UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
61/619,095	04/02/2012		250	0076412-000057		

CONFIRMATION NO. 8494

FILING RECEIPT

OC000000053649757

21839
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

Date Mailed: 04/12/2012

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Simon E.J. PHILLIPS, York, UNITED KINGDOM;
Mehdi Collinge, Braine-l'Alleud, BELGIUM;

Power of Attorney:
Charles Wieland III--33096

If Required, Foreign Filing License Granted: 04/10/2012
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/619,095**
Projected Publication Date: None, application is not eligible for pre-grant publication
Non-Publication Request: No
Early Publication Request: No
Title

SYSTEM AND METHODS FOR PROCESSING MOBILE PAYMENTS FOR MOBILE DEVICES WITHOUT SECURE ELEMENTS

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

APPLICATION FOR
UNITED STATES LETTERS PATENT

FOR

SYSTEMS AND METHODS FOR PROCESSING MOBILE PAYMENTS FOR MOBILE DEVICES WITHOUT SECURE ELEMENTS

By

Simon Phillips

and

Mehdi Collinge

Attorney Docket No. 0076412-000057
BUCHANAN INGERSOLL & ROONEY PC
CUSTOMER NO. 21839
P.O. Box 1404
Alexandria, VA 22313-1404

Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

SYSTEMS AND METHODS FOR PROCESSING MOBILE PAYMENTS FOR MOBILE DEVICES WITHOUT SECURE ELEMENTS

FIELD OF THE DISCLOSURE

[0001] The present disclosure is directed to a method and system providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in the mobile device using in part a financial transaction card processing system or network as a part thereof.

BACKGROUND

[0002] Advances in mobile and communication technologies have created tremendous opportunities, one of which is providing users of mobile computing devices an ability to initiate payment transactions using their mobile device. One approach to enable mobile devices to conduct payment transactions is through the use of near field communication (NFC) technology to securely transmit payment information to a contactless terminal. To enable this, mobile phones with secure element hardware (i.e., a secure element chip) can be used to securely store payment account credentials, such as credit card credentials, have been used. Additionally, the use of mobile devices configured to operate with a PayPass® chip have been proposed. However, not all mobile phones have secure elements. Additionally, not all issuers, acquirers or merchants have host systems that can process chip data elements. As a result, a user who has an NFC-capable mobile device may not be able to use it as a payment device if their mobile device lacks a secure element (SE).

[0003] Accordingly, what are needed are systems and methods that provide technical solutions to allow mobile devices without an SE to complete contactless payments. What is further needed are systems and methods that allow mobile devices without an SE to complete mobile payments using a Cloud-based transaction data generation system which can authenticate and generate payment credentials (i.e., tokens) associated with one or more existing payment accounts, such as, but not limited to, a PayPass® account, so that the user can conduct PayPass® transactions at PayPass®-enabled merchants with a mobile device without having to use an SE and without requiring their acquirer or merchant to make significant changes to their host system(s).

SUMMARY

[0004] Methods and systems are disclosed for enabling payments via a mobile device, such as a smartphone, without requiring use of a secure element (SE) on the mobile device.

[0005] According to an embodiment, a set of processes deliver solutions for contactless payments, such as online transactions at a Point-of-Sale (POS), when using a mobile device but not requiring use or presence of an SE. One embodiment uses a combination of remote authentication and the provisioning of payment credentials to the mobile device for one transaction. In an alternative embodiment, remote authentication is performed and payment credentials are provisioned to a mobile device without an SE for a limited number of transactions.

[0006] In yet another embodiment, payments from mobile devices are processed using an available Trusted Execution Environment (TEE) and the TEE hosts services used during the authentication and payment processing in conjunction with a Mobile Authentication Application (MAA), without requiring use of an SE. Alternatively, payments can be processed when a TEE is not available using secure storage combined with camouflaging data by using a unique Mobile Device ID as a parameter along with the Personal Value.

[0007] According to an embodiment, a contactless payment process between a mobile device and a POS is processed as a standard payment transaction and does not require any update to transaction acquirer or merchant systems.

[0008] Certain exemplary embodiments provide a trusted environment for mobile authentication and/or mobile payment services even when mobile devices lacking or not using an SE are used to initiate payments. An exemplary embodiment disclosed herein uses a non-SE based solution to support mobile authentication by employing an MAA.

[0009] A high level flow for an exemplary embodiment of the process flow begins with provisioning of authentication credentials to a mobile device (i.e., at the edge of a payment processing network), which can subsequently be used for authentication based upon accessing locally stored credentials on the mobile device. Next, payment credentials are accessed from the Cloud (i.e., a Cloud-based transaction data generation system) so that remote identification and authentication can be performed based upon the credentials stored in the Cloud. Then, authentication is performed using an MAA. According to one embodiment, an MAA is a software implementation of MasterCard Authentication Solutions (i.e., two-factor authentication using a Chip Authentication Program (CAP) Token). As used herein, in an embodiment, the CAP Token can be conceptualized as a dynamic One-Time Password (OTP) that cannot be reused. Both CAP and PLA (person-less authentication) technologies use a CAP Token to support the authentication process. PLA technology is discussed in further detail in WIPO Published Application No. 2010/030362, published March 18, 2010, to Collinge et al., which is herein incorporated by reference in its entirety. CAP technology is discussed in further detail in WIPO Published Application No. 2005/001618, published January 6, 2005, to Rutherford et al., which is herein incorporated by reference in its entirety.

[0010] In accordance with another exemplary embodiment, mobile authentication and mobile payment services are implemented as an online-only solution wherein a CAP token is verified online by a CAP Token Validation Service (CTVS). According to this embodiment, a Personal Value, gesture, or passcode is used to retrieve a valid attribute, such as an AC_{CMK} key, which may be used to generate an Application Cryptogram (AC), from a secure container . The solution further includes a wrong key detection mechanism (as result of wrong Personal Value or passcode tries). In one embodiment, the wrong key detection is supported by an issuer (e.g., CAP Token validation failure). Advantageously, the solution does not persistently or permanently store any additional sensitive assets, such as a primary account number (PAN) in the MAA. In an embodiment, a PAN is not stored for authentication services, but some payment credentials are stored for a limited time, including track data. These payment credentials are protected using a storage key, but they contain PAN information. In one embodiment, a protocol is defined in

PAN information. In one embodiment, a protocol is defined in order to avoid any disclosure of complete AC values. Another advantage of solution is that it uses secure coding best practices (e.g., rules for management of sensitive assets such as a Personal Value and/or temporary values such as a generated AC).

[0011] In order to prevent cloning of camouflaged data, an embodiment uses a unique Mobile Device ID as a parameter along with the Personal Value.

[0012] As a consequence, the non-SE based solution disclosed herein can be used for mobile authentication services, including services that access payment credentials stored in the Cloud.

[0013] According to another exemplary embodiment, a solution provides architecture for completing a two-step process for remote authentication and remote payment. This solution overcomes the lack access to a trusted environment from a mobile device without impacting the security level of the architecture, even when payment credentials are stored in the MAA to support proximity payment when there is no connectivity to the Cloud (i.e., when a mobile device momentarily lacks Wi-Fi/ General packet radio service (GPRS) network connectivity).

[0014] Exemplary methods for provisioning payment account credentials from a Cloud-based system using a "mobile cloud account" to an NFC-enabled mobile device on behalf of an issuer are described in U.S. Provisional Application Serial No. 61/605,588 entitled "Systems and Methods For Mapping a Mobile Cloud Account to a Payment Account," filed on March 1, 2012, the disclosure of which is hereby incorporated by reference in its entirety.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Figure 1 is a diagram of an exemplary system in which a Mobile Authentication Application (MAA) can be used to process an electronic payment from a mobile device without requiring a secure element (SE), in accordance with an exemplary embodiment of the present disclosure.

[0016] Figure 2 is a storyboard depicting a provisioning process for downloading, installing, provisioning, activating and using a mobile payment application with a mobile computing device, in accordance with exemplary embodiments of the present disclosure.

[0017] Figure 3 is a diagram of a system illustrating a high level process flow between system components for completing a contactless payment from a mobile computing device without requiring an SE, in accordance with an exemplary embodiment of the present disclosure.

[0018] Figure 4 is a diagram depicting components of a system for completing a contactless payment from a mobile computing device without requiring an SE, in accordance with an exemplary embodiment of the present disclosure.

[0019] Figure 5 illustrates a process flow for provisioning payment credentials for a contactless payment, in accordance with an exemplary embodiment of the present disclosure.

[0020] Figure 6 illustrates a process flow for processing a contactless payment transaction, in accordance with an exemplary embodiment of the present disclosure.

[0021] Figure 7 illustrates a process flow for approving a contactless payment transaction, in accordance with an exemplary embodiment of the present disclosure.

[0022] Figure 8 is a detailed diagram of an exemplary system illustrating the process flow for completing a contactless payment from a mobile computing device without requiring an SE, in accordance with an exemplary embodiment of the present disclosure.

[0023] Figure 9 depicts an example computer system in which embodiments of the present invention may be implemented.

[0024] The features and advantages of the present disclosure will become more apparent from the detailed description set forth below when taken in conjunction with the drawings, in which like reference characters identify corresponding elements throughout. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. Generally, the drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

DETAILED DESCRIPTION

[0025] As used herein, "payment account", “credit card number" and "credit card" are sometimes used interchangeably. These terms mean a credit card, debit card, pre-paid card, hybrid card, plastic or virtual card number (VCN)(single use, limited use or simply virtual), or nearly any other account number that facilitates a financial transaction using a transaction clearance system. VCNs and pre-paid card numbers and other financial transaction card number that can be generally viewed as being more readily issued and disposed of because they do not require the establishment of a line of credit, and optionally can be linked to various controls (amounts, cumulative amounts, duration, controls on spending by amounts, cumulative amounts, types of merchants, geographic controls, to name a few). As used herein, these types of cards (VCN, pre-paid, etc.) are sometimes referred to as intelligent transaction card (ITC) numbers. As used herein, the term "payment account" is sometimes used interchangeably with a payment account number and means a credit card, the account number for a credit card, or any identifier that can be used to link a payment account to a purchase transaction initiated from a mobile device.

[0026] As used herein, the terms "user", "customer", “account holder”, "cardholder", and "card user" can be used interchangeably and can include any user making purchases of goods and/or services. Unless specifically stated differently or from context, in exemplary embodiments, a user may be interchangeably used herein to identify a human customer, a software application, or a group of customers and/or software applications executed by one or more consumers to conduct a purchase transaction. Besides a human customer who can purchase items using a mobile device, a software application can be used to process purchases. Accordingly, unless specifically stated, the terms "user", "customer", "cardholder", “account user” and "card user" as used herein do not necessarily pertain to a human being.

[0027] Further, as used herein, the term "issuer" can include, for example, a financial institution (e.g., bank) issuing a card, a merchant issuing a merchant specific card, a stand-in processor configured to act on-behalf of the card-issuer, or any other suitable institution configured to issue a financial card. Finally, as used herein, the term "transaction acquirer" can include, for example, a merchant, a merchant terminal, a point-of-sale (POS) terminal at a merchant, or any other suitable institution or device configured to initiate a financial transaction per the request of a customer.

[0028] Exemplary phone-based electronic wallets capable of providing authenticated transactions across multiple channels of commerce are described in U.S. Application No. 13/209,312, entitled "Multi-Commerce Channel Wallet for Authenticated Transactions," filed on August 12, 2011, which claims the benefit of U.S. Provisional Application Serial No. 61/372,955 filed August 12, 2010 and U.S. Provisional Application Serial No. 61/468,847 filed March 29, 2011, the disclosures of which are hereby incorporated by reference in their entireties.

[0029] Identification of PayPass® Magstripe transactions performed using the solution described below with reference to Figures 3-8 may require identification of a primary account number (PAN) using, for example, a specific range (and/or BIN). Examples of systems and methods for routing electronic transactions through financial processing systems (e.g., debit/credit networks) as a part of an electronic payment system are described in U.S. Application No. 13/078,374, entitled "Method for Performing Acquirer Routing and Priority Routing of Transactions," filed on April 1, 2011, which is incorporated herein by reference in its entirety.

