Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2958140 A1 2012/02/16

(21) 2 958 140

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2011/08/12

(41) Mise à la disp. pub./Open to Public Insp.: 2012/02/16

(62) Demande originale/Original Application: 2 823 685

(30) Priorités/Priorities: 2010/08/12 (US61/372,955);
2011/03/29 (US61/468,847)

(51) Cl.Int./Int.Cl. *G06Q 20/40* (2012.01),
G06F 17/00 (2006.01)

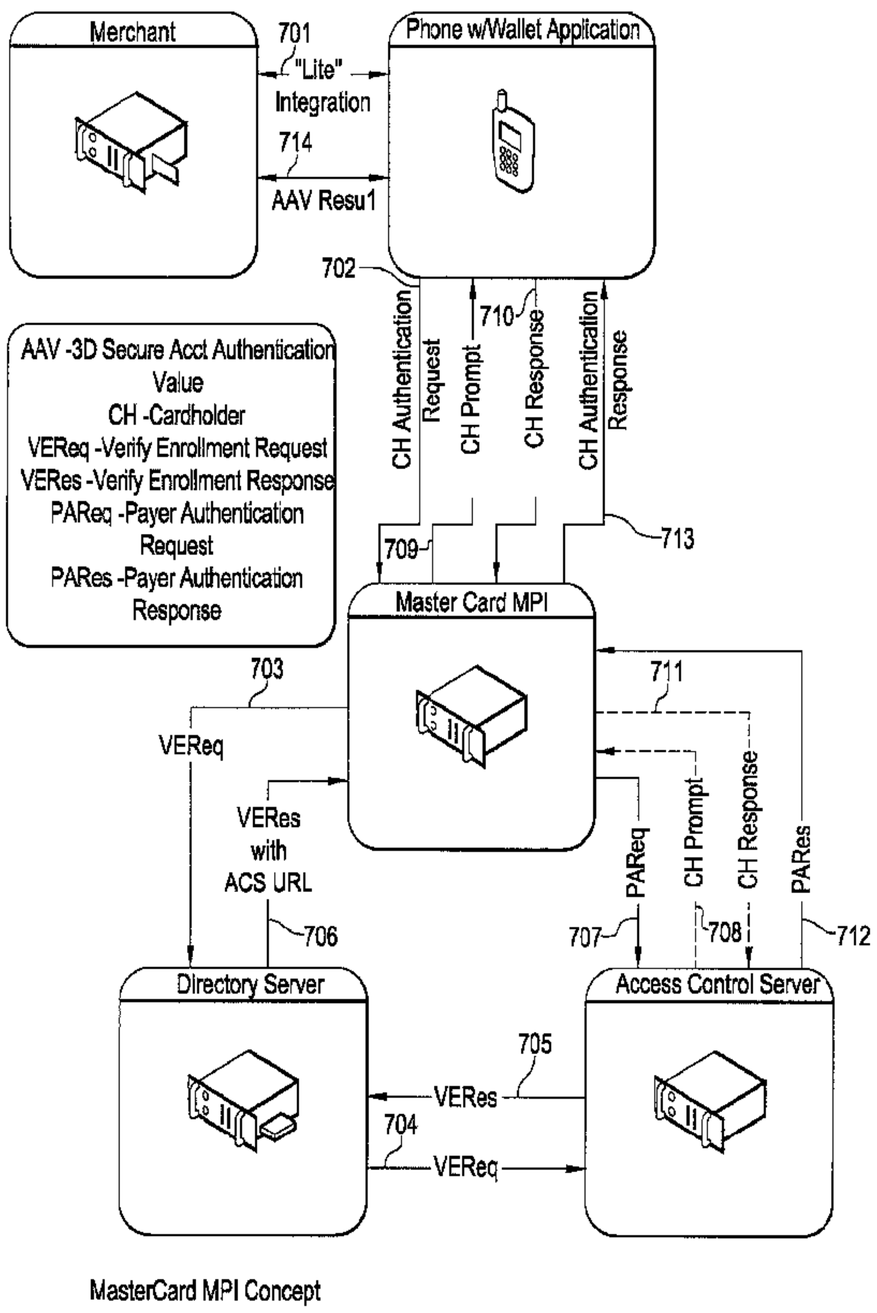
(71) Demandeur/Applicant:
MASTERCARD INTERNATIONAL, INC., US

(72) Inventeurs/Inventors:
WONG, SHOON PING, US;
MOY, KENNETH CHUNG LEM, US;
MARTIG, CELINE, SG;
FOUREZ, PABLO, BE;
MUSHING, ALAN, GB;
LUNDEQUIST, FREDRIK, US;
SHAON, MICHAEL, US;
AMEISS, MICHAEL, US

(74) Agent: PIASETZKI NENNIGER KVAS LLP

(54) Titre : PORTEFEUILLE UTILISANT DES CANAUX DE COMMERCE MULTIPLES POUR EFFECTUER DES TRANSACTIONS AUTHENTIFIEES

(54) Title: MULTI-COMMERCE CHANNEL WALLET FOR AUTHENTICATED TRANSACTIONS



MasterCard MPI Concept

(57) Abrégé/Abstract:
A phone-based electronic wallet providing authenticated transactions across multiple channels of commerce. The electronic wallet may be used for point-of- sale payments, remote mobile payments and/or web-based payments, and may use authentication tools such as offline PINs, SecureCode PINs and/or online PINs.

ABSTRACT

A phone-based electronic wallet providing authenticated transactions across multiple channels of commerce. The electronic wallet may be used for point-of-sale payments, remote mobile payments and/or web-based payments, and may use authentication tools such as offline PINs, SecureCode PINs and/or online PINs.

MULTI-COMMERCE CHANNEL WALLET FOR AUTHENTICATED TRANSACTIONS

BACKGROUND OF THE INVENTION

[0001] The present invention relates to transactions for payment of goods/services and, more particularly, to a phone-based electronic wallet providing authenticated transactions across multiple channels of commerce.

[0002] Both credit cards and debit cards are commonly used in the retail environment for the purchase of goods and/or services. Such cards are popular with consumers, and merchants accept these cards as a necessary part of doing business, i.e., they provide an effective substitute to cash and checks.

[0003] These card-based transactions are typically performed across multiple channels of commerce. For example, card-based transactions may be performed in person at a retail outlet, via a computer connected to the internet, via a mobile phone and/or via a company-based call center (e.g., a 1-800 number for a catalog company). These various transactions are conducted in different ways and, accordingly, have different levels of fraud risk associated therewith. In addition, the mentioned transactions generally require that the consumer have his or her card in hand to either present to the cashier in a retail environment, or to enter the requested information via the internet and/or over the telephone. Those knowledgeable in the field will recognize that the risk of financial fraud is greater during remote transactions because there is less ability for the merchant to verify the identity and authenticity of the cardholder.

[0004] It will also be appreciated that in today's environment it is common for a consumer to carry his or her cell/mobile phone on their person at all times. In fact, on many occasions it is more likely that the consumer will be carrying his/her phone, than carrying his/her wallet. Companies have attempted to tap into this trend by offering/facilitating various phone-based applications directed to a whole range of services. The recent growth of so-called "smart phones" has greatly increased the

interest of companies in this area. As a result, more and more transactions are likely to be performed from a remote location, e.g., ordering a product over the internet while standing in line. However, as the number of remote transactions increase, so does the risk of financial fraud.

[0005] There is therefore a need in the art for a method and system for authenticating electronic transactions across multiple channels of commerce. There is a further need in the art for a method and system which operates in conjunction with a phone (e.g., a smart phone) for authenticating financial transactions whether initiated in person, over the internet via a stand alone terminal, via the placement of a call to the call center of a company, and/or via a transaction initiated with the very same phone. Finally, there is a need in the art for a method and system which allows a bank or other financial institution to reduce fees to merchants conducting remote electronic transactions when utilizing enhanced authentication techniques, and to limit/reverse the shifting of fraud liability to the merchant for such remote transactions.

SUMMARY OF THE INVENTION

[0006] The present invention provides a mobile-phone centric electronic wallet providing the security of a virtual card terminal for online and off-line purchases. A wallet server (e.g., an application running in a cloud) and synchronized companion mobile and computer interface enables consumers to make purchases (which can include: retail, e-commerce, mobile, call center, etc) and use the mobile phone to authenticate against one of the authentication techniques tied to the chosen card (which can include: an offline PIN utilizing a secure memory chip, a MasterCard SecureCode PIN, and/or an online PIN such as an ATM PIN) where the necessary transaction and card specific authentication and processing method is directed by a central directory. The authentication process of the present invention allows participating banks to deem such transactions as more fully authenticated, which will allow them to lower the costs charged to merchants. The authentication process of the present invention will also limit/reverse the shifting of liability to the merchant since these more fully authenticated transactions will have less fraud associated therewith.

[0007] This system with its various authentication mechanisms will preferably utilize a central, hosted directory, which, when queried by the wallet application during a

transaction, will instruct the wallet how the transaction needs to be authenticated and processed, depending on the card used and type of transaction. In all instances, the authentication result and authentication method will be communicated from the wallet to the merchant via specific transaction codes and/or transaction tokens that will further enable proper risk scoring, authorization processing, and enforcement of specific scheme rules and terms and conditions (e.g. pricing, rules, liability shift, etc.) by the merchant acquirer. The wallet facilitates authentication from multi-commerce channels and will leverage multi-band communication to facilitate transaction authentication.

[0008] For retail (Point-of-sale (POS)/ Face-to-Face (F2F)) purchase transactions, the consumer may use the PayPass contactless capabilities which may be a feature of a chip located in the phone. For higher transaction value amounts where a PIN may be required, the wallet will prompt the user for the PIN on the phone. Successful authentication will be communicated from the wallet to the merchants or its Acquirer directly for approval processing.

[0009] For some remote (e-commerce, mobile or call center) purchase transactions, the consumer will employ his/her mobile phone and the wallet capabilities as a virtual POS terminal. In this case, when the consumer makes a purchase (e.g., through a computer or the mobile phone itself), the wallet will prompt the user for the PIN on the phone and enable a secure verification of the PIN value entered by the user, either in a pure offline mode, against the algorithm associated with the secure element on the phone, using for example the EMV protocol, or in an online mode, by encrypting the PIN and transmitting it. Successful authentication will be communicated from the wallet to the merchant's checkout system to be relayed to the Acquirer for approval processing.

[0010] For other remote (e-commerce, mobile or call center) purchase transactions, this invention builds on the pre-existing MasterCard SecureCode (MSC) system. It is contemplated herein that the SecureCode protocol can be extended to include a novel SecureCode wallet Application Programming Interface (API), to enable a MSC validation within the wallet interface through the wallet API, instead of through an internet browser session/window to communicate with the bank's authentication server. To facilitate this, the mobile phone will prompt the user for entry of the MSC

password or PIN within the wallet-driven interface on the phone and communicate securely with the ACS (the bank's MSC authentication server). Successful authentication will be communicated from the wallet to the merchant's checkout system to be relayed to the Acquirer for approval. This last step preferably replaces the pre-existing MSC Merchant software, thus reducing the implementation requirements for the merchant. Finally, this interface will preferably allow setup and reset of a MSC password or PIN, again without the need to use a separate browser window or session with the bank's authentication server.

