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

(11) EP 2 835 004 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
06.11.2019 Bulletin 2019/45

(21) Application number: **13772978.6**

(22) Date of filing: **21.03.2013**

(51) Int Cl.:
H04W 12/06 *(2009.01)* ***H04W 12/04*** *(2009.01)*
G06Q 20/32 *(2012.01)* ***G06Q 20/38*** *(2012.01)*
H04W 12/00 *(2009.01)* *G06Q 20/34* *(2012.01)*

(86) International application number:
PCT/US2013/033322

(87) International publication number:
WO 2013/151797 (10.10.2013 Gazette 2013/41)

(54) **SYSTEMS AND METHODS FOR PROCESSING MOBILE PAYMENTS BY PROVISIONING CREDENTIALS TO MOBILE DEVICES WITHOUT SECURE ELEMENTS**

SYSTEME UND VERFAHREN ZUR VERARBEITUNG MOBILER ZAHLUNGEN DURCH BEREITSTELLUNG VON BERECHTIGUNGSNACHWEISEN AN MOBILE VORRICHTUNGEN OHNE SICHERE ELEMENTE

SYSTÈMES ET PROCÉDÉS DE TRAITEMENT DE PAIEMENTS MOBILES PAR FOURNITURE DE JUSTIFICATIFS D'IDENTITÉ À DES DISPOSITIFS MOBILES SANS ÉLÉMENTS SÉCURISÉS

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **02.04.2012 US 201261619095 P**
18.04.2012 US 201261635248 P
10.12.2012 US 201261735383 P
07.02.2013 US 201361762098 P
14.03.2013 US 201313827042

(43) Date of publication of application:
11.02.2015 Bulletin 2015/07

(73) Proprietor: **MasterCard International Incorporated**
Purchase, NY 10577 (US)

(72) Inventors:
- **COLLINGE, Mehdi**
  1420 Braine-l'Alleud (BE)
- **THOMPSON, Susan**
  Burland
  Nantwich CW5 8LR (GB)
- **SMETS, Patrik**
  2560 Nijlen (BE)
- **ROBERTS, David Anthony**
  Appleton
  Warrington WA4 5RD (GB)
- **WARD, Michael Christopher**
  Bridgewater
  Somerset TA5 1DB (GB)

(74) Representative: **AWA Sweden AB**
P.O. Box 11394
404 28 Göteborg (SE)

(56) References cited:
US-A1- 2008 040 285 **US-A1- 2008 051 122**
US-A1- 2010 332 391

- **STIG FRODE MJOLSNES ET AL.: 'Localized Credentials for Server Assisted Mobile Wallet' 2001 IEEE 2001, pages 203 - 204, XP010565895**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

IPR2025-01145
Apple EX1074 Page 1

Description

RELATED APPLICATIONS

[0001] This application claims the priority benefit of commonly assigned U.S. Provisional Application No. 61/619,095, filed April 2, 2012, entitled "Method and System for Processing Mobile Payments for Devices Without Secure Elements"; U.S. Provisional Application No. 61/639,248, filed April 18, 2012, entitled "Method and System for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements"; U.S. Provisional Application No. 61/735,383, filed December 10, 2012, entitled "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements," by Mehdi Collinge et al.; U.S. Provisional Application No. 61/762,098, filed February 7, 2013, entitled "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements," by Mehdi Collinge et al.; and U.S. Patent Application No. 13/827,042, filed March 14, 2013, entitled "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements," by Mehdi Collinge et al..

FIELD

[0002] The present disclosure relates to provisioning of payment credentials to a mobile device lacking a secure element, specifically the provisioning and storage of payment credentials for use in conducting a near field financial transaction using a mobile device lacking a secure element.

BACKGROUND

[0003] Advances in both mobile and communication technologies have created tremendous opportunities, one of which is providing user of mobile computing devices the ability to initiate payment transactions using their mobile device. One such approach to enable mobile devices to conduct payment transactions has been the use of near field communication (NFC) technology to securely transmit payment information to a nearby contactless point-of-sale terminal. In order to achieve this, mobile phones with secure element hardware (e.g., a Secure Element chip) are used to securely store payment account credentials, such as credit card credentials.

[0004] However, not all mobile devices have secure elements. Furthermore, some issuers may not have access to a secure element on a mobile device, even if the mobile device has one available. As a result, a consumer who has a NFC-capable mobile device may not be able to use their device to conduct payment transactions if their mobile device lacks a secure element, and even in some cases where their mobile device has a secure element.

[0005] Thus, there is a need for a technical solution to enable a mobile device lacking a secure element to conduct contactless payment transactions.

[0006] US2008040285 discloses a method and apparatus for conducting a secure transaction involving generation of a dynamic authentication code on a mobile device, based on secret data which does not identify an account. The authentication code and financial account identifying information are transmitted to a validating entity, which shares information about the secret data, to authorize the transaction.

SUMMARY

[0007] The present disclosure provides a description of a systems and methods for the provisioning of payment credentials to mobile devices lacking secure elements for use in mobile payment transactions.

[0008] According to independent claim 1, there is provided a method for generating and provisioning payment credentials to a mobile device lacking a secure element, comprising: generating, by a processing device of a remote system, a card profile associated with a payment account, wherein the card profile includes at least payment credentials corresponding to the associated payment account and a profile identifier; provisioning, by the remote system, to a mobile device, the generated card profile; receiving, by the remote system, from the mobile device, a key request, wherein the key request includes at least a mobile personal identification number, PIN, and the profile identifier; in response to receiving the key request from the mobile device, determining, by an authentication device of the remote system, whether the mobile PIN is authentic; based on the determination of authenticity of the mobile PIN generating, by the processing device of the remote system, a single use key, wherein (i) the single use key is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and (ii) the single use key includes at least the profile identifier, an application transaction counter, and a generating key; and transmitting, by a transmitting device of the remote system, the generated single use key to the mobile device, wherein the mobile device lacks a secure element.

[0009] According to independent claim 7, there is provided a method for generating a payment cryptogram in a mobile device lacking a secure element, comprising: receiving, by a receiving device of the mobile device, a card profile from a remote system, wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier; receiving, by an input device of the mobile device, a mobile personal identification number, PIN, input by a user of the mobile device; transmitting, by a transmitting device of the mobile device, a key request to the remote system, wherein the key request includes at least the profile identifier and a mobile personal identification number, PIN, wherein said key request causes said remote device to generate

IPR2025-01145
Apple EX1074 Page 2

a single use key; receiving, by the receiving device of the mobile device, the single use key from the remote system, wherein the single use key (i) is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and (ii) the single use key includes at least an application transaction counter, a generating key, and the profile identifier; generating, by a processing device of the mobile device, the payment cryptogram valid for the single financial transaction based on at least the received single use key and the mobile PIN; and transmitting, by the mobile device, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction.

[0010] Another method for generating and provisioning payment credentials to a mobile device lacking a secure element includes: storing, in a database, at least a storage key, a plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program; provisioning, to the mobile device, at least the storage key, an authentication component, and static payment credentials, wherein the static payment credentials are associated with a payment account; receiving, from a mobile device, a chip authentication program (CAP) token; validating, by a validation device, the authenticity of the received CAP token; generating, by a processing device, a session key unpredictable number (KS_{UN}); generating, by the processing device, a cloud unpredictable number (UN_{CLOUD}); identifying, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KD_{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the plurality of dynamic card validation code keys, the KS_{UN}, and the application transaction counter; transmitting, by a transmitting device, the encrypted payload to the mobile device for use in generating a dynamic card validation code for use in a financial transaction; and transmitting, by the transmitting device, at least the KSUN, UN_{CLOUD}, and application transaction counter to an issuer associated with the payment account for use in validating the generated dynamic card validation code used in the financial transaction.

[0011] A method for generating a dynamic card validation code in a mobile device lacking a secure element includes: receiving, by a receiving device, at least a storage key, an authentication component, and static payment credentials; receiving, by an input device, at least one additional credential; generating, by a processing device, a chip authentication program (CAP) token, wherein the CAP token is based on at least the authentication component and the at least one additional credential; transmitting, by a transmitting device, the generated CAP token; receiving, by the receiving device, an encrypted payload, wherein the encrypted payload includes at least a supplied dynamic card validation code, session key unpredictable number, and application transaction counter; decrypting, by the processing device, the encrypted payload using at least the received storage key; receiving, via near field communication, a reader unpredictable number from a point-of-sale terminal; generating, by the processing device, a payment dynamic card validation code based on at least the supplied dynamic card validation code, the session key unpredictable number, the application transaction counter, and the reader unpredictable number; and transmitting, via near field communication, the generated payment dynamic card validation code and the application transaction counter to the point-of-sale terminal for including in an authorization request for a financial transaction.

[0012] According to independent claim 14, there is provided a system for generating and provisioning payment credentials to a mobile device lacking a secure element, comprising: a transmitting device of a remote system; a processing device, of the remote system configured to generate a card profile associated with a payment account, wherein the card profile includes at least payment credentials corresponding to the associated payment account and a profile identifier; a provisioning device, of the remote system, configured to provision, to a mobile device lacking a secure element, the generated card profile; a receiving device, of the remote system, configured to receive, from the mobile device, a key request, wherein the key request includes at least a mobile personal identification number, PIN, and the profile identifier; and an authentication device, of the remote system, configured to authenticate the mobile PIN in response to receiving the key request, wherein the processing device, of the remote system, is further configured to generate a single use key on a basis of mobile PIN authenticity, wherein the single use key (i) is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and (ii) includes at least the profile identifier, an application transaction counter, and a generating key for use in generating the payment cryptogram valid for the single financial transaction, and the transmitting device, of the remote system, is configured to transmit the generated single use key to the mobile device.

[0013] According to independent claim 19, there is provided a system for generating a payment cryptogram in a mobile device lacking a secure element, comprising: a processing device, of the mobile device; a receiving device, of the mobile device, configured to receive a card profile from a remote system, wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier; an input device, of the mobile device, configured to receive a mobile personal identification number, PIN, input by a user of the mobile device; and a transmitting device, of the mobile device, configured to transmit a key request to the remote system, wherein the key request (i) includes at least the profile identifier and a mobile personal identification number, PIN, and (ii) causes said remote device to generate a single use key, wherein the receiving de-

IPR2025-01145
Apple EX1074 Page 3

vice, of the mobile device, is further configured to receive the single use key from the remote system, wherein the single use key (i) is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and (ii) the single use key includes at least an application transaction counter, a generating key, and the profile identifier, the processing device, of the mobile device, is configured to generate the payment cryptogram valid for the single financial transaction based on at least the received single use key and the mobile PIN, and the transmitting device, of the mobile device, is further configured to transmit, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction.

[0014] Another system for generating and provisioning payment credentials to a mobile device lacking a secure element includes a database, a provisioning device, a receiving device, a processing device, and a transmitting device. The database is configured to store at least a storage key, a plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program. The provisioning device is configured to provision, to the mobile device, at least the storage key, an authentication component, and static payment credentials, wherein the static payment credentials are associated with a payment account. The receiving device is configured to receive, from a mobile device, a chip authentication program (CAP) token. The processing device is configured to: validate the authenticity of the received CAP token; generate a session key unpredictable number (KS_{UN}); generate a cloud unpredictable number (UN_{CLOUD}); and identify an encrypted payload based on a derived dynamic card validation code key (KD_{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the plurality of dynamic card validation code keys, the KS_{UN}, and the application transaction counter. The transmitting device is configured to: transmit the encrypted payload to the mobile device for use in generating a dynamic card validation code for use in a financial transaction; and transmit at least the KSUN, UN_{CLOUD}, and application transaction counter to an issuer associated with the payment account for use in validating the generated dynamic card validation code used in the financial transaction.

[0015] A system for generating a dynamic card validation code in a mobile device lacking a secure element includes a receiving device, an input device, a processing device, and a transmitting device. The receiving device is configured to receive at least a storage key, an authentication component, and static payment credentials. The input device is configured to receive at least one additional credential. The processing device is configured to generate a chip authentication program (CAP) token, wherein the CAP token is based on at least the authentication component and the at least one additional credential. The transmitting device is configured to transmit the generated CAP token. The receiving device is further configured to receive an encrypted payload, wherein the encrypted payload includes at least a supplied dynamic card validation code, session key unpredictable number, and application transaction counter. The processing device is further configured to decrypt the encrypted payload using at least the received storage key. The receiving device is further configured to receive, via near field communication, a reader unpredictable number from a point-of-sale terminal. The processing device is further configured to generate a payment dynamic card validation code based on at least the supplied dynamic card validation code, the session key unpredictable number, the application transaction counter, and the reader unpredictable number. The transmitting device is further configured to transmit, via near field communication, the generated payment dynamic card validation code and the application transaction counter to the point-of-sale terminal for including in an authorization request for a financial transaction.

[0016] The embodiments and/or examples disclosed in the following description which are not covered by the appended claims are considered as not being part of the present invention.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0017] The scope of the present disclosure is best understood from the following detailed description of exemplary embodiments when read in conjunction with the accompanying drawings. Included in the drawings are the following figures:

FIG. 1 is a high level diagram illustrating a system for generating and provisioning payment credentials to a mobile device in accordance with exemplary embodiments.

FIG. 2 is a block diagram illustrating the payment token payload of the system of FIG. 1 in accordance with exemplary embodiments.

FIG. 3 is a high level diagram illustrating an alternative system for provisioning payment credentials to a mobile device in accordance with exemplary embodiments.

FIG. 4 is a diagram illustrating a method for dual channel communication for use in the system of FIG. 1 in accordance with exemplary embodiments.

FIG. 5 is a flow chart illustrating the experience of a user of the mobile device of the system of FIG. 1 in accordance with exemplary embodiments.

FIG. 6 is a high level diagram illustrating methods for provisioning payment credentials to a mobile device and generating a payment cryptogram in accordance with exemplary embodiments.

FIG. 7 is a high level diagram illustrating methods for provisioning payment credentials to a mobile device and generating a dynamic card validation code in accordance with exemplary embodiments.

FIG. 8 is a flow diagram illustrating a method for reg-

IPR2025-01145
Apple EX1074 Page 4

istration of a mobile device for use in the system of FIG. 1 in accordance with exemplary embodiments.
FIG. 9 is a flow diagram illustrating a method for the initialization of a mobile application program on the mobile device of the system of FIG. 1 in accordance with exemplary embodiments.
FIG. 10 is a flow diagram illustrating a method for remote management of the mobile application program of the mobile device in accordance with exemplary embodiments.
FIG. 11 is a flow diagram illustrating a method for the delivery of a card profile to the mobile device of the system of FIG. 1 in accordance with exemplary embodiments.
FIG. 12 is a flow diagram illustrating a method for the delivery of a single use key to the mobile device of the system of FIG. 1 in accordance with exemplary embodiments.
FIG. 13 is a flow diagram illustrating a method for managing the mobile application program following the update of a mobile personal identification number of the mobile device of the system of FIG. 1 in accordance with exemplary embodiments.
FIG. 14 is a flow diagram illustrating a method for conducting a payment transaction using the mobile device of the system of FIG. 1 in accordance with exemplary embodiments.
FIG. 15 is a flow chart illustrating an exemplary method for generating and provisioning payment credentials to a mobile device lacking a secure element in accordance with exemplary embodiments.
FIG. 16 is a flow chart illustrating an exemplary method for generating a payment cryptogram in a mobile device lacking a secure element in accordance with exemplary embodiments.
FIG. 17 is a flow chart illustrating an alternative method for generating and provisioning payment credentials to a mobile device lacking a secure element in accordance with exemplary embodiments.
FIG. 18 is a flow chart illustrating an exemplary method for generating a dynamic card validation code in a mobile device lacking a secure element in accordance with exemplary embodiments.
FIG. 19 is a block diagram illustrating a computer system architecture in accordance with exemplary embodiments.

[0018] Further areas of applicability of the present disclosure will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description of exemplary embodiments are intended for illustration purposes only and are, therefore, not intended to necessarily limit the scope of the disclosure.

DETAILED DESCRIPTION

Definition of Terms

[0019] Payment Network - A system or network used for the transfer of money via the use of cash-substitutes. Payment networks may use a variety of different protocols and procedures in order to process the transfer of money for various types of transactions. Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc. Payment networks may be configured to perform transactions via cash-substitutes, which may include payment cards, letters of credit, checks, financial accounts, etc. Examples of networks or systems configured to perform as payment networks include those operated by MasterCard®, VISA®, Discover®, American Express®, etc.

[0020] Payment Account - A financial account that may be used to fund a transaction, such as a checking account, savings account, credit account, virtual payment account, etc. A payment account may be associated with an entity, which may include a person, family, company, corporation, governmental entity, etc. In some instances, a payment account may be virtual, such as those accounts operated by PayPal®, etc.

[0021] Payment Card - A card or data associated with a payment account that may be provided to a merchant in order to fund a financial transaction via the associated payment account. Payment cards may include credit cards, debit cards, charge cards, stored-value cards, prepaid cards, fleet cards, virtual payment numbers, virtual card numbers, controlled payment numbers, etc. A payment card may be a physical card that may be provided to a merchant, or may be data representing the associated payment account (e.g., as stored in a communication device, such as a smart phone or computer). For example, in some instances, data including a payment account number may be considered a payment card for the processing of a transaction funded by the associated payment account. In some instances, a check may be considered a payment card where applicable.

System for Generating and Provisioning Payment Credentials

[0022] FIG. 1 is a diagram illustrating a system 100 for the generating and provisioning of payment credentials to a mobile device lacking a secure element.

[0023] The system 100 may include a user 102. The user 102 may possess a mobile device 104. The mobile device 104 may be any type of mobile computing device suitable for performing the functions as disclosed herein, such as a cellular phone, smart phone, tablet computer, personal digital assistant, etc. In an exemplary embodiment, the mobile device 104 may not include a secure element.

IPR2025-01145
Apple EX1074 Page 5

[0024] The mobile device 104 may include a mobile payment application 106, which may be an application program stored in data storage of the mobile device 104 and executed by a processor included in the mobile device 104. The mobile payment application 106 may be configured to receive and store payment credentials and conduct payment transactions via near field communication without the use of a secure element, as discussed in more detail herein.

[0025] The user 102 may have a payment account with an issuer 108, such as a credit card account. The user 102 may desire to use their mobile device 104 to conduct payment transactions using their payment account with the issuer 108 for funding of the transactions. Payment credentials corresponding to the payment account may be stored by a remote-SE (remote-secure element) system 110 for provisioning to the mobile device 104. The remote-SE system 110 may include at least a payment credentials management service 112 and a remote notification server 114, each of which are discussed in more detail below.

[0026] The remote-SE system 110 may build a payment token payload in order to provision the payment credentials to the mobile device 104 for use in a payment transaction. The payment token payload (PTP) may be a container used to carry payment credentials from the remote-SE system 100 to the mobile payment application 106 in the mobile device 104. The payment token payload may include a card profile 116 and a single use key 118, discussed in more detail below. The card profile 116 may include the payment credentials, and the single use key 118 may be a single use (e.g., one-time use) key used to generate a payment cryptogram valid for a single payment transaction. In some embodiments, the remote-SE system 110 and the mobile device 104 may communicate using dual channel communication, discussed in more detail below.

[0027] The mobile device 104 may be further configured to transmit a generated payment cryptogram and payment credentials to a point-of-sale terminal 120 at a merchant. The point-of-sale terminal 120 may be any type of point-of-sale terminal or device suitable for receiving payment credentials via near field communication (NFC). Suitable methods and protocols for the secure transmission of information via NFC will be apparent to persons having skill in the relevant art. The point-of-sale terminal 120 may transmit the received payment credentials and other transaction information (e.g., transaction amount, product details, etc.) to an acquirer 122, such as an acquiring bank.

[0028] The acquirer 122 may submit an authorization request for the payment transaction to a payment network 124. The payment network 124 may be configured to process the authorization request, such as by querying the issuer 108 for approval of the payment transaction (e.g., based on funds or credits in the payment account). The payment network 124 may then submit an authorization response to the acquirer 122 and/or the merchant, who may then finalize the payment transaction with the user 102. Methods and systems suitable for the processing of a financial transaction will be apparent to persons having skill in the relevant art.

[0029] The system 100 and the use of the payment token payload may enable the user 102 to use the mobile device 104 to conduct NFC payment transactions without the use of a secure element.

Payment Token Payload

[0030] FIG. 2 is a diagram illustrating the payment token payload provisioned to the mobile device 104 in additional detail.

[0031] As discussed above, the payment token payload may include the card profile 116 and the single use key 118. The card profile 116 may include payment credentials provisioned to the mobile payment application 106 by the remote-SE system for use in conducting payment transactions. The payment credentials included in the card profile 116 may include common payment credentials 202, magnetic stripe (mag stripe) payment credentials 204, and m/chip payment credentials 206.