I. Exemplary System Embodiment

[0030] Figure 1 is a block diagram of an exemplary system 100 for processing an electronic payment initiated by a mobile device without an SE, according to exemplary embodiments of the present disclosure. As implemented in the presently described exemplary embodiment, the system 100 depicted in Figure 1 includes a mobile device 104 without an SE, a point of sale (POS) terminal 181, a payment processor 103 (e.g., MasterCard) with a payment processing network 170 (e.g., MasterCard's Worldwide Network) that facilitates routing of mobile payment transactions for authorization, a mobile authentication application (MAA) 111, a transaction acquirer 166, and an issuer 180. As will be appreciated by those skilled in the relevant art(s), while the exemplary POS terminal 181 is depicted as a

MasterCard PayPass® terminal, other contactless POS terminals 181 with NFC capabilities can be used.

[0031] The system 100 performs authentication using the MAA 111. According to an embodiment, the MAA 111 is a software implementation of MasterCard Authentication Solutions (two-factor authentication using a CAP Token). A CAP Token Generation Service (CTGS) can be integrated in a mobile application to build a MasterCard Authentication Solution for mobile device 104 where the cardholder 113 uses the Mobile Authentication Application (MAA) to generate a CAP Token.

[0032] Although the MAA 111 is depicted in Figure 1 as being hosted by the mobile device 104, it is to be understood that in alternative embodiments, the MAA 111 can be hosted by the issuer 180 or a third party such as transaction processors. As used herein, in an embodiment, a transaction is distinguished from an authentication transaction, which is used to get access to payment credentials managed in the cloud-based transaction data generation system) and the payment transaction (i.e., a standard PayPass® Magstripe transaction). For example, it should be understood that the MAA 111 can alternatively be external to the payment processor 103. By way of example and not limitation, in one embodiment, the MAA 111 can reside on a computing device associated with the issuer 180. According to embodiments, generation of the CAP Token can be done by the MAA 111 component of the mobile payment application or might be done using another form factor. Examples of third party transaction processors that may host autilize the MAA 111 include, but are not limited to, outsourced transaction processors such as PrePaid Services (PPS), ElectraCard Services (ECS), First Data Resources (FDR), and providers of mobile wallet applications such as the MasterCard wallet. Examples of such mobile wallet applications capable of providing authenticated transactions across multiple channels of commerce are described in U.S. Application No. 13/209,312, entitled "Multi-Commerce Channel Wallet for Authenticated Transactions," filed on August 12, 2011, which claims the benefit of U.S. Provisional Application Serial No. 61/372,955 filed August 12, 2010 and U.S. Provisional Application Serial No. 61/468,847 filed March 29, 2011, the disclosures of which are hereby incorporated by reference in their entireties.

[0033] The system 100 allows a user 113 to use nearly any mobile computing device 104 having near field communications (NFC) capabilities to make purchases with a payment account, including, but not limited to, a Personal Digital Assistant (PDA), a tablet computing device, an iPhone^{TM}, an iPod^{TM}, an iPad^{TM}, a device operating the Android operating system (OS) from Google Inc., a device running the Microsoft Windows® Mobile OS, a device running the Microsoft Windows® Phone OS, a device running the Symbian OS, a device running the webOS from Hewlett Packard, Inc., a mobile phone, a BlackBerry® device, a smartphone, a hand held computer, a netbook computer, a palmtop computer, a laptop computer, an ultra-mobile PC, a portable gaming system, or another similar type of mobile computing device having a capability to make electronic purchases using a payment account (i.e., credit card).

[0034] With reference to Figure 1, the payment processor 103, provide various services and product offerings to support customers and vendors. In one embodiment, the payment processor 103 can use the MasterCard Internet Service, which includes the InControl™ product offering. Examples of such product offerings are described in U.S. Patent No. 6,315,193; U.S. Patent No. 6,793,131; U.S. Application No. 10/914,766, filed on August 9, 2004; U.S. Application No. 11/560,112, filed on November 15, 2006; U.S. Application No. 12/219,952, filed on July 30, 2008; and International Application No. PCT/US2009/002029, filed on September 19, 2009, U.S. Published Patent Applicaton No. 2009/0037333, filed on July 30, 2008, all incorporated herein by reference in their entirety (herein the controlled payment numbers or CPN Patents).

[0035] The communication links depicted in the system 100 between the various components can be through public and/or private networks or virtual private networks (e.g., the Internet and mobile networks particularly with respect to communications with mobile device 104, and private networks such as payment processing network 170).

[0036] As shown in Figure 1, system 100 processes the payment by user 113 at the POS terminal 181 using a standard process for the payment transaction using a transaction acquirer 166, a payment processor 103, and an issuer 180.

[0037] The processing for a payment in system 100 begins when a transaction is initiated by a user 113 with a mobile device 104 at a POS terminal 181. As illustrated in Figure 1, the mobile device 104 does not have a secure element (SE).

[0038] Authentication to the Cloud is performed within system 100 in order to retrieve an encrypted payload 112 from a cloud-based transaction data generation system 106 to the mobile device 104. The cloud-based transaction data generation system 106 comprises a transaction data generation service 108 that is configured to generate payment tokens and other data needed to complete purchases using the mobile device 104. As shown in Figure 1, the cloud-based transaction data generation system 106 further comprises key storage 110 for storing keys and encrypted information 113. In the exemplary embodiment of Figure 1, the encrypted information 113 has been encrypted using $K_{Storage}$ and includes Track 1 data, and/or Track 2 data. As shown in Figure 1 the encrypted payload 112 is provisioned to the mobile device 104 from the cloud-based transaction data generation system 106. The cloud-based transaction data generation system 106 also includes a payment credentials management system 114 and an authentication service 116. In the exemplary embodiment of Figure 1, the authentication service 116 is configured to perform CVTS CAP Token validation (CTVS) and can use a Chip Authentication Program (CAP) token for authentication.

[0039] As described below with reference to Figure 2, a cardholder (i.e., a user) 113 can provision a mobile payment application to the mobile device 104.

[0040] Next, an authorization request 168 is submitted. As shown in Figures 3-8, the encrypted payload 112 is not sent to the acquirer 166 or a merchant. The mobile payment application uses the content of the encrypted payload 112 to perform the PayPass® Magstripe transaction. This can be done using information from the a PayPass® reader, such as, but not limited to, an UN_{Reader}.

[0041] The acquirer 166 then routes authorization request 168 to a payment processing network 170 associated with the payment processor 103 (e.g., MasterCard).

[0042] Based on information contained in the authorization request 168, using at least the included content of the encrypted payload 112, payment credentials 174 are generated and provisioned to the MAA 111.

[0043] At this point, the payment process is done by the mobile payment application by using the payment credentials 174 in a payment credentials management system 114. As shown in Figure 1, it is to be understood that the payment credentials management system 114 can optionally be connected to the issuer 180.

[0044] The mobile payment application may generate a cryptogram. This cryptogram may be forwarded with the authorization request 168 to the acquirer 166. As shown in Figure 1, this can be further sent to the payment processing network 170. In an embodiment, the cryptogram 178 may be generated using key management services (i.e., through CVC3 validation, including dynamic CVC3 validation).

[0045] The payment processor 103 then routes an authorization request 168 based on the payment credentials 174 and the cryptogram 178 to the issuer 180 and the issuer 180 responds to the authorization request 168 with the authorization response 172.

[0046] In one embodiment, system 100 may include a connection 178 between the issuer 180 and a payment credentials management system 114.

[0047] After receiving the authorization response 172, the payment processor 103 forwards the authorization response 172 to the acquirer 166, which in turn routes the authorization response 172 back to the POS terminal 181.

II. Mobile Payment Application Provisioning Method

[0048] Figure 2 is a storyboard depicting a provisioning process for 200 downloading, installing, provisioning, activating, and using a mobile payment application with a mobile computing device 104, in accordance with exemplary embodiments of the present disclosure. Figure 2 is described with continued reference to the embodiment illustrated in Figure 1. However, Figure 2 is not limited to that embodiment.

[0049] In step 201 a user registration process is completed. As shown in Figure 2, this step can be accomplished using input supplied by a cardholder or user 113 via a GUI 202 of the user's 113 mobile device 104.

[0050] In step 203, the mobile payment application is downloaded and installed.

[0051] In step 205, authentication credentials associated with a payment card are provisioned to the mobile device 104.

[0052] In step 207, the mobile device 104 is authenticated to the Cloud-based transaction data generation system 106 in order to retrieve payment credential, such as, but not limited to tokens. As shown in Figure 2, this step comprises synchronization between the Cloud-based transaction data generation system 106 and the issuer 180 systems.

[0053] In step 209, the mobile payment application is activated. As shown in Figure 2, this step can be accomplished using a mobile payment application to activate a contactless interface in order to enable a contactless payment using the mobile device 104 to make a payment at a POS terminal 181. For example, step 209 can comprise activating an NFC interface using the mobile payment application. Payment credentials, such as, but not limited to tokens, can then be redeemed at the POS terminal 181 to make a payment using the mobile payment application. In this step, the Cloud-based transaction data generation system 106 looks at credentials/transaction tokens stored in a mobile device 104 (i.e., the smart phone depicted in Figure 2).

[0054] In step 211, the mobile device 104 is ready for a subsequent, next payment (i.e., by repeating step 209, or can be used to retrieve additional payment credentials by returning control to step 207.

[0055] Exemplary processes for authentication, payment, and synchronization are described below.

[0056] Authentication Process

The principles for the authentication process (Mobile to Cloud) are:

1. Integrate MasterCard MAA solution (with a CAP Token) in the SE-less Mobile Payment Application to generate a CAP Token to support the authentication process.

2. Any use of MAA assumes the availability of a process to install the MAA component and provision it with a Virtual Card Profile used for authentication purposes. The Virtual Card Profile is associated with a Payment Card (Payment Credentials).
3. Access control must be defined to grant access to the assets of MAA (e.g. protected using some mechanisms such as camouflage). Online PIN value cannot be used to grant access to MAA and the generation of a valid CAP Token. A gesture or a password must be used instead.
4. If the validation of the CAP Token is successful, the Cloud generates the CVC3 value using a genuine KD_{CVC3} and returns an encrypted payload to the Mobile Payment Application.
5. If the validation of the CAP Token is NOT successful, the Cloud generates CVC3 using a 'fake' KD_{CVC3} and returns an encrypted payload to the Mobile Payment Application. At the same time an alarm is triggered to the Issuer.

Synchronization Process

The principles for the synchronization process (Cloud to Issuer) are:

1. The $Cloud\_CVC3_{TRACK 1/2}$ generation is managed in the Cloud. This encompasses the generation of KS_{UN} and UN_{CLOUD}, and the ATC management.
2. (KS_{UN}, $Cloud\_CVC3_{TRACK 1/2}$ and ATC) are returned using an encrypted Payload to the Mobile Payment Application.
3. (UN_{CLOUD} and ATC) [Including optionally some status information] are sent to the Issuer.
4. The Issuer has a means (e.g. Using PAN or information available in the Payment Transaction) to identify transactions that require additional processing for the retrieval of the UN_{CLOUD} and KS_{UN} values using the ATC value provided in that Payment Transaction.

Payment Process

The principles for the payment process (Mobile to Cloud) are:

1. The Mobile Payment Application must have retrieved at least one (KS_{UN}, $Cloud\_CVC3_{TRACK 1/2}$, ATC) before the Tap.

2. The dynamic values (CVC3 and ATC) are used as a first form factor to authenticate the payment transaction. The Online PIN can be used as a second form factor.

III. Exemplary Authentication and Transaction Process Flows

[0057] Figures 3-8 are diagrams of the system 100 illustrating data flows for authentication and transactions used to process contactless payments from a mobile computing device without requiring an SE. Figures 3-8 depict varying levels of detail for data and process flows for contactless payments that do not require use of an SE. Figures 3-8 are is described with continued reference to the embodiments illustrated in Figures 1 and 2. However, Figures 3-8 are not limited to those embodiments.

[0058] As shown in Figure 3, authentication to the Cloud-based transaction data generation system 106 is performed to retrieve the payment credentials 174.

[0059] System 100 includes an authentication module configured to perform authentication of a user 113 based on information the user 113 knows. In embodiments, the authentication module can use a user ID or account number in conjunction with other information the user 113 knows, such as passcode, gesture or other suitable Personal Value.

