCVV or ARQC or CAP/DPA token) from the card. The MPI receives the portable consumer device information and the cryptogram through the reader, the MPI then communicates the information to an internet protocol (IP) Gateway 104. As discussed previously, the Visa 3DS protocol can be utilized to perform this secure communication.

[0037] The cryptogram can be a dynamic card verification value (dCVV), application request cryptogram (ARQC), card authentication program (CAP) token or dynamic passcode authentication (DPA) token or a similar type of cryptographic data. The cryptogram may be generated on the card each time a transaction occurs. In some embodiments, the user may need to enter the card's personal identification number (PIN) in order to generate the cryptogram. Alternatively, the cryptogram may be generated by the access device and passed to the MPI, or manually entered by the user during each transaction. If the cryptogram is manually entered, it can be generated by a secondary device, such as a DPA reader or one time passcode (OTP) generator. A OTP generator is a device able to generate one time passcodes that are synchronized with the issuer host values.

[0038] In step (3), the IP Gateway communicates the first identifier and cryptogram (e.g., PAN, dCVV/ARQC/CAP token and other data) to the directory server.

[0039] In step (4), the portable consumer device information, including the primary account number and cryptogram, is utilized by the directory server to identify an issuing entity (host). This can be done through referencing a database coupled to the directory server. When the issuer host is identified, the directory server 105 forwards the portable consumer device information to the ACS 106 associated with the issuer 107.

[0040] In step (5), the ACS then communicates the portable consumer device information (e.g., the cryptogram (dCVV or ARQC or CAP) and other required data) to the issuer host for validation through the personal account number (PAN) and cryptogram generated by the portable consumer device during the transaction. This is a first factor of authentication.

[0041] A pop-up window 110 can be also generated by the issuer host 107and made visible to the user through the web browser of the access device on which the user is performing an online transaction. This is a second factor of authentication. If the passcode is incorrect, the user's online transaction session can timeout and the transaction can be terminated. If the user enters a correct passcode, the issuer can continue the validation process.

[0042] In step (6), during the validation process, the issuer host can generate a second identifier associated with the portable consumer device. The second identifier can include a temporary personal account number or CAVV or other type of data which is both dynamic and unique for each transaction and can be used to the complete the transaction. In this way, the user's actual personal account number associated with the portable consumer device never needs to be entered to complete the online transaction. Once the second identifier is generated, it is sent to the directory server from the issuer host 107 through the ACS 106. The second identifier is associated with the validated payment information of the portable consumer device.

[0043] In step (7) , the directory server forwards the second identifier (e.g., CAVV or TPAN) via the Visa IP Gateway or other secure IP Gateway, to the MPI. When the MPI receives the second identifier, the MPI can communicate this information to the reader. The reader can include software which is then used to populate the web browser fields provided to the user during checkout, such as a self form-complete function. The fields may include user information, such as billing and

shipping information as well as payment information. Once the merchant required information is completed, the user can complete checkout.

[0044] In step (8), the user's payment information is then submitted to the merchant, who forwards the information (e.g., PAN with CAVV or TPAN) to an acquirer for processing and authorization of the transaction. The payment information may include both the user's personal account number and the second identifier, though the second identifier is the only number visible to the user in the populated fields of the browser. In another embodiment, the second identifier may not even be visible to the user although the information is provided to the merchant in order to authorize the transaction.

[0045] In step (9) of FIG. 1, the payment information and any other information associated with the transaction is The acquirer submits the transaction to a payment processing network (e.g., VisaNet). In alternative embodiments, the payment processing network is not used and information is sent directly to the issuer 107 by the acquirer 109. In still another embodiment, the acquirer is not utilized and the merchant directly forward the PAN and CAVV or TPAN directly to the payment processing network. The payment information can be sent through a network 108, such as the Internet, via a hard-wired or wireless connection. The network may be a wireless local area network (WLAN), local area network (LAN) or cellular network such as EV-DO, 3G, 4G or other network known in the art which can securely communicate data between two entities.

[0046] In step (10) of FIG. 1, the issuer receives the authorization request from the acquirer 109 through a network 108. The issuer can authorize the transaction by validating the previously generated second identifier (i.e., the issuer validates the CAVV or TPAN generated at step (6)). If the second identifier matches the previously created second identifier by the issuer, the transaction is validated and an authorization response is sent the acquirer. If the second identifier does not match the second identifier which the issuer has previously generated, the transaction is denied.

[0047] Referring now to FIG. 2, an exemplary embodiment is illustrated of a system which can be used to implement the transaction flow of FIG. 1. As previously discussed, a user 101 can be shopping on a merchant website on an access device 111in communication with the world wide web (WWW).

[0048] The "merchant" 103 is typically an entity that engages in transactions and can sell goods or services. The user 101 is the owner of an account associated with a portable consumer device. A user can also be referred to as cardholder, account holder, or similar term. The access device 111 can be a laptop computer, personal computer or cellular telephone, such as a Smartphone, PDA, or a similar type of device having internet capabilities via a wired or wireless connection. The access device 111 can additionally be coupled with a reader 112, such as a card reader, through an interface. The interface can be a wired interface (shown), such as a universal serial bus (USB) connection, or a wireless interface, such as WiFi, WLAN or Bluetooth. In some embodiments, the reader may be incorporated into the access device.

[0049] The reader 112 can be in the form of a USB dongle 102, or other module which can be coupled to an access device 111. The reader can be coupled to the access device via wired or wireless connection. The reader can include merchant plug in (MPI) software, which offers compatibility with the online merchant who also implements the MPI software functionality. The MPI essentially opens a gateway which allows for direct communication between the reader, access device, user and a directory server, such as Visa Directory Server (VDS) over the network.