[0032] The common payment credentials 202 may include all data elements common to any type of payment transactions, such as both mag stripe and m/chip payment transactions. Such data elements may include payment account number, tracking data, and card layout description data. The mag stripe payment credentials 204 may include data elements specific to mag stripe transactions, such as the number of digits in an application transaction counter and a bitmap for an unpredictable number and the application transaction counter. The m/chip payment credentials 206 may include data elements specific to m/chip payment transactions, such as issuer action codes, risk management data, and offline data authentication object lists. In some embodiments, the mag stripe payment credentials 204 may be mandatory in the card profile 116 and the m/chip payment credentials 206 may be optional.

[0033] The single use key 118 may be a payment token used one time to generate a payment cryptogram to be used in a payment transaction. The single use key may include an application transaction counter (ATC) and a generating key 208. The application transaction counter may be a count of transactions used for fraud management and authentication as will be apparent to persons having skill in the relevant art. The generating key 208 may be a key used to generate a payment cryptogram used in a financial transaction. In one embodiment, the generating key 208 may generate a dynamic card validation code (CVC3) or an application cryptogram (AC). In a further embodiment, the application cryptogram may be optional.

[0034] The single use key 118 may also include an identifier used to identify the card profile 116 to which it corresponds to. In some embodiments, the single use key 118 may be protected based on a mobile personal

IPR2025-01145
Apple EX1074 Page 6

identification number (PIN) value. In such an embodiment, the user 102 may provide a mobile PIN for authentication. If the mobile PIN provided is incorrect, an incorrect value of the single use key may be used by the mobile payment application 106. In such an instance, the issuer 108 will not authorize the payment transaction. Such an embodiment may result in additional security for the user 102, the issuer 108, and the merchant involved in the payment transaction.

Alternative System for Generating and Provisioning Payment Credentials

[0035] FIG. 3 illustrates an alternative system 300 for generating and provisioning payment credentials to the mobile device 104 lacking a secure element.

[0036] In the system 300, the mobile device 104 may include the mobile payment application 106. The mobile device 104 may also include storage 304, such as a database. The remote-SE system 110 may include a cloud system 302. The cloud system 302 may store keys, payment credentials, and an application transaction counter, which may be provisioned from the cloud system 302 to the mobile device 104 and stored in the storage 304.

[0037] The mobile device 104 may generate a chip authentication program (CAP) token. The generation and use of CAP tokens will be apparent to persons having skill in the relevant art. The mobile device 104 may transmit the generated CAP token to the cloud system 302. The cloud system 302 may then authenticate (e.g., validate) the CAP token, such as by using a CAP token validation system as will be apparent to persons having skill in the relevant art. The cloud system 302 may then generate unpredictable numbers, and may generate an encrypted payload including a derived dynamic card validation code key (KD_{CVC3}) and the generated unpredictable number. The cloud system 302 may also transmit at least some of the information to the issuer 108. The issuer 108 may store the received information in an issuer database 310.

[0038] The encrypted payload may be transmitted to the mobile device 104, which may decrypt the payload and then generate a dynamic card validation code based on the information included in the encrypted payload and stored payment credentials. The user 102 may shop at a merchant 306, and, when goods or services have been selected for purchase, may transmit the payment credentials and dynamic card validation code from the mobile device 104 to the point-of-sale terminal 120. The point-of-sale terminal 120 may transmit the information and relevant transaction information to the acquirer 122.

[0039] An acquirer processing server 312 may receive the information at the acquirer 122 and may generate and submit an authorization request for the financial transaction including the payment credentials and dynamic card validation code to the payment network 124. The payment network 124 may forward relevant information to the issuer 108 for authorization of the transaction for a specific transaction amount. The issuer 108 may include an issuer processing server 308. The issuer processing server 308 may authenticate the dynamic card validation code based on the information stored in the issuer database 310 and received from the cloud system 302. The issuer 108 may then, based on the authentication, approve or deny the payment transaction.

[0040] The issuer 108 may submit a response to the payment network 124, which may then submit an authorization response to the acquirer 122. The acquirer may inform the merchant 306 of the results of the authorization, who may then finalize the transaction with the cardholder 102. Methods for provisioning payment credentials to the mobile device 104 and for processing a payment transaction via the mobile device 104 are discussed in more detail below.

Dual Channel Communication

[0041] FIG. 4 illustrates a method for dual channel communication for use in the system 100 of FIG. 1 for communication between the mobile device 104 and the remote-SE system 110. Dual channel communication may enable the mobile device 104 and the remote-SE system 110 to communicate using multiple protocols, which may allow for faster and/or more secure transmissions between the two systems.

[0042] Dual channel communication may include using remote notification 402 as a first channel, and mutual authentication 404 as a second channel. Remote notification 402 may be performed between the remote notification service 114 and the mobile device 104. In some embodiments, the payment credentials management service 112 may generate information, such as the single use key 118, to be provided to the mobile payment application 106. The payment credentials management service 112 may generate a message including the single use key encrypted with a random key to be provided and may encrypt the message using the mobile key.

[0043] The remote notification service 114 may then transmit the message to the mobile device 104 using remote notification. The mobile device 104 may provide the message to the mobile payment application 106, which may then decrypt the message using the shared mobile key, and then may decrypt the encrypted single use key with the random key, and thus use the single use key in a payment transaction. Methods for transmission of message using remote notification will be apparent to persons having skill in the relevant art.

[0044] Mutual authentication 404 may be used in instances where additional security may be desired, such as in forming an initial connection between the mobile device 104 and the remote-SE system 110. The mutual authentication 404 may use SSL/TLS communication to authenticate the remote-SE system 110 to the mobile device 104, and may use an authentication code, discussed in more detail below, to authenticate the mobile device 104 to the remote-SE system 110. In such an

IPR2025-01145
Apple EX1074 Page 7

instance, the authentication of both systems to the other provides the mutual authentication and additional security.

[0045] SSL/TLS communication is a standard method of communication as will be apparent to persons having skill in the relevant art. The authentication code may be a hash computed over a set of data known by both the remote-SE system 110 and the mobile device 104. For example, the authentication code may be computed over a unique identifier defined by the remote-SE system 110 to uniquely identify the mobile device 104, which may be provided to the mobile payment application 106 during initialization, discussed in more detail below. In an exemplary embodiment, the authentication code may be based on, in part, a session identifier. The session identifier may be transmitted from the remote-SE system 110 to the mobile device 104 using remote notification 402. In a further embodiment, the session identifier may be encrypted (e.g., using the mobile key). In such an embodiment, the mobile key may be used to decrypt the session identifier to be used to build the authentication code to be used for the mutual authentication 404.

[0046] The mobile device 104 and the remote-SE system 110 may both include the mobile key to be used as a shared key for the encrypting and decrypting of messages transmitted via remote notification. The mobile payment application 106 may also include a local storage encryption key. The local storage encryption key may be generated by the mobile payment application 106 and used to provide the storage 304 as an encrypted local database. The storage 304 may then store the shared mobile key, received payment credentials, and any additional information in the mobile device 104 to prevent unauthorized access.

Initialization and Use of the Mobile Payment Application

[0047] FIG. 5 illustrates a method 500 for the initialization and use of the mobile payment application 106 in the mobile device 104.

[0048] In step 502, the user 102 may register with the remote-SE system 110 to use the mobile device 104 for contactless payment transactions. The user 102 may register with the remote-SE system 110 using the mobile device 104 or another computing device, such as a desktop computer. Registration may be performed via a web browser, application program, or any other suitable method as will be apparent to persons having skill in the relevant art. As part of the registration, the user 102 may provide account information for the payment account with which the user 102 wants to use for payment transactions using the mobile device 104. The user 102 may receive an activation code and may also identify and/or receive a unique identifier used to identify the user 102.

[0049] In step 504, the user 102 may install the mobile payment application 106 on the mobile device 104. Methods for installing application programs on a mobile device will be apparent to persons having skill in the relevant art and may include using a web browser or application program on the mobile device 104 to identify and download the mobile payment application 106. It will also be apparent to persons having skill in the relevant art that step 504 may be performed before or concurrently with step 502.

[0050] In step 506, the user 102 may initialize/activate the mobile payment application 106. The user 102 may enter the activation code received in step 502 into the mobile payment application 106. The mobile payment application 106 may then communicate with the remote-SE system 110 and may receive the shared mobile key. The mobile payment application 106 may also generate the local storage encryption key and encrypt the storage 304 to create the local encrypted database.

[0051] In step 508, the remote-SE system 110 may transmit the card profile 116 to the mobile device 104. In one embodiment, the mobile device 104 may receive a remote notification message to notify the user 102 that the mobile payment application 106 must connect with the remote-SE system 110 using mutual authentication 404. Once connected, the remote-SE system 110 may then transmit the card profile including payment credentials for the account specified by the user 102 in step 502, which may then be stored by the mobile payment application 106 in the local encrypted database 304.

[0052] In step 510, the remote-SE system 110 may transmit a single use key 118 to the mobile payment application 106. In some embodiments, the transmission may be performed using mutual authentication 404 in the same process performed in step 510. In some embodiments, steps 508 and 510 may be combined in a single step, such that the remote-SE system may transmit both the card profile 116 and a single use key 118 to the mobile payment application 106 in a single or consecutive transactions.

[0053] In step 512, the mobile device 104 may conduct a contactless/NFC payment transaction using the mobile payment application 106 and the single use key 118. The mobile payment application 106 may generate a payment cryptogram, discussed in more detail below, and may transmit the generated cryptogram and payment credentials to a point-of-sale terminal 120. Methods for transmitting payment credentials and a payment cryptogram to a point-of-sale terminal 120 via NFC will be apparent to persons having skill in the relevant art.

[0054] In step 514, the mobile payment application 106 may identify if there are any single use keys 118 available for use in subsequent payment transactions. If there are additional keys 118 available for use, then the method 500 may return to step 512 where additional payment transactions may be conducted with the remaining single use key(s) 118. If there are no single use keys 118 remaining, then, the method 500 may return to step 510 where connection may be made with the remote-SE system 110 and a new single use key 118 provisioned to the mobile device 104.

IPR2025-01145
Apple EX1074 Page 8

Method for Provisioning Payment Credentials and Generating a Payment Cryptogram

[0055] FIG. 6 illustrates a more detailed version of the system 100 and illustrates the process by which payment credentials may be generated and provisioned to the mobile device 104 and the mobile device 104 used to conduct a contactless payment transaction without the use of a secure element.

[0056] The user 102 may register with the remote-SE system 110. The remote-SE system 110 may store the user registration information (e.g., payment account information) in a database 602 and may return an activation code to the user 102. The user 102 may then install the mobile payment application 106 on the mobile device 104 and activate the mobile payment application 106 using the activation code. As part of the activation, the remote-SE system 110 may transmit a shared mobile key 604 to the mobile payment application 106. The mobile payment application 106 may also generate a local storage encryption key and may encrypt the storage 304 on the mobile device 104. The mobile key 604 may be stored in the local encrypted database 304.

[0057] The payment credentials management service112 may store the shared mobile key 604 in the database 602. The payment credentials management service 112 may also identify payment credentials corresponding to the payment account indicated by the user, and build the card profile 116 including the payment credentials. The remote notification service 114 may transmit a remote notification to the mobile device 104 to indicate to the user 102 that the card profile 116 is ready to be downloaded to the mobile payment application 106. The mobile payment application 106 may then communicate with the payment credentials management service 112 using mutual authentication and receive the card profile 116 from the remote-SE system. The mobile payment application 106 may then store the received card profile 116 in the local encrypted database 304.

[0058] The payment credentials management service 112 may also generate a single use key 118 including a generating key. In some embodiments, the single use key 118 may be generated in response to the receipt of a key request from the mobile device 104. In a further embodiment, the key request may include a mobile PIN. The payment credentials management service 112 may have previously stored the mobile PIN (e.g., as set by the user 102) in the database 602.

[0059] The payment credentials management service 112 may then transmit the generated single use key 118 to the mobile device 104, which may then store the single use key 118 in the local encrypted database 304. In some instances, the single use key 118 may be incorrect (e.g., fake, not genuine, etc.) if the key request includes a mobile PIN for which authentication is unsuccessful. In some embodiments the key may have been combined with the PIN such that when used it is incorrect without any explicit authentication step. In some embodiments, the card profile 116 and/or the single use key 118 may be encrypted by the payment credentials management service 112 prior to transmission to the mobile device 104, such as by using the mobile key 604. The mobile payment application 106 may then decrypt the received message, also using the shared mobile key 604, or, in some embodiments, a random key.

[0060] Once the mobile payment application 106 includes both the card profile 116 and the single use key 118, the user 102 may shop at a merchant 306 and select goods or services for purchase. The user 102 may then input to the mobile payment application 106 that a payment transaction is to be conducted. The mobile payment application 106 may then generate a payment cryptogram using the generating key included in the single use key 118. The payment cryptogram may be, for example, an application cryptogram or a dynamic card validation code (CVC3). The mobile payment application 106 may transmit the payment cryptogram to the merchant point-of-sale terminal 120.

[0061] The merchant point-of-sale terminal 120 may transmit the received payment information and any additional transaction information (e.g., transaction amount, merchant identifier, etc.) to the acquirer processing server 312 of the acquirer 122. The acquirer processing server 312 may then generate and submit an authorization request for the financial transaction to the payment network 124. The payment network 124 may transmit relevant transaction data, such as the payment information and transaction amount, to the issuer processing server 308. The issuer processing server 308 may then validate the application cryptogram. If the validation is successful, the issuer may approve the payment transaction for the transaction amount (e.g., based on an available amount, credit, etc. for the payment account). If the validation is unsuccessful, the issuer may deny the payment transaction. Methods for validating a cryptogram will be apparent to persons having skill in the relevant art.

[0062] In some embodiments, the remote-SE system 110 may transmit information to the issuer 108 for storage in the issuer database 310, such as for fraud management. Such information will be apparent to persons having skill in the relevant art and may include, for example, application transaction counters. Methods suitable for performing the functions as disclosed herein are discussed in more detail below with respect to the flow diagrams illustrated in FIGS. 8-14.

Alternative Method for Provisioning Payment Credentials and Generating a Payment Cryptogram

[0063] FIG. 7 illustrates a more detailed version of the alternative system 300 and illustrates the process by which payment credentials may be generated and provisioned to the mobile device 104 and the mobile device 104 used to conduct a contactless payment transaction without the use of a secure element.

[0064] The user 102 may install the mobile application

IPR2025-01145
Apple EX1074 Page 9

program 106 on the mobile device 104. Prior to the beginning of the process, at stage A, the mobile application program 106 may store authentication keys and credentials in the storage 304 as received from the remote-SE system 110. At stage B, a storage key ($K_{STORAGE}$) may be stored in the storage 304 as well. At stage C, additional information, including static payment credentials, may be stored in the storage 304.

[0065] At stage 1, the user 102 may launch the mobile payment application 106 using the mobile device 104. At stage 2a, the mobile payment application 106 may connect with the remote-SE system 110 via the cloud system 302, such as by using SSL authentication or any other suitable method for authenticated transmission. The cloud system 302 may transmit payment credentials to the mobile payment application 106, which may then be stored in the storage 304. At stage 2b, the mobile payment application 106 may generate a CAP token used for authentication. In some embodiments, the user 102 may supply additional authentication credentials, such as a gesture, a password, or a biometric identifier.

[0066] In stage 3, the mobile payment application 106 may transmit the generated CAP token to the remote-SE system 100. At stage 4, the CAP token may be forward to a CAP token validation service (CTVS) 702. At stage 5, the CTVS 702 may validate the CAP token using methods apparent to persons having skill in the relevant art. At stage 6, the results of the validation may be sent to the payment credentials management system 704. In some embodiments, the payment credentials management system 704 may be operated by or on behalf of the issuer 108.

[0067] At stage 7, the payment credentials management system 704 may generate an encrypted payload. As part of the encrypted payload, the payment credentials management system 704 may generate a session key unpredictable number (KS_{UN}), a cloud unpredictable number (UN_{CLOUD}), and may identify and/or store a plurality of dynamic card validation code (CVC3) keys and the $K_{STORAGE}$. Methods and systems for the generation of unpredictable numbers will be apparent to persons having skilled in the relevant art. The encrypted payload may include at least one CVC3 key, the KSUN, and the application transaction counter and may be generated using a derived CVC3 key (KD_{CVC3}). In one embodiment, the KD_{CVC3} used may be fake if the CAP token validation is unsuccessful. The payload may be encrypted using the $K_{STORAGE}$.

[0068] At stage 8a, the payment credentials management system 704 may perform a synchronization process with the issuer 108. The synchronization process may include defining rules for the validity of the values generated by the mobile payment application 106 for conducting a payment transaction. In one embodiment, the process may include transmitting at least the KS_{UN}, application transaction counter, and UN_{CLOUD} to the issuer 108 for storage in the issuer database 310.

[0069] At stage 8b, the encrypted payload may be transmitted to the cloud system 302 for transmitting to the mobile payment application 106 in stage 9. At stage 10, the encrypted payload may be decrypted using the $K_{STORAGE}$ and stored in the storage 304. At stage 11, the user 102 may shop at the merchant 306 and select goods or services for purchase. As part of the purchase, at stage 12, the mobile payment application 106 may generate a payment CVC3 value. In one embodiment, the mobile device 104 may communicate with the point-of-sale terminal 120. The point-of-sale terminal 120 may generate a reader unpredictable number (UN_{READER}) and transmit the UN_{READER} to the mobile payment application 106, which may then generate the payment CVC3 value using the information in the encrypted payload and the UN_{READER}. The generated payment CVC3 value and the application transaction counter may be transmitted to the point-of-sale terminal 120 via NFC.

[0070] In some embodiments, the user 102 may be required to enter a PIN at the point-of-sale terminal 120 for additional authentication at stage 13. At stage 14, the point-of-sale terminal 120 may execute standard NFC payment transaction processes as will be apparent to persons having skill in the relevant art. At stage 15, the point-of-sale terminal 120 may generate an authorization request for the payment transaction, which may include the UN_{READER}, the generated CVC3 value, the application transaction counter, and, if applicable, the PIN value input by the user 102. At stage 16, the acquirer processing server 312 may translate the PIN included in the authorization request using methods apparent to persons having skill in the relevant art. It will be further apparent that stage 16 may be optional.

[0071] At stage 17, the authorization request may be forwarded to the payment network 124, which may forward the authorization request and/or information included in the authorization request to the issuer 108. At optional stage 18, the issuer may verify the translated PIN. At stage 19a, the issuer 108 may identify if additional processing is necessary and may, if necessary, retrieve the values stored in the issuer database 310. At stage 19b, the issuer processing server 308 may validate the payment CVC3 value using at least the UN_{READER}, UN_{CLOUD}, and application transaction counter. Methods for validating a CVC3 will be apparent to persons having skill in the relevant art. At stage 20, the issuer 108 may submit a response based on the validation, and the method may proceed accordingly as in traditional payment transactions.

Method for Registration of a User for Remote Payment Transactions

[0072] FIG. 8 is a flow diagram illustrating a method for the user 102 to register with the remote-SE system 110 to enable a payment account for remote payment transactions using a mobile device 104 lacking a secure element.

[0073] At step 806, the user 102 may access the reg-

IPR2025-01145
Apple EX1074 Page 10

istration system of the remote-SE system 110. The user 102 may access the system via a web browser 804, which may be executed on a computing device. In one embodiment, the computing device may be the mobile device 104. The user 102 may navigate to a webpage hosted by or on behalf of the remote-SE system 110. At step 808, the user 102 may register with the payment credentials management service 112 via the browser 804. As part of the registration, the user 102 may provide account details for a payment account, and the payment credentials management service 112 may ensure the payment account is eligible for remote payment transactions.

[0074] At step 810, the payment credentials management service 112 may create a user profile for the user 102 in the remote-SE system 110. In some embodiments, a user profile may also be created in the issuer system 108. As part of the creation of the user profile, the payment credentials management service 112 may generate and/or identify an activation code. At step 812, the user registration may be completed and the activation code transmitted back to the 102 via the browser 804. At step 814, the payment credentials management service 112 may synchronize information (e.g., the user profile, activation code status, etc.) with the issuer 108 for fraud management. It will be apparent to persons having skill in the relevant art that step 814 may be optional.

[0075] At step 816, the user 102 may receive the activation code via the web browser 804. At step 818, the user 102 may download the mobile payment application 106 to the mobile device 104. In one embodiment, the user 102 may utilize an app store 802, such as the Apple® App Store, to download the mobile payment application 106. The mobile payment application 106 may be validated and installed on the mobile device at step 820 using methods and systems apparent to persons having skill in the relevant art. At step 822, the mobile payment application 106 may be successfully installed on the mobile device 104 and may await initialization.

Method for Initialization of the Mobile Payment Application

[0076] FIG. 9 is a flow diagram illustrating a method for initialization of the mobile payment application 106 on the mobile device 104 for use in contactless payment transactions.

[0077] At step 902, the user may start (e.g., execute) the mobile payment application on the mobile device 104. At step 904, the mobile payment application 106 may perform an integrity check. As part of the integrity check, the mobile payment application 106 may authenticate the user 102 and request the activation code provided to the user 102 during the registration process (e.g., at step 812 in FIG. 8). At step 906, the mobile payment application 106 may generate a unique identifier and additional values and keys, such as a local database storage key (e.g., mobile storage key).