[0060] After the authentication module 202 authenticates the user 113, the user 113, who in the exemplary embodiment of system 100 is depicted as a cardholder, initiates shopping by making a selection 304 of one or more items to place in a shopping cart 306. As would be understood by persons skilled in the relevant art, selection 304 and shopping cart 306 can be performed at 'brick and mortar' merchants at a POS, with payments for items in shopping cart 306 being made via a proximity payment. As shown in FIG. 3, the system 100 routes a payment request 307 to the merchant's POS terminal 181.

[0061] Exemplary data flow stages depicted in Figures 5-7 are described in Table 1 below.

Table 1

Stage	Description
A1	The solution can support several levels of authentication: • The Access to the Mobile Device (e.g. Device Locking mechanism) • The Access to the Mobile Payment Application • The Access to the Cloud System
A2	The Authentication component (using MAA technology) has to be provisioned
B	At time of the authentication credentials provisioning, a storage key is also stored in the Mobile Payment Application. This key is used to protect the static payment credentials and the transport of the payload from the Cloud to the Mobile Payment Application
C	At time of the authentication credentials provisioning, static payment credentials are also provisioned
1	The Cardholder uses a SE-less Mobile *PayPass* Payment Application
2a	The Cardholder connects to the Cloud to retrieve Payment credentials
2b	The Cardholder uses the MAA component of the Mobile Payment Application to generate a CAP Token for the authentication transaction. The Cardholder has to supply some credentials (e.g. A gesture, a password…)
3	Mobile Payment Application sends a CAP Token to the Cloud
4	The Payment System (in the Cloud) validates the CAP Token using a CAP Token Validation Service (CTVS). The Payment System can be operated by MasterCard or by the Issuer.
5	The CTVS validates the CAP Token. The CTVS can be operated by MasterCard or by the Issuer.

Table 1

Stage	Description
6	The result of the CAP Token validation is sent to the Payment Credentials Management System. The Payment Credentials Management System can be operated by MasterCard or by the Issuer.
7	Upon successful authentication, a genuine KD_{CVC3} is used and (KS_{UN}, Cloud_CVC3$_{TRACK1/2}$, ATC) is returned. Upon unsuccessful authentication, a fake KD_{CVC3} key is used and (KS_{UN}, Cloud_CVC3$_{TRACK1/2}$, ATC) is returned and an alarm is triggered.
8a	There is synchronization process between the Cloud and the Issuer. The synchronization process may include the definition of rules for the validity of the generated CVC3 values.
8b	(KS_{UN}, Cloud_CVC3$_{TRACK1/2}$, ATC) is returned to the front-end of the Cloud system for delivery to the Mobile Payment Application.
9	(KS_{UN}, Cloud_CVC3$_{TRACK1/2}$, ATC) is returned to the Mobile Payment Application. This can encompass additional payment assets.
10	(KS_{UN}, Cloud_CVC3$_{TRACK1/2}$, ATC) and the additional assets are stored. The Mobile Payment Application is ready to support a *PayPass* Magstripe Payment using a Mobile Device
11	Standard shopping experience.
12	Standard *PayPass* Magstripe payment experience using a Mobile Device. The Mobile Payment Application use a specific process to generate the CVC3 using (KS_{UN}, Cloud_CVC3$_{TRACK1/2}$, ATC and UN_{READER})

Table 1

Stage	Description
13	The Cardholder may need to enter the Online PIN at the POS (using a PED).
14	The *PayPass* Terminal executes the standard payment transaction process.
15	A standard payment transaction authorization message is used. It contains the UN from the *PayPass* Reader ([Partial Info] UN_{READER}), the CVC3 and the ATC [Partial Info] provided by the Mobile Payment Application. It contains the PIN Block when Online PIN is used.
16	A standard Online PIN translation process can take place between the Acquiring environment and the Issuing environment.
17	The standard processes are used for the Payment Transaction.
18	The standard Online PIN verification process applies (if applicable)
19a	The Issuer has a mean to identify transaction that requires additional processing for CVC3 validation when the solution using SE-less Mobile Contactless Payment is used. Using the ATC provided in the Payment Transaction, the Issuer is able to retrieve the UN_{CLOUD} and KS_{UN} values that were used by the Payment Credential Management System to generate the CVC3 value. Detection of unsuccessful authentication can also take place at this stage.
19b	A standard process applies for the CVC3 validation using the UN_{CLOUD} and KS_{UN} values.
20	The completion of the Payment transaction process remains unchanged.

[0062] As shown in Figures 3-8, generation of the payment credentials 174 and provisioning of the payment credentials 174 to the MAA 111 is then performed. In system 100, this can be accomplished by using AC for an authentication process and using the CVC3 keys 118 for a payment process. System 100 can obtain authentication keys 118, CVC3 keys 403, and payment credentials 174 from a cloud-based transaction data generation system 106 and provisioning the retrieved payment credentials 174 to the MAA 111. The mobile device 104 can then complete transmission 308 to return the CVC3 values (Track 1 and Track 2) to the POS terminal 181 as part of a payment transaction for the selections 304 in shopping cart 306.

[0063] Payment at the POS terminal 181 then occurs using a standard process for payment transaction. For example the transaction acquisition processing by a transaction acquirer 166, payment processor 103, and issuer 180 can be carried out as described above with reference to Figure 1.

[0064] In the exemplary embodiments of Figures 6-8, an authorization request 168 can be routed from the POS terminal 181 to the acquirer 166, wherein the authorization request 168 includes DExx CVC3 track data 610 to facilitate payment between the POS terminal 181 and the acquirer 166 or a bank. In an embodiment, the track data DExx CVC3 610 can be DE35/DE45 (CVC3) track 2 or track 1 data. According to an embodiment Track 2 Data (DE 35) comprises information encoded on track 2 of a payment card's magnetic stripe as defined in ISO 7813, including field separators, but excludes beginning and ending sentinels and Longitudinal Redundancy Check (LRC) characters. In an embodiment, Track 1 Data (DE 45) includes information encoded on track 1 of a bankcard's magnetic stripe as defined in ISO 7813, including field separators. However, this excludes beginning and ending sentinels and LRC characters.

[0065] As discussed above with reference to Figure 1 and shown in Figures 3-8, the system 100 can be configured to make use of an connection 178 between the issuer 180 and the payment credentials management system 114. As also shown in Figures 3-8, the issuer 180 in system 100 accesses the CVC3 keys 203.

[0066] The payment credentials management system 114 may manage the CVC3 keys 403. As shown in Figure 5, the authentication service 512 in system 100 may be a CAP Token Validation Service (CTVS).

[0067] Upon completion of the authorization, the issuer 180 will respond back to the payment processor 103 (e.g., MasterCard) as described above with reference to Figure 1.

[0068] Exemplary solutions and embodiments disclosed herein can incorporate several core principles outlined below:

- ➢ Storage Key ($K_{Storage}$) defined at time of authentication profile and static Payment credentials provisioning
- ➢ Authentication credentials protected using MAA rules (e.g. Key Camouflage) (**Not** using $K_{Storage}$)

- ➢ SSL Layer between Mobile Payment Application and Cloud System
    - o Server Authentication using SSL
    - o Client Authentication using CAP Token

  Additional Storage Key used to counter Man-in-the-Middle attack (eavesdropping) at time of Payment Credentials provisioning from the Cloud to the Mobile Payment Application

- ➢ Authentication process between Mobile and Cloud to retrieve credentials
    - o Identification (~ Virtual Card Profile ID (which may be any identifier defined by the Issuer and known by the Cardholder (e.g. Masked PAN…))
    - o Authentication Transaction (e.g. Challenge / Response)
- ➢ CTVS validation
    - o Successful > Use valid IMK_{CVC3} & IMK_{UN}
    - o Failed > Use fake IMK_{CVC3} & IMK_{UN}

- ➢ The values KD_{CVC3} and $IVCVC3_{Track1/2}$ are static (if one considers a given PAN (and PSN) value, the values KDCVC3 and IVCVC3Track1/2 remain the same during the entire lifespan of the card. Those values are static. It also means that once the value is disclosed, you can reuse it.) for a given PAN (and PSN). The PSN (if available) can be part of the KDCVC3 derivation process. This avoids mandating any change regarding the management of this value at issuer level even if the PSN may be used to identify a SE-less 'virtual card' defined for a given PAN.

- The $CVC3_{Track1/2}$ is a dynamic data for a given *PayPass* Transaction (UN, ATC, $IVCVC3_{Track1/2}$ and KD_{CVC3})
- Key derivation process in the Cloud (KD_{CVC3} + KD_{UN})
- Session key generation (KS_{UN}) in the Cloud to bind (ATC, UN_{CLOUD}, PAN and PSN) at the Edge (Mobile Payment Application)
- 'CVC3' generation in the Cloud (Using UN_{CLOUD}) >> $Cloud\_CVC3_{TRACK1/2}$
- Delivery of Encrypted Payload [using $K_{Storage}$] (KS_{UN}, $Cloud\_CVC3_{TRACK1/2}$ and ATC) to Mobile Payment Application

- CVC3 generation in the Mobile (Using UN_{READER} , KS_{UN}, $Cloud\_CVC3_{TRACK1/2}$ and ATC)

Crypto

KD_{CVC3}

[0069] Concatenate from left to right the **PAN** (without any 'F' padding) with the **PSN** (if the PAN sequence number is not available, then it is replaced by a '00' byte). .

[0070] If the result X is less than 16 digits long, pad it to the left with hexadecimal zeros in order to obtain an eight-byte number Y in numeric (n) format. .

[0071] If X is at least 16 digits long, then Y consists of the 16 rightmost digits of X in numeric (n) format.

Generate KD_{CVC3} using:

$Z_L := DES3(IMK_{CVC3})[Y]$

$Z_R := DES3(IMK_{CVC3})[Y \oplus (\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'})]$

$KD_{CVC3} := (Z_L \,||\, Z_R)$

This key is kept in the Cloud/Issuer (No disclosure to Mobile Payment Application)

KD_{UN}

Reuse Value Y as defined above

Generate KD_{UN} using:

$Z_L := DES3(IMK_{UN})[Y]$

$Z_R := DES3(IMK_{UN})[Y \oplus (\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'})]$

$KD_{UN} := (Z_L \ || \ Z_R)$

This key is disclosed to the Mobile Payment Application (Some protection mechanisms can apply - e.g. Camouflage)

$IVCVC3_{TRACK1/2}$

$IVCVC3_{TRACK1}$ is a MAC calculated over the Track 1 Data using KD_{CVC3}

$IVCVC3_{TRACK2}$ is a MAC calculated over the Track 2 Data using KD_{CVC3}

Those values are kept in the Cloud/Issuer (No disclosure to Mobile Payment Application)

$Cloud\_CVC3_{TRACK1/2}$

1. Concatenate the following data to obtain an 8 byte data block (D):
   - $IVCVC3_{TRACK1/2}$ (2 bytes)
   - UN_{CLOUD} (4 bytes)
   - ATC (2 bytes)

2. Calculate O as follows:
   $O := DES3(KD_{CVC3})[D]$

The two least significant bytes of O are the $CVC3_{TRACK1/2}$

$CVC3_{TRACK1/2}$ generated in the Cloud are called $Cloud\_CVC3_{TRACK1/2}$

UN_{CLOUD} is **not** sent to the Mobile device.

UN_{CLOUD} is part of the payload exchanged between the Cloud and the Issuer.

KS_{UN}

Generate KS_{UN} using:

U_L := DES3(KD_{UN})[(ATC || 'F0' || '00' || UN_{CLOUD})]

U_R := DES3(KD_{UN})[(ATC || '0F' || '00' || UN_{CLOUD})]

KS_{UN} := (U_L || U_R)

(Static) Information known by the Mobile Payment Application

- ◊ FCI (PPSE)
- ◊ AID (Application Identifier)
- ◊ FCI (File Control Information)
- ◊ AFL (Application File Locator)
- ◊ AIP (Application Interchange Profile)
- ◊ AVN (Application Version Number)
- ◊ Encrypted (using $K_{Storage}$) Payment Credentials provisioned at time of authentication credentials provisioning. The Issuer should implement segregation rules in order to prevent any use of leaked static payment credentials for CNP transactions (e.g. Misuse PAN for eCommerce / MOTO transactions).
    - o Track 1 Data
    - o Track 2 Data
    - o $PCVC3_{TRACK1/2}$
    - o $PUNATC_{TRACK1/2}$
    - o $NATC_{TRACK1/2}$

Encrypted (using $K_{Storage}$) Payload sent to the Mobile Payment Application (Valid for one contactless payment transaction)

◊ Cloud_CVC3$_{TRACK1/2}$

◊ ATC

◊ KS_{UN}

Payload sent to the Issuer

◊ Identifier (PAN…)

◊ UN_{CLOUD}

◊ ATC

◊ Authentication Status Info + Additional Generation Information (e.g. Validity)

CVC3$_{TRACK1/2}$

Mobile Payment Application to perform CVC3 generation using:

◊ Information from the Reader

◊ Stored Information

◊ Credentials previously retrieved from the Cloud

CVC3 value to be included in Payment Authorization message (Track 2 (and Track 1) information).