[0050] When the user 101 proceeds to “checkout” to purchase an item on a merchant website, the user 101 can couple a portable consumer device to the reader 112. A portable consumer device can be a credit card, debit card, gift card, gift certificate or any other similar physical portable consumer device that has an associated value and is associated with the user. The portable consumer device can come in contact with the reader 112, or wirelessly communicate payment information to the reader 112. In some embodiments, the user can enter the portable consumer device information to the MPI manually through an interface such as a keyboard on the access device. The portable consumer device, reader, or another third party source in communication with the user’s access device 111, can generate a cryptogram associated with the portable consumer device and the immediate transaction. In one embodiment, the cryptogram is generated by the reader. This cryptogram can also be communicated through the reader 112 interface or through manual entry through the keyboard interface on the access device 111.

[0051] Information associated with the portable consumer device, including the cryptogram is collected and forwarded to a directory server from the access

device11 through an merchant plug in (MPI). The directory server 105 can communicate through a secure network with the reader 112 coupled to the access device 112 on which the user is initiating the online purchase. The directory server 105 can be a third party server, such as an acquirer 109, a server associated with the issuer 107 of the portable consumer device, or a server associated with the payment processor, such as VISA.

[0052] In one embodiment, the directory server 105 can be part of a payment, or transaction, processing network. The processing network can include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the transaction processing network may comprise a server computer, coupled to a network interface, and a database of information. An exemplary transaction processing network may include VisaNet™. Transaction processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0053] As noted above, the transaction processing network may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The transaction processing network may use any suitable wired or wireless network, including the Internet.

[0054] In one embodiment in which the directory server 105 is associated with the payment processor and/or acquirer, a database 107 can be coupled to the server 105 in order to retrieve information associated with the portable consumer device. For instance, payment information collected from the portable consumer device can include a primary account number (PAN), which can be a 16 digit account number associated with a bank account with an issuer. In alternative embodiments, the payment information can include a first identifier, which is associated with the PAN, such as a temporary PAN, email address, phone number, etc. The PAN, or first identifier, can be used to determine the issuer of the portable consumer device

through database including of information associated with the portable consumer device. When the issuer of the portable consumer device is known, the directory server can communicate the initial purchase notification and portable consumer device information to the issuer. This communication can also be done through a network, such as the WWW or through a cellular network.

[0055] An "issuer" 107 is typically a business entity (e.g., a bank) which maintains financial accounts for the user 101 and often issues a portable consumer device such as a credit or debit card to the user.

[0056] The issuer 107 can communicate with an access control server (ACS) computer (not shown) coupled to an issuer host. The ACS can receive the payment information, check the information with the associated account of the issuer host, and perform any additional security steps to authenticate the user of the portable consumer device. When the validations step is complete, the issuer host can generate a temporary identifier, also referred to as the second identifier, and send this second identifier to the directory server. The temporary identifier can be a 16 digit number, similar to a PAN or another identifier, which is linked to the authenticated user account. The directory server 105 forwards the second identifier back to the user's access device 111. The access device 111 communicates the second identifier and other associated payment information (e.g., name, billing address, email, etc.) to the online merchant 103 through the MPI.

[0057] After receiving the second identifier and performing an initial validation of the payment information through authentication, the user can complete a purchase on the merchant website. The transaction is completed similar to that in a merchant location. The payment information is sent to an acquirer, who communicates an authorization request to a payment processing network, such as VisaNet™. In the embodiment shown in FIG. 2, the directory server 105 is part of the processing network. The processing network then communicates the transaction information and authorization request to the issuer of the portable consumer device for authorization. The authorization response from the issuer is communicated through VisaNet™ to the acquirer. The acquirer then provides the response to the merchant. In one embodiment, the acquirer is not utilized and the processing network associated with the directory server, as shown in FIG. 2, functions as the acquirer. In another embodiment, the directory server and associate payment processing network can perform all the validation and authorization steps during a

transaction, such as user authentication and transaction authorization (e.g., through direct communication with the issuer). In this manner, less communication is necessary over the network, which can reduce chances of the fraudsters intercepting payment information during an online transaction.

[0058] **II. Exemplary Methods**

[0059] Methods according to embodiments of the invention are described with reference to FIGS. 3-4.

[0060] Referring to FIG. 3, a flowchart provides a method for completing a multifactor authenticated online transaction on an access device is described.

[0061] At stage 301, a user (e.g., a cardholder) communicates with an online merchant through an access device, such as a home computer. When the user begins to checkout and initializes a final purchase (i.e., a transaction) at stage 302, the merchant communicates a request to the user to enter payment information. The request can ask for manual entry through the access device or through a reader which is coupled to the access device, such as a card reader.

[0062] After the user initializes a purchase at stage 302, the user is prompted to provide their payment information. The user can bring a portable consumer device within proximity to the access device in order to transmit the information to the access device. For instance, a user may make contact with the reader, such as inserting the portable consumer device into the reader (e.g., Magstripe card), tapping the portable consumer device on the reader (e.g., chip card), or waving the card near the reader (e.g., contactless chip card).

[0063] At stage 303, the reader captures the account information and cryptogram stored on the portable consumer device. The account information and the cryptogram are then sent to the access device through a wired or wireless interface. The access device enters the information and cryptogram into the MPI. Again, the MPI can be stored on the computer readable medium of the access device or on the reader itself. The MPI can be run when the user enters the merchant website or by use of the reader or access device.

[0064] At stage 304, once the MPI obtains the portable consumer device information and the cryptogram from the reader, the MPI then communicates the information to the directory server. The MPI and the directory server can

communicate through a network on a secure platform, such as through Visa's 3-D Secure protocol. The access device then waits, while the first identifier and the cryptogram are validated.

[0065] At stage 305, if the first identifier is validated by an issuer, a second identifier associated with the validated first identifier is received from the directory server by the access device. The second identifier is received through the MPI, which provides the secure communication between the access device and the directory server.