[0078] At step 908, the mobile payment application 106 may connect to the payment credentials management service 112 using mutual authentication. The mobile payment application 106 may transmit the activation code and any other additional user authentication information (e.g., a user identifier, a password, etc.) as a method of authentication. The mobile payment application 106 may also transmit the generated unique identifier. In some embodiments, the user 102 may also provide a mobile PIN to be transmitted to the payment credentials management service 112 as part of step 908.

[0079] At step 910, the payment credentials management service 112 may validate the mobile payment application 106 using the provided authentication information and may, if validated, update the user profile to include the unique identifier. At step 912, the payment credentials management service 112 may also register the mobile device 104 with the remote notification service 114 using the unique identifier. At step 914, the payment credentials management service 112 may generate the shared mobile key 604 and may store the shared mobile key 604 in the user profile. At optional step 916, the payment credentials management service 112 may synchronize with the issuer 108 for fraud management.

[0080] At step 918, the mobile payment application 106 may receive the shared mobile key 604 from the payment credentials management service 112 and may store the mobile key 604 in the encrypted local storage 304. At step 920, the mobile payment application 106 may wipe the mobile storage key, such that the encrypted local storage 304 may not be access without authorization. The mobile payment application 106 may store data with which the mobile storage key is generated separate from the encrypted local storage 304 for use in regenerating the mobile storage key for access to the encrypted local storage 304. At step 922, the mobile payment application 106 may be ready for remote management by the payment credentials management service 112. In some embodiments, the mobile payment application 106 may notify the user 102 when initialization is completed.

Method for Remote Management of the Mobile Payment Application

[0081] FIG. 10 is a flow diagram illustrating a method for remote management of the mobile payment application 106 of the mobile device 104 via the payment credentials management service 112.

[0082] In step 1002, the payment credentials management service 112 may receive a trigger to start the remote management of the mobile payment application 106. In some embodiments, the trigger may be received from the payment credentials management service 112 itself based on predefined rules. In another embodiment, the trigger may be received from the issuer 108. In step 1004, the payment credentials management service 112 may prepare data for remote notification. The preparation of data may include the building of a notification based on a function to be performed, such as the provisioning of

IPR2025-01145
Apple EX1074 Page 11

the card profile 116, provisioning of a single use key 118, changing of the mobile PIN, etc. An exemplary method for provisioning of the card profile 116 to the mobile device 104 is discussed in more detail below with reference to FIG. 11.

[0083] The payment credentials management service 112 may build a message including the notification and a session identifier, and then may encrypt the message using the mobile key 604. The payment credentials management service 112 may also identify the mobile device 104 for receipt using the unique identifier in the user profile. In embodiments where step 1004 may include the provisioning of the single use key 118, the single use key 118 may be encrypted using a random key (e.g., or suitable key other than the mobile key 604), and then the encrypted single use key may be encrypted using the mobile 604 and provisioned to the mobile payment application 106 similar to the encryption and transmission of the message as disclosed herein.

[0084] In step 1006, the payment credentials management service 112 may transmit the encrypted message to the mobile payment application 106 using remote notification 402. As discussed above, remote notification 402 may include the forwarding of the encrypted message to the remote notification service 114, which may transmit the encrypted message to the mobile device 104 using remote notification, which may then make the encrypted message available to the mobile payment application 106. In step 1008, the mobile payment application 106 may receive the encrypted message.

[0085] In step 1010, the user 102 may start the mobile payment application 106. It will be apparent to persons having skill in the relevant art that step 1010 may be optional (e.g., the mobile payment application 106 may start upon receipt of the encrypted message, the mobile payment application 106 may always run in the background, etc.). In step 1012, the mobile payment application 106 may start, which may include regenerating the mobile storage key, retrieving the mobile key 406 from the local encrypted storage 304, and decrypting the message using the retrieved mobile key 406.

[0086] In step 1014, the mobile payment application 106 may connect to the payment credentials management service 112 using mutual authentication 404 as discussed above, such as by generating, transmitting, and then wiping an authentication code including the session identifier. At step 1016, the payment credentials management service 112 may validate the authentication credentials transmitted by the mobile payment application 106. If validated, the payment credentials management service 112 may then have a secure connection with the mobile payment application 106 and may proceed with the function indicated in the notification.

Method for Provisioning of a Card Profile to the Mobile Payment Application

[0087] FIG. 11 is a flow diagram illustrating a method for provisioning the card profile 116 to the mobile payment application 106 of the mobile device 104 by the payment credentials management service 112.

[0088] Utilizing the connection made upon the triggering of remote management illustrated in FIG. 10, at step 1102 the payment credentials management service 112 may build the payment token payload card profile 116. The card profile 116 may include payment credentials for the payment account indicated by the user 102 during registration, which may have been stored in the user profile. The payment credentials management service 112 may build the card profile by generating a message including the payment credentials, generating a mobile session key, and encrypting the message using the mobile session key. The payment credentials management service 112 may store the card profile 116 in the user profile and, in step 1104, may transmit the message including the card profile 116 to the mobile payment application 106.

[0089] In step 1106, the mobile payment application 106 may receive the message and may generate the mobile session key used for decrypting the message. At step 1108, the mobile payment application 106 may decrypt the message using the generated mobile session key and may validate the message. Once validated, at step 1110 the mobile payment application 106 may build a receipt message indicating successful receipt and validation of the card profile 116, and may be used as an activation message and/or used to carry information from the mobile payment application 106 to the remote-SE system 110. The receipt message may be encrypted using the mobile session key. The mobile payment application 106 may also update a status to indicate that the card profile 116 is successfully received and stored.

[0090] In step 1112, the receipt message may be received by the payment credentials management service 112 and may be decrypted using the mobile session key and validated. Upon successful validation, in step 1114 the payment credentials management service 112 may activate the card profile 116 and may update the user profile accordingly. In step 1116, the payment credentials management service 112 may transmit a notification to the mobile payment application 106 that the card profile 116 has been activated and may wipe the mobile session key. In step 1118, the payment credentials management service 112 may synchronize the user profile indicating activation of the card profile 116 with the issuer 108 for fraud management.

[0091] In step 1120, the mobile payment application 106 may analyze the return code indicating activation of the card profile 116. In step 1122, the mobile payment application 106 may wipe the mobile session key, and in step 1124 may be ready to receive single use keys 118 for use in conducting payment transactions. In some embodiments, the mobile payment application 106 may display a notification to the user 102 via a user interface to indicate that single use keys 118 may be received.

IPR2025-01145
Apple EX1074 Page 12

Method for Provisioning Single Use Keys to the Mobile Payment Application

[0092] FIG. 12 is a flow diagram illustrating a method for the provisioning of single use keys 118 to the mobile payment application 106 in the mobile device 104 by the payment credentials management service 112 for use in payment transactions.

[0093] In an exemplary embodiment, while performing the connection with the payment credentials management service 112 made upon the triggering of remote management illustrated in FIG. 10, the encrypted single use key 118, may be previously transmitted to the mobile payment application 106 in a message encrypted by the mobile key 604. At step 1202, the payment credentials management service 112 may build a message with an action to activate (e.g., decrypt) the previously provisioned single use key 118, the message including the random key used to encrypt the single use key 118. The payment credentials management service 112 may then generate a mobile session key and then may encrypt the message including the random key using the mobile session key. The payment credentials management service 112 may then, in step 1204, transmit the message including the random key to the mobile payment application 106.

[0094] In step 1206, the mobile payment application 106 may receive the message and may generate the mobile session key used for decrypting the message. At step 1208, the mobile payment application 106 may decrypt the message using the generated mobile session key and may validate the message. The mobile payment application 106 may also decrypt the single use key 118 using the random key included in the decrypted message, and may validate the decrypted single use key 118. Once validated, at step 1210 the mobile payment application 106 may build a receipt message indicating successful receipt and validation of the single use key 118. The receipt message may be encrypted using the mobile session key. The mobile payment application 106 may also update a status to indicate that the single use key 118 is successfully received and stored and that the mobile payment application 106 is ready to conduct a payment transaction.

[0095] In step 1212, the receipt message may be received by the payment credentials management service 112 and may be decrypted using the mobile session key and validated. Upon successful validation, in step 1214 the payment credentials management service 112 may activate the single use key 118 and may update the user profile accordingly. In step 1216, the payment credentials management service 112 may transmit a notification to the mobile payment application 106 that the single use key 118 has been activated and may wipe the mobile session key. In step 1218, the payment credentials management service 112 may synchronize the user profile indicating activation of the single use key 118 with the issuer 108 for fraud management.

[0096] In step 1220, the mobile payment application 106 may analyze the return code indicating activation of the single use key 118. In step 1222, the mobile payment application 106 may wipe the mobile session key, and in step 1224 may be ready to conduct a contactless payment transaction. In some embodiments, the mobile payment application 106 may display a notification to the user 102 via a user interface to indicate that the mobile payment application 106 is ready to conduct a contactless payment transaction.

Method for Modification of Mobile PIN in the Mobile Payment Application

[0097] FIG. 13 is a flow diagram illustrating a method for the management of a change in the mobile PIN of the user 102 in the mobile payment application 106 by the payment credentials management service 112.

[0098] Utilizing the connection made upon the triggering of remote management illustrated in FIG. 10, at step 1302 the payment credentials management service 112 may build a remote management action indicating a change to the mobile PIN and removal of all stored single use keys 118. The payment credentials management service 112 may build a message including the remote management action, generate a mobile session key, and encrypt the message using the mobile session key. The payment credentials management service 112 may, in step 1304, transmit the message including remote management action to the mobile payment application 106.

[0099] In step 1306, the mobile payment application 106 may receive the message and may generate the mobile session key used for decrypting the message. At step 1308, the mobile payment application 106 may decrypt the message using the generated mobile session key and may validate the message. Once the message has been validated, the mobile payment application may update the card profile 116 accordingly and may remove any available single use keys 118 from the encrypted local storage 304. Then, at step 1310, the mobile payment application 106 may build a receipt message indicating successful receipt and execution of the remote management action. The receipt message may be encrypted using the mobile session key.

[0100] In step 1312, the receipt message may be received by the payment credentials management service 112 and may be decrypted using the mobile session key and validated. Upon successful validation, in step 1314 the payment credentials management service 112 may update the user profile accordingly. In step 1316, the payment credentials management service 112 may transmit a notification to the mobile payment application 106 that the user profile has been updated and no single use keys 118 have been issued, and may wipe the mobile session key. In step 1318, the payment credentials management service 112 may synchronize the user profile indicating the change to the mobile PIN and wiping of single use keys 118 with the issuer 108 for fraud management.

IPR2025-01145
Apple EX1074 Page 13

[0101] In step 1320, the mobile payment application 106 may analyze the return code. In step 1322, the mobile payment application 106 may wipe the mobile session key, and in step 1324 may be ready to receive single use keys 118 for use in conducting payment transactions. In some embodiments, the mobile payment application 106 may display a notification to the user 102 via a user interface to indicate that single use keys 118 may be received.

Method for Conducting a Payment Transaction Using the Mobile Payment Application

[0102] FIG. 14 is a flow diagram illustrating a method for conducting a contactless payment transaction using the mobile payment application 106 on the mobile device 104 using the card profile 116 and single use key 118 provisioned by the payment credentials management service 112.

[0103] In step 1402, the user 102 may start the mobile payment application 106 on the mobile device 104. In step 1404, the mobile payment application 106 may prepare for payment. To prepare for payment, the mobile payment application 106 may regenerate the mobile storage key and may retrieve the payment credentials and generating key from the card profile 116 and the single use key 118 in the encrypted local storage 304. The generating key may be used by the mobile payment application 106 to generate a payment cryptogram for use in the payment transaction. The mobile payment application 106 may also indicate to the user 102 that the application is ready for payment.

[0104] In step 1406, a NFC payment method may be executed between the user 102, the mobile device 104, the mobile payment application 106, and the point-of-sale terminal 120. Methods for executing transmission of payment credentials from a mobile device to a point-of-sale terminal will be apparent to persons having skill in the relevant art.

[0105] In step 1408, the point-of-sale terminal 120 at the merchant 306 may provide transaction data to the acquirer 122 including the payment credentials and payment cryptogram. In step 1410, the acquirer 122 may submit an authorization request including the transaction data to the payment network 124. In step 1412, the payment network 124 may seek authorization from the issuer 108 for the payment transaction and may forward relevant information to the issuer 108. In step 1414, the issuer 108 may validate the payment cryptogram using methods that will be apparent to persons having skill in the relevant art. The issuer 108 may, once the payment cryptogram is validated, approve or deny the payment transaction (e.g., based on a transaction amount and available credit in the payment account for the user 102) and notify the payment network 124. At step 1416, the payment network 124 may submit an authorization response to the acquirer 122, which may then forward the response to the merchant 306 and/or point-of-sale terminal 120 at step 1418. At step 1420, the merchant may finalize the payment transaction, such as by providing the transacted goods or services to the user 102 or by providing a receipt to the user 102.

[0106] Once the payment transaction has been completed, the mobile payment application 106 may, at step 1422, update the payment token payload stored in the encrypted local storage 304 based on the outcome of the payment transaction. At step 1424, the mobile payment application 106 may wipe the mobile storage key, and at step 1426, may indicate (e.g., to the user 102) that the mobile payment application 106 is ready for another contactless payment transaction (e.g., if additional single use keys 118 are available) or to receive single use keys 118.

[0107] In some embodiments, the payment transaction may be conducted via the use of local data authentication (LDA). In some instances, the storage of payment credentials received by the mobile device 104 in the encrypted local storage 304 (e.g., and not in a Secure Element) may be such that CDA (combined dynamic data authentication/application cryptogram generation) may be unavailable to support traditional card verification methods to verify the payment credentials used in the financial transaction. As a result, the point-of-sale terminal 120 may be configured such that it may require authentication by the user 102 at both the mobile device 104 (e.g., entering of the mobile PIN) and the point-of-sale terminal 120 (e.g., entering of an online PIN or signature).

[0108] LDA may be used in order to provide card authentication support such that a financial transaction may be supported by the point-of-sale terminal 120 utilizing a single point of authentication (e.g., the mobile PIN). In order to perform LDA, the card profile 116 may further include one RSA key pair and certificate. The performing of the LDA may include the swapping of the meaning of the effective date and the expiration date in the payment credentials included in the card profile 116, and the setting of at least one issuer action code to force the payment transaction to be an online transaction. In a further embodiment, the expiration date may be set as a date prior to the date of issuance, or the effective date may be set as a date beyond the expiry date, or both may be set as defined. This may result in the point-of-sale terminal 120 declining the transaction due to the expiration and/or effective dates, but transmitting the transaction for online authorization, which may result in processing of the transaction using the single point of authentication by the user 102. In a further embodiment, the expiration date may be set as a previous date, or the effective date may be set as a future date, or both may be set as defined. In some embodiments, performing LDA may further include setting an issuer action code configured to decline offline transactions (e.g., such that if the point-of-sale terminal 120 is an offline-only terminal it may decline all such transactions).

[0109] It is noted that, although the method illustrated in FIG. 14 and described above is a method for conducting a contactless payment transaction, such a method

IPR2025-01145
Apple EX1074 Page 14

may also be used for conducting a remote payment transaction, for the secure transmission of payment credentials, for use as part of an authentication solution (whether part of a transaction or otherwise), or in other applications as will be apparent to persons having skill in the relevant art and not limited to those illustrated herein.

Exemplary Method for Generating and Provisioning Payment Credentials

[0110] FIG. 15 is a flow chart illustrating a method 1500 for generating and provisioning payment credentials to a mobile device lacking a secure element.

[0111] At step 1502, a card profile (e.g., the card profile 116) associated with a payment account may be generated by a processing device (e.g., of the payment credentials management service 112), wherein the card profile 116 includes at least payment credentials corresponding to the associated payment account and a profile identifier. At step 1504, the generated card profile 116 may be provisioned to a mobile device (e.g., the mobile device 104) lacking a secure element. In one embodiment, provisioning the card profile 116 may include building a message including the generated card profile 116, generating an encryption key, encrypting the message using the generated encryption key, and provisioning the encrypted message to the mobile device 104.

[0112] At step 1506, a key request may be received from the mobile device 104, wherein the key request includes at least a mobile personal identification number (PIN) and the profile identifier. At step 1508, an authentication device (e.g., of the payment credentials management service 112) may use the mobile PIN. In one embodiment, the authentication device may use the mobile PIN using an XOR method. At step 1510, a single use key (e.g., the single use key 118) may be generated by the processing device, wherein the single use key 118 includes at least the profile identifier, an application transaction counter, and a generating key for use in generating a payment cryptogram valid for a single financial transaction. In some embodiments, the single use key 118 may be genuine if the mobile PIN is successfully authenticated in step 1508, and fake if the mobile PIN is unsuccessfully authenticated. In one embodiment, the method 1500 may further include transmitting the generated single use key 118 to an issuer associated with the payment account. In some embodiments, the generated single use key 118 may be inactive.

[0113] At step 1512, the generated single use key 118 may be transmitted, by a transmitting device, to the mobile device 104. In one embodiment, transmitting the generated single use key 118 may include building a message including the generated single use key 118, generating an encryption key, encrypting the message using the generated encryption key, and provisioning the encrypted message to the mobile device 104.

[0114] In embodiments where the generated single use key 118 may be inactive, the method 1500 may further include receiving, from the mobile device 104, and indication of use of the single use key 118 and activating, by the processing device, the generated single use key 118. In a further embodiment, the method 1500 may also include transmitting, by the transmitting device, an indication of activation of the single use key 118 to an issuer (e.g., the issuer 108) associated with the payment account.

Method for Generating a Payment Cryptogram

[0115] FIG. 16 is a flow chart illustrating a method 1600 for generating a payment cryptogram in a mobile device (e.g., the mobile device 104) lacking a secure element.

[0116] In step 1602, a card profile (e.g., the card profile 116) may be received by a receiving device (e.g., in the mobile device 104), wherein the card profile 116 includes at least payment credentials corresponding to a payment account and a profile identifier. In one embodiment, receiving the card profile 116 may include receiving an encrypted message including the card profile 116, generating a mobile session key, and decrypting the message using the generated mobile session key to obtain the included card profile 116. In some embodiments, the card profile 116 may be configured to utilize local data authentication, wherein the local data authentication includes swapping, in the payment credentials, the meaning of an expiration date and an effective date, and setting an issuer action code configured to force the financial transaction to be an online transaction. In a further embodiment, the expiration date may be set as a date prior to the date of issuance, or the effective date may be set as a date beyond the expiry date, or both may be set as defined. In a further embodiment, the card profile 116 may further include one RSA key pair and certificate.

[0117] In step 1604, an input device (e.g., of the mobile device 104, such as a touch screen) may receive a mobile personal identification number (PIN) input by a user (e.g., the user 102) of the mobile device 104. In step 1606, a transmitting device may transmit a key request, wherein the key request includes at least the profile identifier.

[0118] In step 1608, a single use key (e.g., the single use key 118) may be received, by the receiving device, wherein the single use key 118 includes at least an application transaction counter and a generating key. In one embodiment, receiving the single use key 118 may include receiving an encrypted message including the single use key 118, generating a mobile session key, and decrypting the message using the generated mobile session key to obtain the included single use key 118.

[0119] In step 1610, a payment cryptogram valid for a single payment transaction may be generated, by a processing device, based on at least the received single use key 108 and the mobile PIN. In some embodiments, the payment cryptogram may be an application cryptogram or a dynamic card validation code. In step 1612, at least the payment credentials and the generated payment cryptogram may be transmitted, via near field com-

IPR2025-01145
Apple EX1074 Page 15

munication, to a point-of-sale terminal (e.g., the point-of-sale terminal 120) for use in a financial transaction.

[0120] In some embodiments, the method 1600 may further include receiving, by the input device, an indication of use of the received single use key 118, transmitting, by the transmitting device, an activation request including at least the profile identifier, and receiving, by the receiving device, an indication of activation of the single use key 118. In a further embodiment, the payment credentials and generated payment cryptogram may be transmitted to the point-of-sale terminal 120 in response to receiving the indication of activation of the single use key 118. In an alternative further embodiment, the payment cryptogram may be generated in response to receiving the indication of activation of the single use key 118.

Alternative Method for Generating and Provisioning Payment Details

[0121] FIG. 17 is a flow chart illustrating an alternative method 1700 for generating and provisioning payment details to a mobile device (e.g., the mobile device 104) lacking a secure element.

[0122] In step 1702, at least a storage key, a plurality of dynamic card validation code (CVC3) keys, and an application transaction counter associated with a mobile application program (e.g., the mobile payment application 106) may be stored in a database (e.g., the storage 304). In step 1704, at least the storage key, an authentication component, and static payment credentials may be provisioned to the mobile device 104, wherein the static payment credentials are associated with a payment account.