UN_{READER} (4 bytes) >> Discard all but PUNATC-NATC least significant digits, padding to 8 digits with 0's.

1. Concatenate the following data to obtain an 8 byte data block (M):
   - Cloud_CVC3$_{TRACK1/2}$ (2 bytes)
   - UN_{READER} (4 bytes)
   - ATC (2 bytes)
2. Calculate T as follows:

   T := DES3(KS_{UN})[M]

The two least significant bytes of T are the $\text{CVC3}_{\text{TRACK1/2}}$

Note:

◊ $\text{Cloud\_CVC3}_{\text{TRACK1/2}}$ (2 bytes) is used instead of $\text{IVCVC3}_{\text{TRACK1/2}}$ (2 bytes)

◊ KS_{UN} is used instead of KD_{CVC3}

◊ Binding between $\text{UN}_{\text{READER}}$ and UN_{CLOUD} is implicitly done using the crypto (KS_{UN})

[0072] Issuer Validation Process

[0073] An exemplary validation process is described below wherein the Issuer 180 uses the information provided in the payment transaction:

- Identifier – e.g. PAN Information
- $\text{UN}_{\text{READER}}$ (4 bytes) – Partial Information retrieved from Track data (Discretionary Information)
- ATC (2 bytes) – Partial Information retrieved from Track data (Discretionary Information)
- $\text{CVC3}_{\text{TRACK1/2}}$ – Partial Information retrieved from Track data (Discretionary Information)

[0074] A The Identifier & ATC values are used to retrieve the information provided by the Cloud system:

◊ Identifier (PAN,...)

◊ UN_{CLOUD}

◊ ATC

◊ Authentication Status Info + Additional Generation Information (e.g. Validity)

The Issuer system is able to compute **$\text{Cloud\_CVC3}_{\text{TRACK1/2}}$** using:

◊ $\text{IVCVC3}_{\text{TRACK1/2}}$ (2 bytes)

◊ UN_{CLOUD} (4 bytes)

◊ ATC (2 bytes)

The Issuer system is able to compute $CVC3_{TRACK1/2}$ using:

◊ Cloud_$CVC3_{TRACK1/2}$ (2 bytes)

◊ UN_{READER} (4 bytes)

◊ ATC (2 bytes)

The Issuer can validate the $CVC3_{TRACK1/2}$.

[0075] A Glossary of terms and acronyms described above and depicted in Figures 3-8 is provided in Table 2 below:

Table 2

Stage	Description
⊕	XOR Operator
||	Concatenation Operator
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
ATC	Application Transaction Counter
AVN	Application Version Number
CAP	Chip Authentication Program
CNP	Card Not Present
CVC	Card Validation Code
CVC3	Dynamic CVC
DE	Data Element
DES	Data Encryption Standard
DES3	Triple DES
FCI	File Control Information
IMK	Issuer Master Key

Table 2

Stage	Description
⊕	XOR Operator
||	Concatenation Operator
IV	Initial Vector
KD	Derived Key
KS	Session Key
MAA	MasterCard Authentication Application
MAC	Message Authentication Code
NFC	Near Field Communication
PAN	Primary Account Number
PED	PIN Entry Device
PIN	Personal Identification Number
POS	Point of Sale
PPSE	Proximity Payment System Environment
PSN	PAN Sequence Number
SE	Secure Element
UN	Unpredictable Number

IV. Exemplary Computer System Implementation

[0076] As would be appreciated by someone skilled in the relevant art(s) and described below with reference to Figure 9, part or all of one or more aspects of the methods and apparatus discussed herein may be distributed as an article of manufacture that itself comprises a computer readable medium having computer readable code means embodied thereon. The computer readable program code means is operable, in conjunction with a computer system, to carry out all or some of the steps to perform the methods or create the apparatuses discussed herein. The computer readable medium may be a recordable medium (e.g., hard drives, compact disks, EEPROMs, or memory cards). Any tangible medium known or developed that can store information suitable for use with a computer system may be used. The computer-readable code means is any mechanism for allowing a computer to read instructions and data, such as magnetic variations on a magnetic media or optical characteristic variations on the surface of a compact disk. The medium can be distributed on multiple physical devices (or over multiple networks). For example, one device could be a physical memory media associated with a terminal and another device could be a physical memory media associated with a processing center.

[0077] The computer systems and servers described herein each contain a memory that will configure associated processors to implement the methods, steps, and functions disclosed herein. Such methods, steps, and functions can be carried out, e.g., by processing capability on mobile device 104, POS terminal 181, payment processor 103, acquirer 166, issuer 180, or by any combination of the foregoing. The memories could be distributed or local and the processors could be distributed or singular. The memories could be implemented as an electrical, magnetic or optical memory, or any combination of these or other types of storage devices. Moreover, the term "memory" should be construed broadly enough to encompass any information able to be read from or written to an address in the addressable space accessed by an associated processor.

[0078] Aspects of the present disclosure shown in Figures 1-8, or any part(s) or function(s) thereof, may be implemented using hardware, software modules, firmware, tangible computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems.

[0079] Figure 9 illustrates an example computer system 900 in which embodiments of the present disclosure, or portions thereof, may be implemented as computer-readable code. For example, systems 100 and 300 of Figures 1 and 3-8, and methods and GUI 202 depicted in Figure 2 can be implemented in computer system 900 using hardware, software, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Hardware, software, or any combination of such may embody any of the modules and components used to implement the systems and methods described above with reference to Figures 1-8.

[0080] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. One of ordinary skill in the art may appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device.

[0081] For instance, at least one processor device and a memory may be used to implement the above described embodiments. A processor device may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor "cores."

[0082] Various embodiments of the present disclosure are described in terms of this example computer system 900. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the present disclosure using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0083] The processor device 904 may be a special purpose or a general purpose processor device. As will be appreciated by persons skilled in the relevant art, processor device 904 may also be a single processor in a multi-core/multiprocessor system, such system operating alone, or in a cluster of computing devices operating in a cluster or server farm. Processor device 904 is connected to a communication infrastructure 906, for example, a bus, message queue, network, or multi-core message-passing scheme.

[0084] The computer system 900 also includes a main memory 908, for example, random access memory (RAM), and may also include a secondary memory 910. Secondary memory 910 may include, for example, a hard disk drive 912, removable storage drive 914. Removable storage drive 914 may comprise a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, or the like.

[0085] The removable storage drive 914 reads from and/or writes to a removable storage unit 918 in a well-known manner. The removable storage unit 918 may comprise a floppy disk, magnetic tape, optical disk, etc. which is read by and written to by removable storage drive 914. As will be appreciated by persons skilled in the relevant art, the removable storage unit 918 includes a non-transitory computer usable storage medium having stored therein computer software and/or data.

[0086] In alternative implementations, the secondary memory 910 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 900. Such means may include, for example, a removable storage unit 922 and an interface 920. Examples of such means may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an EPROM, or PROM) and associated socket, and other removable storage units 922 and interfaces 920 which allow software and data to be transferred from the removable storage unit 922 to computer system 900.

[0087] The computer system 900 may also include a communications interface 924. The communications interface 924 allows software and data to be transferred between the computer system 900 and external devices. The communications interface 924 may include a modem, a network interface (such as an Ethernet card), a communications port, a PCMCIA slot and card, or the like. Software and data transferred via the communications interface 924 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals capable of being received by communications interface 924. These signals may be provided to the communications interface 924 via a communications path 926. The communications path 926 carries signals and may be implemented using wire or cable, fiber optics, a phone line, a cellular/wireless phone link, an RF link or other communications channels.

[0088] In this document, the terms "computer program medium," "non-transitory computer readable medium," and "computer usable medium" are used to generally refer to tangible media such as removable storage unit 918, removable storage unit 922, and a hard disk installed in hard disk drive 912. Signals carried over the communications path 926 can also embody the logic described herein. The computer program medium and computer usable medium can also refer to memories, such as main memory 908 and secondary memory 910, which can be memory semiconductors (e.g. DRAMs, etc.). These computer program products are means for providing software to computer system 900.

[0089] Computer programs (also called computer control logic and software) are generally stored in a main memory 908 and/or secondary memory 910. The computer programs may also be received via a communications interface 924. Such computer programs, when executed, enable computer system 900 to become a specific purpose computer able to implement the present disclosure as discussed herein. In particular, the computer programs, when executed, enable the processor device 904 to implement the processes of the present disclosure, such as the method illustrated by Figure 2, discussed above. Accordingly, such computer programs represent controllers of the computer system 900. Where the present disclosure is implemented using software, the software may be stored in a computer program product and loaded into the computer system 900 using the removable storage drive 914, interface 920, and hard disk drive 912, or communications interface 924.

[0090] Embodiments of the present disclosure also may be directed to computer program products comprising software stored on any computer useable medium. Such software, when executed in one or more data processing device, causes a data processing device(s) to operate as described herein. Embodiments of the present disclosure employ any computer useable or readable medium. Examples of computer useable mediums include, but are not limited to, primary storage devices (e.g., any type of random access memory), secondary storage devices (e.g., hard drives, floppy disks, CD ROMS, ZIP disks, tapes, magnetic storage devices, and optical storage devices, MEMS, nanotechnological storage device, etc.), and communication mediums (e.g., wired and wireless communications networks, local area networks, wide area networks, intranets, etc.).

[0091] Accordingly, it will be appreciated that one or more embodiments of the present invention can include a computer program comprising computer program code means adapted to perform one or all of the steps of any methods or claims set forth herein when such program is run on a computer, and that such program may be embodied on a computer readable medium. Further, one or more embodiments of the present invention can include a computer comprising code adapted to cause the computer to carry out one or more steps of methods or claims set forth herein, together with one or more apparatus elements or features as depicted and described herein.

V. Conclusion

[0092] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be apparent to persons skilled in the relevant art that various changes in form and detail can be made therein without departing from the spirit and scope of the invention. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A method for generating and provisioning payment transaction data to a mobile device having a mobile payment application from a Cloud-based transaction data generation system (Cloud), the method comprising:

provisioning a storage key ($K_{Storage}$), authentication credentials and static payment credentials associated with a payment account to the mobile device, wherein the $K_{Storage}$ key is used to protect static payment credentials stored on the mobile device and the transport of a payload from the Cloud to the mobile payment application;

forwarding the payload comprising at least one of a session key generated using an unpredictable number (KS_{UN}), a dynamic CVC value with Track1/Track2 data ($Cloud\_CVC3_{TRACK1/2}$) and an application transaction counter (ATC) to the mobile payment application, wherein the payload is encrypted prior to the forwarding using the $K_{Storage}$ key;

activating the mobile payment application using a contactless interface in order to enable a contactless payment transaction using the mobile device;

forwarding payment credentials comprising at least one token from the Cloud to the mobile device;

receiving, at the Cloud, a token from a mobile authentication application (MAA) component of the mobile payment application;

validating the token based upon the authentication credentials and at least one additional credential received from the mobile device;

determining, by the Cloud and based on rules, if additional payment credentials need to be provisioned to the mobile device; and

in response to determining that additional payment credentials are needed:

generating the additional payment credentials; and

provisioning the additional payment credentials from the Cloud to the mobile device;

authenticating the payment transaction based on the payment credentials; and in response to determining that the authenticating was successful, including a genuine CVC3 derived key (KD_{CVC3}) in the payment credentials and returning an encrypted payload to the mobile device including at least one of the KS_{UN}, the Cloud_CVC3$_{TRACK1/2}$, or the ATC, or in response to determining that the authenticating was unsuccessful including a non-functional KD_{CVC3} key in the payment credentials, returning an encrypted payload to the mobile device without notifying the mobile device of the unsuccessful authentication, and triggering an alarm without notifying the mobile payment application of the unsuccessful authentication,

wherein a secure element in the mobile device is not required.