[0066] At stage 306, the MPI communicates the second identifier to the reader, which can include software used to populate the fields on the checkout page of the merchant website with the second identifier and other information needed in a transaction, such as the user's name, phone number, billing address, shipping, etc. where authorization is completed through. The transaction is then processed similar to a regular online transaction through communication between the merchant, an acquirer, a payment processing network and the issuer. However, during issuer authorization, the second identifier is compared with the second identifier provided by the issuer. If the two identifiers match, the transaction is approved. If they do not match, the transaction is denied. Accordingly, there is multi-factor authentication performed at various stages of the transaction, ensuring a secure online transaction to the user.

[0067] Referring now to FIG. 4, a method for completing an authenticated transaction on a directory server is described.

[0068] At stage 401, the directory server receives data from an MPI running on an access device of a user. The MPI forms a direct communication path between the access device and the directory server over a network. The data can include data associated with an financial account of a user, such as a primary account number or other first identifier that is associated with the user's account. Additionally, the data can include a cryptogram.

[0069] At stage 402, the directory server consults a database to determine which issuer is associated with the portable consumer device. In the case where the payment information does not include the original PAN of the portable consumer device, instead including an alias, the directory server can include a lookup table. For example, if the user manually enters a PAN alias (e.g., a first identifier), such as

an email or telephone number and the cryptogram, the lookup table can include the PAN and other associated card data, such as the expiration, etc., associated with that alias.

[0070] At stage 403, the directory server forwards the portable consumer device information to the issuer of the portable consumer device through an access control server (ACS) associated with the issuer. The information can include all information originally captured from the portable consumer device on the reader and, alternatively, additional information gathered from the directory server database during the issuer lookup.

[0071] Also at stage 403, a second form of authentication can also be implemented by the issuer such as a request for a passcode, (e.g., a personal identification number (PIN) associated with the portable consumer device. The passcode can be known only by the user and the issuer. As previously described, the user can be prompted to enter this information through a pop-up window on the user's web browser or other graphical user interface (GUI) which is communicated by the issuer to the user. The correct entry of a passcode by the user can cause the transaction authentication to continue and the incorrect entry can cause the transaction to be aborted.

[0072] At stage 404, the directory server receives a second identifier from the issuer host through the ACS. The second identifier is generated at the issuer host computer in order to provide an additional layer of security during the online transaction. The second identifier is associated with the authenticated user account and can be utilized to complete the transaction in order to avoid the direct communication of the user's PAN or account number to the merchant. The second identifier can also include additional security parameters, such as time limits for use, embedded cryptograms or other information.

[0073] At stage 405, the directory server forwards the second identifier to the MPI through a secure IP Gateway.

[0074] In one embodiment, the directory server, such as Visa Directory Server (VDS) can function in place of the issuer and provide the first stages (405-408) of validation of payment information. In this capacity, the issuer does not have to generate the second identifier or exchange keys with the directory server, which allow for less communication over the network and an environment less susceptible

to fraud. The directory server may then forward the second identifier to the issuer for use during the final authorization of the transaction. In another embodiment, the VDS can communicate with the issuer during the authorization of the transaction to validate the second identifier so that the issuer is not responsible to maintain the second identifier or perform the validation of the identifier during authorization.

[0075] In whichever embodiment the method of FIG.4 is implemented, two factors of authentication are required: 1) a passcode/PIN, and 2) a cryptogram. Whether both are implemented by the issuer, the payment processor (e.g., Visa), or another third party, the user and portable consumer device are dually authenticated prior to completing an online transaction. By requiring these forms of authentication, a minimal amount of the user's personal information is necessary in an e-commerce environment. This ensures a more secure online transaction over a network, and provides a similar level of authentication as performing a transaction at a merchant location.

[0076] III. Exemplary Portable Devices, Access Devices, and Computer Apparatuses

[0077] Exemplary devices used in the aforementioned systems and methods are described with reference to FIGS. 5-8.

[0078] Referring now to FIG. 5, a block diagram of an access device 50, is illustrated according to an embodiment of the invention. The term access device can be utilized interchangeably with terminal, point of sale (POS) device or terminal, The access device 50 comprises a processor 50(c) operatively coupled to a computer readable medium (CRM) 50(d) (e.g., one or more memory chips, etc.), input elements 50(b) such as buttons or the like, an output device 50(e) (e.g., a display, a speaker, etc.) and one or more interfaces 50(f). In one embodiment, the access device 50 includes only a reader, processor, CRM and interface. A housing can house one or more of these components. The computer readable medium 50(d) can comprise instructions or code, executable by a processor. The CRM may additionally store the MPI software capable of communicating card information through the network to the directory server and the merchant. The one or more interfaces 50(f) can be a wired or wireless interfaces capable of communication with the reader. In another embodiment, interface 50(f) can be a network interface for direct communication with an acquirer, the directory server, the merchant, or issuer.

[0079] Referring now to FIG. 6 the various participants and elements (e.g., the issuer, the directory server, payment processing network, the IP Gateway, the merchant, the acquirer, and the user computer) in FIGS. 1, 2, can operate one or more computer apparatuses (e.g., a server computer) to facilitate the functions described herein. Any of the elements in FIGS. 1, 2 can use any suitable number of subsystems to facilitate the functions described herein. Examples of such subsystems or components are shown in FIG. 6. The subsystems shown in FIG. 6 are interconnected via a system bus 60. Additional subsystems such as a printer 64, keyboard 68, fixed disk 69 (or other memory comprising computer readable media), monitor 71, which is coupled to display adapter 66, and others are shown. Peripherals and input/output (I/O) devices, which coupled to I/O controller 61, can be connected to the computer system by any number of means known in the art, such as serial port 67. For example, serial port 67 or external interface 70 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 63 to communicate with each subsystem and to control the execution of instructions from system memory 62 or the fixed disk 69, as well as the exchange of information between subsystems. The system memory 62 and/or the fixed disk 69 can embody a computer readable medium.