[0123] In step 1706, a chip authentication program (CAP) token may be received from the mobile device 104. In step 1708, the authenticity of the received CAP token may be validated by a validation service (e.g., the CTVS 702). In one embodiment, the CAP token may be validated based on at least the provisioned authentication component and an additional credential received from the mobile device 104. In a further embodiment, the additional credential may be at least one of: a gesture, a password, a passcode, and a biometric identifier. In another embodiment, validating the authenticity of the CAP token may include validating the authenticity of the CAP token based on at least the application transaction counter.

[0124] In step 1710, a session key unpredictable number (KS_{UN}) may be generated by a processing device (e.g., the cloud system 302). In step 1712, a cloud unpredictable number (UN_{CLOUD}) may be generated by the processing device 302. In step 1714, the processing device 302 may identify an encrypted payload based on a derived CVC3 key (KD_{CVC3}), wherein the encrypted payload includes at least a CVC3 key of the plurality of CVC3 keys, the KS_{UN}, and the application transaction counter. In one embodiment, the KD_{CVC3} may be genuine if the received CAP token is successfully validated, and may be fake if the received CAP token is unsuccessfully validated. In some embodiment, the payload may be encrypted using at least the storage key.

[0125] In step 1716, a transmitting device may transmit the encrypted payload to the mobile device 104 for use in generating a CVC3 value for use in a financial transaction. In step 1718, the transmitting device may transmit at least the KS_{UN}, UN_{CLOUD}, and application transaction counter to an issuer (e.g., the issuer 108) associated with the payment account for use in validating the generated CVC3 value used in the financial transaction.

Method for Generating a Dynamic Card Validation Code

[0126] FIG. 18 is a flow chart illustrating a method 1800 for generating a dynamic card validation code (CVC3) value in a mobile device (e.g., the mobile device 104) lacking a secure element.

[0127] In step 1802, at least a storage key, an authentication component, and static payment credentials may be received by a receiving device. In step 1804, at least one additional credential may be received by an input device (e.g., of the mobile device 104). In some embodiments, the at least one additional credential may include at least one of: a gesture, a password, a passcode, and a biometric identifier. In step 1806, a chip authentication program (CAP) token may be generated by a processing device, wherein the CAP token is based on at least the authentication component and the at least one additional credential.

[0128] In step 1808 the generated CAP token may be transmitted by a transmitting device. In step 1810, an encrypted payload may be received by the receiving device, wherein the encrypted payload includes at least a supplied CVC3 value, session key unpredictable number, and an application transaction counter. In step 1812, the processing device may decrypt the encrypted payload using at least the received storage key.

[0129] In step 1814, a reader unpredictable number may be received, via near field communication, from a point-of-sale terminal (e.g., the point-of-sale terminal 120). In step 1816, the processing device may generate a payment CVC3 value based on at least the supplied CVC3 value, the session key unpredictable number, the application transaction counter, and the reader unpredictable number. In step 1818, the generated payment CVC3 value and the application transaction counter may be transmitted, via near field communication, to the point-of-sale terminal 120 for including in an authorization request in a financial transaction.

Computer System Architecture

[0130] FIG. 19 illustrates a computer system 1900 in which embodiments of the present disclosure, or portions thereof, may be implemented as computer-readable code. For example, the payment credentials manage-

IPR2025-01145
Apple EX1074 Page 16

ment 112, the remote notification service 114, the mobile device 104, the acquirer processing server 312, and the issuer processing server 308 may be implemented in the computer system 1900 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 thereof may embody modules and components used to implement the methods of FIGS. 6-18.

[0131] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. A person having 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. For instance, at least one processor device and a memory may be used to implement the above described embodiments.

[0132] A processor device as discussed herein may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor "cores." The terms "computer program medium," "non-transitory computer readable medium," and "computer usable medium" as discussed herein are used to generally refer to tangible media such as a removable storage unit 1918, a removable storage unit 1922, and a hard disk installed in hard disk drive 1912.

[0133] Various embodiments of the present disclosure are described in terms of this example computer system 1900. 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.

[0134] Processor device 1904 may be a special purpose or a general purpose processor device. The processor device 1904 may be connected to a communication infrastructure 1906, such as a bus, message queue, network, multi-core message-passing scheme, etc. The network may be any network suitable for performing the functions as disclosed herein and may include a local area network (LAN), a wide area network (WAN), a wireless network (e.g., WiFi), a mobile communication network, a satellite network, the Internet, fiber optic, coaxial cable, infrared, radio frequency (RF), or any combination thereof. Other suitable network types and configurations will be apparent to persons having skill in the relevant art. The computer system 1900 may also include a main memory 1908 (e.g., random access memory, read-only memory, etc.), and may also include a secondary memory 1910. The secondary memory 1910 may include the hard disk drive 1912 and a removable storage drive 1914, such as a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, etc.

[0135] The removable storage drive 1914 may read from and/or write to the removable storage unit 1918 in a well-known manner. The removable storage unit 1918 may include a removable storage media that may be read by and written to by the removable storage drive 1914. For example, if the removable storage drive 1914 is a floppy disk drive, the removable storage unit 1918 may be a floppy disk. In one embodiment, the removable storage unit 1918 may be non-transitory computer readable recording media.

[0136] In some embodiments, the secondary memory 1910 may include alternative means for allowing computer programs or other instructions to be loaded into the computer system 1900, for example, the removable storage unit 1922 and an interface 1920. Examples of such means may include a program cartridge and cartridge interface (e.g., as found in video game systems), a removable memory chip (e.g., EEPROM, PROM, etc.) and associated socket, and other removable storage units 1922 and interfaces 1920 as will be apparent to persons having skill in the relevant art.

[0137] Data stored in the computer system 1900 (e.g., in the main memory 1908 and/or the secondary memory 1910) may be stored on any type of suitable computer readable media, such as optical storage (e.g., a compact disc, digital versatile disc, Blu-ray disc, etc.) or magnetic tape storage (e.g., a hard disk drive). The data may be configured in any type of suitable database configuration, such as a relational database, a structured query language (SQL) database, a distributed database, an object database, etc. Suitable configurations and storage types will be apparent to persons having skill in the relevant art.

[0138] The computer system 1900 may also include a communications interface 1924. The communications interface 1924 may be configured to allow software and data to be transferred between the computer system 1900 and external devices. Exemplary communications interfaces 1924 may include a modem, a network interface (e.g., an Ethernet card), a communications port, a PCMCIA slot and card, etc. Software and data transferred via the communications interface 1924 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals as will be apparent to persons having skill in the relevant art. The signals may travel via a communications path 1926, which may be configured to carry the signals and may be implemented using wire, cable, fiber optics, a phone line, a cellular phone link, a radio frequency link, etc.

[0139] Computer program medium and computer usable medium may refer to memories, such as the main memory 1908 and secondary memory 1910, which may be memory semiconductors (e.g. DRAMs, etc.). These computer program products may be means for providing

IPR2025-01145
Apple EX1074 Page 17

software to the computer system 1900. Computer programs (e.g., computer control logic) may be stored in the main memory 1908 and/or the secondary memory 1910. Computer programs may also be received via the communications interface 1924. Such computer programs, when executed, may enable computer system 1900 to implement the present methods as discussed herein. In particular, the computer programs, when executed, may enable processor device 1904 to implement the methods illustrated by FIGS. 6-18, as discussed herein. Accordingly, such computer programs may represent controllers of the computer system 1900. Where the present disclosure is implemented using software, the software may be stored in a computer program product and loaded into the computer system 1900 using the removable storage drive 1914, interface 1920, and hard disk drive 1912, or communications interface 1924.

[0140] Techniques consistent with the present disclosure provide, among other features, systems and methods for the provisioning of payment credentials to mobile devices lacking a secure element and the generation of payment cryptograms based thereon. While various exemplary embodiments of the disclosed system and method have been described above it should be understood that they have been presented for purposes of example only, not limitations. It is not exhaustive and does not limit the disclosure to the precise form disclosed.

Claims

1. A method for generating and provisioning payment credentials to a mobile device (104) lacking a secure element, comprising:

generating, by a processing device of a remote system (110), a card profile associated with a payment account, wherein the card profile includes at least payment credentials corresponding to the associated payment account and a profile identifier;
provisioning, by the remote system, to a mobile device, the generated card profile;
receiving, by the remote system, from the mobile device, a key request, wherein the key request includes at least a mobile personal identification number, PIN, and the profile identifier;
in response to receiving the key request from the mobile device, determining, by an authentication device of the remote system, whether the mobile PIN is authentic;
based on the determination of authenticity of the mobile PIN generating, by the processing device of the remote system, a single use key, wherein the single use key is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and the single use key includes at least the profile identifier, an application transaction counter, and a generating key; and
transmitting, by a transmitting device of the remote system, the generated single use key to the mobile device, wherein the mobile device lacks a secure element.

2. The method of claim 1, further comprising:
transmitting, by the transmitting device of the remote system, the generated single use key to an issuer associated with the payment account.

3. The method of claim 1, wherein provisioning, by the remote system, the generated card profile to the mobile device includes building a message including the generated card profile, generating an encryption key, encrypting the message using the generated encryption key, and provisioning the encrypted message to the mobile device.

4. The method of claim 1, wherein transmitting the generated single use key to the mobile device includes building a message, by the remote system, including the generated single use key, generating an encryption key, encrypting the message using the generated encryption key, and provisioning the encrypted message to the mobile device.

5. The method of claim 1, wherein the generated single use key is inactive, said method further comprising:

receiving, by the remote system, from the mobile device, an indication of use of the single use key;
activating, by the processing device of the remote system, the generated single use key; and
transmitting, by the transmitting device of the remote system, an indication of activation of the single use key to an issuer associated with the payment account.

6. The method of claim 1, wherein the payment cryptogram is an application cryptogram or a dynamic card validation code.

7. A method for generating a payment cryptogram in a mobile device (104) lacking a secure element, comprising:

receiving, by a receiving device of the mobile device, a card profile from a remote system (110), wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier;
receiving, by an input device of the mobile device, a mobile personal identification number, PIN, input by a user of the mobile device;
transmitting, by a transmitting device of the mobile device, a key request to the remote system,

IPR2025-01145
Apple EX1074 Page 18

wherein the key request includes at least the profile identifier and a mobile personal identification number, PIN, wherein said key request causes said remote device to generate a single use key;
receiving, by the receiving device of the mobile device, the single use key from the remote system, wherein the single use key is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and the single use key includes at least an application transaction counter, a generating key, and the profile identifier;
generating, by a processing device of the mobile device, the payment cryptogram valid for the single financial transaction based on at least the received single use key and the mobile PIN; and
transmitting, by the mobile device, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction.

8. The method of claim 7, wherein the payment cryptogram is an application cryptogram or a dynamic card validation code.

9. The method of claim 7, wherein receiving, by the mobile device, the card profile includes receiving an encrypted message including the card profile, generating a mobile session key, and decrypting the message using the generated mobile session key to obtain the included card profile.

10. The method of claim 7, wherein receiving, by the mobile device, the single use key includes receiving an encrypted message including the single use key, generating a mobile session key, and decrypting the message using the generated mobile session key to obtain the included single use key.

11. The method of claim 7, further comprising:

receiving, by the input device of the mobile device, an indication of use of the received single use key;
transmitting, by the transmitting device of the mobile device, an activation request, wherein the activation request includes at least the profile identifier; and
receiving, by the receiving device of the mobile device, an indication of activation of the single use key,
wherein the payment credentials and generated payment cryptogram are transmitted, by the mobile device, to the point-of-sale terminal in response to receiving the indication of activation of the single use key.

12. The method of claim 11, wherein the payment cryptogram is generated, by the mobile device, in response to receiving the indication of activation of the single use key.

13. The method of claim 7, wherein
the card profile is configured to utilize local data authentication, and
local data authentication includes one of (1) swapping, in the payment credentials, the meaning of an expiration date and an effective date, (2) setting the expiration date as a date prior to the date of issuance, or (3) setting the effective date as a date beyond the expiry date, or both may be set as the expiration date and effective date as defined, and setting an issuer action code configured to force the financial transaction to be an online transaction.

14. A system (100) for generating and provisioning payment credentials to a mobile device (104) lacking a secure element, comprising:

a transmitting device of a remote system (110);
a processing device, of the remote system configured to generate a card profile associated with a payment account, wherein the card profile includes at least payment credentials corresponding to the associated payment account and a profile identifier;
a provisioning device, of the remote system, configured to provision, to a mobile device lacking a secure element, the generated card profile;
a receiving device, of the remote system, configured to receive, from the mobile device, a key request, wherein the key request includes at least a mobile personal identification number, PIN, and the profile identifier; and
an authentication device, of the remote system, configured to authenticate the mobile PIN in response to receiving the key request, wherein
the processing device, of the remote system, is further configured to generate a single use key on a basis of mobile PIN authenticity, wherein the single use key is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and the single use key includes at least the profile identifier, an application transaction counter, and a generating key for use in generating the payment cryptogram valid for the single financial transaction, and
the transmitting device, of the remote system, is configured to transmit the generated single use key to the mobile device.

15. The system of claim 14, wherein the transmitting device, of the remote system, is further configured to transmit the generated single use key to an issuer

IPR2025-01145
Apple EX1074 Page 19

associated with the payment account.

16. The system of claim 14, wherein the provisioning device, of the remote system, provisions the generated card profile to the mobile device within a message encrypted by an encryption key.

17. The system of claim 14, wherein the transmitting device, of the remote system, transmits the generated single use key to the mobile device within a message encrypted by an encryption key.

18. The system of claim 14, wherein
the generated single use key is inactive,
the receiving device, of the remote system, is further configured to receive from the mobile device, an indication of use of the single use key,
the processing device, of the remote system, is further configured to activate the generated single use key, and
the transmitting device, of the remote system, is further configured to transmit an indication of activation of the single use key to an issuer associated with the payment account.

19. A system (100) for generating a payment cryptogram in a mobile device (104) lacking a secure element, comprising:

a processing device, of the mobile device;
a receiving device, of the mobile device, configured to receive a card profile from a remote system (110), wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier;
an input device, of the mobile device, configured to receive a mobile personal identification number, PIN, input by a user of the mobile device; and
a transmitting device, of the mobile device, configured to transmit a key request to the remote system, wherein the key request includes at least the profile identifier and a mobile personal identification number, PIN, and causes said remote device to generate a single use key, wherein

the receiving device, of the mobile device, is further configured to receive the single use key from the remote system, wherein the single use key is configured to be used one time, by the mobile device, to generate a payment cryptogram valid for a single financial transaction and the single use key includes at least an application transaction counter, a generating key, and the profile identifier,
the processing device, of the mobile device, is configured to generate the payment cryptogram valid for the single financial transaction based on at least the received single use key and the mobile PIN, and
the transmitting device, of the mobile device, is further configured to transmit, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction.

20. The system of claim 19, wherein
the input device, of the mobile device, is further configured to receive indication of use of the received single use key,
the transmitting device, of the mobile device, is further configured to transmit an activation request, wherein the activation request includes at least the profile identifier,
the receiving device, of the mobile device, is further configured to receive an indication of activation of the single use key, and
the transmitting device, of the mobile device, is further configured to transmit the payment credentials and the generated payment cryptogram in response to receipt of the indication of activation of the single use key.

21. The system of claim 20, wherein the processing device, of the mobile device, is configured to generate the payment cryptogram in response to the receipt of the indication of activation of the single use key.

Patentansprüche

1. Verfahren zur Erstellung und Bereitstellung von Zahlungsberechtigungsnachweisen an eine mobile Vorrichtung (104), der ein sicheres Element fehlt, umfassend:

Erstellen, durch eine Verarbeitungsvorrichtung eines Remote-Systems (110), eines Kartenprofils, das mit einem Zahlungskonto assoziiert ist, wobei das Kartenprofil zumindest Zahlungsberechtigungsnachweise, die dem assoziierten Zahlungskonto entsprechen, und eine Profilkennung beinhaltet;
Bereitstellen, durch das Remote-System an eine mobile Vorrichtung, des erstellten Kartenprofils;
Empfangen, durch das Remote-System von der mobilen Vorrichtung, einer Schlüsselanforderung, wobei die Schlüsselanforderung zumindest eine mobile persönliche Identifikationsnummer, PIN, und die Profilkennung enthält;
in Reaktion auf das Empfangen der Schlüsselanforderung von der mobilen Vorrichtung, Be-

IPR2025-01145
Apple EX1074 Page 20

stimmen, durch eine Authentifizierungsvorrichtung des Remote-Systems, ob die mobile PIN authentisch ist;
basierend auf der Authentifizierungsbestimmung der mobilen PIN, Erstellen, durch die Verarbeitungsvorrichtung des Remote-Systems, eines Einmalgebrauchsschlüssels, wobei der Einmalgebrauchsschlüssel dazu konfiguriert ist, ein Mal durch die mobile Vorrichtung zum Erstellen eines Zahlungskryptogramms, das für eine einzelne finanzielle Transaktion gültig ist, benutzt zu werden und der Einmalgebrauchsschlüssel zumindest die Profilkennung, einen Anwendungstransaktionszähler und einen Erstellungsschlüssel enthält; und
Übertragen, durch eine Übertragungsvorrichtung des Remote-Systems, des erstellten Einmalgebrauchsschlüssels an die mobile Vorrichtung, wobei der mobilen Vorrichtung ein sicheres Element fehlt.

2. Verfahren nach Anspruch 1, ferner umfassend:
Übertragen, durch die Übertragungsvorrichtung des Remote-Systems, des Einmalgebrauchsschlüssels an einen Aussteller, der mit dem Zahlungskonto assoziiert ist.

3. Verfahren nach Anspruch 1, wobei das Bereitstellen, durch das Remote-System, des erstellten Kartenprofils an die mobile Vorrichtung das Bilden einer Nachricht, die das erstellte Kartenprofil enthält, Erstellen eines Verschlüsselungsschlüssels, Verschlüsseln der Nachricht unter Verwendung des erstellten Verschlüsselungsschlüssels und Bereitstellen der verschlüsselten Nachricht an die mobile Vorrichtung enthält.

4. Verfahren nach Anspruch 1, wobei das Übertragen des erstellten Einmalgebrauchsschlüssels an die mobile Vorrichtung das Bilden einer Nachricht, durch das Remote-System, die den erstellten Einmalgebrauchsschlüssel enthält, Erstellen eines Verschlüsselungsschlüssels, Verschlüsseln der Nachricht unter Verwendung des erstellten Verschlüsselungsschlüssels und Bereitstellen der verschlüsselten Nachricht an die mobile Vorrichtung enthält.

5. Verfahren nach Anspruch 1, wobei der erstellte Einmalgebrauchsschlüssel inaktiv ist, das Verfahren ferner umfassend:

Empfangen, durch das Remote-System, einer Verwendungsanzeige des Einmalgebrauchsschlüssels;
Aktivieren, durch die Verarbeitungsvorrichtung des Remote-Systems, des erstellten Einmalgebrauchsschlüssels; und
Übertragen, durch die Übertragungsvorrichtung des Remote-Systems, einer Aktivierungsanzeige des Einmalgebrauchsschlüssels an einen Aussteller, der mit dem Zahlungskonto assoziiert ist.

6. Verfahren nach Anspruch 1, wobei das Zahlungskryptogramm ein Anwendungskryptogramm oder ein dynamischer Kartenvalidierungscode ist.

7. Verfahren zum Erstellen eines Zahlungskryptogramms in einer mobilen Vorrichtung (104), der ein sicheres Element fehlt, umfassend:

Empfangen, durch eine Empfangsvorrichtung der mobilen Vorrichtung, eines Kartenprofils von einem Remote-System (110), wobei das Kartenprofil zumindest Zahlungsberechtigungsnachweise, die einem Zahlungskonto entsprechen, und eine Profilkennung beinhaltet;
Empfangen, durch eine Eingabevorrichtung der mobilen Vorrichtung, einer mobilen persönlichen Identifikationsnummer, PIN, die durch einen Benutzer der mobilen Vorrichtung eingegeben wird;
Übertragen, durch eine Übertragungsvorrichtung der mobilen Vorrichtung, einer Schlüsselanforderung an das Remote-System, wobei die Schlüsselanforderung zumindest die Profilkennung und eine mobile persönliche Identifikationsnummer, PIN, enthält, wobei die Schlüsselanforderung bewirkt, dass die Remote-Vorrichtung einen Einmalgebrauchsschlüssel erstellt;
Empfangen, durch die Empfangsvorrichtung der mobilen Vorrichtung, des Einmalgebrauchsschlüssels vom Remote-System, wobei der Einmalgebrauchsschlüssel dazu konfiguriert ist, ein Mal durch die mobile Vorrichtung zum Erstellen eines Zahlungskryptogramms, das für eine einzelne finanzielle Transaktion gültig ist, benutzt zu werden und der Einmalgebrauchsschlüssel zumindest einen Anwendungstransaktionszähler, einen Erstellungsschlüssel und die Profilkennung enthält;
Erstellen, durch eine Verarbeitungsvorrichtung der mobilen Vorrichtung, des Zahlungskryptogramms, das für die einzelne finanzielle Transaktion gültig ist, basierend zumindest auf dem empfangenen Einmalgebrauchsschlüssel und der mobilen PIN; und
Übertragen, durch die mobile Vorrichtung über Nahfeldkommunikation, von zumindest den Zahlungsberechtigungsnachweisen und dem erstellten Zahlungskryptogramm an ein Kassenterminal zum Gebrauch in einer finanziellen Transaktion.