2. The method of claim 1, wherein the at least one additional credential comprises CAP token, a gesture, a password, passcode, or another suitable Personal Value.

3. The method of claim 1, wherein the validating is performed by an issuer.

4. The method of claim 1, wherein the wherein the validating comprises matching an application transaction counter (ATC) from the Cloud with an ATC received from a merchant or transaction acquirer.

5. The method of claim 1, wherein the transaction data comprises an unpredictable number (UN) used as a seed value as input into a cryptographic process, and wherein the UN is used to compute what an acquirer expects a CVC3 value to be for the transaction.

6. The method of claim 5, wherein the cryptographic process uses the triple Data Encryption Standard (DES) algorithm to generate the CVC3 value and wherein transaction data comprises the CVC3 value.

7. The method of claim 6, wherein the CVC3 value is a number generated by the Cloud and used by the Cloud to generate a dynamic CVC3 cryptogram.

8. The method of claim 7, wherein the tokens are CVC3 tokens and the payment credentials comprise the dynamic CVC3 cryptogram.

9. The method of claim 1, wherein the token is a Chip Authentication Program (CAP) token indicating one or more controls on purchases.

10. The method of claim 9, wherein the one or more controls limit purchases based upon one or more of:

a day of week;
a time of day;
an expiration date associated with a CAP token;
an expiration date associated with a payment account;
a merchant category corresponding to a point-of-sale (POS) terminal;
a geographic location of a merchant;
a spending limit for a payment account;
a spending limit for a specified merchant category; and
a spending limit for a duration.

11. The method of claim 1, wherein the validating comprises receiving the authentication credentials from the MAA.

12. The method of claim 1, wherein the retrieving comprises synchronizing between the Cloud and an issuer system.

13. The method of claim 1, wherein the Cloud is hosted by an issuer.

14. The method of claim 1, wherein the Cloud is hosted by a third party.

15. The method of claim 14, wherein the third party is a payment processing network.

16. The method of claim 1, further comprising, prior to the processing:

receiving a registration request for a user associated with the mobile device;

processing the registration request;

in response to determining that the registration request has been fulfilled, provisioning the mobile payment application to the mobile device; and

verifying an installation of the mobile payment application on the mobile device.

17. The method of claim 1, wherein the payment account is one or more of:

a credit card;

a debit card;

a pre-paid card;

a hybrid card; or

a payment account with a virtual card number (VCN),

wherein the VCN is a single use VCN, a limited use VCN, or another account number that facilitates a financial transaction using a transaction clearance system.

18. A method for generating and provisioning payment transaction data to a mobile device from a Cloud-based transaction data generation system (Cloud), the method comprising:

authenticating the mobile device to the Cloud based upon authentication credentials previously provisioned to the mobile device;

in response to determining that the authentication is successful, validating, by the Cloud and based on server-side rules, one or more tokens associated with the mobile device;

in response to determining that the mobile device needs new tokens, generating, in the Cloud, one or more new tokens for the mobile device; and provisioning payment credentials to the mobile device via a mobile payment application previously-provisioned to and installed on the mobile device;

comparing transaction data received from a point-of-sale (POS) with the payment credentials previously-provisioned to the mobile device; and

processing a payment transaction based on the comparing,

wherein a secure element in the mobile device is not required.

19. The method of claim 18, wherein the provisioning of the payment credentials is a pull request from the mobile device.

20. The method of claim 18, wherein the provisioning of the payment credentials is a push from the Cloud.

21. The method of claim 18, wherein the authentication is based at least in part on a CAP token, and a received password, passcode, gesture, or Personal Value associated with a user of the mobile device.

22. The method of claim 18, wherein the one or more tokens are based upon one or more merchant categories a payment account associated with the mobile device is authorized for.

23. The method of claim 18, wherein the tokens have time controls on their usage.

24. The method of claim 22, wherein the time controls comprise an expiration date for the one or more new transaction tokens.

25. The method of claim 22, wherein the time controls comprise time of day controls for the tokens.

26. The method of claim 22, wherein the time controls comprise day of week controls for the tokens.

27. The method of claim 3, further comprising verifying, by an issuer, the transaction data.

28. The method of claim 3, wherein the transaction data comprises a dynamic CVC3 cryptogram.

ABSTRACT OF THE DISCLOSURE

A method for providing technical solutions for processing electronic payments initiated from a mobile device without requiring a secure element (SE) in a mobile device, comprising: provisioning authentication credentials and payment credentials associated with a payment account to the mobile device; activating a mobile payment application on the mobile device using a contactless interface to enable a payment transaction using the mobile device; forwarding payment credentials from the cloud to the mobile device; sending a token from a mobile authentication application (MAA) component of the mobile payment application to the cloud; validating the token based on upon authentication credentials; determining if additional payment credentials need to be provisioned to the mobile device; and authenticating the contactless payment transaction based on the payment credentials.

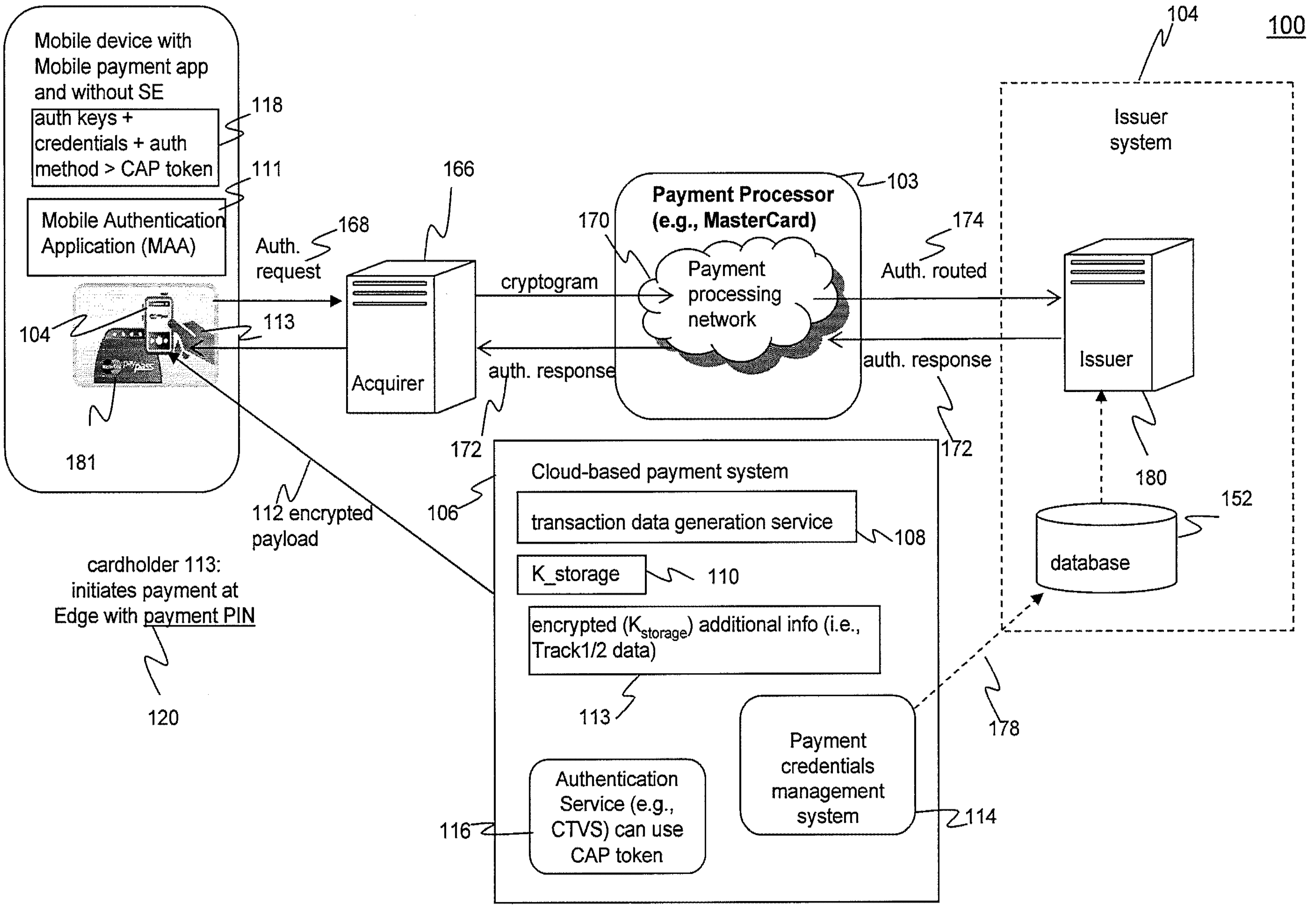

104
100
Mobile device with
Mobile payment app
and without SE
118
auth keys +
credentials + auth
method > CAP token
111
Mobile Authentication
Application (MAA)
166
168
Auth.
request
104
113
181
Acquirer
cryptogram
Payment Processor
(e.g., MasterCard)
103
170
Payment
processing
network
174
Auth. routed
Issuer
system
Issuer
auth. response
auth. response
172
172
180
Cloud-based payment system
106
transaction data generation service
108
K_storage
110
encrypted ($K_{storage}$) additional info (i.e., Track1/2 data)
113
database
152
112 encrypted
payload
cardholder 113:
initiates payment at
Edge with payment PIN
120
178
Payment
credentials
management
system
114
Authentication
Service (e.g.,
CTVS) can use
CAP token
116

FIG. 1

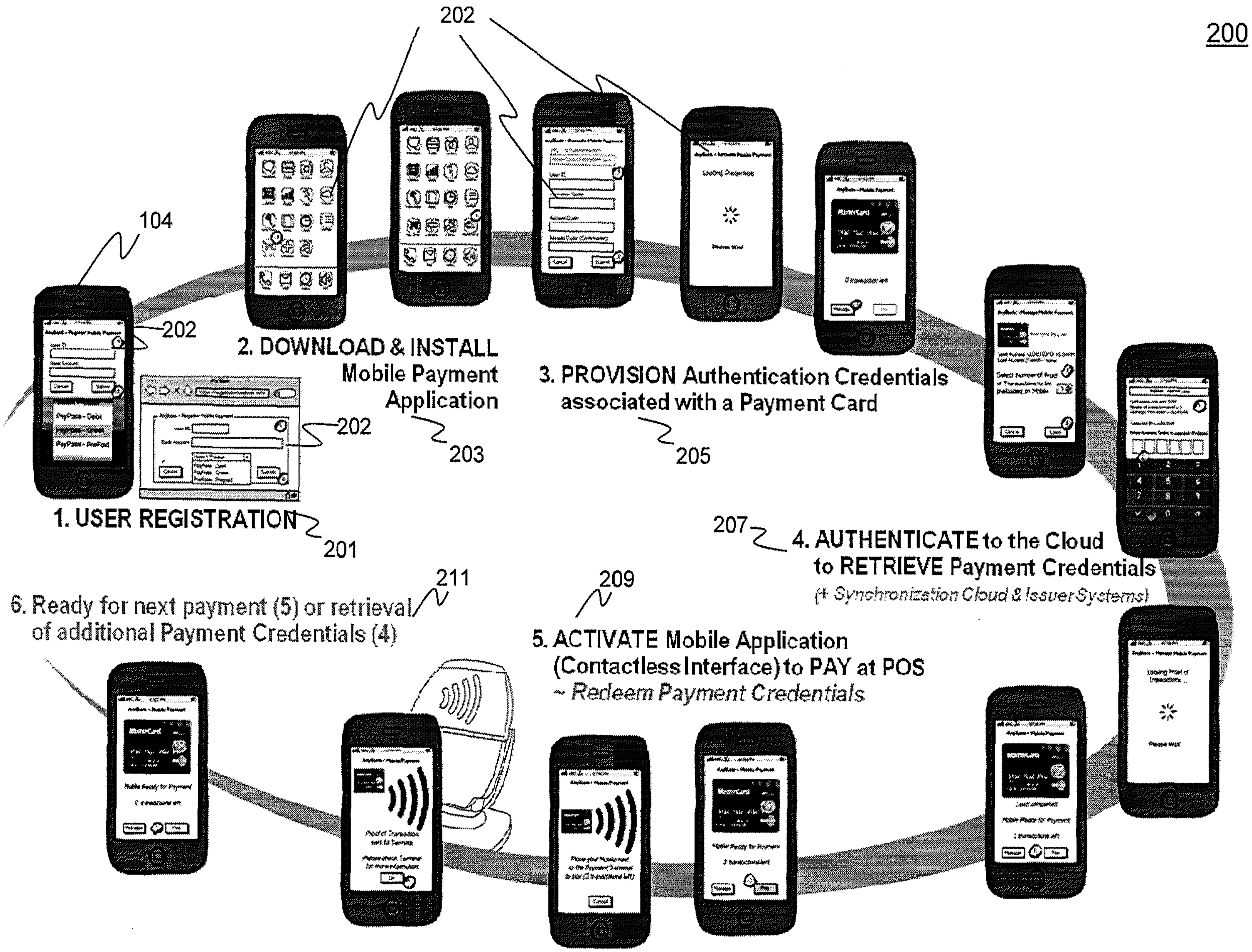

200
202
104
202
202
1. USER REGISTRATION
201
2. DOWNLOAD & INSTALL Mobile Payment Application
203
3. PROVISION Authentication Credentials associated with a Payment Card
205
207
4. AUTHENTICATE to the Cloud to RETRIEVE Payment Credentials
(+ Synchronization Cloud & Issuer Systems)
209
5. ACTIVATE Mobile Application (Contactless Interface) to PAY at POS
~ Redeem Payment Credentials
211
6. Ready for next payment (5) or retrieval of additional Payment Credentials (4)
PayPass - Debit
PayPass - Credit
PayPass - PrePaid
MasterCard