[0080] Referring now to FIG. 7, a reader is illustrated in one embodiment. The reader may include an interface 75 (e.g., Universal Serial Bus (USB) connector, wired connection, etc.), input element (chip card reader, Magstripe reader, barcode scanner, etc.) 76, a housing 77, and a computer readable medium (CRM) 78. In one embodiment, the reader is capable of generating a cryptogram each time a portable consumer device is read. In the case of contactless communication with the portable consumer device, the input element 75 can be a transceiver capable of short range, or near field communication (NFC), such as an radio frequency RF transceiver, or an optical scanner. The reader can also be referred to as a card terminal or card reader.

[0081] The portable consumer devices according to embodiments of the invention may be in any suitable form. A payment device may be referred to interchangeably as a consumer device, payment device, portable device, or card. Suitable portable consumer devices may be hand-held and compact so that they fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart

cards, credit or debit cards, or any consumer payment device that has a communication interface, such as a contactless interface, a contact chip interface, cellular communication interface, etc. Accordingly, other examples of portable devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0082] Each portable consumer device may comprise a body, and a memory comprising a computer readable medium disposed on or within the body. The memory may store data, and may be in any suitable form including a memory chip, etc. The memory may be used to store data such as user identification or authentication information, user account information, transaction data, etc. Stored financial information may include information such as bank account information, bank identification number (BIN), credit or debit card account number information, account balance information, expiration date, consumer information such as name, date of birth, etc. Note that such data may additionally or alternatively be stored in a secure data storage element, such as secure data storage or a similar secure memory that is part of a contactless element. As described, the memory may also contain instructions which when executed by processor implement operations or processes that are part of the operation of the device or of applications installed on the device. In addition, the portable consumer device may also include a processor coupled to the memory, where greater functionality and/or security are desired. For example, the portable consumer device may include an application implemented by the processor that generates a cryptogram each time the card is in communication with a reader.

[0083] FIG. 8 shows one embodiment of a portable consumer device that may be used in an embodiment of the invention. The portable consumer device 80 may be in form of a credit, debit, or prepaid card having one or both of a contact interface 80(h) and a contactless interface 80(d). The contact interface 80(h), which may be in the form of a chip plate, allowing the portable consumer device 80 to perform a transaction by having the contact interface come in direct contact with a second contact interface on a reader (or other type of POS terminal or card terminal). In some embodiments, a secondary contact interface 80(a), such as a magnetic stripe can also be located on the portable consumer device 80. Stored card information

80(b) including financial data (e.g., an account number) can be sent from the card 80 to the reader when they are in contact with each other. The contactless interface 80(d) can communicate with the reader using a contactless interface at the reader. An antenna 80(d) coupled to an integrated circuit (IC) chip 80(i) may form at least part of a contactless element, which is used to wirelessly transmit the stored card information to the reader.

[0084] Specific details regarding some of the above-described aspects are provided below. The specific details of the specific aspects may be combined in any suitable manner without departing from the spirit and scope of embodiments of the invention.

[0085] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software

[0086] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0087] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0088] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0089] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A method for authenticating a cardholder account, the method comprising:

obtaining a first identifier and a cryptogram from a first entity, wherein the first identifier is associated with the cardholder account;

identifying an issuer associated with the cardholder account;

forwarding the first account identifier and the cryptogram to a second entity for validation;

receiving a second identifier from the second entity, wherein the second identifier is generated by the second entity and associated with a validated form of the first identifier; and

sending the second identifier to the first entity.

2. The method of claim 1, wherein the method is performed on a directory server computer.

3 The method of claim 1, wherein the first identifier includes a primary account number (PAN).

4. The method of claim 1, wherein the first identifier includes any one or more of an electronic mail address, a telephone number, a card authentication program (CAP) token, a dynamic passcode authentication (DPA) token, or a one time passcode (OTP) cryptogram.

5. The method of claim 1, wherein the method further comprises consulting a lookup table to retrieve a primary account number (PAN) associated with the first identifier.

6. The method of claim 1, wherein the second entity is an access control server computer associated with the issuer.

7. The method of claim 1, wherein the first entity is an access device.

8. The method of claim 7, wherein the access device is coupled to a reader that reads the first identifier from a portable consumer device.

9. The method of claim 8, further comprising:

entering a third identifier associated with the portable consumer device, wherein the third identifier is received by the issuer in order to continue validation of the cardholder account.

10. The method of claim 8, wherein the reader includes a merchant plug in (MPI).

11. The method of claim 10, wherein the second identifier is any one of a temporary primary account number (TPAN) or cardholder authentication verification value (CAVV).

12. The method of claim 11, wherein the merchant plug in (MPI) communicates with the reader to populate browser fields in a browser on the access device with a primary account number (PAN) and the card authentication verification value (CAVV) or the temporary primary account number (TPAN).

13. The method of claim 12, further comprising sending the primary account number (PAN) and the card authentication verification value (CAVV) or the temporary primary account number (TPAN) to an acquirer, wherein the acquirer forwards the primary account number and the card authentication verification value (CAVV) to the issuer via a payment processing network for authorization of a transaction.

14. A server computer for use in an authenticated transaction, the server computer comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor to implement a method comprising:

receiving a first identifier and a cryptogram from an access device;

identifying an issuer associated with the first identifier;

sending the first identifier and the cryptogram to the issuer for validation;

receiving a second identifier from the issuer, wherein the second identifier is associated with a validated form of the first identifier; and

providing the second identifier to the access device, wherein the access device communicates the second identifier to a merchant to complete the authenticated transaction.

15. The server computer of claim 14, wherein the access device is coupled to a reader and receives the first identifier and cryptogram from a portable consumer device through any one of a contact interface or a contactless interface.

16. The server computer of claim 15, wherein the reader is a universal serial bus dongle capable of interfacing with a portable consumer device.