8. Verfahren nach Anspruch 7, wobei das Zahlungskryptogramm ein Anwendungskryptogramm oder

IPR2025-01145
Apple EX1074 Page 21

ein dynamischer Kartenvalidierungscode ist.

9. Verfahren nach Anspruch 7, wobei das Empfangen, durch die mobile Vorrichtung, des Kartenprofils das Empfangen einer verschlüsselten Nachricht, die das Kartenprofil beinhaltet, Erstellen eines mobilen Sitzungsschlüssels und Entschlüsseln der Nachricht unter Verwendung des erstellten Sitzungsschlüssels zum Erhalten des beinhalteten Kartenprofils umfasst.

10. Verfahren nach Anspruch 7, wobei das Empfangen, durch die mobile Vorrichtung, des Einmalgebrauchsschlüssels das Empfangen einer verschlüsselten Nachricht, die den Einmalgebrauchsschlüssel beinhaltet, Erstellen eines mobilen Sitzungsschlüssels und Entschlüsseln der Nachricht unter Verwendung des erstellten Sitzungsschlüssels zum Erhalten des beinhalteten Einmalgebrauchsschlüssels umfasst.

11. Verfahren nach Anspruch 7, ferner umfassend:

Empfangen, durch die Eingabevorrichtung der mobilen Vorrichtung, einer Verwendungsanzeige des empfangenen Einmalgebrauchsschlüssels;
Übertragen, durch die Übertragungsvorrichtung der mobilen Vorrichtung, einer Aktivierungsanforderung, wobei die Aktivierungsanforderung zumindest die Profilkennung enthält; und
Empfangen, durch die Empfangsvorrichtung der mobilen Vorrichtung, einer Aktivierungsanzeige des Einmalgebrauchsschlüssels,
wobei die Zahlungsberechtigungsnachweise und das erstellte Zahlungskryptogramm durch die mobile Vorrichtung in Reaktion auf das Empfangen der Aktivierungsanzeige des Einmalgebrauchsschlüssels an das Kassenterminal übertragen werden.

12. Verfahren nach Anspruch 11, wobei das Zahlungskryptogramm durch die mobile Vorrichtung in Reaktion auf das Empfangen der Aktivierungsanzeige des Einmalgebrauchsschlüssels erstellt wird.

13. Verfahren nach Anspruch 7, wobei
das Kartenprofil zum Nutzen von lokaler Datenauthentifikation konfiguriert ist, und
lokale Datenauthentifikation eines von (1) Austauschen, in den Zahlungsberechtigungsnachweisen, der Bedeutung eines Ablaufdatums und eines Wirksamkeitsdatums, (2) Einstellen des Ablaufdatums als ein Datum vor dem Ausstellungsdatum oder (3) Einstellen des Wirksamkeitsdatums als ein Datum über das Ablaufdatum hinaus, oder wobei beide als das Ablaufdatum und Wirksamkeitsdatum wie definiert eingestellt werden können, und Einstellen eines Aussstelleraktionscodes, der zum Erzwingen, dass die finanzielle Transaktion eine Online-Transaktion ist, konfiguriert ist, beinhaltet.

14. System (100) zur Erstellung und Bereitstellung von Zahlungsberechtigungsnachweisen an eine mobile Vorrichtung (104), der ein sicheres Element fehlt, umfassend:

eine Übertragungsvorrichtung eines Remote-Systems (110);
eine Verarbeitungsvorrichtung des Remote-Systems, die zum Erstellen eines Kartenprofils, das mit einem Zahlungskonto assoziiert ist, konfiguriert ist, wobei das Kartenprofil zumindest Zahlungsberechtigungsnachweise, die dem assoziierten Zahlungskonto entsprechen, und eine Profilkennung beinhaltet;
eine Bereitstellungsvorrichtung des Remote-Systems, das zum Bereitstellen des erstellten Kartenprofils an eine mobile Vorrichtung, der ein sicheres Element fehlt, konfiguriert ist;
eine Empfangsvorrichtung des Remote-Systems, die zum Empfangen einer Schlüsselanforderung von der mobilen Vorrichtung konfiguriert ist, wobei die Schlüsselanforderung zumindest eine mobile persönliche Identifikationsnummer, PIN, und die Profilkennung enthält; und
eine Authentifizierungsvorrichtung des Remote-Systems, die zum Authentifizieren der mobilen PIN in Reaktion auf das Empfangen der Schlüsselanforderung konfiguriert ist, wobei
die Verarbeitungsvorrichtung des Remote-Systems ferner zum Erstellen eines Einmalgebrauchsschlüssels auf einer Basis mobiler PIN-Authentizität konfiguriert ist, wobei der Einmalgebrauchsschlüssel dazu konfiguriert ist, ein Mal durch die mobile Vorrichtung zum Erstellen eines Zahlungskryptogramms, das für eine einzelne finanzielle Transaktion gültig ist, benutzt zu werden und der Einmalgebrauchsschlüssel zumindest die Profilkennung, einen Anwendungstransaktionszähler und einen Erstellungsschlüssel zum Gebrauch beim Erstellen des Zahlungskryptogramms, das für die einzelne finanzielle Transaktion gültig ist, enthält; und
die Übertragungsvorrichtung des Remote-Systems zum Übertragen des erstellten Einmalgebrauchsschlüssels an die mobile Vorrichtung konfiguriert ist.

15. System nach Anspruch 14, wobei die Übertragungsvorrichtung des Remote-Systems ferner zum Übertragen des Einmalgebrauchsschlüssels an einen Aussteller, der mit dem Zahlungskonto assoziiert ist, konfiguriert ist.

16. System nach Anspruch 14, wobei die Bereitstel-

IPR2025-01145
Apple EX1074 Page 22

lungsvorrichtung des Remote-Systems das erstellte Kartenprofil an die mobile Vorrichtung innerhalb einer Nachricht, die durch einen Verschlüsselungsschlüssel verschlüsselt ist, konfiguriert ist.

17. System nach Anspruch 14, wobei die Übertragungsvorrichtung des Remote-Systems den erstellten Einmalgebrauchsschlüssel an die mobile Vorrichtung innerhalb einer Nachricht, die durch einen Verschlüsselungsschlüssel verschlüsselt ist, überträgt.

18. System nach Anspruch 14, wobei
der erstellte Einmalgebrauchsschlüssel inaktiv ist,
die Empfangsvorrichtung des Remote-Systems ferner zum Empfangen, von der mobilen Vorrichtung, einer Verwendungsanzeige des Einmalgebrauchsschlüssels konfiguriert ist,
die Verarbeitungsvorrichtung des Remote-Systems ferner zum Aktivieren des erstellten Einmalgebrauchsschlüssels konfiguriert ist, und
die Übertragungsvorrichtung des Remote-Systems ferner zum Übertragen einer Aktivierungsanzeige des Einmalgebrauchsschlüssels an einen Aussteller, der mit dem Zahlungskonto assoziiert ist, konfiguriert ist.

19. System (100) zum Erstellen eines Zahlungskryptogramms in einer mobilen Vorrichtung (104), der ein sicheres Element fehlt, umfassend:

eine Verarbeitungsvorrichtung der mobilen Vorrichtung;
eine Empfangsvorrichtung der mobilen Vorrichtung, die zum Empfangen eines Kartenprofils von einem Remote-System (110) konfiguriert ist, wobei das Kartenprofil zumindest Zahlungsberechtigungsnachweise, die einem Zahlungskonto entsprechen, und eine Profilkennung beinhaltet;
eine Eingabevorrichtung der mobilen Vorrichtung, die zum Empfangen einer mobilen persönlichen Identifikationsnummer, PIN, welche durch einen Benutzer der mobilen Vorrichtung eingegeben wird, konfiguriert ist; und
eine Übertragungsvorrichtung der mobilen Vorrichtung, die zum Übertragen einer Schlüsselanforderung an das Remote-System konfiguriert ist, wobei die Schlüsselanforderung zumindest die Profilkennung und eine mobile persönliche Identifikationsnummer, PIN, enthält, und bewirkt, dass die Remote-Vorrichtung einen Einmalgebrauchsschlüssel erstellt, wobei
die Empfangsvorrichtung der mobilen Vorrichtung ferner zum Empfangen des Einmalgebrauchsschlüssels vom Remote-System konfiguriert ist, wobei der Einmalgebrauchsschlüssel dazu konfiguriert ist, ein Mal durch die mobile Vorrichtung zum Erstellen eines Zahlungskryptogramms, das für eine einzelne finanzielle Transaktion gültig ist, benutzt zu werden und der Einmalgebrauchsschlüssel zumindest einen Anwendungstransaktionszähler, einen Erstellungsschlüssel und die Profilkennung enthält;
die Verarbeitungsvorrichtung der mobilen Vorrichtung zum Erstellen des Zahlungskryptogramms, das für die einzelne finanzielle Transaktion gültig ist, basierend zumindest auf dem empfangenen Einmalgebrauchsschlüssel und der mobilen PIN konfiguriert ist, und
die Übertragungsvorrichtung der mobilen Vorrichtung ferner zum Übertragen, über Nahfeldkommunikation, von zumindest den Zahlungsberechtigungsnachweisen und dem erstellten Zahlungskryptogramm an ein Kassenterminal zum Gebrauch in einer finanziellen Transaktion konfiguriert ist.

20. System nach Anspruch 19, wobei
die Eingabevorrichtung der mobilen Vorrichtung ferner zum Empfangen einer Verwendungsanzeige des empfangenen Einmalgebrauchsschlüssels konfiguriert ist,
die Übertragungsvorrichtung der mobilen Vorrichtung ferner zum Übertragen einer Aktivierungsanforderung konfiguriert ist, wobei die Aktivierungsanforderung zumindest die Profilkennung enthält,
die Empfangsvorrichtung der mobilen Vorrichtung ferner zum Empfangen einer Aktivierungsanzeige des Einmalgebrauchsschlüssels konfiguriert ist, und
die Übertragungsvorrichtung der mobilen Vorrichtung ferner zum Übertragen der Zahlungsberechtigungsnachweise und des erstellten Zahlungskryptogramm in Reaktion auf den Empfang der Aktivierungsanzeige des Einmalgebrauchsschlüssels konfiguriert ist.

21. System nach Anspruch 20, wobei die Verarbeitungsvorrichtung der mobilen Vorrichtung zum Erstellen des Zahlungskryptogramms in Reaktion auf den Empfang der Aktivierungsanzeige des Einmalgebrauchsschlüssels konfiguriert ist.

Revendications

1. Procédé pour la génération et de fourniture d'identifiants de paiement à un dispositif mobile (104) sans éléments sécurisés, comprenant :

la génération d'un profil de carte associé à un compte de paiement, par un dispositif de traitement d'un système distant (110), le profil de carte comprenant au moins des identifiants de paiement correspondant au compte de paiement associé et à un identifiant de profil ;

IPR2025-01145
Apple EX1074 Page 23

la fourniture du profil de carte généré, par le système distant, à un dispositif mobile ;
la réception d'une demande de clé par le système distant, en provenance du dispositif mobile, la demande de clé comprenant au moins un numéro d'identification personnel mobile, PIN, et l'identifiant de profil ;
en réponse à la réception de la demande de clé provenant du dispositif mobile, la détermination de l'authenticité du PIN mobile, par un dispositif d'authentification du système distant ;
sur la base de la détermination de l'authenticité du PIN mobile, la génération d'une clé à usage unique, par le dispositif de traitement du système distant, la clé à usage unique étant configurée pour être utilisée une seule fois, par le dispositif mobile, pour générer un cryptogramme de paiement valide pour une seule transaction financière, et la clé à usage unique comprenant au moins l'identifiant de profil, un compteur de transaction d'application, et une clé de génération ; et
la transmission de la clé à usage unique générée au dispositif mobile par un dispositif de transmission du système distant, le dispositif mobile manquant d'éléments sécurisés.

2. Procédé selon la revendication 1, comprenant en outre :
la transmission de la clé à usage unique générée à un émetteur associé au compte de paiement, par le dispositif de transmission du système distant.

3. Procédé selon la revendication 1, dans lequel la fourniture du profil de carte généré au dispositif mobile par le système distant comprend la création d'un message comprenant le profil de carte généré, la génération d'une clé de cryptage, le cryptage du message à l'aide de la clé de cryptage générée, et la fourniture du message crypté au dispositif mobile.

4. Procédé selon la revendication 1, dans lequel la transmission de la clé à usage unique générée au dispositif mobile comprend la création, par le système distant, d'un message comprenant la clé à usage unique générée, la génération d'une clé de cryptage, le cryptage du message à l'aide de la clé de cryptage générée, et la fourniture du message crypté au dispositif mobile.

5. Procédé selon la revendication 1, dans lequel la clé à usage unique générée est inactive, ledit procédé comprenant en outre :

la réception d'une indication d'utilisation de la clé à usage unique, par le système distant en provenance du dispositif mobile ;
l'activation, par le dispositif de traitement du système distant, de la clé à usage unique générée ; et
la transmission d'une indication d'activation de la clé à usage unique, par le dispositif de transmission du système distant, à un émetteur associé au compte de paiement.

6. Procédé selon la revendication 1, dans lequel le cryptogramme de paiement est un cryptogramme d'application ou un code de validation de carte dynamique.

7. Procédé pour la génération d'un cryptogramme de paiement dans un dispositif mobile (104) sans éléments sécurisés, comprenant :

la réception d'un profil de carte par un dispositif récepteur du dispositif mobile, à partir d'un système distant (110), le profil de carte comprenant au moins des identifiants de paiement correspondant à un compte de paiement et à un identifiant de profil ;
la réception, par un dispositif de saisie du dispositif mobile, d'un numéro d'identification personnel mobile, PIN, saisi par un utilisateur du dispositif mobile ;
la transmission d'une demande de clé par un dispositif de transmission du dispositif mobile au système distant, la demande de clé comprenant au moins un identifiant de profil et un numéro d'identification personnel mobile, PIN, ladite demande de clé incitant ledit dispositif distant à générer une clé à usage unique ;
la réception de la clé à usage unique par le dispositif récepteur du dispositif mobile, en provenance du système distant, la clé à usage unique étant configurée pour être utilisée une seule fois, par le dispositif mobile, pour générer un cryptogramme de paiement valide pour une seule transaction financière, et la clé à usage unique comprenant au moins un compteur de transaction d'application, une clé de génération et l'identifiant de profil ;
la génération, par un dispositif de traitement du dispositif mobile, du cryptogramme de paiement valide pour la transaction financière unique, au moins sur la base de la clé à usage unique reçue et du PIN mobile ; et
la transmission, par le dispositif mobile, via une communication en champ proche, au moins des identifiants de paiement et du cryptogramme de paiement généré, à un terminal de point de vente pour une utilisation dans une transaction financière.

8. Procédé selon la revendication 7, dans lequel le cryptogramme de paiement est un cryptogramme d'application ou un code de validation de carte dy-

IPR2025-01145
Apple EX1074 Page 24

namique.

9. Procédé selon la revendication 7, dans lequel la réception du profil de carte par le dispositif mobile comprend la réception d'un message crypté comprenant le profil de carte, la génération d'une clé de session mobile, et le décryptage du message à l'aide de la clé de session mobile générée pour obtenir le profil de carte inclus.

10. Procédé selon la revendication 7, dans lequel la réception de la clé à usage unique par le dispositif mobile comprend la réception d'un message crypté comprenant la clé à usage unique, la génération d'une clé de session mobile, et le décryptage du message à l'aide de la clé de session mobile générée pour obtenir la clé à usage unique incluse.

11. Procédé selon la revendication 7, comprenant en outre :

la réception, par le dispositif de saisie du dispositif mobile, d'une indication d'utilisation de la clé à usage unique reçue ;
la transmission, par le dispositif de transmission du dispositif mobile, d'une demande d'activation, la demande d'activation comprenant au moins l'identifiant de profil ; et
la réception, par le dispositif récepteur du dispositif mobile, d'une indication d'activation de la clé à usage unique,
dans lequel les identifiants de paiement et le cryptogramme de paiement généré sont transmis par le dispositif mobile au terminal de point de vente en réponse à la réception de l'indication d'activation de la clé à usage unique.

12. Procédé selon la revendication 11, dans lequel le cryptogramme de paiement est généré par le dispositif mobile en réponse à la réception de l'indication d'activation de la clé à usage unique.

13. Procédé selon la revendication 7, dans lequel
le profil de carte est configuré pour utiliser une authentification de données locale, et
l'authentification de données locale comprend l'un parmi (1) le remplacement, dans les identifiants de paiement, de la signification d'une date d'expiration et d'une date effective, (2) le réglage de la date d'expiration comme date antérieure à la date d'émission, ou (3) le réglage de la date effective comme date postérieure à la date d'expiration, ou les deux peuvent être réglées comme date d'expiration et date effective telles que définies, et le réglage d'un code d'action d'émetteur configuré pour forcer la transaction financière à devenir une transaction en ligne.

14. Système (100) pour la génération et la fourniture d'identifiants de paiement à un dispositif mobile (104) sans éléments sécurisés, comprenant :

un dispositif de transmission d'un système distant (110) ;
un dispositif de traitement du système distant, configuré pour générer un profil de carte associé à un compte de paiement, le profil de carte comprenant au moins des identifiants de paiement correspondant au compte de paiement associé et à un identifiant de profil ;
un dispositif de fourniture du système distant, configuré pour fournir le profil de carte généré à un dispositif mobile sans éléments sécurisés ;
un dispositif de réception du système distant, configuré pour recevoir une demande de clé en provenance du dispositif mobile, la demande de clé comprenant au moins un numéro d'identification personnel mobile, PIN, et l'identifiant de profil ; et
un dispositif d'authentification du système distant, configuré pour authentifier le PIN mobile en réponse à la réception de la demande de clé, dans lequel
le dispositif de traitement du système distant est en outre configuré pour générer une clé à usage unique sur une base d'authenticité de PIN mobile, la clé à usage unique étant configurée pour être utilisée une seule fois par le dispositif mobile, pour générer un cryptogramme de paiement valide pour une seule transaction financière, et la clé à usage unique comprenant au moins un identifiant de profil, un compteur de transaction d'application et une clé de génération destinée à être utilisée dans la génération du cryptogramme de paiement valide pour la transaction financière unique, et
le dispositif de transmission du système distant est configuré pour transmettre la clé à usage unique générée au dispositif mobile.

15. Système selon la revendication 14, dans lequel le dispositif de transmission du système distant est en outre configuré pour transmettre la clé à usage unique générée à un émetteur associé au compte de paiement.

16. Système selon la revendication 14, dans lequel le dispositif de fourniture du système distant fournit le profil de carte généré au dispositif mobile dans un message crypté par une clé de cryptage.

17. Système selon la revendication 14, dans lequel le dispositif de transmission du système distant transmet la clé à usage unique générée au dispositif mobile dans un message crypté par une clé de cryptage.

18. Système selon la revendication 14, dans lequel

IPR2025-01145
Apple EX1074 Page 25

la clé à usage unique générée est inactive,
le dispositif récepteur du système distant est en outre configuré pour recevoir une indication d'utilisation de la clé à usage unique en provenance du dispositif mobile,
le dispositif de traitement du système distant est en outre configuré pour activer la clé à usage unique générée, et
le dispositif de transmission du système distant est en outre configuré pour transmettre une indication d'activation de la clé à usage unique à un émetteur associé au compte de paiement.

19. Système (100) destiné à générer un cryptogramme de paiement dans un dispositif mobile (104) sans éléments sécurisés, comprenant :

un dispositif de traitement du dispositif mobile ;
un dispositif récepteur du dispositif mobile, configuré pour recevoir un profil de carte en provenance d'un système distant (110), le profil de carte comprenant au moins des identifiants de paiement correspondant à un compte de paiement et à un identifiant de profil ;
un dispositif de saisie du dispositif mobile, configuré pour recevoir un numéro d'identification personnel mobile, PIN, saisi par un utilisateur du dispositif mobile ; et
un dispositif de transmission du dispositif mobile, configuré pour transmettre une demande de clé au système distant, la demande de clé comprenant au moins un identifiant de profil et un numéro d'identification personnel mobile, PIN, et incitant ledit dispositif mobile à générer une clé à usage unique, dans lequel
le dispositif récepteur du dispositif mobile est en outre configuré pour recevoir la clé à usage unique en provenance du système distant, la clé à usage unique étant configurée pour être utilisée une seule fois, par le dispositif mobile, pour générer un cryptogramme de paiement valide pour une seule transaction financière, et la clé à usage unique comprenant au moins un compteur de transaction d'application, une clé de génération, et l'identifiant de profil,
le dispositif de traitement du dispositif mobile est configuré pour générer le cryptogramme de paiement valide pour la transaction financière unique au moins sur la base de la clé à usage unique reçue et du PIN mobile, et
le dispositif de transmission du dispositif mobile est en outre configuré pour transmettre, par le biais d'une communication en champ proche, au moins les identifiants de paiement et le cryptogramme de paiement généré, à un terminal de point de vente pour une utilisation dans une transaction financière.