FIG. 2

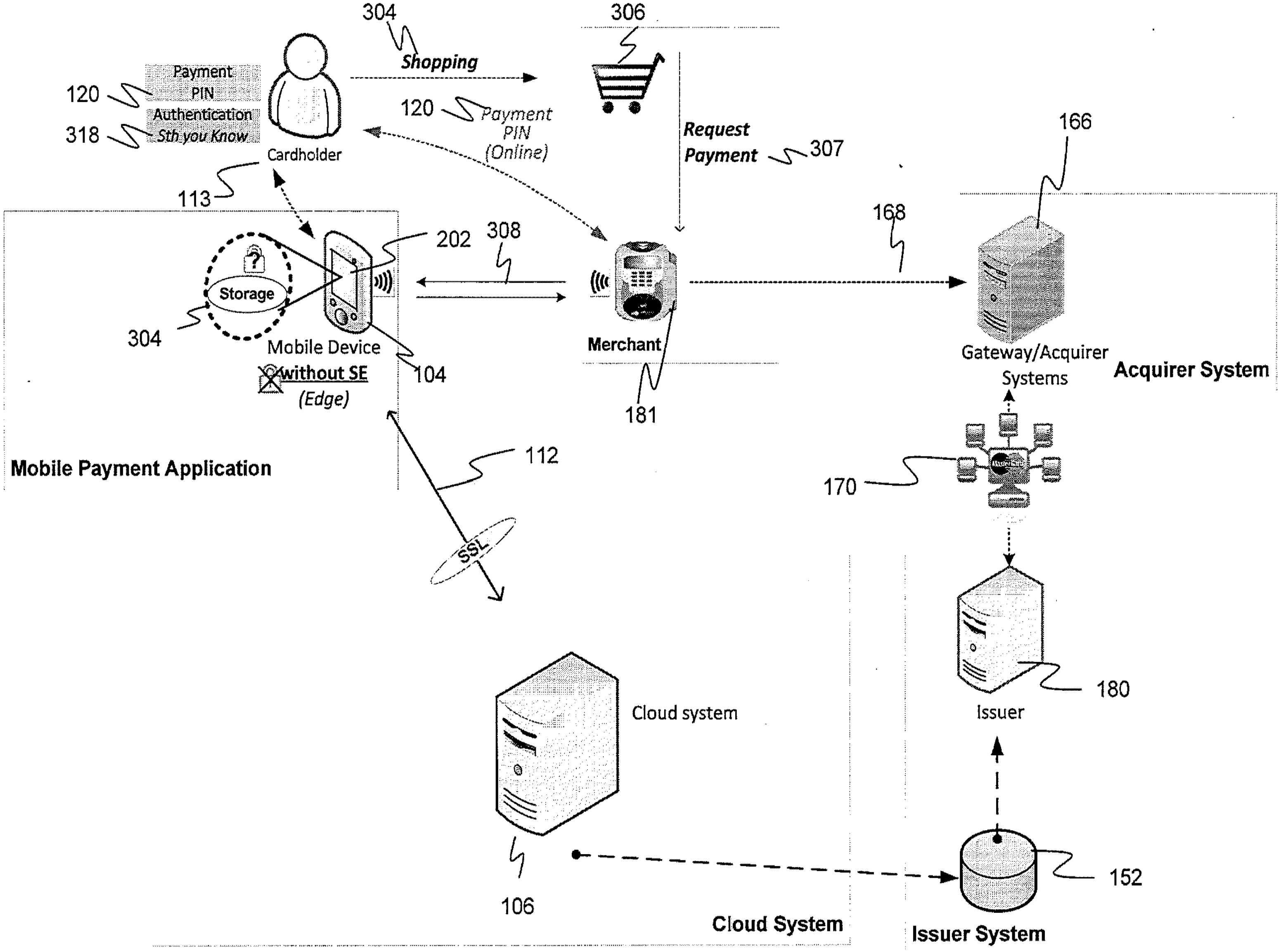

304
Shopping
306
Payment
PIN
120
Authentication
Sth you Know
318
Cardholder
120
Payment
PIN
(Online)
Request
Payment
307
166
113
168
202
308
Storage
304
Mobile Device
without SE
(Edge)
104
Merchant
181
Gateway/Acquirer
Systems
Acquirer System
Mobile Payment Application
112
SSL
170
180
Issuer
Cloud system
106
152
Cloud System
Issuer System

FIG. 3

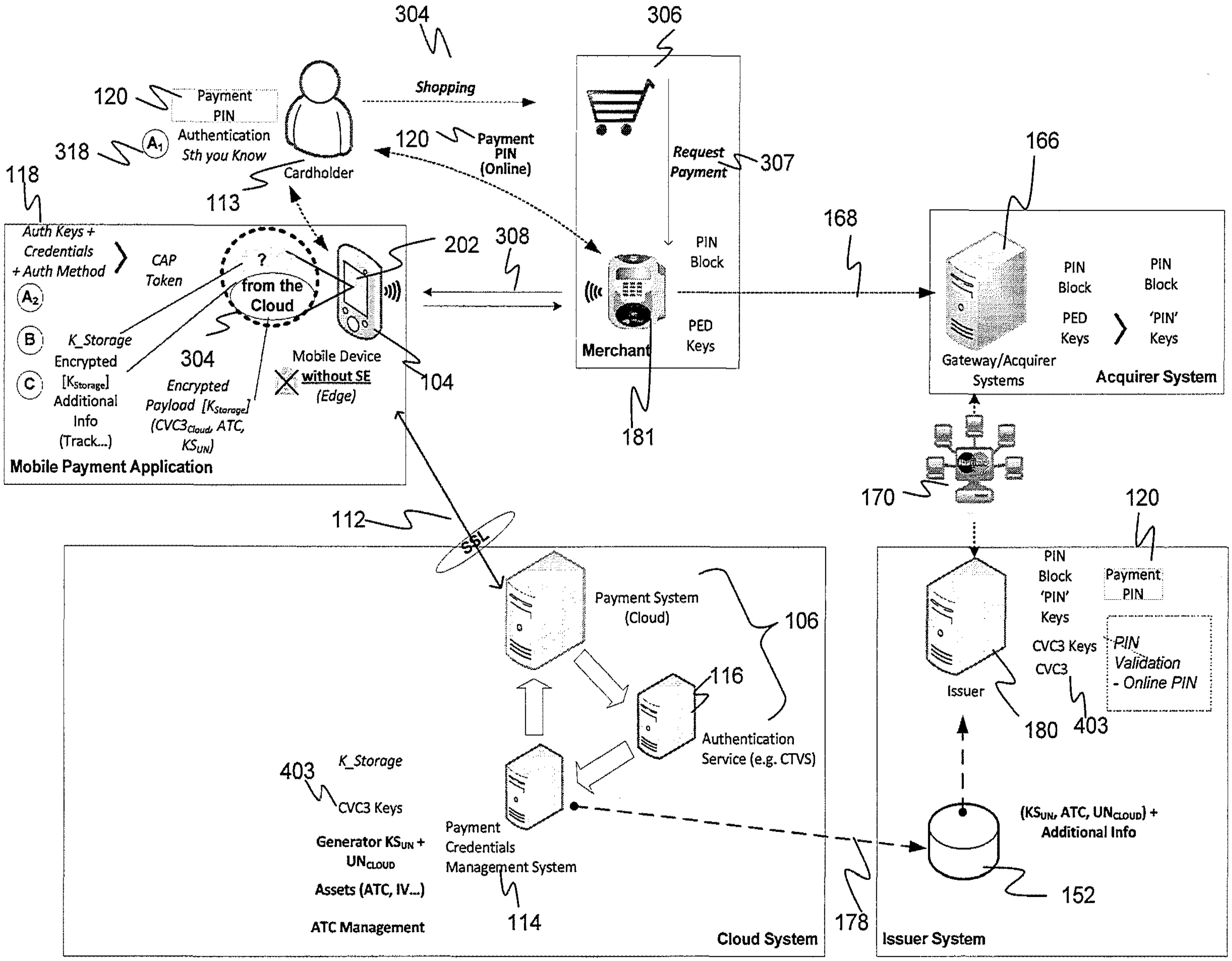

304
306
120
Payment PIN
Authentication
Sth you Know
318
A1
Cardholder
113
Shopping
120
Payment PIN (Online)
Request Payment
307
118
Auth Keys + Credentials + Auth Method
CAP Token
A2
B
K_Storage Encrypted [K_Storage]
C
Additional Info (Track...)
?
from the Cloud
202
308
304
Encrypted Payload [K_Storage] (CVC3_Cloud, ATC, KS_UN)
Mobile Device without SE (Edge)
104
Mobile Payment Application
PIN Block
PED Keys
Merchant
181
168
166
PIN Block
PED Keys
PIN Block
'PIN' Keys
Gateway/Acquirer Systems
Acquirer System
170
112
SSL
Payment System (Cloud)
106
116
Authentication Service (e.g. CTVS)
403
K_Storage
CVC3 Keys
Generator KS_UN + UN_CLOUD
Assets (ATC, IV...)
ATC Management
Payment Credentials Management System
114
Cloud System
178
120
PIN Block
'PIN' Keys
Payment PIN
CVC3 Keys
CVC3
PIN Validation - Online PIN
Issuer
180
403
(KS_UN, ATC, UN_CLOUD) + Additional Info
152
Issuer System