17. The server computer of claim 15, wherein the reader includes a software module with a merchant plug in.

18. The server computer of claim 14, further comprising a database, wherein the database includes information used to identify an issuer associated with the first identifier.

19. The server computer of claim 14, wherein the first identifier is a primary account number.

20. A computer readable medium comprising code executable by a processor, for implementing a method comprising:

obtaining a first identifier and a cryptogram from a first entity, wherein the first identifier is associated with a cardholder account;

identifying a second entity associated with the cardholder account;

forwarding the first identifier and the cryptogram to the second entity for validation;

receiving a second identifier from the second entity, wherein the second identifier is generated at the second entity and associated with a validated form of the first identifier; and

sending the second identifier to the first entity.

21. A method for authenticating a transaction on an access device, the method comprising:

accessing a merchant website;

initiating a transaction on the merchant website, wherein the merchant sends a request for payment during the transaction;

interfacing with a reader, wherein the reader captures a first identifier stored on a portable consumer device and a cryptogram in response to the request for payment;

forwarding the first identifier and the cryptogram to a directory server through a merchant plug in, wherein the directory server communicates the first identifier and the cryptogram to an issuer of the portable consumer device for validation;

receiving a second identifier through the MPI, wherein the second identifier is associated with the validated first identifier; and

communicating the second identifier to the reader from the MPI.

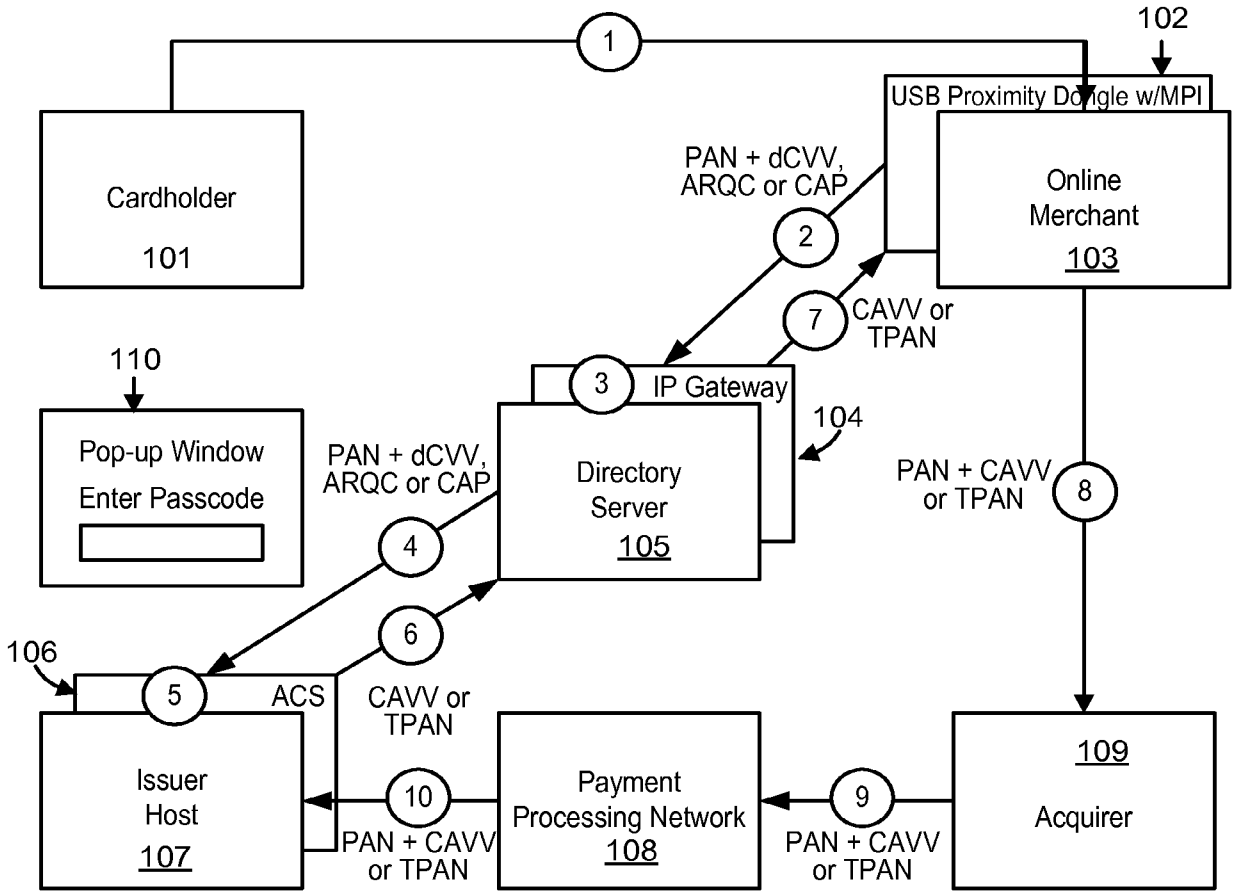
1
102
USB Proximity Dongle w/MPI
Cardholder
101
PAN + dCVV,
ARQC or CAP
2
Online
Merchant
103
7
CAVV or
TPAN
110
3
IP Gateway
104
Pop-up Window
Enter Passcode
PAN + dCVV,
ARQC or CAP
Directory
Server
105
PAN + CAVV
or TPAN
8
4
6
106
5
ACS
CAVV or
TPAN
Issuer
Host
107
10
Payment
Processing Network
108
9
109
Acquirer
PAN + CAVV
or TPAN
PAN + CAVV
or TPAN