20. Système selon la revendication 19, dans lequel
le dispositif de saisie du dispositif mobile est en outre configuré pour recevoir une indication d'utilisation de la clé à usage unique reçue,
le dispositif de transmission du dispositif mobile est en outre configuré pour transmettre une demande d'activation, la demande d'activation comprenant au moins l'identifiant de profil,
le dispositif récepteur du dispositif mobile est en outre configuré pour recevoir une indication d'activation de la clé à usage unique, et
le dispositif de transmission du dispositif mobile est en outre configuré pour transmettre les identifiants de paiement et le cryptogramme de paiement généré en réponse à la réception de l'indication d'activation de la clé à usage unique.

21. Système selon la revendication 20, dans lequel le dispositif de traitement du dispositif mobile est configuré pour générer le cryptogramme de paiement en réponse à la réception de l'indication d'activation de la clé à usage unique.

IPR2025-01145
Apple EX1074 Page 26

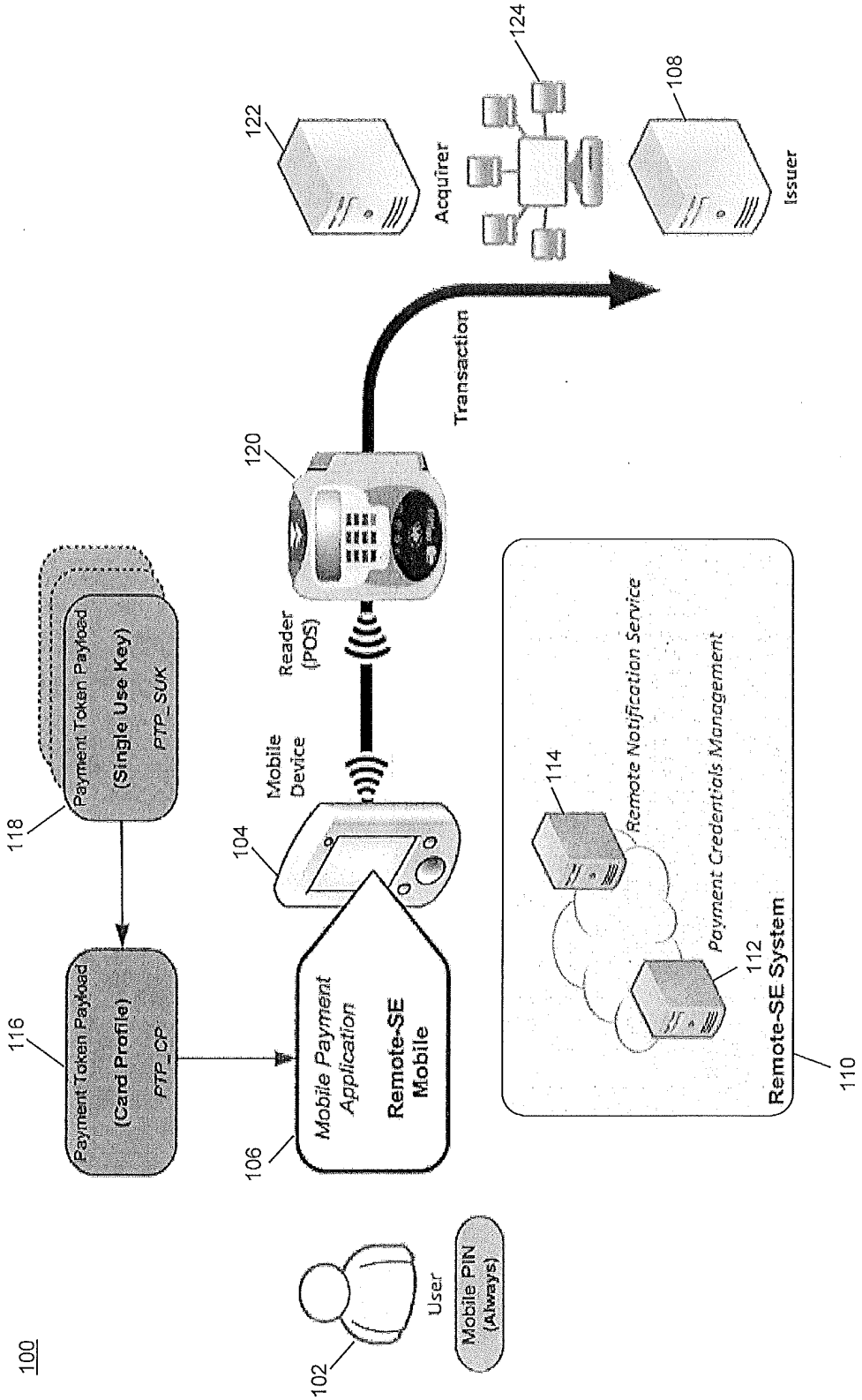
100
102
User
Mobile PIN
(Always)
106
Mobile Payment
Application
Remote-SE
Mobile
104
Mobile
Device
116
Payment Token Payload
(Card Profile)
PTP_CP
118
Payment Token Payload
(Single Use Key)
PTP_SUK
120
Reader
(POS)
Transaction
122
Acquirer
124
108
Issuer
110
Remote-SE System
112
Payment Credentials Management
114
Remote Notification Service

FIG. 1

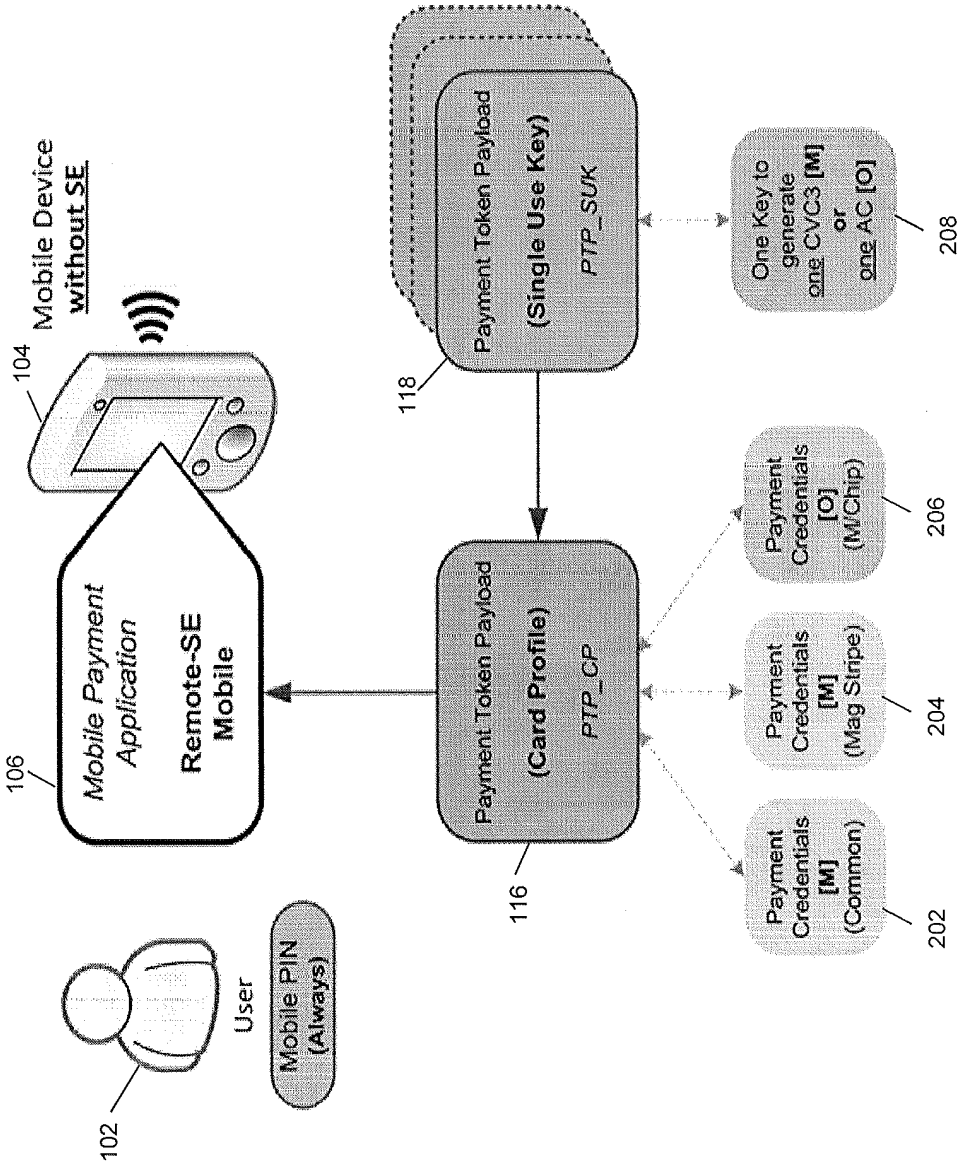
Mobile Device
without SE
104
Mobile Payment
Application
Remote-SE
Mobile
106
User
102
Mobile PIN
(Always)
Payment Token Payload
(Card Profile)
PTP_CP
116
Payment Token Payload
(Single Use Key)
PTP_SUK
118
Payment
Credentials
[M]
(Common)
202
Payment
Credentials
[M]
(Mag Stripe)
204
Payment
Credentials
[O]
(M/Chip)
206
One Key to
generate
one CVC3 [M]
or
one AC [O]
208

FIG. 2

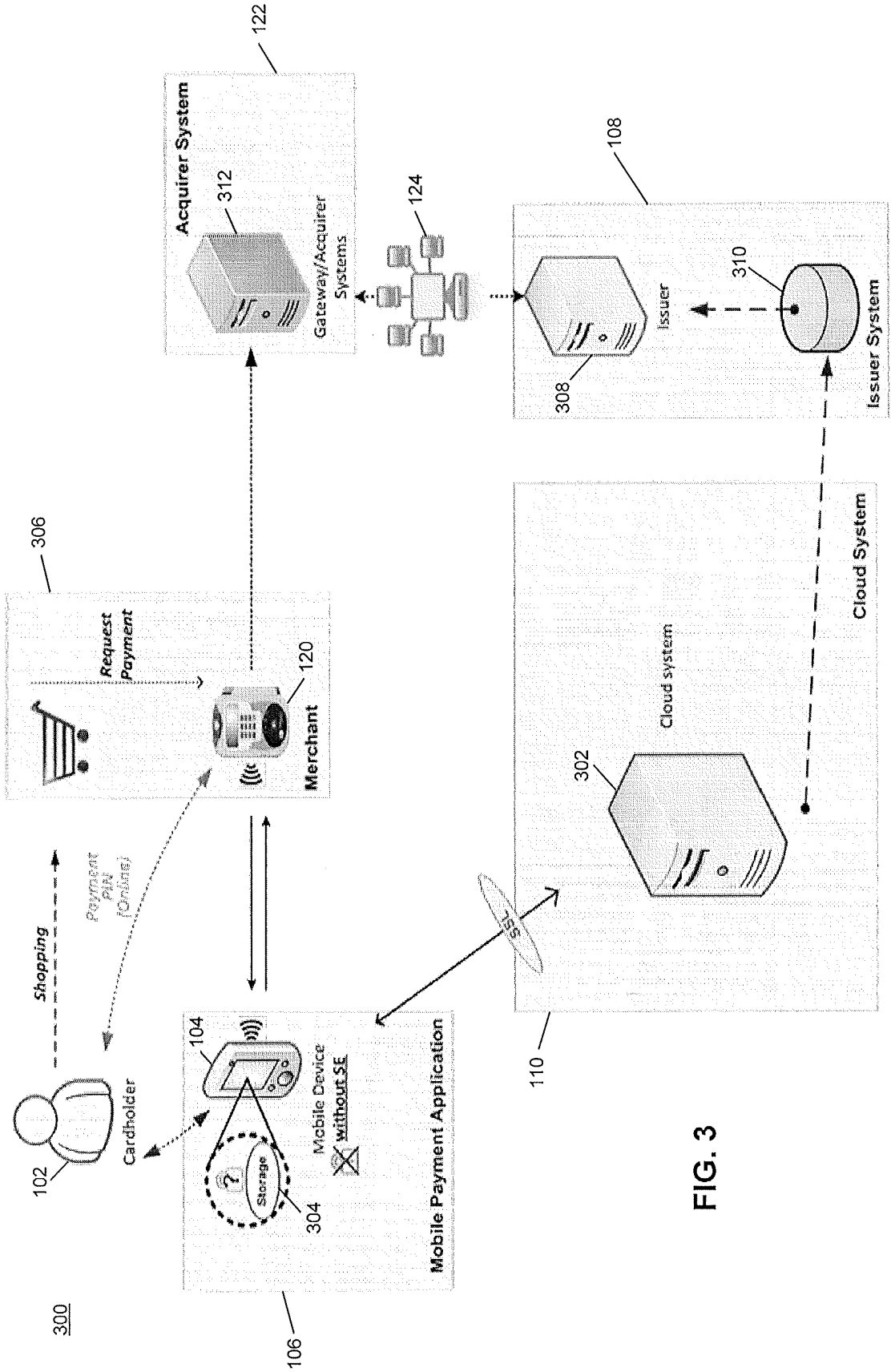
300
102
Cardholder
Shopping
Payment
PIN
(Online)
306
Request
Payment
Merchant
120
Acquirer System
122
312
Gateway/Acquirer
Systems
124
108
Issuer
308
310
Issuer System
Cloud System
Cloud system
302
110
SSL
104
Mobile Device
without SE
Storage
304
Mobile Payment Application
106

FIG. 3

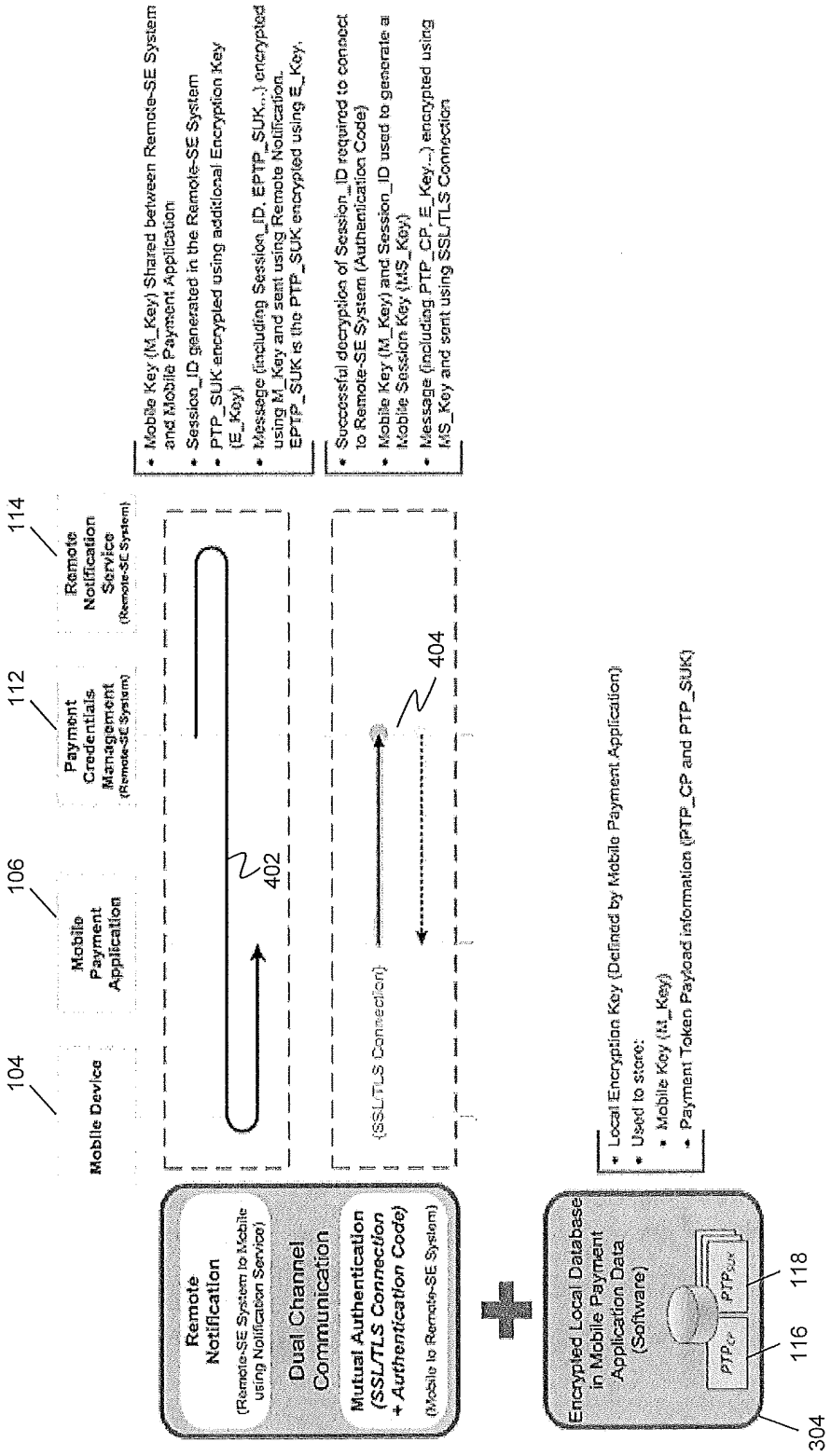
104
Mobile Device
106
Mobile Payment Application
112
Payment Credentials Management (Remote-SE System)
114
Remote Notification Service (Remote-SE System)
Remote Notification
(Remote-SE System to Mobile using Notification Service)
Dual Channel Communication
Mutual Authentication (SSL/TLS Connection + Authentication Code)
(Mobile to Remote-SE System)
402
(SSL/TLS Connection)
404
Mobile Key (M_Key) Shared between Remote-SE System and Mobile Payment Application
Session_ID generated in the Remote-SE System
PTP_SUK encrypted using additional Encryption Key (E_Key)
Message (including Session_ID, EPTP_SUK...) encrypted using M_Key and sent using Remote Notification. EPTP_SUK is the PTP_SUK encrypted using E_Key.
Successful decryption of Session_ID required to connect to Remote-SE System (Authentication Code)
Mobile Key (M_Key) and Session_ID used to generate a Mobile Session Key (MS_Key)
Message (including PTP_CP, E_Key...) encrypted using MS_Key and sent using SSL/TLS Connection
Encrypted Local Database in Mobile Payment Application Data (Software)
PTP_CP
PTP_SUK
Local Encryption Key (Defined by Mobile Payment Application)
Used to store:
Mobile Key (M_Key)
Payment Token Payload information (PTP_CP and PTP_SUK)
304
116
118