[0011] Thus, the system and method of the present invention provide an electronic wallet for authenticating transactions across multiple channels of commerce using the consumer's own mobile phone. The present invention provides better economics for merchants through lower fee structures, and limits/reduces the shifting of fraud liability to the merchant for remote transactions. The present invention is scalable in design to provide easy integration for merchants, and to avoid issuer by issuer sales and implementations. It is also easy to deploy directly to customers. Finally, the present invention will promote profitability by driving transaction volumes and revenues.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Figure 1 is a schematical representation of a mobile phone-based payment/authentication system;

[0013] Figure 2 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction originating via a computer, the wallet application cooperating with a secure element on the phone and an offline PIN;

[0014] Figure 3 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction originating via computer, the wallet application cooperating with a SecureCode PIN for authentication;

[0015] Figure 4 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction originating via a phone, the wallet application utilizing an online PIN for authentication;

[0016] Figure 5 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction originating via a phone, the wallet application not being associated with an offline PIN, a SecureCode PIN and/or online PIN;

[0017] Figure 6 is a flow chart depicting an existing 3D Secure process;

[0018] Figure 7 is a flow chart showing a new authentication process in accordance with the present invention;

[0019] Figure 8 is a flow chart showing a new authentication process in accordance with the present invention;

[0020] Figure 9a is a flow chart showing the process of authenticating the wallet application using a SecureCode process;

[0021] Figure 9b is a flow chart showing an authenticated wallet application being used for subsequent purchases; and

[0022] Figure 10 is a flow chart showing an authentication system wherein the features of the MPI and the ACS has been incorporated into the wallet server.

DETAILED DESCRIPTION OF THE INVENTION

[0023] Referring now to Figure 1, the present invention is centered around a mobile phone 10 associated with a payment card, e.g., a credit card, debit card or prepaid card. The mobile phone is preferably capable of storing and/or running a wallet application 12, which is preferably a browser-based mobile application capable of storing selected information such as a cardholder name, card alias, billing/shipping address, etc., locally on the phone or in a cloud server. In one preferred embodiment, the mobile phone is a "smart phone", and the wallet application is stored in a memory device located in the phone. It is contemplated herein that the system and method of the present invention will enable payments across multiple channels of commerce, e.g., a POS payment 14 by, for example, a PayPass terminal, a remote mobile payment 16 initiated by a mobile phone, and/or a web-based payment 18.

[0024] As further described in Figure 1, the present invention contemplates the use of various authentication tools including an offline PIN 20, a SecureCode PIN 22, and/or an online PIN 24. It will be recognized that the foregoing mentioned PINs are currently in use in the marketplace and, accordingly, the use of such already existing PINs can facilitate the implementation of the present system. Of course, it is contemplated herein that a new independent PIN (apart from the mentioned PINs) can be created specifically for use with the present invention.

[0025] Offline PIN 20 preferably utilizes an offline PIN verification process whereby the PIN entered by the consumer is verified by a secure element located on phone 10. In this process, the wallet plays the role of a "virtual terminal", interacting with the secure element, and upon verification of the PIN, passes the CHIP token (ARQC) to the merchant for authorization. In this "virtual terminal", the secure element serves the role as the "card". Offline PIN 20 can, for example, be used in connection with a PayPass payment.

[0026] Secure Code PIN 22 is a PIN associated with a card enrolled in the MasterCard SecureCode system. It is contemplated herein that the SecureCode system could also utilize a password and/or code, rather than a PIN.

[0027] Online PIN 24 is used in an online PIN verification process whereby the wallet application 12 plays the role of a "virtual terminal", interacting to encrypt the PIN for transmission to the merchant. The use of an online PIN verification process may provide greater flexibility in authenticating transactions by, for example, allowing an issuing bank to authenticate the transactions associated with its cardholders without the need for the issuing bank to enroll/register its cardholders and/or adopt new infrastructure.

[0028] Users may have different instances of wallet application 12 on different phones. A sync service can maintain the various instances synchronized with an online server (similar to how browser bookmarks can be stored offline in different instances of an internet browser and be synchronized between various machines.) Merchants can add a piece of code to their checkout button that invokes the wallet application. During checkout, users select card and shipping address (if needed). The authentication PIN is entered into the phone in response to a prompt from the mobile

application. The wallet passes back the information to the merchant who submits this information through existing channels (internet gateway or payment processor), i.e., no changes are required to existing processes or integration.

[0029] In one preferred embodiment, the wallet application may be a browser HTML 5 application (not a native application) that self-installs in the mobile phone or computer browser on the first use.

[0030] In another preferred embodiment, the wallet application can securely store information on the phone (shipping address, card alias, secure token, etc.). This information can be used to authenticate to the remote server. This also enables offline transactions. The mobile application can preferably "talk" to the secure element on the phone. In this regard, the mobile application could play the role of a virtual POS terminal in initiating card present CHIP plus PIN transactions.

[0031] In accordance with the present invention, a consumer may use his phone or computer to shop at a web-based retailer. When the consumer is ready to check out, he will preferably have the option of clicking a checkout button associated with the present system. Clicking the button prompts the consumer to provide his username and password to log-in, and to confirm both the payment card to be used and the shipping address to which the item is to be sent. Thereafter, the system will prompt the consumer to enter the authenticating PIN, and the transaction is then completed. At that point, the consumer is preferably returned to the merchant's site.

[0032] The present invention provides several benefits to the consumer. More particularly, the present invention provides easy and convenient checkout through a form fill or pass through function, which is preferably part of the wallet application. The present invention offers secure payments via a PIN, or other biometric parameters such as a voice print or fingerprint. In this regard, the smart phone may be provided with a biometric reader and/or analyzer.

[0033] The present invention also provides benefits to the merchant including a potential liability shift from the merchant to the authorizing bank for all wallet-based transactions. More particularly, the use of an authentication process for remote transactions reduce the risk of fraud associated with such transactions, and may limit/reverse the shifting of fraud liability from the authorizing bank to the merchant.

The use of the authentication process described herein may also provide more attractive economics to the merchant through access to lower fee structures, depending on the consumer authentication method. The present invention also provides limited integration impact in that it provides a simple wallet API to pass card details, shipping information and security tokens, and does not require any new contractual relationships (i.e., it leverages existing card acceptance). Finally, the present invention is backwards compatible, (i.e., it provides native support for SecureCode) thus resulting in better consumer experience/ergonomics.

[0034] The wallet application of the present invention provides a comprehensive solution to financial transactions conducted across multiple channels of commerce. The present wallet application provides a simple and winning proposition to consumers, and provides a form fill option in an innovative application. The present invention can use existing payment networks (e.g., Mastercard worldwide system) which are already accepted by merchants, thereby eliminating the need for heavy integration, while providing more security and better economics. The present invention does not require issuing banks to implement new requirements since the system can function with existing authorization techniques, e.g., SecureCode, CHIP and PIN and/or online PIN. The present invention also contemplates the long term convergence path of the three commerce platforms – retail, e-commerce and mobile - towards a mobile phone centric system. The present invention also provides the potential to deliver incremental top line revenue growth by 1) protection of transaction volumes and revenues; 2) by providing an innovative and proprietary approach with the option to price different services to issuers, merchants or partners (e.g., directory service, wallet service, etc.); and 3) by providing flexibility for later expansion (new funding source, secure elements, etc.).

[0035] It is also contemplated that the authentication processes described herein can be used in applications where the consumer owns a "dumb phone". For example, in applications where the consumer is conducting an e-commerce transaction through his computer, or has initiated a call to a call center, and the consumer does not own a smart phone, the present system can utilize existing SMS messaging or other messaging technology to contact the "dumb phone" of the consumer and request the

entry of a PIN. Upon receipt of the PIN from the "dumb phone", the transaction can be authenticated and completed.

[0036] Figure 2 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction (e.g., a computer-initiated transaction) with a secure element and an offline PIN. In step 100, the consumer selects the "wallet" icon on the merchant's site. The wallet application is then opened at step 102 by the browser on the user's computer. The consumer then logs into the wallet application (step 104). The appropriate payment card and shipping details are selected (step 106), and the card's PAN is then sent to the wallet server (step 108). In step 110, the wallet server requests the Card Verification Method (CVM) from the MasterCard directory. This directory may be based on an expanded version of the currently existing SecureCode directory, or may be an entirely new directory. The appropriate CVM is confirmed at step 112. The wallet server then initiates the CVM check (step 114). A message to enter the PIN is then displayed on the browser (step 116) and on the mobile phone (step 118). The consumer then enters the offline PIN into the mobile phone in step 120. In step 122, the offline PIN is verified by the secure element on the phone. An "OK" message is displayed on the phone (step 124), and the ARQC is transmitted to the wallet server (step 126). The browser is refreshed (step 128), the authentication result is transmitted to the MasterCard directory (step 130), and the authorization data is transmitted to the browser (step 132). The transaction is then authorized by the merchant at step 134, and the approval is displayed at step 136, resulting in a happy consumer (step 138).

[0037] Figure 3 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction (e.g., a computer-initiated transaction) with a SecureCode PIN. In step 200, the consumer selects the "wallet" icon on the merchant's site. The wallet application is then opened at step 202 by the browser on the user's computer. The consumer then logs into the wallet application (step 204). The appropriate payment card and shipping details are selected (step 206), and the card's PAN is then sent to the wallet server (step 208). In step 210, the wallet server requests the Card Verification Method (CVM) from the MasterCard directory. This directory may be based on an expanded version of the currently existing SecureCode directory, or may be an entirely new directory. The appropriate CVM is

confirmed at step 212. The wallet server then initiates the SecureCode authentication process (step 214). A "check phone" message is then displayed on the browser of the computer (step 216) and a message to enter the SecureCode PIN is displayed on the mobile phone (step 218). The consumer then enters the SecureCode PIN into the mobile phone in step 220. In step 222, the wallet server packages the SecureCode for validation. The SecureCode is then verified at step 224. This verification process will be discussed in greater detail hereinbelow. Once verified, an AAV is sent to the wallet server (step 226). An "OK" message is displayed on the browser (step 228) and on the phone (step 230). The authentication result is transmitted to the MasterCard directory (step 232), and the authorization data (step 234) is transmitted to the merchant for authorization (step 236). The transaction is then authorized at step 238, and the approval is displayed at step 240, resulting in a happy consumer (step 242).

[0038] Figure 4 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction (e.g., a phone-initiated transaction) with an online PIN. In step 300, the consumer selects the "wallet" icon on the merchant's site. The consumer then selects the wallet application (step 302), which then displays a log in form (step 304). Alternatively, the wallet may be auto-detected. The consumer logs in at step 306, views the listed cards at step 308, and thereafter selects the appropriate payment card and shipping details (step 310). At step 312, the wallet questions whether an online PIN is associated with the card. The existence of the online PIN is confirmed at step 314. In step 316, the wallet requests entry of the online PIN into the phone. The online PIN is entered at step 318. Thereafter, the online PIN is encrypted (step 320), and forwarded to the merchant for authorization (step 322). The transaction is validated at step 324, payment is approved at step 326, resulting in a happy consumer (step 328).