FIG. 4

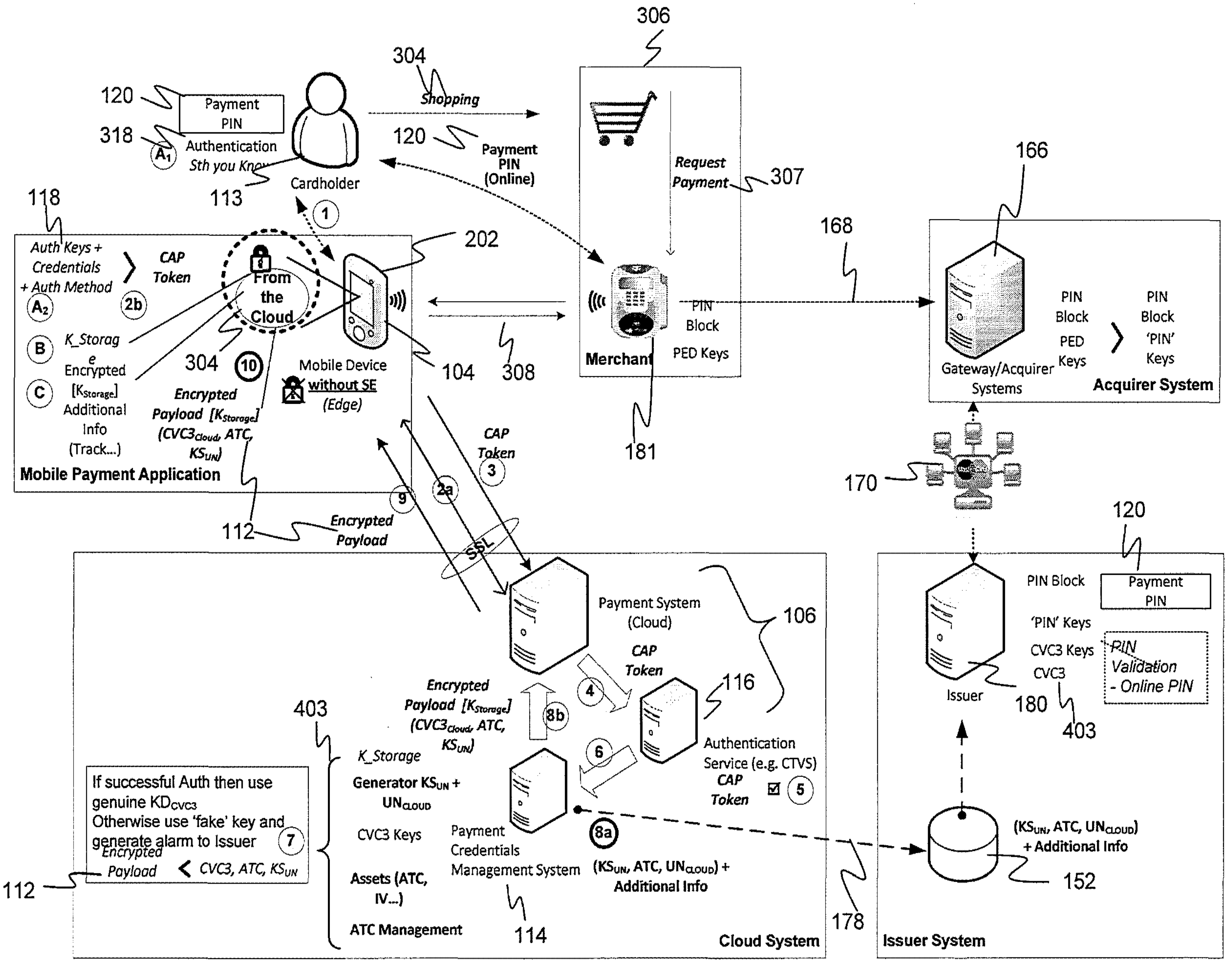

306
304
Shopping
120
Payment PIN
318
A1
Authentication
Sth you Know
Cardholder
120
Payment PIN (Online)
Request Payment
307
113
1
118
Auth Keys + Credentials + Auth Method
A2
CAP Token
2b
From the Cloud
202
166
168
B
K_Storage
Encrypted
C
[KStorage]
Additional Info
(Track...)
304
10
Encrypted Payload [KStorage] (CVC3Cloud, ATC, KSUN)
Mobile Device
without SE
(Edge)
104
308
Merchant
PIN Block
PED Keys
181
PIN Block
PED Keys
PIN Block
'PIN' Keys
Gateway/Acquirer Systems
Acquirer System
Mobile Payment Application
CAP Token
3
9
2a
112
Encrypted Payload
SSL
170
120
Payment System (Cloud)
106
CAP Token
4
116
PIN Block
Payment PIN
'PIN' Keys
CVC3 Keys
CVC3
PIN Validation
- Online PIN
Issuer
180
403
Encrypted Payload [KStorage] (CVC3Cloud, ATC, KSUN)
8b
403
K_Storage
Generator KSUN + UNCLOUD
CVC3 Keys
Assets (ATC, IV...)
ATC Management
6
Authentication Service (e.g. CTVS)
CAP Token
☑ 5
8a
Payment Credentials Management System
(KSUN, ATC, UNCLOUD) + Additional Info
114
(KSUN, ATC, UNCLOUD) + Additional Info
152
If successful Auth then use genuine KDCVC3
Otherwise use 'fake' key and generate alarm to Issuer
7
Encrypted Payload
CVC3, ATC, KSUN
112
Cloud System
178
Issuer System

FIG. 5

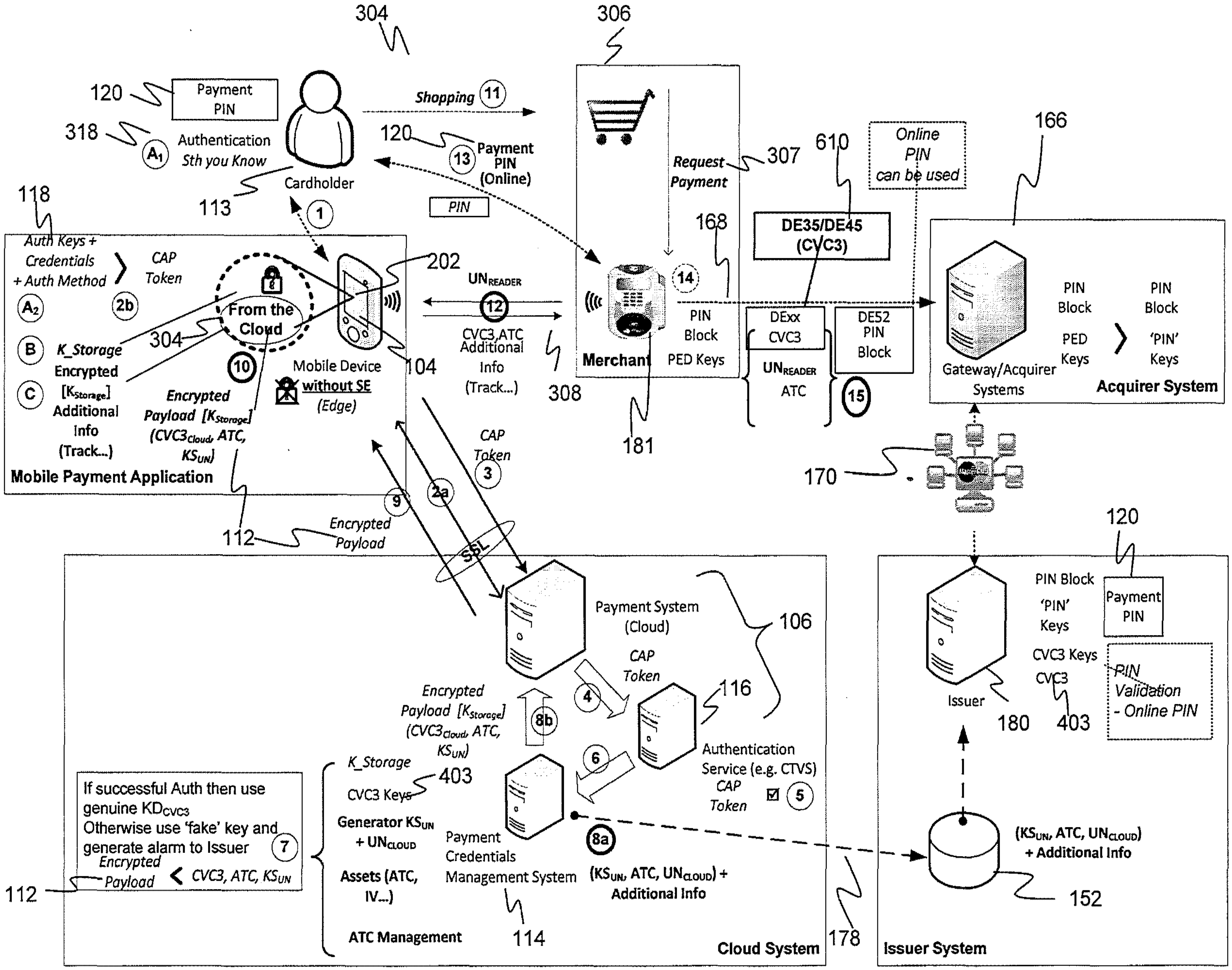
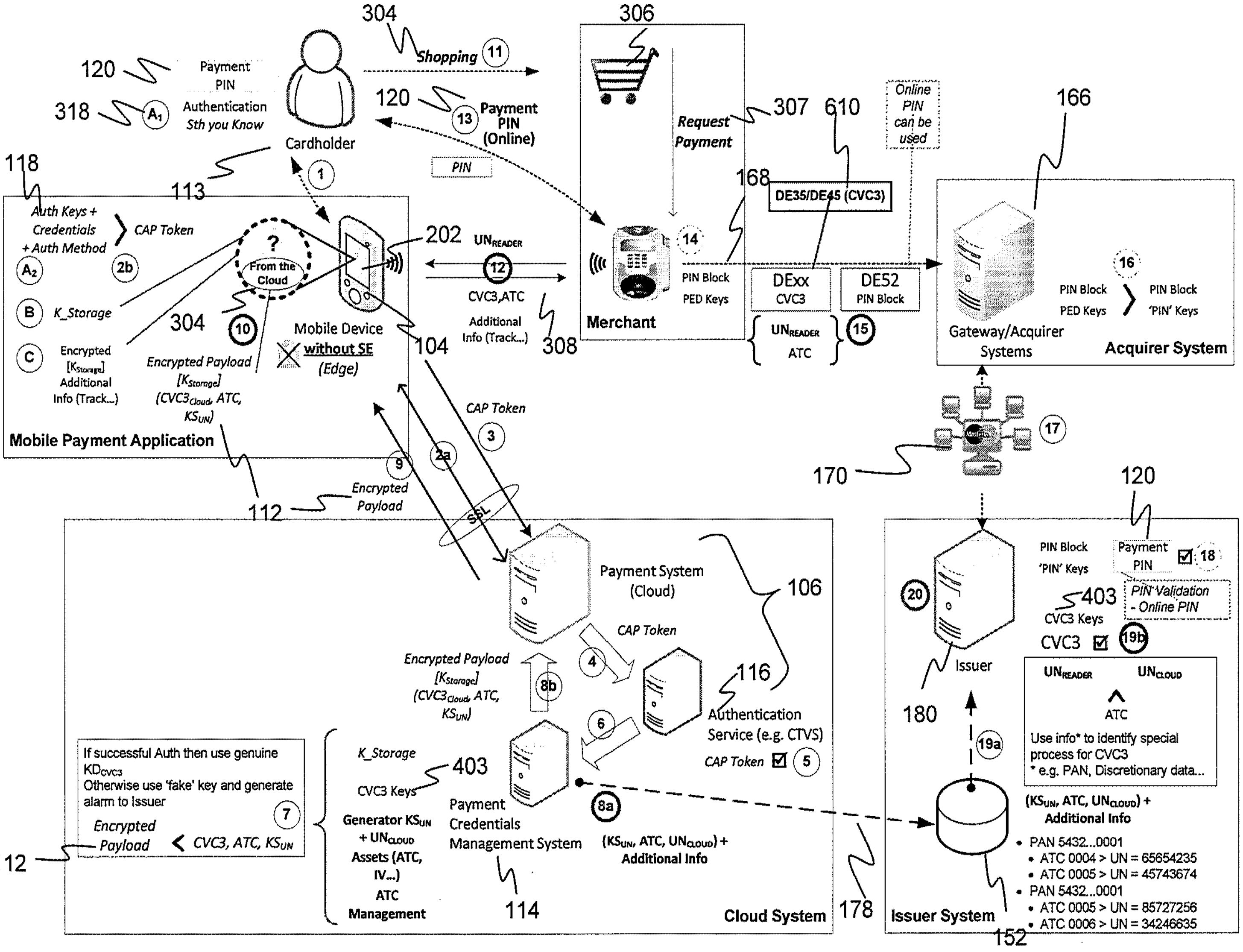
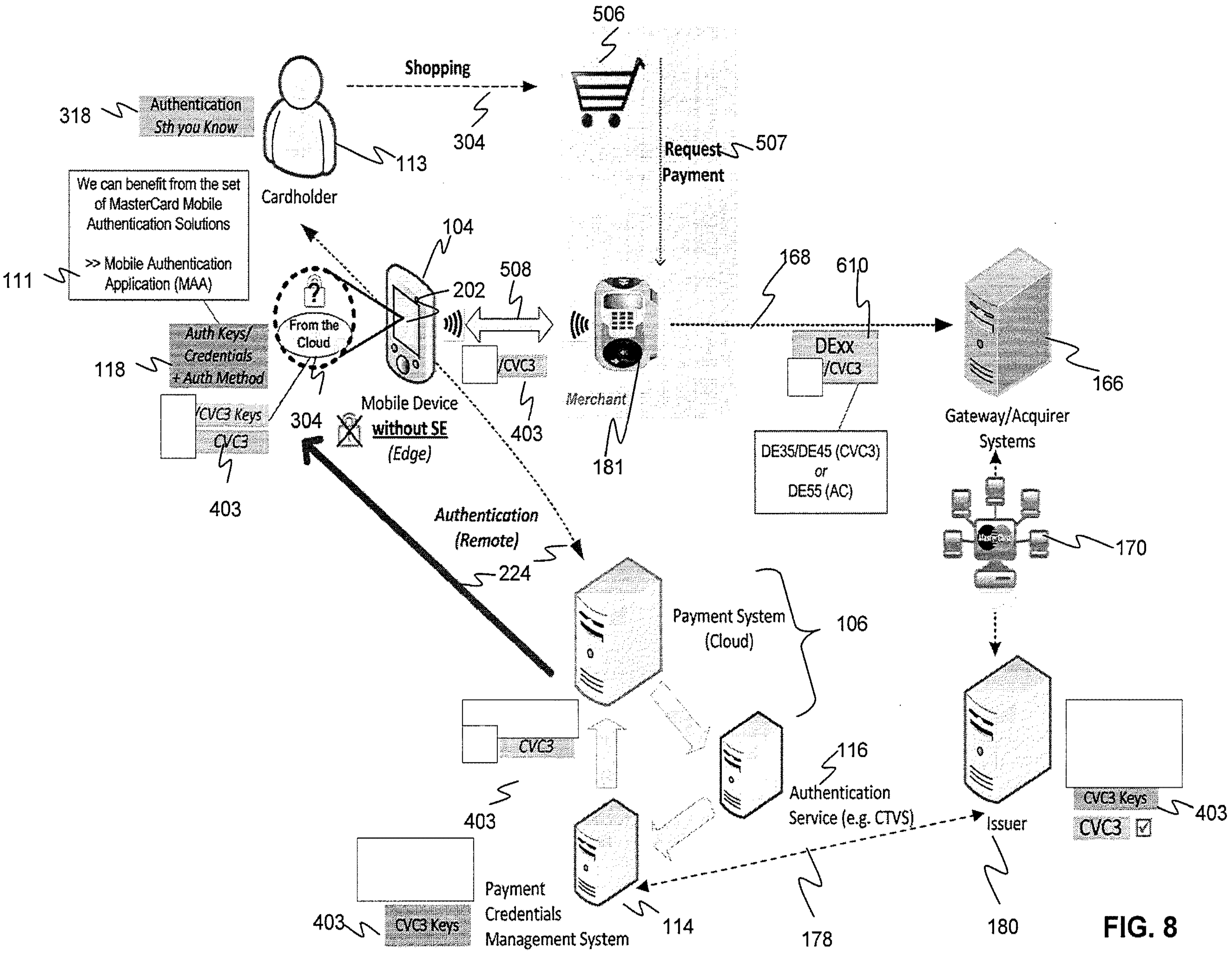