FIG. 4

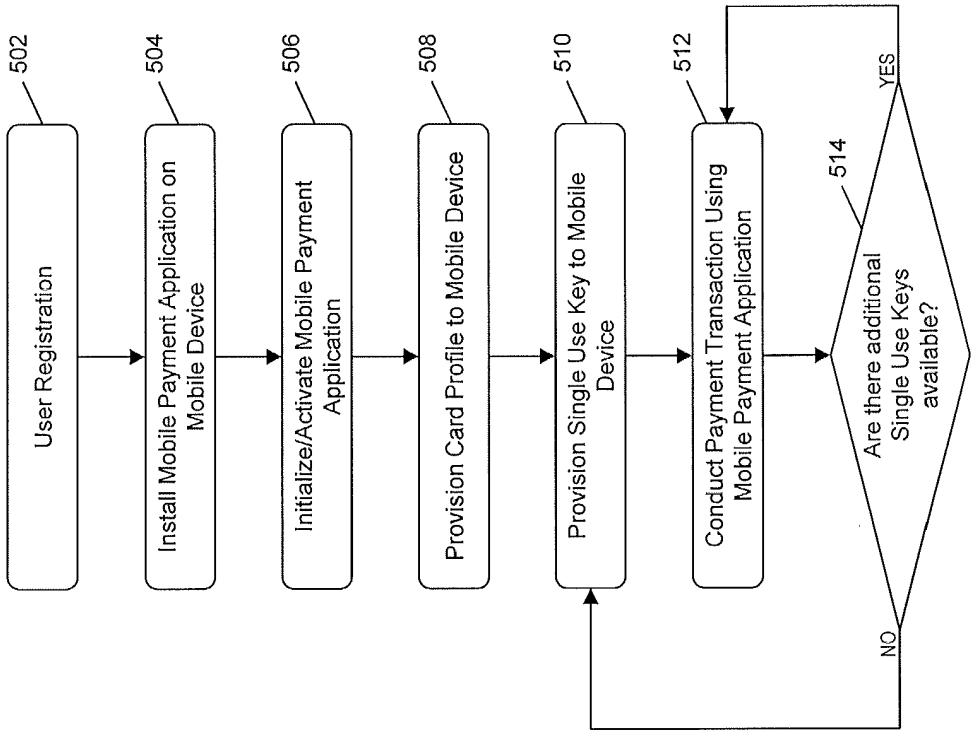

FIG. 5

IPR2025-01145
Apple EX1074 Page 31

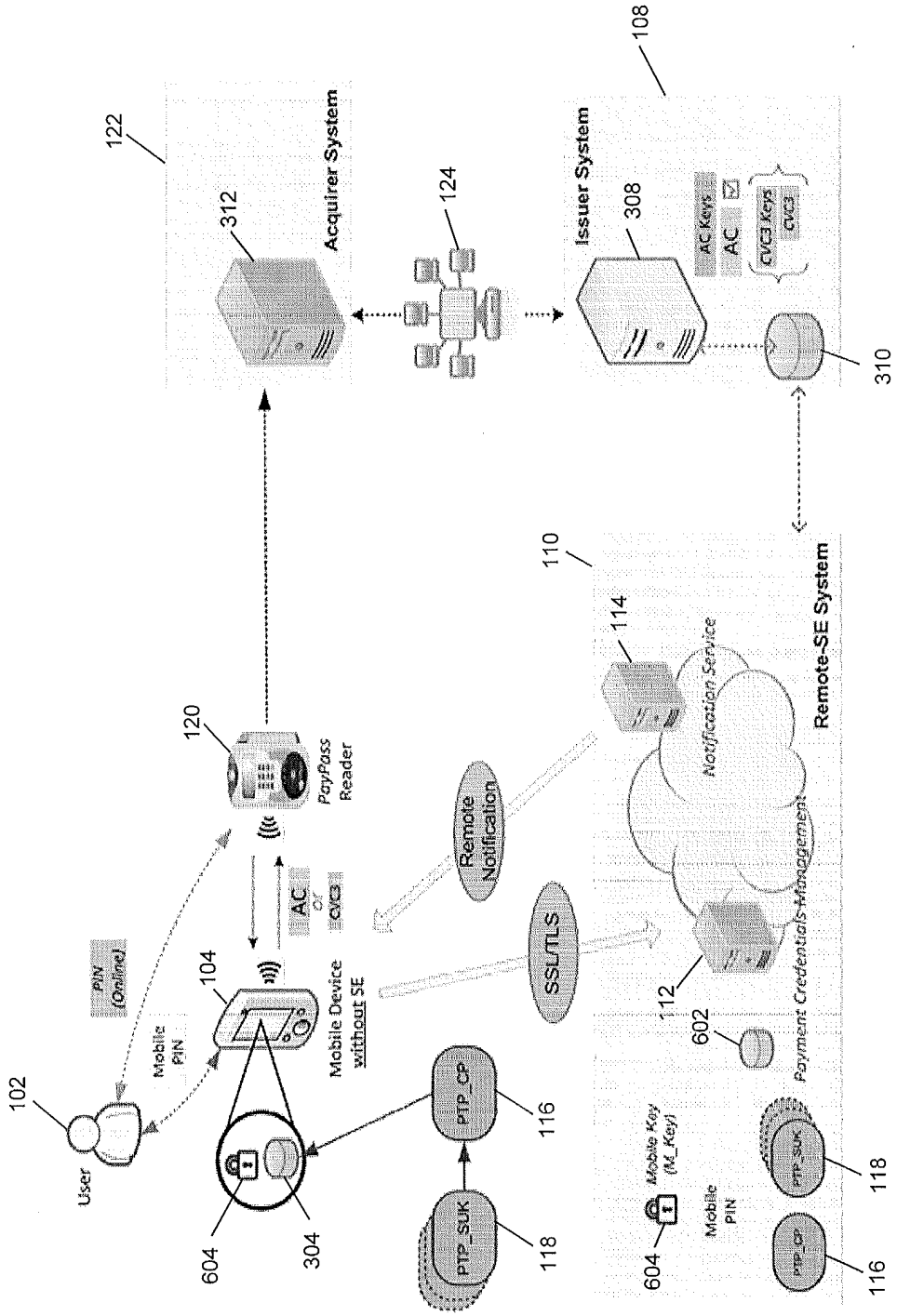
122
Acquirer System
312
124
108
Issuer System
308
AC Keys
AC
CVC3 Keys
CVC3
310
110
114
Notification Service
Remote-SE System
120
PayPass Reader
Remote Notification
AC
or
CVC3
104
Mobile Device without SE
SSL/TLS
112
602
Payment Credentials Management
PIN (Online)
Mobile PIN
102
User
604
304
PTP_CP
116
PTP_SUK
118
Mobile Key (M_Key)
604
Mobile PIN
PTP_SUK
118
PTP_CP
116

FIG. 6

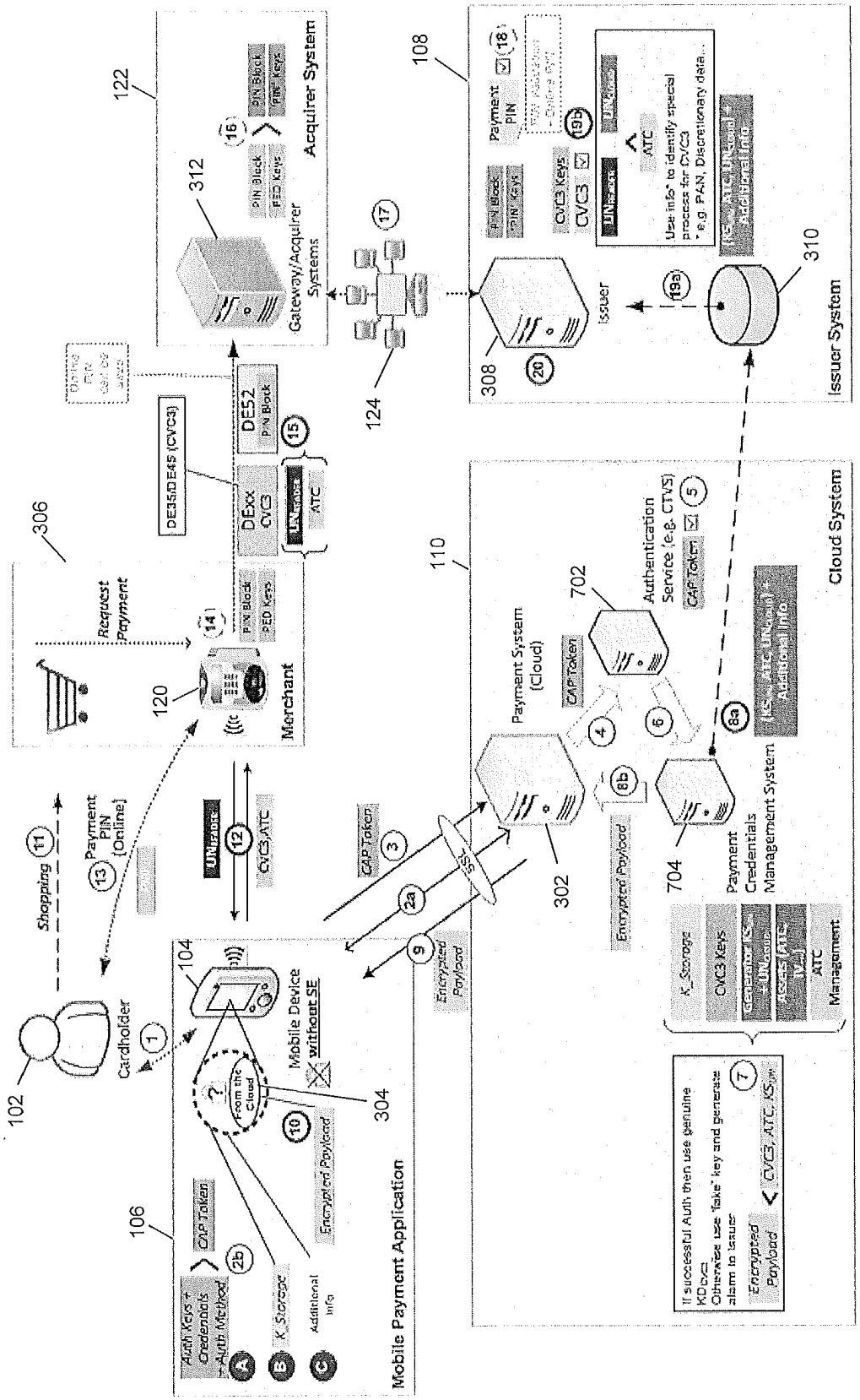
Cardholder
Shopping
Payment PIN (Online)
Request Payment
Merchant
Mobile Device without SE
Mobile Payment Application
Auth Keys + Credentials + Auth Method
K_Storage
Additional Info
CAP Token
Encrypted Payload
CVC3/ATC
DE35/DE45 (CVC3)
DE52 PIN Block
DExx CVC3
ATC
PIN Block
PED Keys
Gateway/Acquirer Systems
Acquirer System
Payment PIN
CVC3 Keys
CVC3
Issuer
Issuer System
Payment System (Cloud)
Authentication Service (e.g. CTVS)
Payment Credentials Management System
ATC Management
Cloud System
If successful Auth then use genuine KDcvc3 Otherwise use "fake" key and generate alarm to Issuer
CVC3, ATC, KSUM
102
104
106
108
110
120
122
124
302
304
306
308
310
312
702
704

FIG. 7

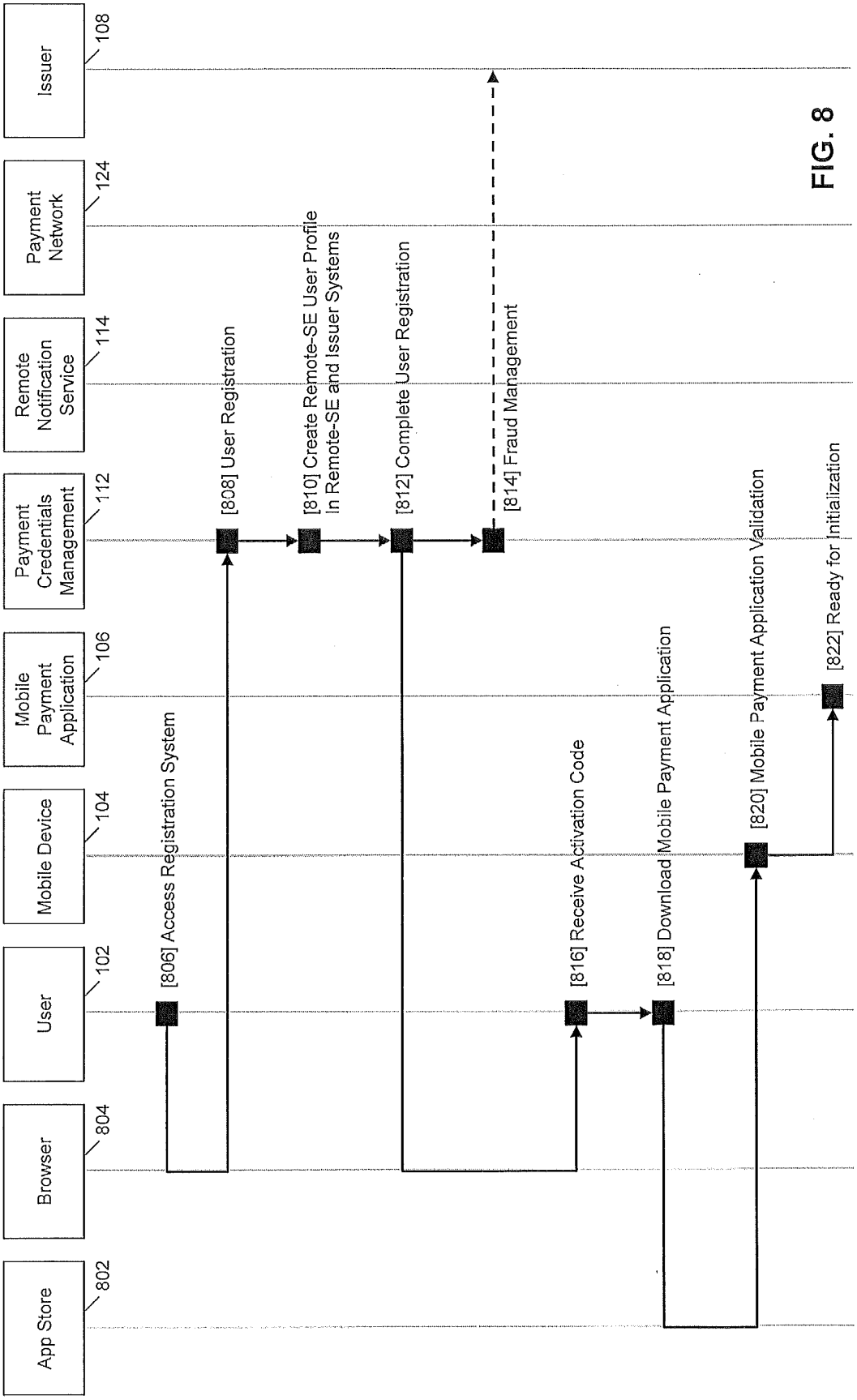
App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[806] Access Registration System
[808] User Registration
[810] Create Remote-SE User Profile in Remote-SE and Issuer Systems
[812] Complete User Registration
[814] Fraud Management
[816] Receive Activation Code
[818] Download Mobile Payment Application
[820] Mobile Payment Application Validation
[822] Ready for Initialization

FIG. 8

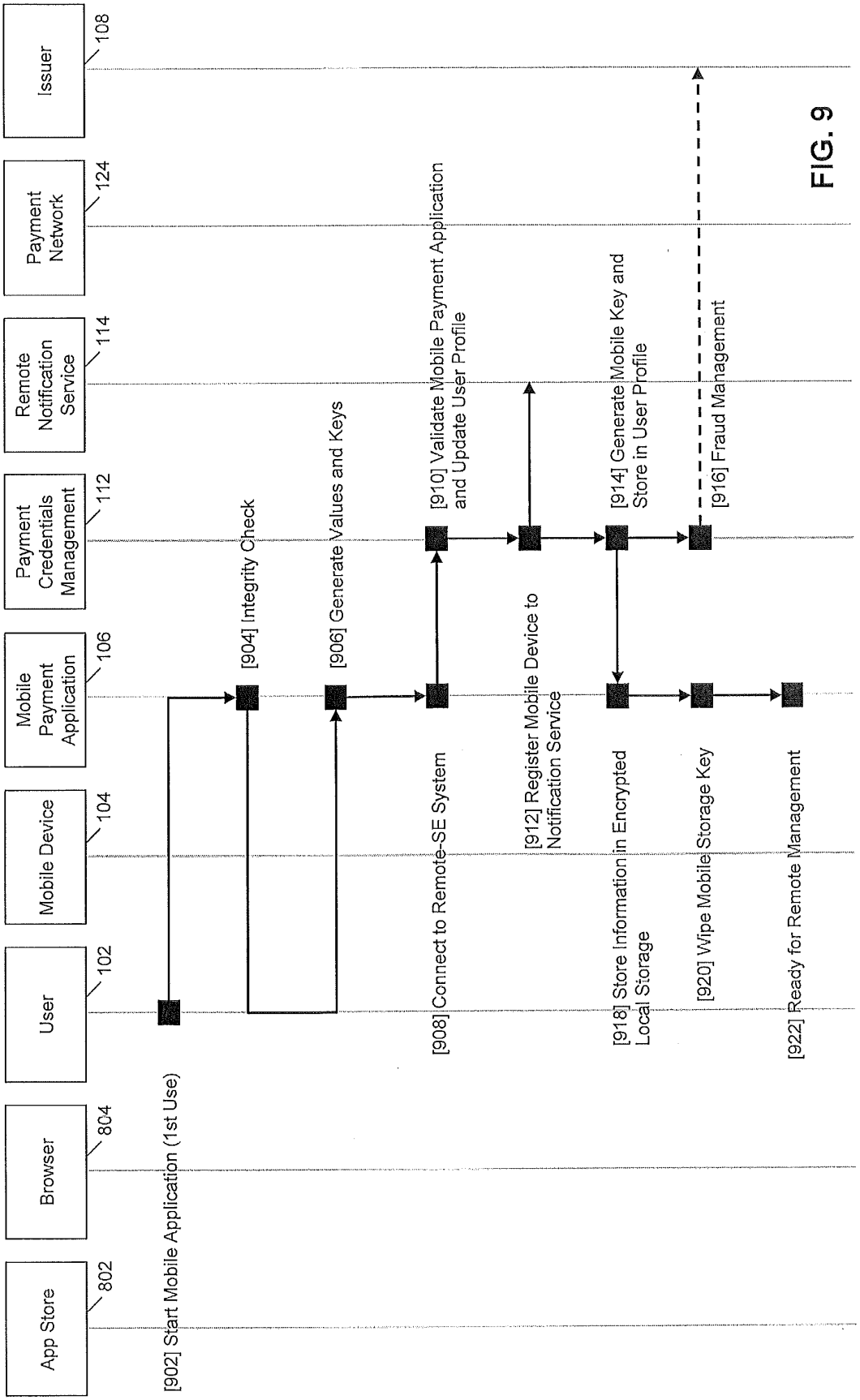
App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[902] Start Mobile Application (1st Use)
[904] Integrity Check
[906] Generate Values and Keys
[908] Connect to Remote-SE System
[910] Validate Mobile Payment Application and Update User Profile
[912] Register Mobile Device to Notification Service
[914] Generate Mobile Key and Store in User Profile
[916] Fraud Management
[918] Store Information in Encrypted Local Storage
[920] Wipe Mobile Storage Key
[922] Ready for Remote Management

FIG. 9

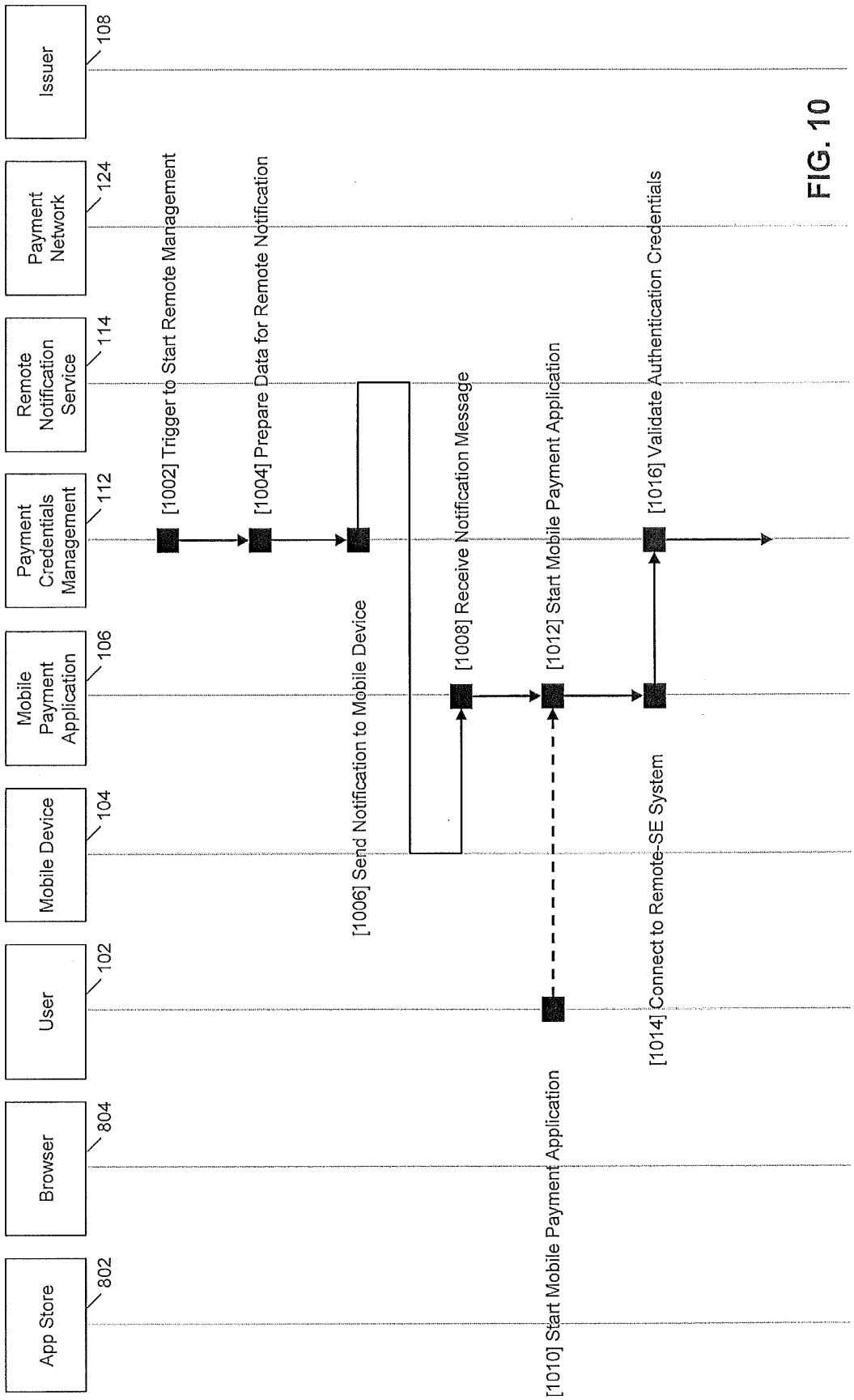
Issuer
108
Payment Network
124
Remote Notification Service
114
Payment Credentials Management
112
Mobile Payment Application
106
Mobile Device
104
User
102
Browser
804
App Store
802
[1002] Trigger to Start Remote Management
[1004] Prepare Data for Remote Notification
[1006] Send Notification to Mobile Device
[1008] Receive Notification Message
[1010] Start Mobile Payment Application
[1012] Start Mobile Payment Application
[1014] Connect to Remote-SE System
[1016] Validate Authentication Credentials