[0039] Figure 5 is a flow chart depicting the wallet application of the present invention being used in an e-commerce transaction (e.g., a phone-initiated transaction) without a secure element on the phone, without a SecureCode, and without an online PIN. In step 400, the consumer selects the "wallet" icon on the merchant's site. The consumer then selects the wallet application (step 402), which then displays a log in form (step 404). Alternatively, the wallet may be auto-detected.

The consumer logs in at step 406, views the listed cards at step 408, and thereafter selects the appropriate payment card and shipping details (step 410). At step 412, the wallet questions whether a SecureCode is associated with the card. The card is determined not to be in the SecureCode directory at step 414. The authorization data is then passed to the wallet at step 416, which sends such data to the merchant for authorization (step 418). The transaction is validated at step 420, payment is approved at step 422, resulting in a happy consumer (step 424). In this type of scenario, the issuing bank can accept or decline the transaction in accordance with its existing standards. For example, the issuing bank may establish protocols whereby certain e-commerce and/or remote transactions are not approved in the absence of a successful authentication process.

[0040] An existing 3D Secure process is shown in the flow chart of Figure 6. More particularly, the existing 3D Secure process includes step 501 wherein a merchant initiates an authentication request, and pings the merchant plug-in (MPI) with the cardholder financial instrument information. It should be understood that the cardholder has already accessed the merchant's webpage, and has indicated his desire to purchase a particular product using a particular payment card. In step 502, the MPI identifies the appropriate card type, and sends an authentication request (VEReq) to the relevant directory server. In step 503, the directory server identifies the appropriate access control server (ACS), and requests an authentication response. In step 504, the ACS identifies the card and cardholder, and sends a response (VERes) with authentication prompts within the ACS URL. In step 505, the directory server forwards the authentication response (with the ACS URL) to the MPI. In step 506, the MPI sends the payment authentication request (PAReq) to the merchant for display during checkout. The payment authentication request includes the ACS URL. In step 507, the payment authentication request is sent from the merchant to the ACS – in other words, the merchant calls the ACS URL. In step 508, the ACS sends a pop-up window to the merchant which appears on the cardholder's browser requesting the cardholder to enter authentication credential. In step 509, the cardholder enters the requested authentication credentials, and such information is sent back to the ACS for authentication. In step 510, the ACS validates the authentication credentials, and if correct, sends an AAV confirming authentication to the merchant. Thereafter, the merchant proceeds to authorize the transaction in customary fashion.

[0041] One drawback to the process described above with respect to Figure 6 is that the authentication process requires the use of a pop-up window appearing during the online transaction process. Many online shoppers have been taught to be suspicious of pop-up windows, and are reluctant to enter relevant financial information in such a window for fear that the pop-up window could be coming from a fraudulent website and/or be a part of a phishing scam.

[0042] The new embodiments of the present invention shown in Figures 7 and 8 not only address the drawbacks of relying upon pop-up windows during authentication, but provide the merchant with better control over the checkout experience presented to its customers. These new processes are shown in the context of a phone with a wallet application. However, it is to be understood herein that these processes can also be used in conventional cardholder browser/merchant transactions, i.e., a transaction performed without a phone and/or wallet application.

[0043] Turning first to Figure 7, the wallet detects the checkout page and makes a payment request (step 601). The wallet then authenticates the user, at which point the user can select the payment type (step 602). The wallet server then determines which branded 3DS Directory to use based on the account number selected (step 603). The user's participation is then verified (step 604). Next, the wallet retrieves the SecureCode (step 605). In particular, the user is prompted to enter his/her SecureCode as part of the wallet sign-in or as a separate prompt (step 605a), and/or the wallet retrieves/generates the user's SecureCode which has been securely stored on the phone and wallet server (step 605b). The SecureCode is then sent to the bank for verification (step 606). Next, the wallet form fills the payment details, including the AAV, in the merchant page (step 607). The merchant then authorizes the transaction in normal fashion (step 608), and receives the necessary approval (step 609).

[0044] Turning now to Figure 8, the process includes a step 701 wherein the merchant initiates a transaction request. It should be understood that the merchant has already integrated his existing payment system with the wallet application such that the merchant can receive authentication information from the wallet. In step 702, the wallet initiates an authentication request, and pings the MasterCard Merchant Plug-In (MC-MPI) formed in accordance with the present invention with the cardholder

financial instrument information. In step 703, the MC-MPI identifies the appropriate card type, and sends a verify enrollment request (VEReq) to the relevant directory server. In step 704, the directory server identifies the appropriate ACS, and forwards the verify enrollment request (VEReq), expecting a verify enrollment (VERes) response. In step 705, the ACS identifies the card and cardholder, and sends a response (VERes) with the ACS URL. In step 706, the directory server forwards the response (VERes with the ACS URL) to the MC-MPI. At this point, rather than MC-MPI communicating back to the wallet application, the MC-MPI communicates directly with the ACS. More particularly, in step 707, the MC-MPI sends a payer authentication request (PAReq) to the ACS. In other words, the MC-MPI formats the expected request and calls the ACS URL. In step 708, the ACS responds with the traditional browser HTML markup to the MC-MPI. In step 709, the MC-MPI then interprets the HTML markup, including the authenticating criteria, and extracts the needed elements from the HTML markup and translates into the API protocol which is then communicated to the wallet. The wallet then displays an authentication request to the cardholder, requesting that the cardholder enter their authentication credentials. In step 710, the wallet communicates the cardholder authentication credentials to the MC-MPI via API protocol. In step 711, the MC-MPI translates the cardholder authentication credentials into the format expected by the ACS and uses an HTTP POST to communicate the credentials to the ACS. In step 712, the ACS validates the authentication credentials, and sends a payer authentication response (PARes including AAV) back to the MC-MPI representing the authentication result. In step 713, the MC-MPI passes the AAV and information received from the ACS to the wallet via API protocol. In step 714, the wallet passes the AAV and authentication message to the merchant via API protocol. The merchant then proceeds to authorize the transaction in customary fashion.

[0045] As described, in step 708 of Figure 8, the ACS sends the authentication criteria to the MC-MPI for translation. In other words, rather than sending a the HTML markup served by the ACS directly back to the wallet application, the necessary information for authentication is sent to the MC-MPI via the HTML markup, which then can translate that information and forward it in a predetermined manner. More particularly, with respect to a wallet application, such application could be designed to communicate with the MC-MPI in a consistent and known

manner whereby a consumer does not receive a "suspicious" pop-up window. Rather, the wallet application can cooperate with the MC-MPI such that every authentication transaction is conducted in a recognized window.

[0046] As mentioned hereinabove, the processes described in Figures 7 and 8 are also applicable to non-wallet based transactions. More particularly, for browser-based transactions utilizing a 3D Secure process, or other similar process, the forwarding of a pop-up window from the ACS directly back to the merchant can introduce uncertainty into the authentication process. Accordingly, the MC-MPI shown in Figure 8 could, in another application, communicate directly with a cardholder browser/merchant in the absence of a phone. Such an arrangement could allow the merchant to control how the authentication request appears to the customer during the checkout process. In other words, by sending the authentication criteria through the MC-MPI (where it is translated), the translating information can be sent back to the merchant's webpage in a predetermined and selected manner, thus giving the merchant greater control over the shopping experience of its customers – while also eliminating the usage of pop-up windows.

[0047] In another embodiment, the wallet is used as a security supplement. In one application, this is accomplished by authenticating the wallet itself. More particularly, the wallet application is loaded onto the phone, and a payment card is entered into the application. The user's identity is verified, and the wallet thereafter holds the payment data in a secure manner. When the user subsequently uses the wallet to make a purchase, the wallet can communicate to the merchant that the wallet itself has been authenticated, thus decreasing the likelihood of a fraudulent transaction. Referring to Figure 9A, the SecureCode process can be used to authenticate a wallet. In this regard, the user signs into the wallet and registers a card (step 800). The SecureCode process is initiated for authentication (step 801). The 3DS directory is then accessed at step 802. Next, the user is prompted for the SecureCode (step 803). The SecureCode is verified by the ACS (step 804). If authenticated, the payment card is accepted and stored in the wallet in a secure manner (step 805). Of course, it is contemplated herein that other process could be used to authenticate the wallet, such as an online PIN or a unique wallet PIN/code provided by the issuing bank.

[0048] During a future transaction, the wallet can communicate to the merchant that the card has previously been authenticated, thus reducing the likelihood of a fraudulent transaction. Turning now to Figure 9B, the process shown is similar to that shown in Figure 7 with the exception of step 810. After the user signs into the wallet, the wallet can determine whether to seek additional authentication from the user. For example, for certain transactions (e.g., a transaction exceeding a particular monetary value, a transaction outside of the user's normal spending habits, etc.) the issuing bank can require authentication beyond the wallet authentication. Thus, if additional authentication is required, the wallet will initiate the SecureCode process. If additional authentication is not required, the wallet will bypass the SecureCode process and proceed with the transaction. Of course, it is contemplated herein that the subsequent authentication process can be other than the SecureCode process, e.g., an online PIN.

[0049] In another preferred embodiment, a wallet MPI is contemplated wherein the wallet becomes the new SecureCode MPI for merchants. Referring to Figure 10, the wallet detects checkout at the merchant at step 901. The wallet then authenticates the user (step 902), and payment details are selected (step 902). The wallet server then determines that the bank is the wallet ACS customer, and that no further authentication is necessary (step 803). The remainder of the process is the same as shown in Figure 7. It is to be noted that the process shown in Figure 10 does not require the MPI and the ACS shown and described in Figure 7. Thus, this embodiment may provide a simple way for merchants to deploy the SecureCode process without the need for investment in infrastructure by both the merchant and the issuing bank.

[0050] While reference has been made to various preferred embodiments of the invention other variations, implementations, modifications, alterations and embodiments are comprehended by the broad scope of the appended claims. Some of these have been discussed in detail in this specification and others will be apparent to those skilled in the art. Those of ordinary skill in the art having access to the teachings herein will recognize these additional variations, implementations, modifications, alterations and embodiments, all of which are within the scope of the present invention, which invention is limited only by the appended claims.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for removing pop-up windows during an authentication process involving a cardholder using a payment card in an electronic transaction, comprising the steps of:

sending authentication criteria directly from an access control sever to a merchant plug-in;

translating said authentication criteria to a language compatible with said merchant plug-in;

forwarding said authentication criteria through said merchant plug-in to a device operated by said cardholder for entry of said authentication credentials associated with said payment card in the absence of a pop up window.

2. The method according to claim 1, wherein said authentication criteria are transmitted in HTML markup, and further comprising the step of translating said HTML markup into application programming interface protocol.

3. The method according to claim 2, further comprising the step of returning said authentication credentials through said merchant plug-in to said access control server for validation of said credentials.