FIG. 1

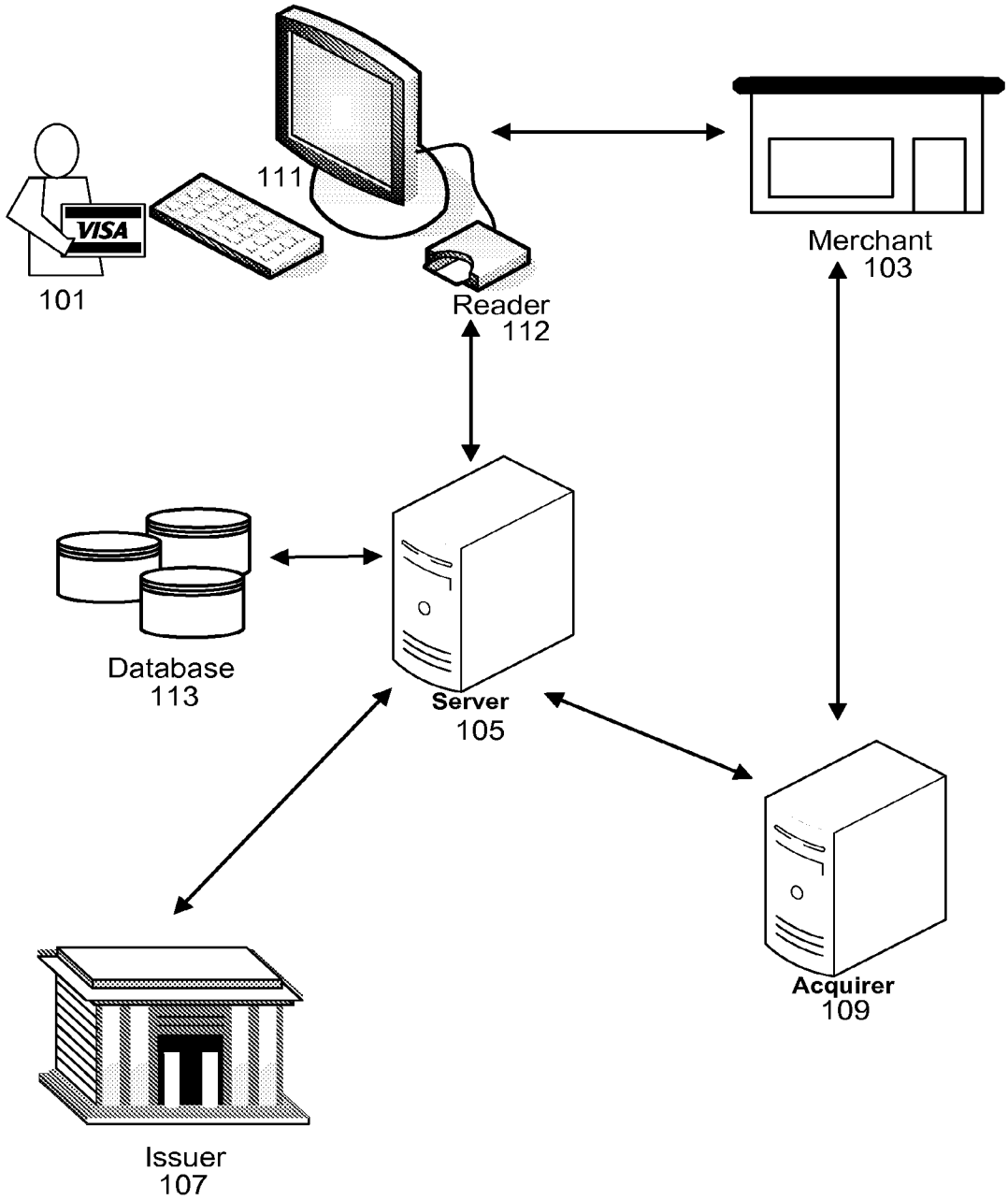
VISA
101
111
Reader
112
Merchant
103
Database
113
Server
105
Acquirer
109
Issuer
107

FIG. 2

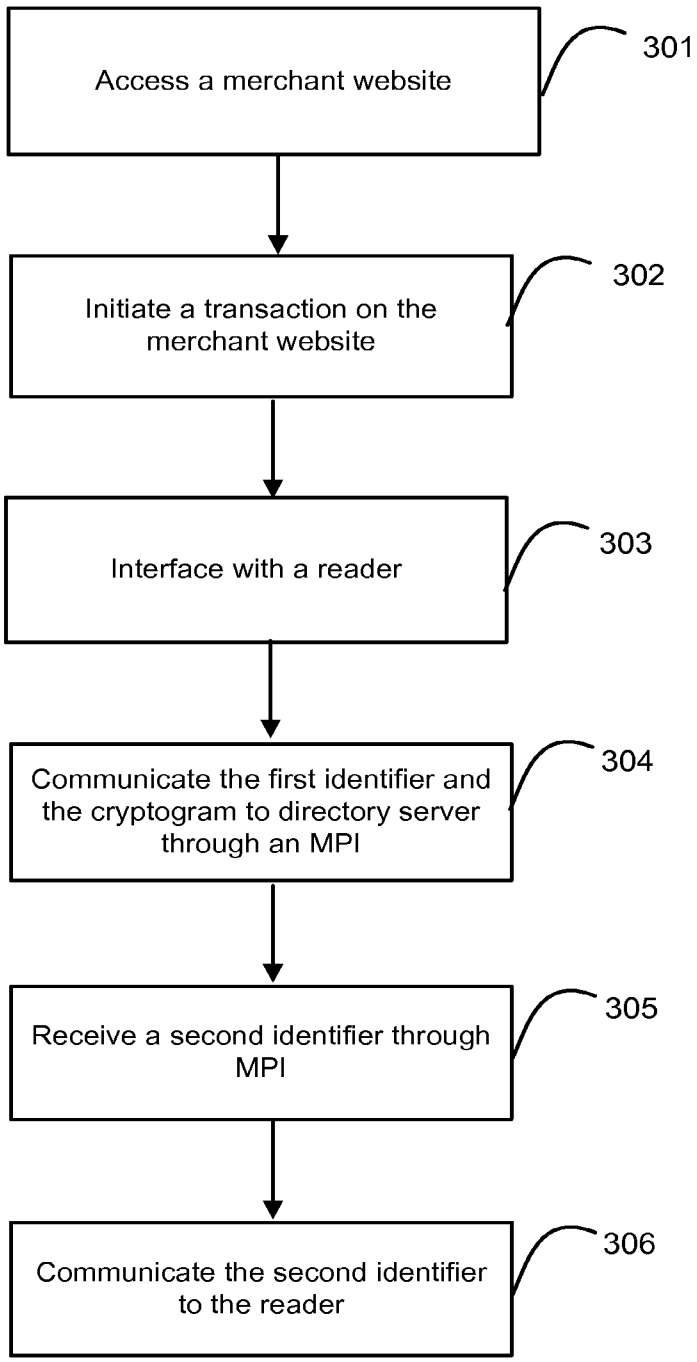
Access a merchant website
301
Initiate a transaction on the merchant website
302
Interface with a reader
303
Communicate the first identifier and the cryptogram to directory server through an MPI
304
Receive a second identifier through MPI
305
Communicate the second identifier to the reader
306