304
306
120
Payment PIN
318
A1
Authentication
Sth you Know
Cardholder
113
Shopping 11
120
13 Payment PIN (Online)
PIN
1
Request Payment
307
610
Online PIN can be used
166
118
Auth Keys + Credentials + Auth Method
CAP Token
A2
2b
B
K_Storage
Encrypted
C
[K_Storage]
Additional Info (Track...)
304
From the Cloud
10
Encrypted Payload [K_Storage] (CVC3_Cloud, ATC, KS_UN)
202
Mobile Device without SE (Edge)
104
UN_READER
12
CVC3,ATC Additional Info (Track...)
308
Merchant
14
168
PIN Block
PED Keys
DE35/DE45 (CVC3)
DExx CVC3
DE52 PIN Block
UN_READER ATC
15
Gateway/Acquirer Systems
PIN Block
PED Keys
PIN Block
'PIN' Keys
Acquirer System
Mobile Payment Application
CAP Token
3
181
170
9
2a
112
Encrypted Payload
SSL
120
Payment System (Cloud)
106
CAP Token
4
116
Encrypted Payload [K_Storage] (CVC3_Cloud, ATC, KS_UN)
8b
6
Authentication Service (e.g. CTVS)
CAP Token
☑ 5
PIN Block
'PIN' Keys
Payment PIN
CVC3 Keys
CVC3
PIN Validation - Online PIN
Issuer
180
403
If successful Auth then use genuine KD_CVC3
Otherwise use 'fake' key and generate alarm to Issuer
7
112
Encrypted Payload
CVC3, ATC, KS_UN
K_Storage
CVC3 Keys
403
Generator KS_UN + UN_CLOUD
Assets (ATC, IV...)
ATC Management
Payment Credentials Management System
114
8a
(KS_UN, ATC, UN_CLOUD) + Additional Info
(KS_UN, ATC, UN_CLOUD) + Additional Info
152
178
Cloud System
Issuer System

FIG. 6



304
306
120
Payment
PIN
Authentication
Sth you Know
318
A1
Cardholder
Shopping
11
120
13
Payment
PIN
(Online)
PIN
Request
Payment
307
610
Online
PIN
can be
used
166
118
113
1
168
DE35/DE45 (CVC3)
Auth Keys +
Credentials
+ Auth Method
CAP Token
2b
A2
B
K_Storage
C
Encrypted
[KStorage]
Additional
Info (Track...)
?
From the
Cloud
304
10
Encrypted Payload
[KStorage]
(CVC3Cloud, ATC,
KSUN)
Mobile Device
without SE
(Edge)
Mobile Payment Application
202
UNREADER
12
CVC3,ATC
Additional
Info (Track...)
308
104
14
PIN Block
PED Keys
Merchant
DExx
CVC3
DE52
PIN Block
UNREADER
ATC
15
16
PIN Block
PED Keys
PIN Block
'PIN' Keys
Gateway/Acquirer
Systems
Acquirer System
CAP Token
3
2a
9
Encrypted
Payload
112
SSL
17
170
120
Payment System
(Cloud)
106
CAP Token
4
Encrypted Payload
[KStorage]
(CVC3Cloud, ATC,
KSUN)
8b
116
Authentication
Service (e.g. CTVS)
6
CAP Token ☑
5
If successful Auth then use genuine
KDCVC3
Otherwise use 'fake' key and generate
alarm to Issuer
7
Encrypted
Payload
CVC3, ATC, KSUN
112
K_Storage
CVC3 Keys
403
Generator KSUN
+ UNCLOUD
Assets (ATC,
IV...)
ATC
Management
Payment
Credentials
Management System
114
8a
(KSUN, ATC, UNCLOUD) +
Additional Info
Cloud System
178
PIN Block
'PIN' Keys
Payment
PIN
☑
18
20
403
PIN Validation
- Online PIN
CVC3 Keys
CVC3 ☑
19b
Issuer
180
UNREADER
UNCLOUD
ATC
Use info* to identify special
process for CVC3
* e.g. PAN, Discretionary data...
19a
(KSUN, ATC, UNCLOUD) +
Additional Info
PAN 5432...0001
ATC 0004 > UN = 65654235
ATC 0005 > UN = 45743674
PAN 5432...0001
ATC 0005 > UN = 85727256
ATC 0006 > UN = 34246635
Issuer System
152

FIG. 7



506
Shopping
304
318
Authentication
Sth you Know
113
Cardholder
Request
Payment
507
We can benefit from the set of MasterCard Mobile Authentication Solutions
>> Mobile Authentication Application (MAA)
111
104
202
508
168
610
From the Cloud
Auth Keys/ Credentials + Auth Method
118
/CVC3 Keys
CVC3
403
304
Mobile Device
without SE
(Edge)
/CVC3
403
Merchant
181
DExx
/CVC3
166
Gateway/Acquirer Systems
DE35/DE45 (CVC3)
or
DE55 (AC)
Authentication
(Remote)
224
170
Payment System
(Cloud)
106
CVC3
403
116
Authentication Service (e.g. CTVS)
Issuer
CVC3 Keys
403
CVC3 ☑
403
CVC3 Keys
Payment Credentials Management System
114
178
180

FIG. 8

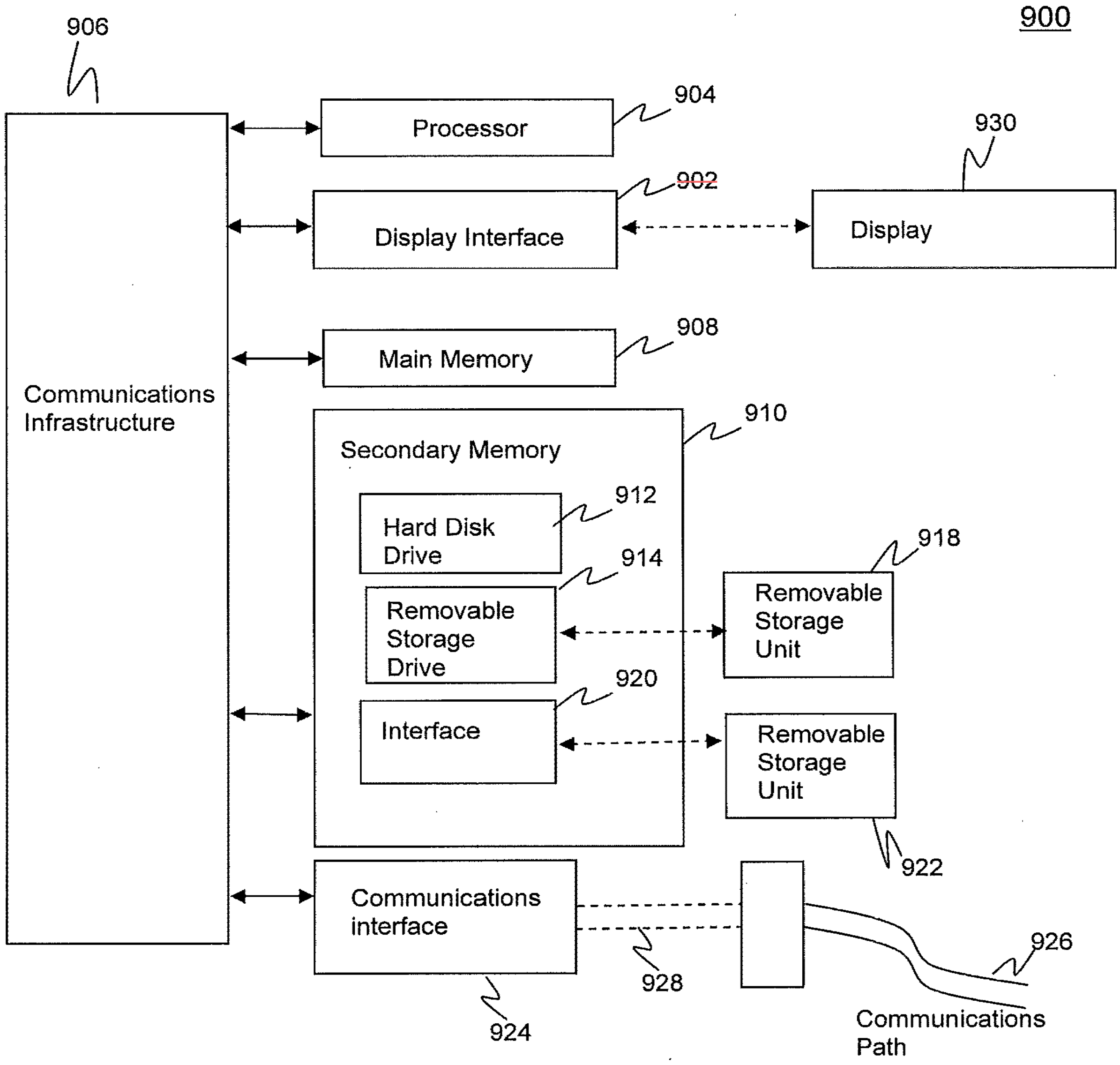

900
906
Communications Infrastructure
Processor
904
Display Interface
902
930
Display
Main Memory
908
Secondary Memory
910
Hard Disk Drive
912
Removable Storage Drive
914
Removable Storage Unit
918
Interface
920
Removable Storage Unit
922
Communications interface
924
928
926
Communications Path

FIG. 9