4. The method according to claim 3, further comprising the step of translating the authentication credentials received by said merchant plug-in from said application programming interface protocol to said HTML markup.

5. The method according to claim 4, further comprising the step of sending a validation response from said access control server to said merchant plug-in for subsequent transmission to a merchant participating in said electronic transaction.

6. A method for eliminating the need for an HTML authentication pop-up window for entry by a cardholder of authentication credentials during an authentication process of an electronic transaction between the cardholder and a merchant over a payment network, the cardholder using a mobile device having an

application having at least one payment card, and an application programming interface (API), the cardholder mobile device being in communication with a server device and having access to a merchant plug-in operational by a processor of the server device, the method being carried-out by the server device via the merchant plug-in and comprising the steps of:

receiving, by the server device via the merchant plug-in, a cardholder authentication request from the cardholder mobile device API;

sending, by the server device, a payer authentication request to an access control server device;

receiving, from the access control server device and in response to the payer authentication request, cardholder authentication criteria in HTML markup;

extracting, by the server device via the merchant plug-in, the cardholder authentication criteria from the HTML markup;

sending, by the server device via the merchant plug-in, the cardholder authentication criteria extracted from the HTML markup to the API of the cardholder mobile device for entry by the cardholder of authentication credentials using the cardholder mobile device and API;

receiving, from the cardholder mobile device and API, the authentication credentials of the cardholder; and

sending, by the server device, the authentication credentials of the cardholder to the access control server device for validation.

7. The method according to claim 6, further comprising the steps of:

receiving, from the access control server, an authentication response of validation of the authentication credentials of the cardholder; and

sending, by the server device via the merchant plug-in, the authentication response to the cardholder mobile device and the API.

8. The method according to claim 6, further comprising the step of receiving, by the server device via the merchant plug-in, an access server device identification from a directory server device.

9. A system for authenticating an identity of a cardholder during authentication of an electronic transaction involving a payment card and without an HTML

authentication pop-up window, the electronic transaction being conducted over a payment network between a merchant having access to a merchant plug-in and a cardholder using a mobile device having an electronic wallet having at least the payment card and an application programming interface (API), the system comprising:

a directory server device for verification of enrollment of the payment card in an authentication program;

an access control server device in communication with the directory server device and the merchant plug-in, the access control server device containing cardholder authentication credentials associated with the payment card; and

a wallet server device having a merchant plug-in operational by a processor of the wallet server device and in communication with the directory server device and the access control server device and the cardholder device;

wherein the wallet server device via the merchant plug-in receives cardholder authentication criteria in HTML markup directly from the access control server device, extracts the cardholder authentication criteria from the HTML markup, transmits the cardholder authentication criteria to the electronic wallet API of the cardholder mobile device, receives, from the cardholder mobile device and the electronic wallet API, cardholder authentication credentials, and sends the cardholder authentication credentials to the access control server device for validation.

10. The system according to claim 9, wherein the merchant plug-in further receives, from the access control server device, an authentication response of validation of the cardholder authentication credentials, and sends the authentication response to the cardholder mobile device and the electronic wallet API.

11. A method of reducing fraudulent transactions associated with electronic commerce, comprising the steps of:

providing a wallet application for storage on a mobile phone;

entering of data associated with a payment card into said wallet application;

authenticating the identity of the cardholder associated with said payment card via an authentication process;

placing said wallet application into an authenticated state whereby the data associated with said payment card is stored in a secure manner within said wallet application; and

communicating said authenticated state of said wallet to a merchant during said electronic translation.

12. The method according to claim 11, comprising the further steps of:

analyzing said financial transaction to assign a risk factor to such transaction; and

determining whether further authentication is required based upon said assigned risk factor.

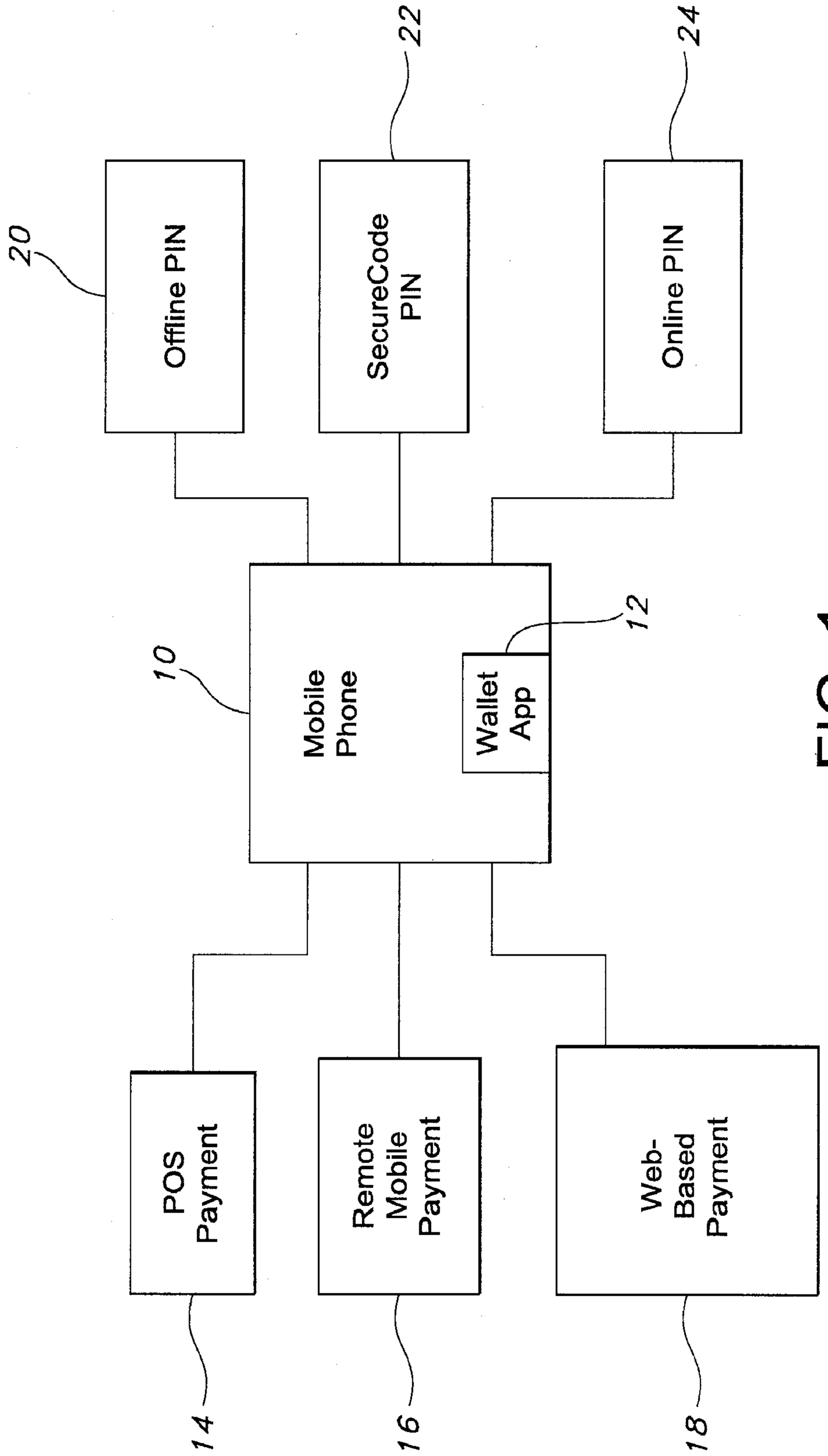

22
24
20
Offline PIN
SecureCode PIN
Online PIN
10
Mobile Phone
Wallet App
12
POS Payment
Remote Mobile Payment
Web-Based Payment
14
16
18

FIG. 1

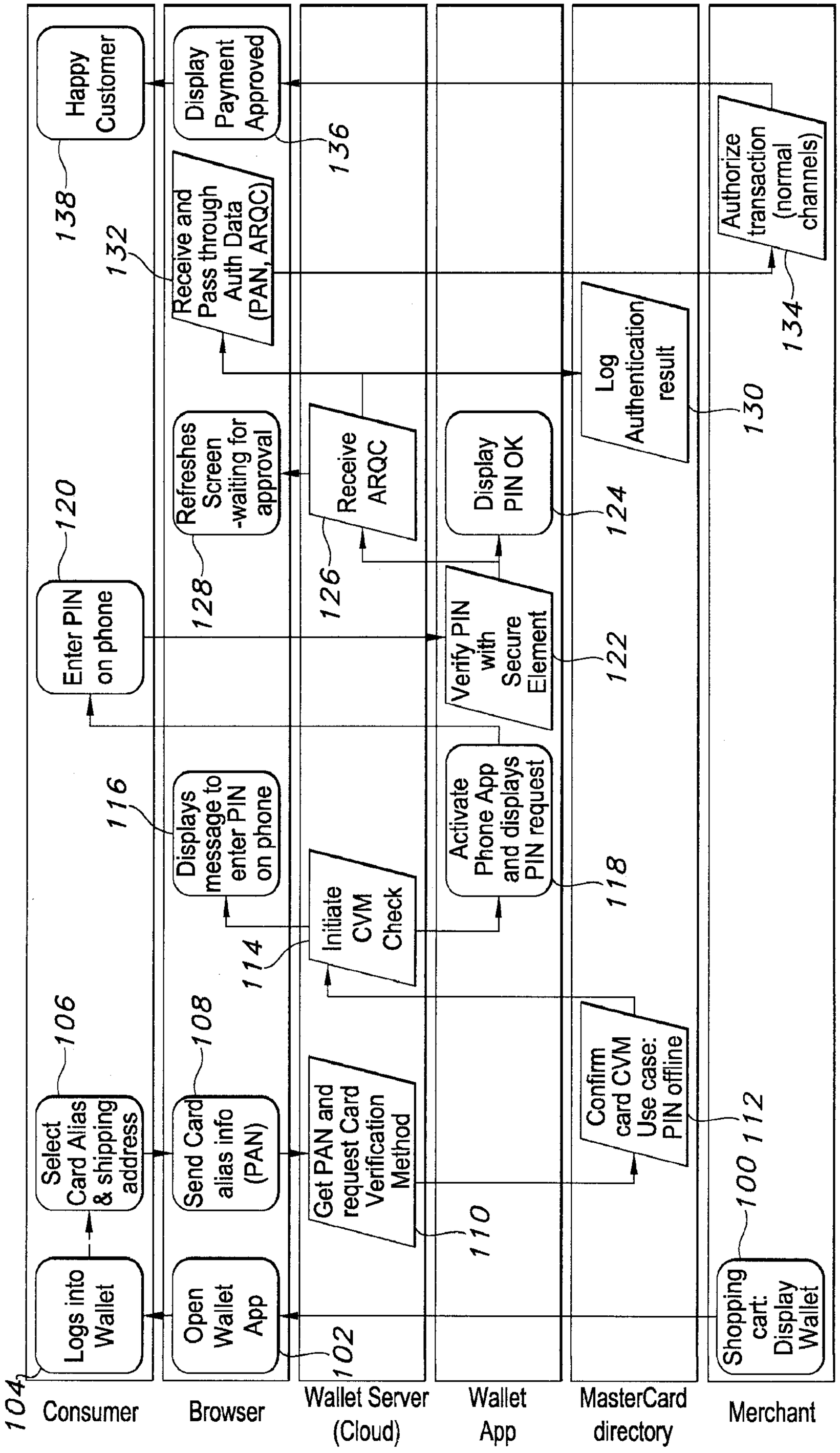

Consumer
Browser
Wallet Server (Cloud)
Wallet App
MasterCard directory
Merchant
104
Logs into Wallet
Open Wallet App
102
Shopping cart: Display Wallet
100
Select Card Alias & shipping address
106
Send Card alias info (PAN)
108
Get PAN and request Card Verification Method
110
Confirm card CVM Use case: PIN offline
112
Initiate CVM Check
114
Activate Phone App and displays PIN request
118
Displays message to enter PIN on phone
116
Enter PIN on phone
120
Verify PIN with Secure Element
122
Display PIN OK
124
Receive ARQC
126
Refreshes Screen -waiting for approval
128
Log Authentication result
130
Authorize transaction (normal channels)
134
Receive and Pass through Auth Data (PAN, ARQC)
132
Display Payment Approved
136
Happy Customer
138