FIG. 3

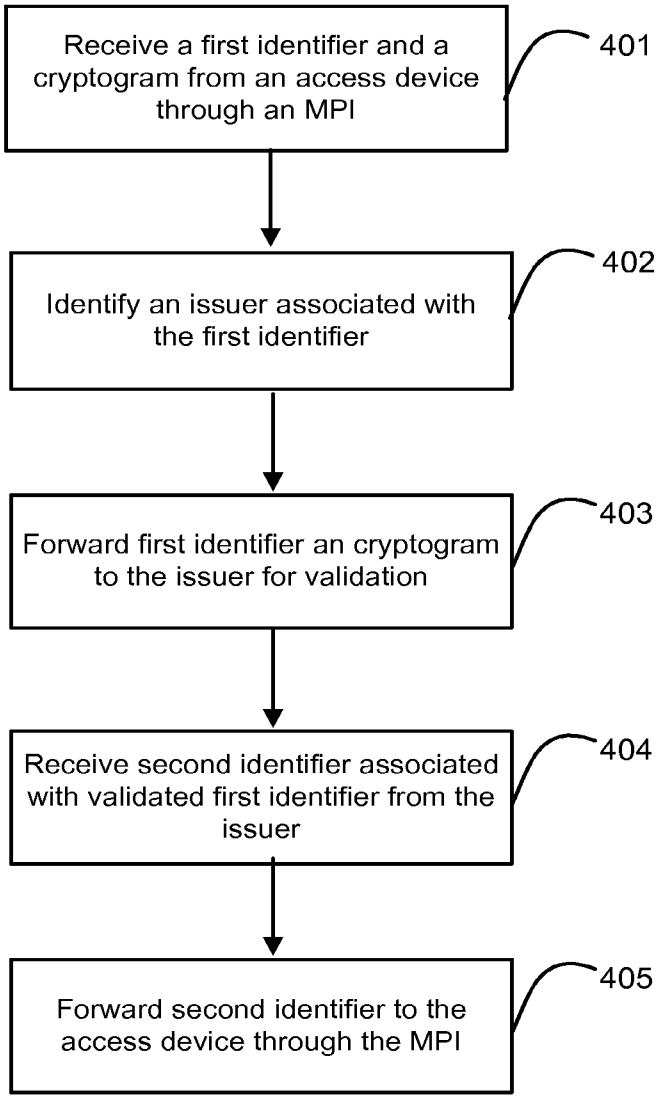
Receive a first identifier and a cryptogram from an access device through an MPI
401
Identify an issuer associated with the first identifier
402
Forward first identifier an cryptogram to the issuer for validation
403
Receive second identifier associated with validated first identifier from the issuer
404
Forward second identifier to the access device through the MPI
405

FIG. 4

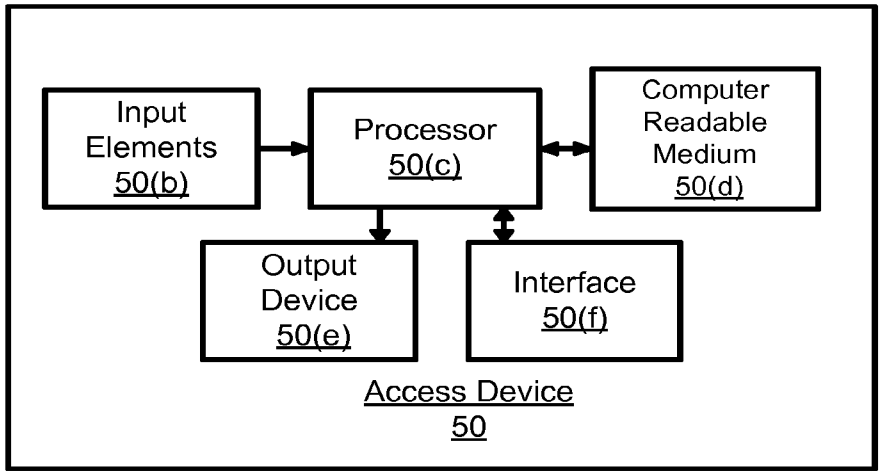
Input Elements 50(b)
Processor 50(c)
Computer Readable Medium 50(d)
Output Device 50(e)
Interface 50(f)
Access Device 50