FIG. 2

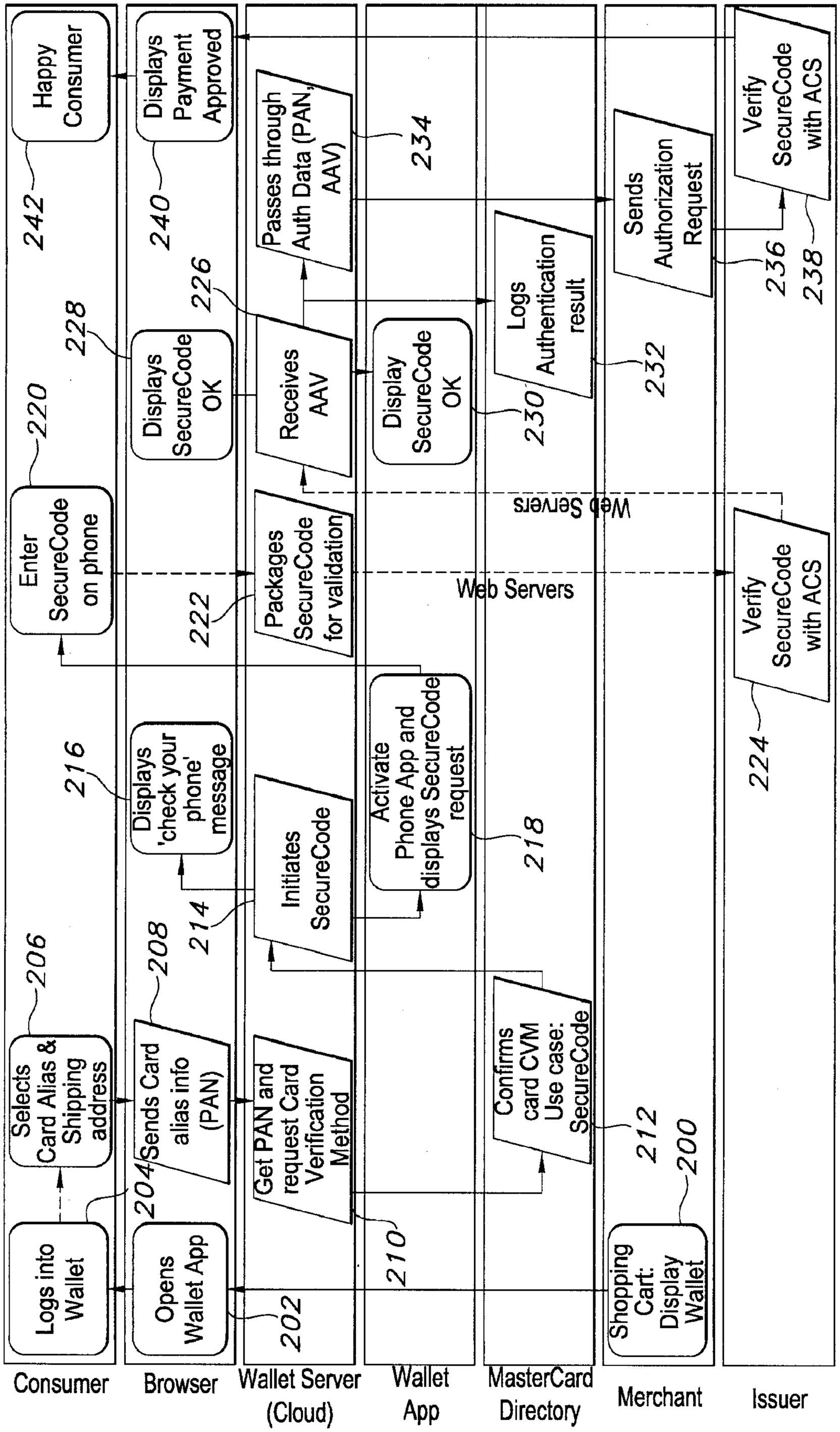
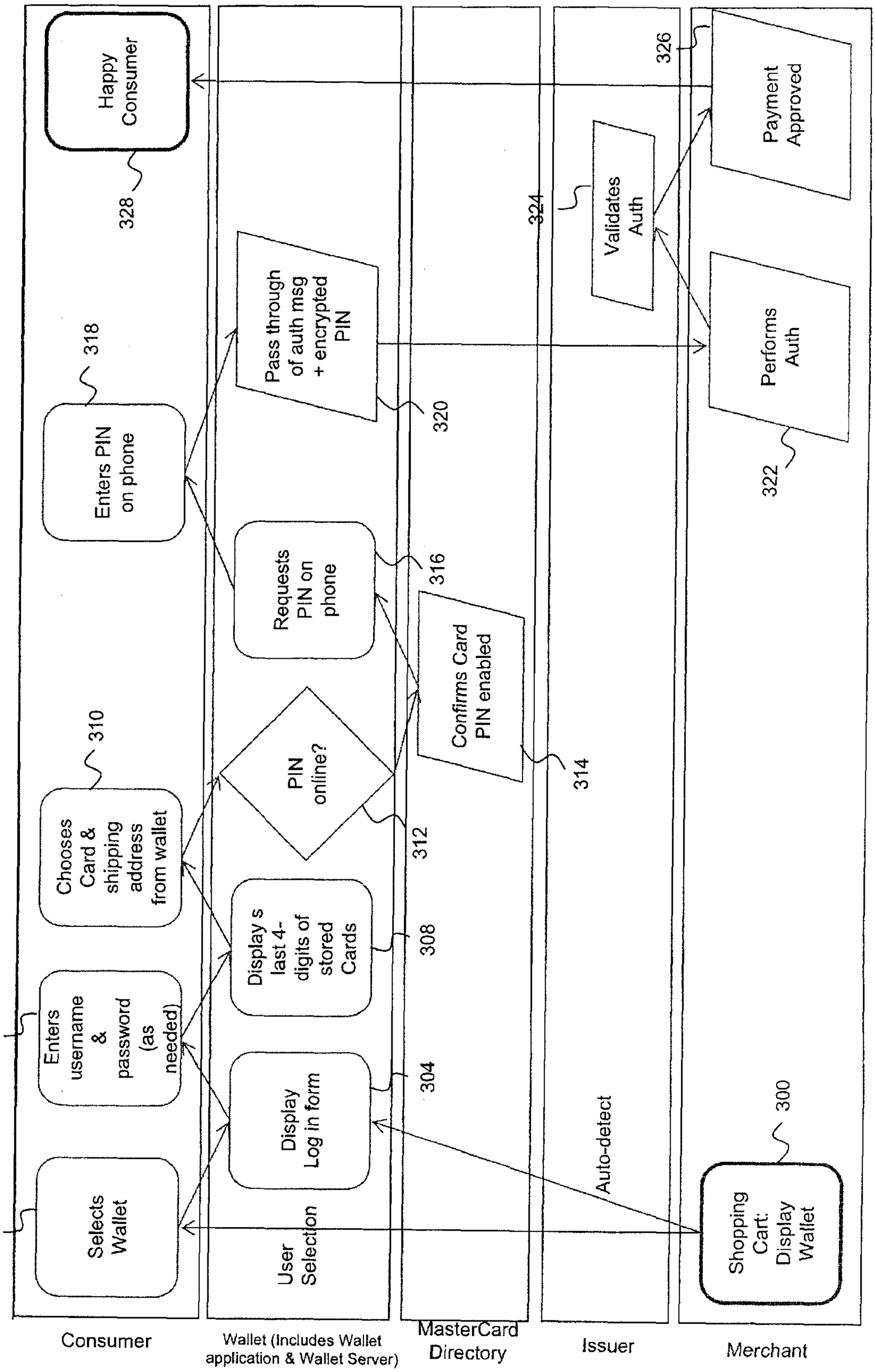

Consumer
Browser
Wallet Server (Cloud)
Wallet App
MasterCard Directory
Merchant
Issuer
Logs into Wallet
Selects Card Alias & Shipping address
Enter SecureCode on phone
Happy Consumer
Opens Wallet App
Sends Card alias info (PAN)
Displays 'check your phone' message
Displays SecureCode OK
Displays Payment Approved
Get PAN and request Card Verification Method
Initiates SecureCode
Packages SecureCode for validation
Receives AAV
Passes through Auth Data (PAN, AAV)
Activate Phone App and displays SecureCode request
Display SecureCode OK
Confirms card CVM Use case: SecureCode
Logs Authentication result
Shopping Cart: Display Wallet
Sends Authorization Request
Verify SecureCode with ACS
Verify SecureCode with ACS
Web Servers
Web Servers
202
204
206
208
210
212
214
216
218
220
222
224
226
228
230
232
234
236
238
240
242

FIG. 3

Fig. 4


Happy Consumer
328
Enters PIN on phone
318
Requests PIN on phone
316
Pass through of auth msg + encrypted PIN
320
Validates Auth
324
Payment Approved
326
Performs Auth
322
Confirms Card PIN enabled
314
PIN online?
312
Chooses Card & shipping address from wallet
310
Display s last 4-digits of stored Cards
308
Enters username & password (as needed)
306
Display Log in form
304
Selects Wallet
302
Auto-detect
Shopping Cart: Display Wallet
300
Consumer
Wallet (Includes Wallet application & Wallet Server)
MasterCard Directory
Issuer
Merchant

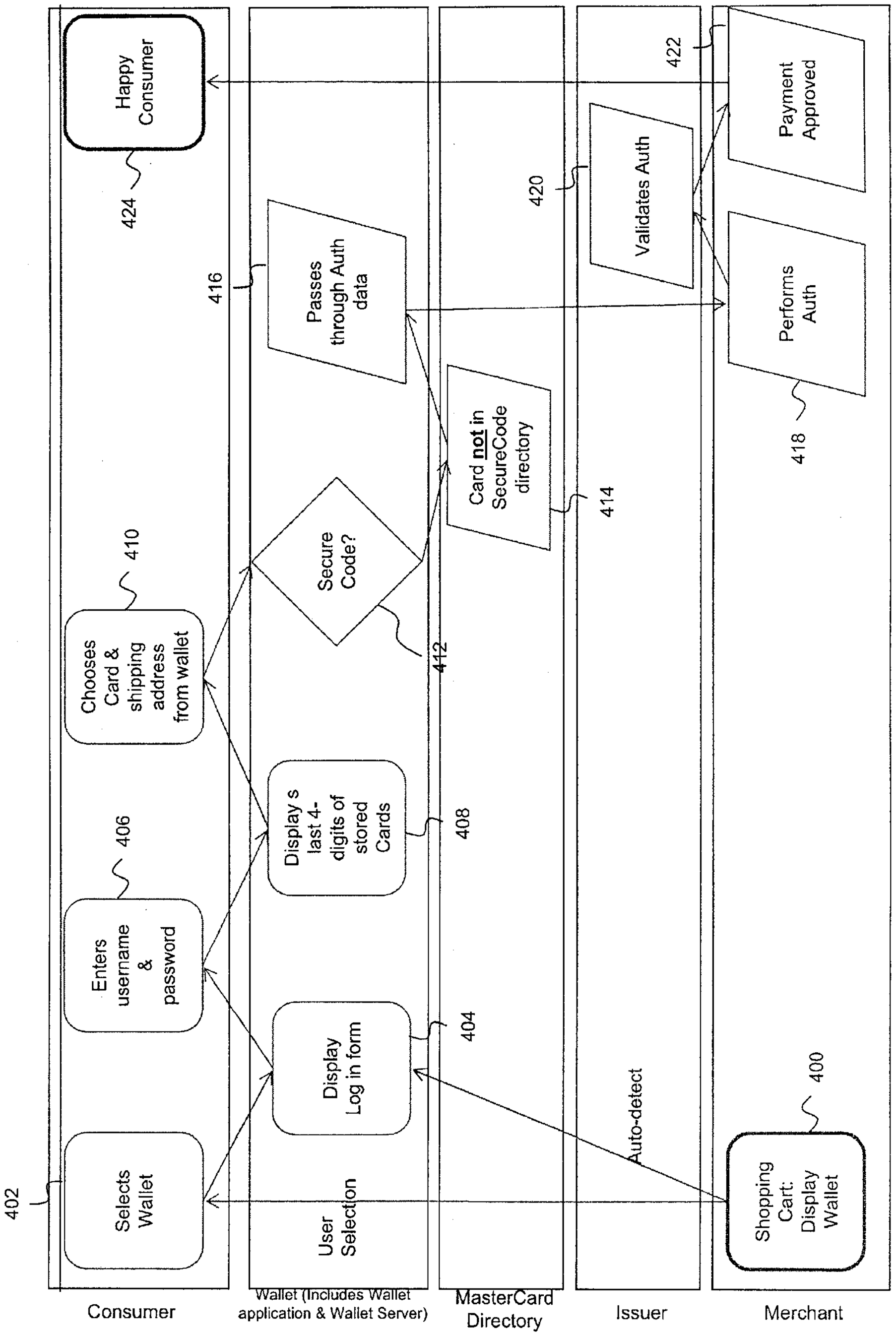
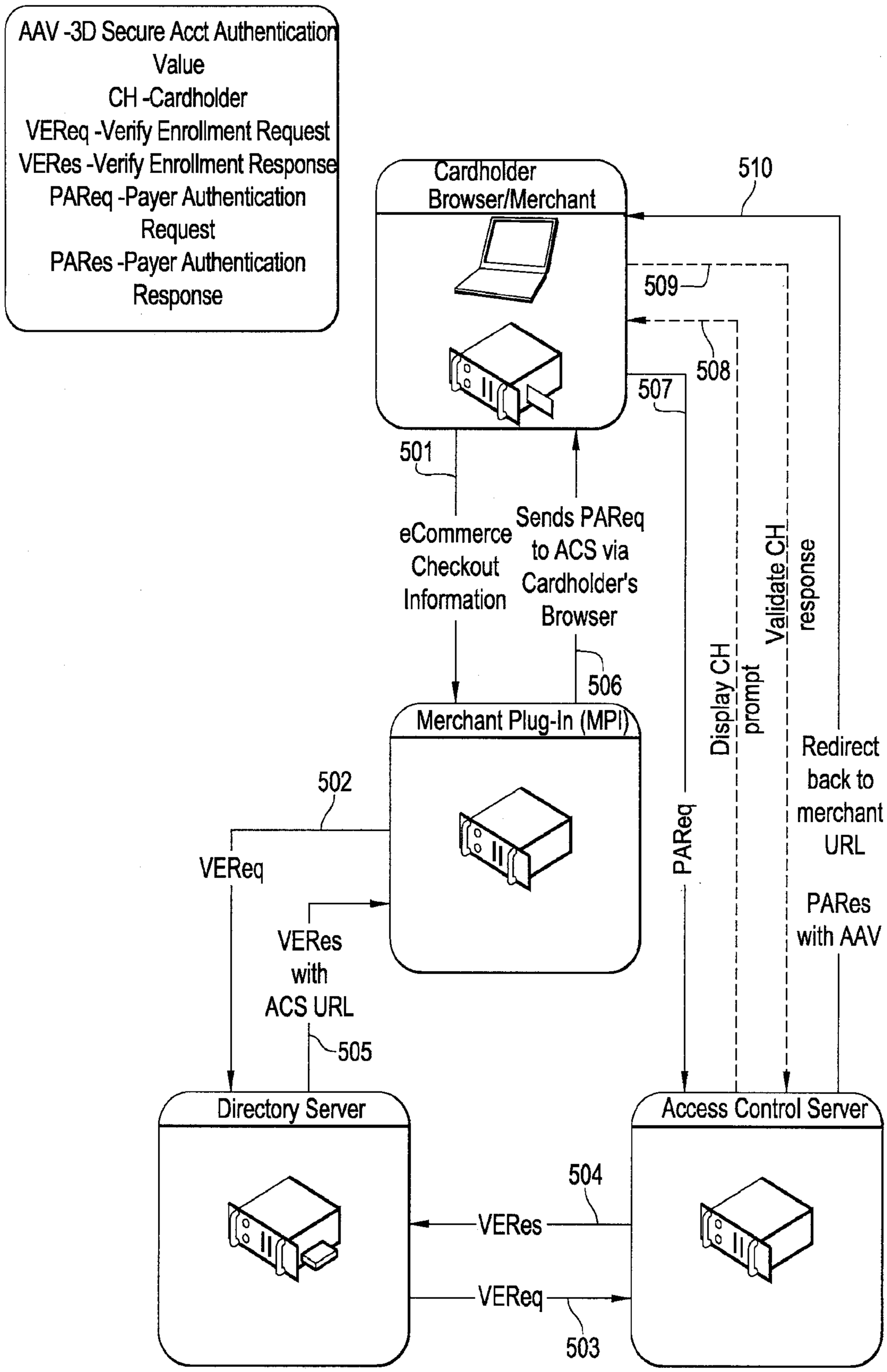

Consumer
Wallet (Includes Wallet application & Wallet Server)
MasterCard Directory
Issuer
Merchant
402
Selects Wallet
User Selection
Shopping Cart: Display Wallet
400
Auto-detect
Display Log in form
404
Enters username & password
406
Display s last 4-digits of stored Cards
408
Chooses Card & shipping address from wallet
410
Secure Code?
412
Card not in SecureCode directory
414
Passes through Auth data
416
Performs Auth
418
Validates Auth
420
Payment Approved
422
Happy Consumer
424

Fig. 5

AAV -3D Secure Acct Authentication Value
CH -Cardholder
VEReq -Verify Enrollment Request
VERes -Verify Enrollment Response
PAReq -Payer Authentication Request
PARes -Payer Authentication Response