FIG. 5

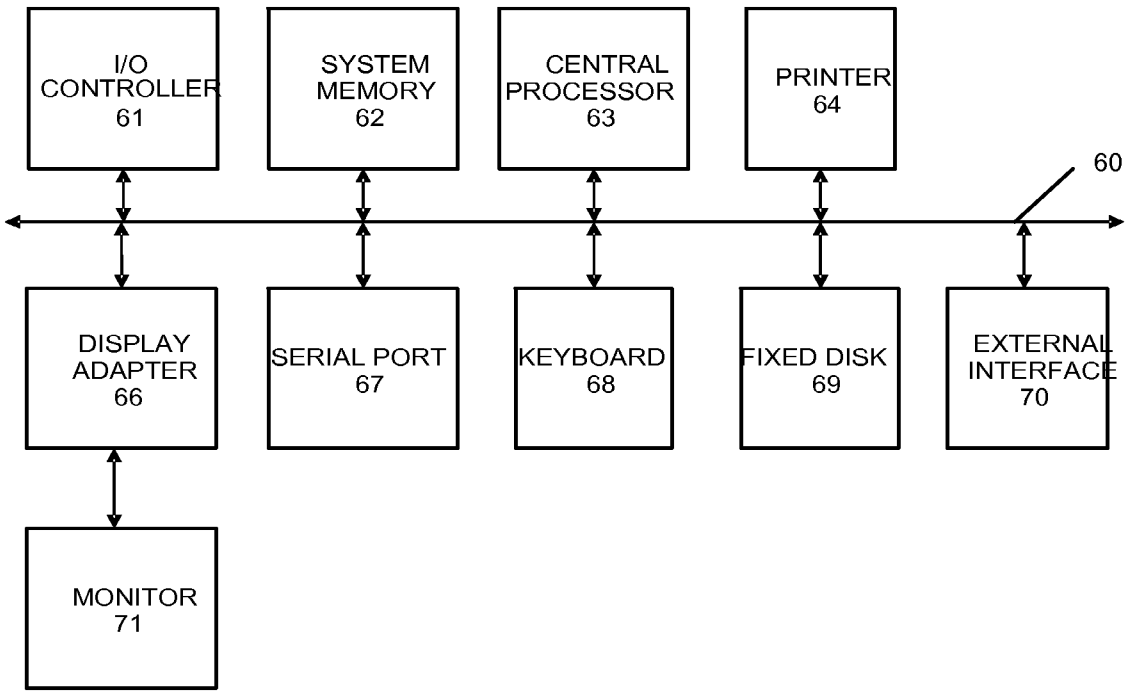
I/O CONTROLLER 61
SYSTEM MEMORY 62
CENTRAL PROCESSOR 63
PRINTER 64
60
DISPLAY ADAPTER 66
SERIAL PORT 67
KEYBOARD 68
FIXED DISK 69
EXTERNAL INTERFACE 70
MONITOR 71

FIG. 6

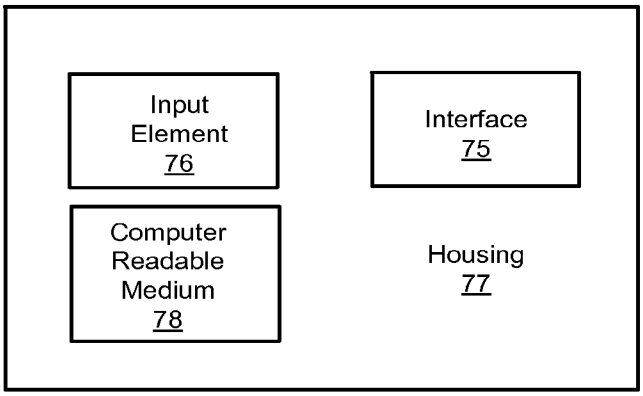
Input Element 76
Interface 75
Computer Readable Medium 78
Housing 77

FIG. 7

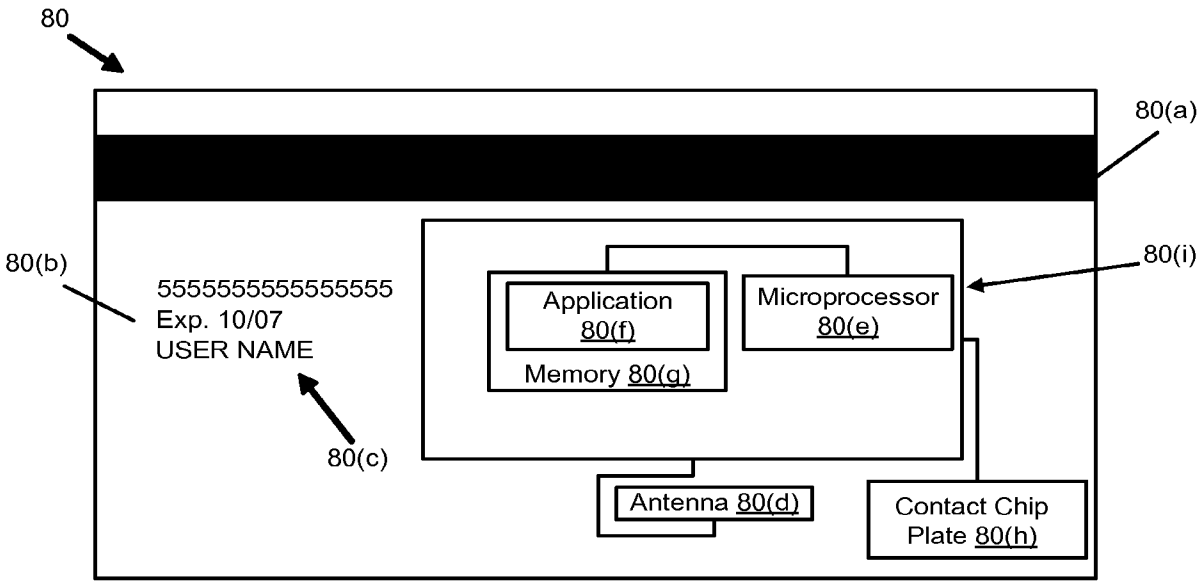
80
80(a)
80(b)
5555555555555555
Exp. 10/07
USER NAME
80(c)
80(i)
Application 80(f)
Microprocessor 80(e)
Memory 80(g)
Antenna 80(d)
Contact Chip Plate 80(h)

FIG. 8