Existing 3D Secure Implementation

FIG. 6

7/11

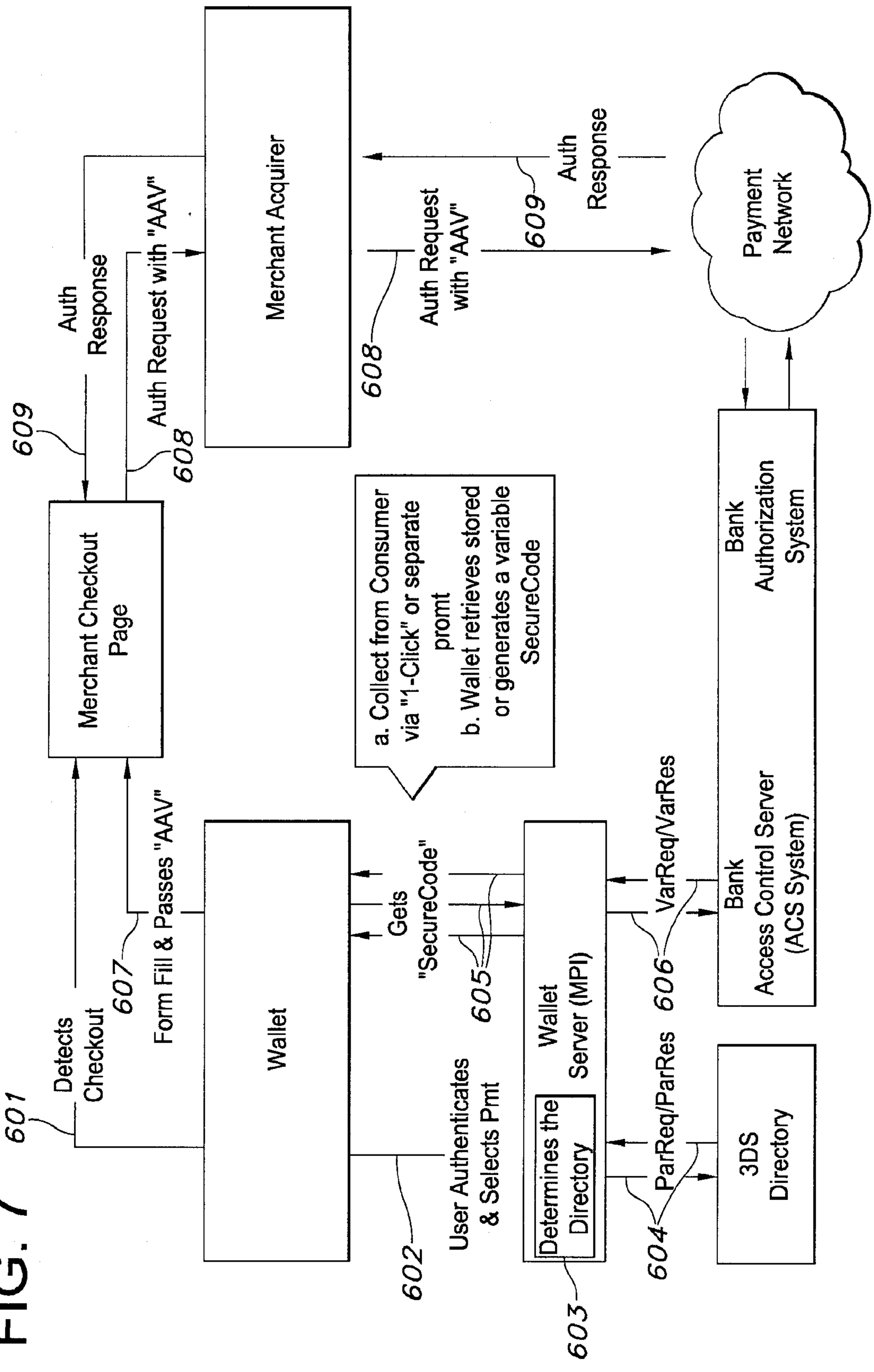
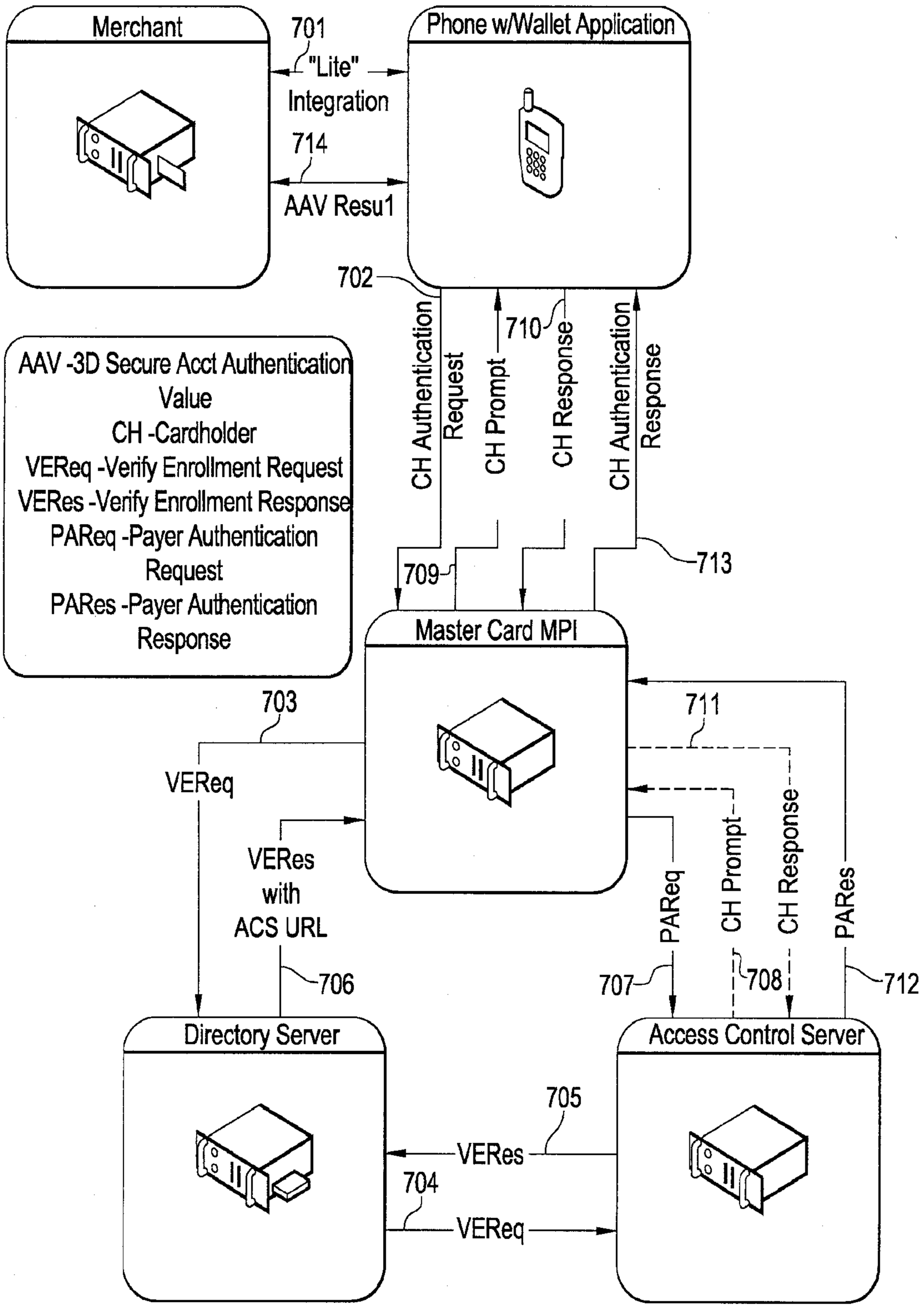

601
Detects Checkout
607
Form Fill & Passes "AAV"
602
Wallet
603
Determines the Directory
604
ParReq/ParRes
605
Gets "SecureCode"
606
VarReq/VarRes
608
Auth Request with "AAV"
609
Auth Response
Merchant Acquirer
Merchant Checkout Page
Bank Access Control Server (ACS System)
3DS Directory
Wallet Server (MPI)
Payment Network
Bank Authorization System
a. Collect from Consumer via "1-Click" or separate promt
b. Wallet retrieves stored or generates a variable SecureCode
User Authenticates & Selects Pmt

FIG. 7



MasterCard MPI Concept

FIG. 8

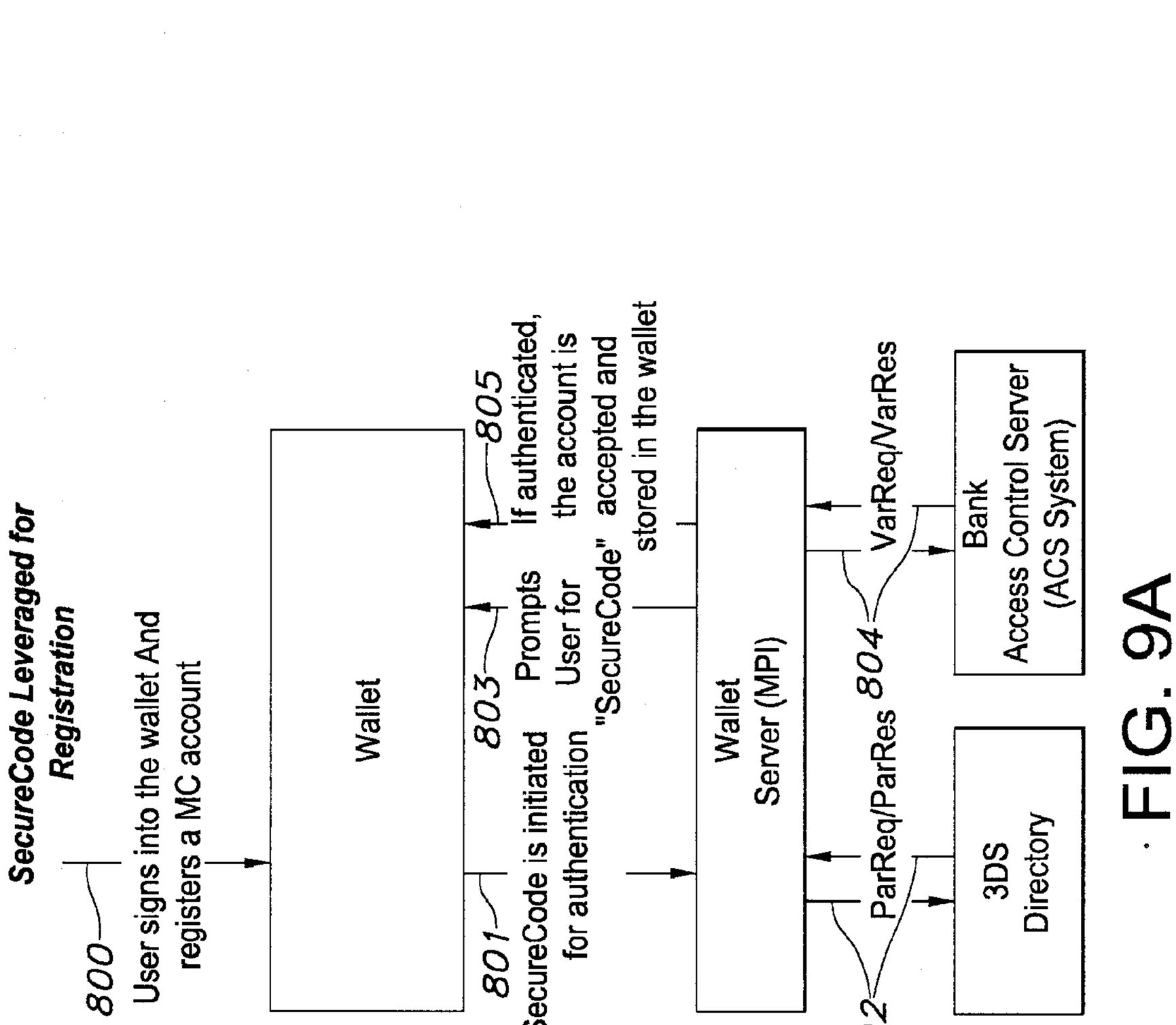

SecureCode Leveraged for Registration
800
User signs into the wallet And registers a MC account
Wallet
801
SecureCode is initiated for authentication
803
Prompts User for "SecureCode"
805
If authenticated, the account is accepted and stored in the wallet
Wallet Server (MPI)
802
ParReq/ParRes
804
VarReq/VarRes
3DS Directory
Bank
Access Control Server (ACS System)

FIG. 9A

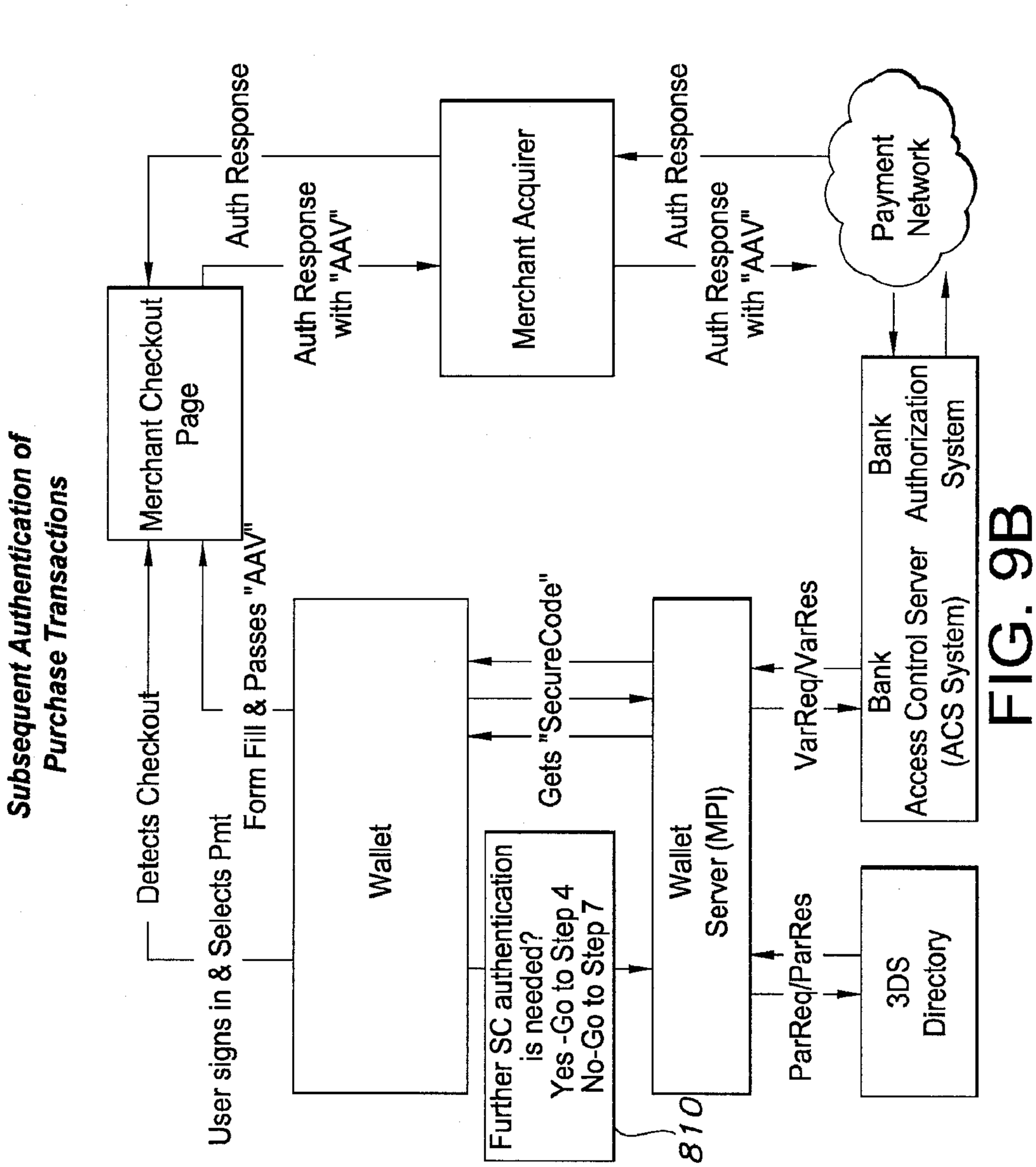

Subsequent Authentication of Purchase Transactions
Detects Checkout
User signs in & Selects Pmt
Merchant Checkout Page
Form Fill & Passes "AAV"
Auth Response
Auth Response with "AAV"
Wallet
Further SC authentication is needed?
Yes -Go to Step 4
No-Go to Step 7
Merchant Acquirer
Auth Response
Auth Response with "AAV"
Gets "SecureCode"
Wallet Server (MPI)
Payment Network
VarReq/VarRes
ParReq/ParRes
Bank Access Control Server (ACS System)
Bank Authorization System
3DS Directory
810

FIG. 9B

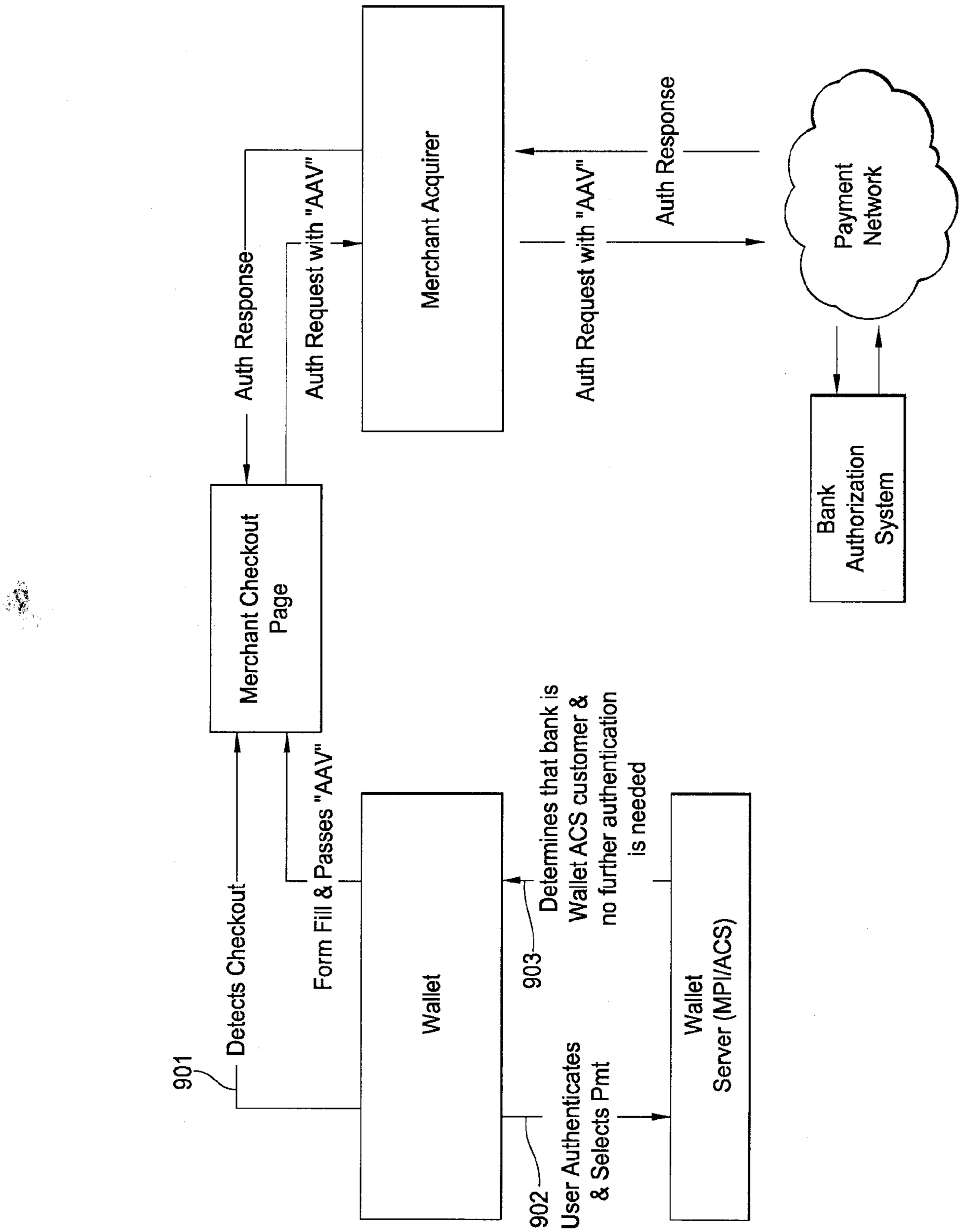
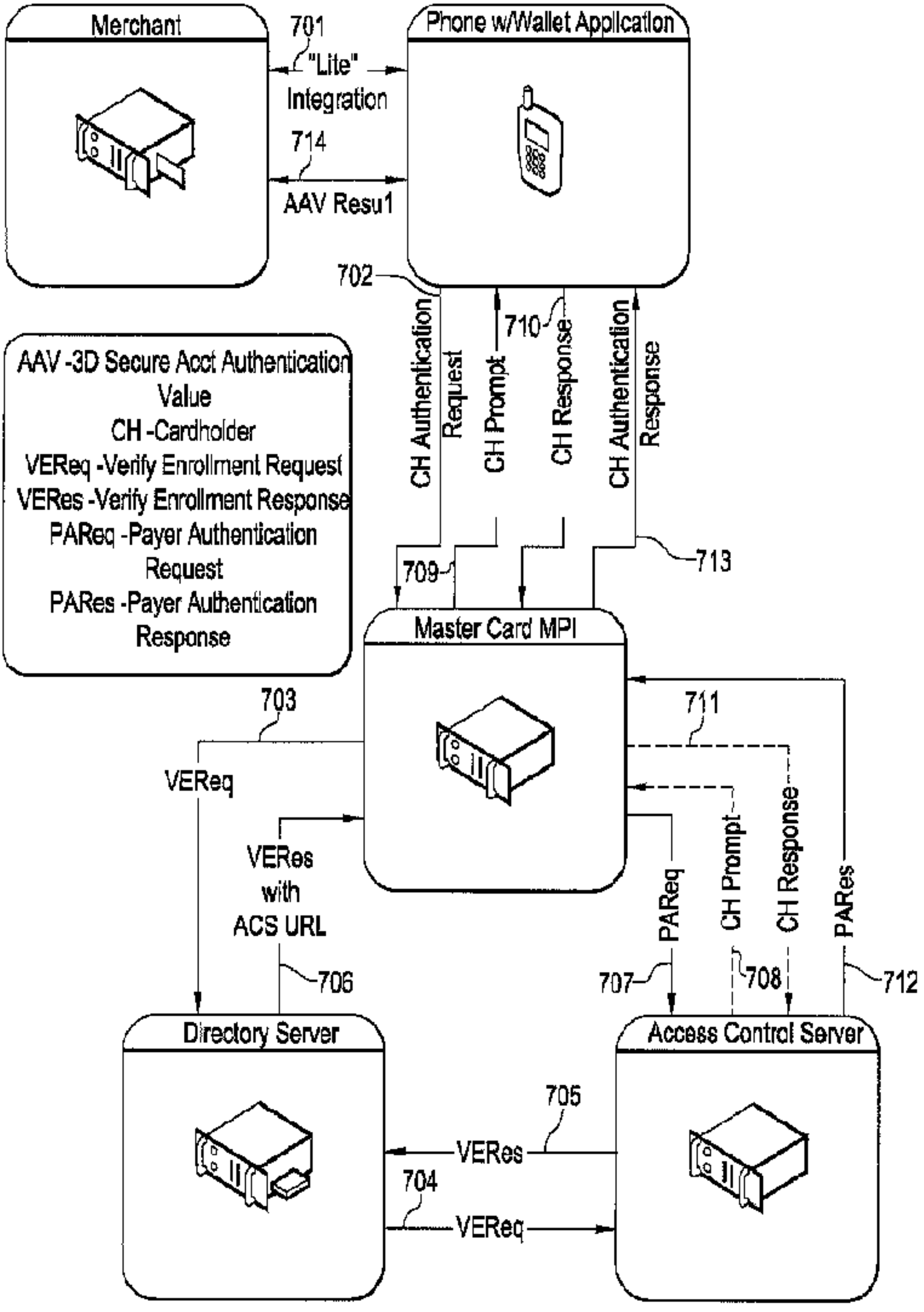

Merchant Checkout Page
Merchant Acquirer
Payment Network
Bank Authorization System
Auth Response
Auth Request with "AAV"
Auth Request with "AAV"
Auth Response
Wallet
Wallet Server (MPI/ACS)
901
Detects Checkout
Form Fill & Passes "AAV"
902
User Authenticates & Selects Pmt
903
Determines that bank is Wallet ACS customer & no further authentication is needed

FIG. 10



MasterCard MPI Concept