FIG. 10

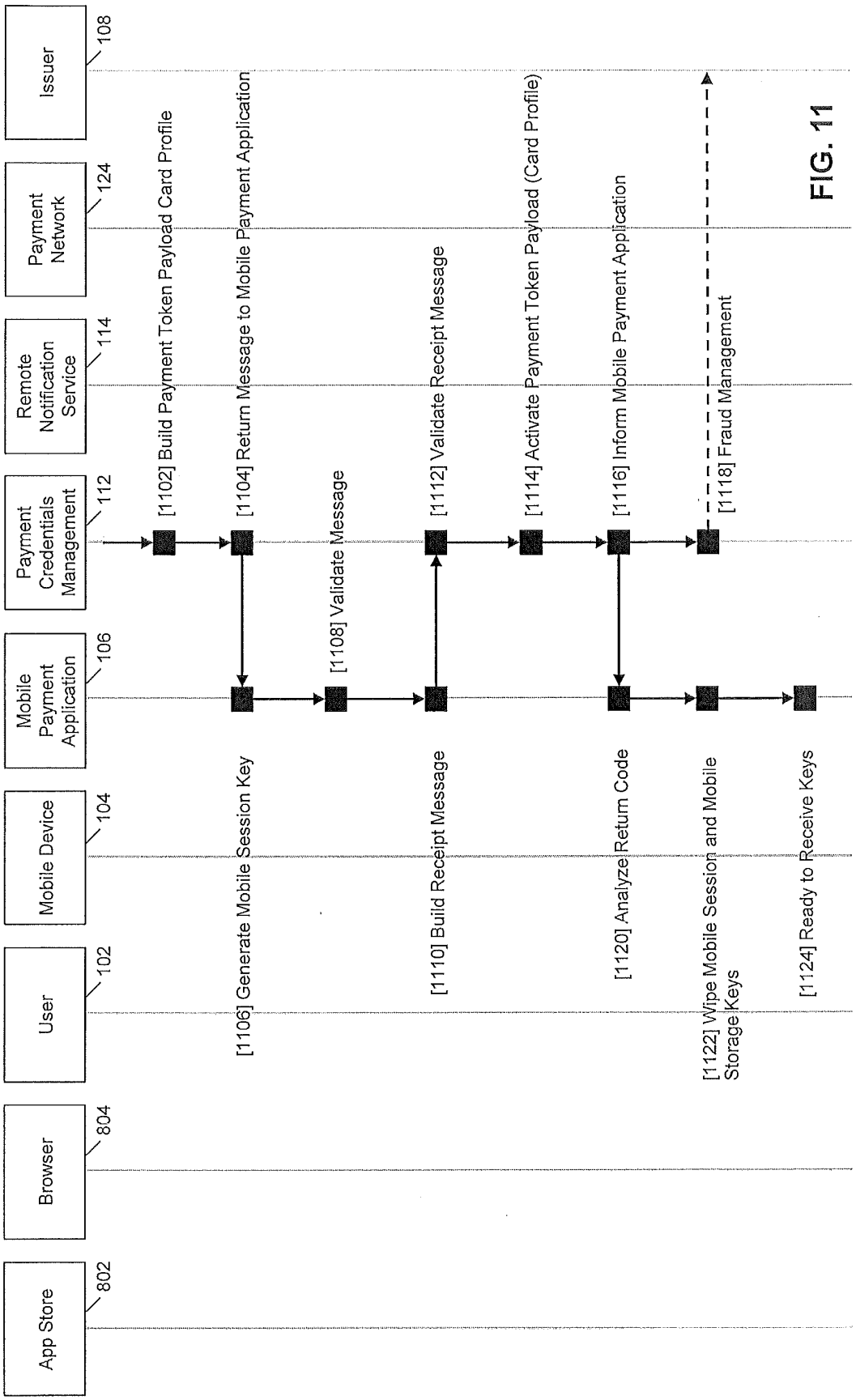
App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[1102] Build Payment Token Payload Card Profile
[1104] Return Message to Mobile Payment Application
[1106] Generate Mobile Session Key
[1108] Validate Message
[1110] Build Receipt Message
[1112] Validate Receipt Message
[1114] Activate Payment Token Payload (Card Profile)
[1116] Inform Mobile Payment Application
[1118] Fraud Management
[1120] Analyze Return Code
[1122] Wipe Mobile Session and Mobile Storage Keys
[1124] Ready to Receive Keys

FIG. 11

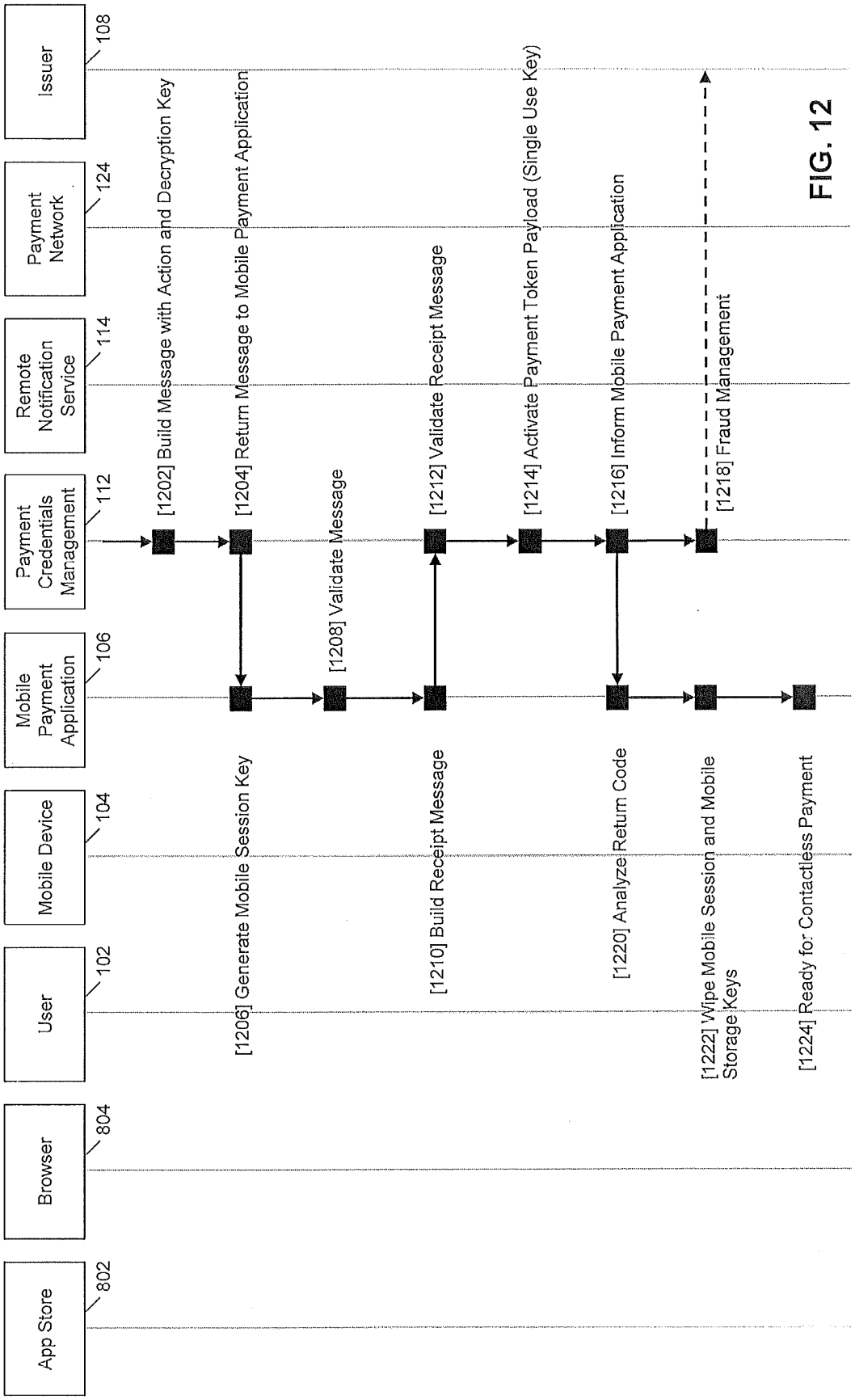
App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[1202] Build Message with Action and Decryption Key
[1204] Return Message to Mobile Payment Application
[1206] Generate Mobile Session Key
[1208] Validate Message
[1210] Build Receipt Message
[1212] Validate Receipt Message
[1214] Activate Payment Token Payload (Single Use Key)
[1216] Inform Mobile Payment Application
[1218] Fraud Management
[1220] Analyze Return Code
[1222] Wipe Mobile Session and Mobile Storage Keys
[1224] Ready for Contactless Payment

FIG. 12

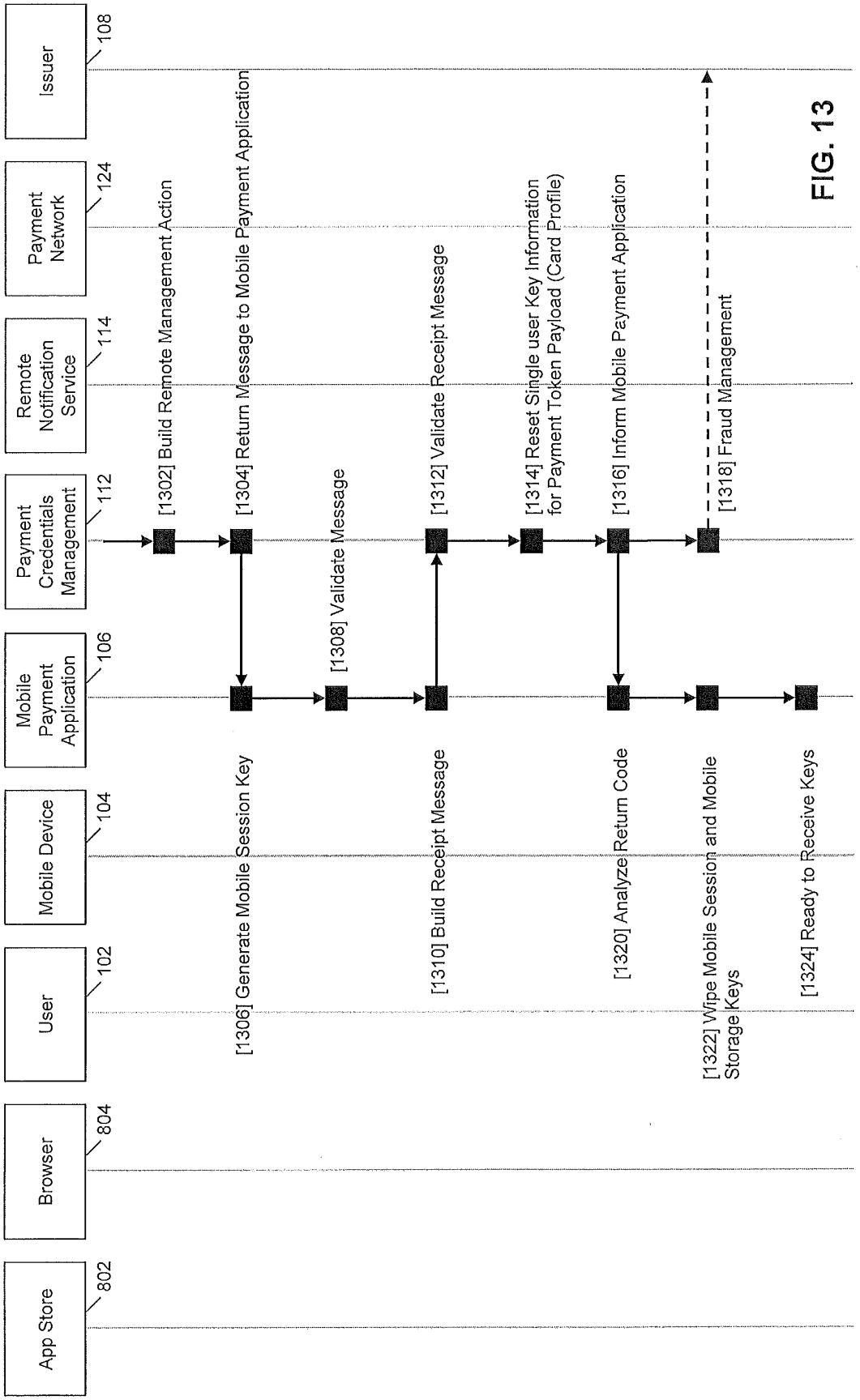
App Store
802
Browser
804
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Payment Network
124
Issuer
108
[1302] Build Remote Management Action
[1304] Return Message to Mobile Payment Application
[1306] Generate Mobile Session Key
[1308] Validate Message
[1310] Build Receipt Message
[1312] Validate Receipt Message
[1314] Reset Single user Key Information for Payment Token Payload (Card Profile)
[1316] Inform Mobile Payment Application
[1318] Fraud Management
[1320] Analyze Return Code
[1322] Wipe Mobile Session and Mobile Storage Keys
[1324] Ready to Receive Keys

FIG. 13

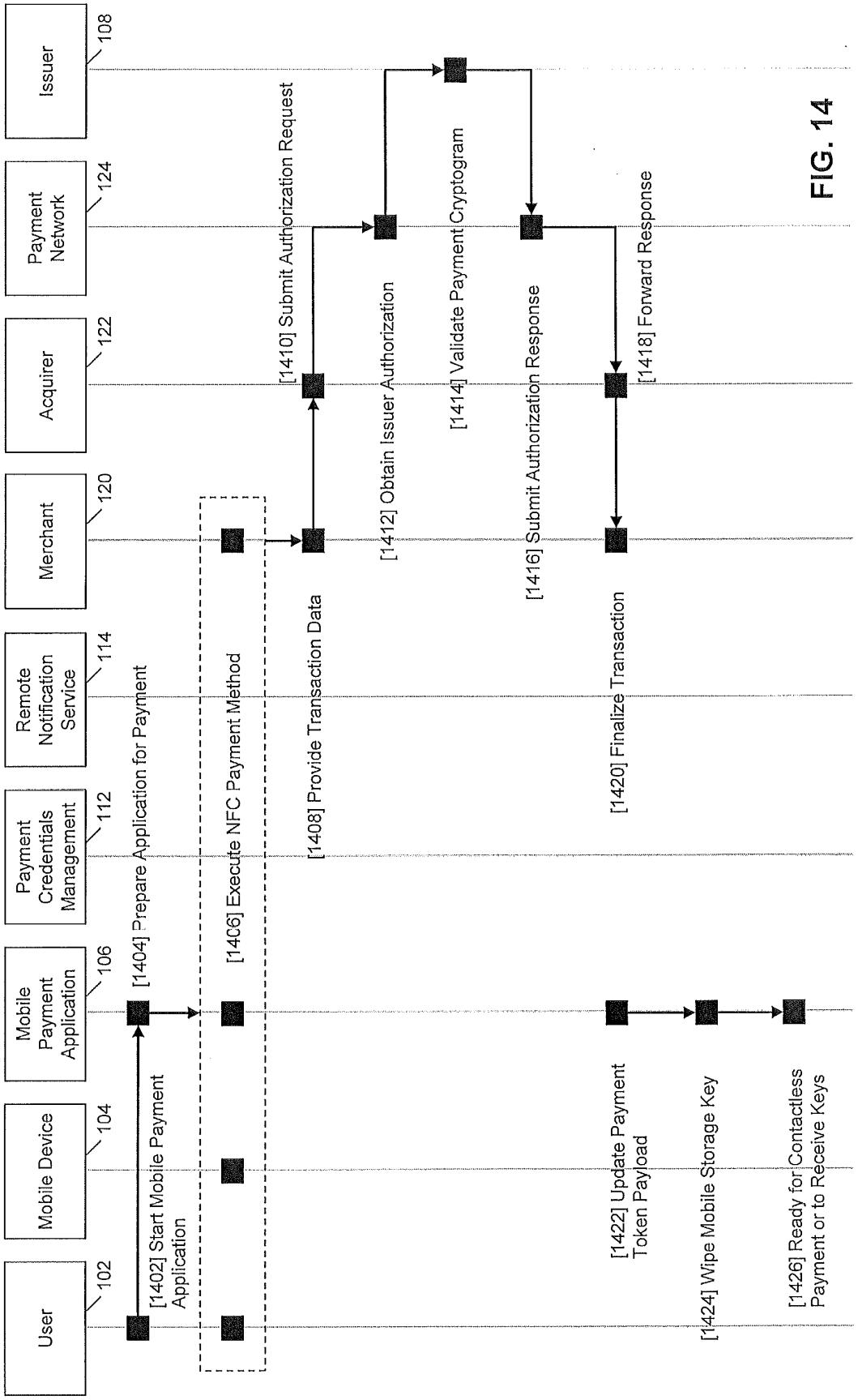
User
102
Mobile Device
104
Mobile Payment Application
106
Payment Credentials Management
112
Remote Notification Service
114
Merchant
120
Acquirer
122
Payment Network
124
Issuer
108
[1402] Start Mobile Payment Application
[1404] Prepare Application for Payment
[1406] Execute NFC Payment Method
[1408] Provide Transaction Data
[1410] Submit Authorization Request
[1412] Obtain Issuer Authorization
[1414] Validate Payment Cryptogram
[1416] Submit Authorization Response
[1418] Forward Response
[1420] Finalize Transaction
[1422] Update Payment Token Payload
[1424] Wipe Mobile Storage Key
[1426] Ready for Contactless Payment or to Receive Keys

FIG. 14

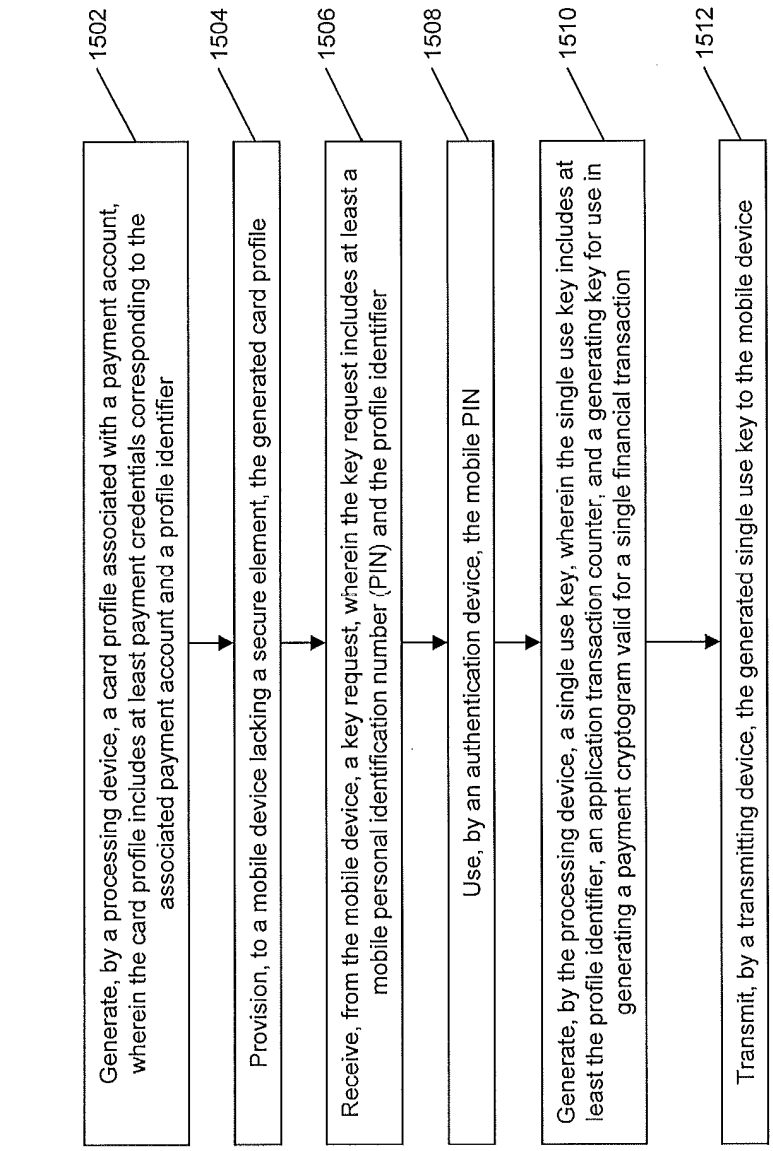

FIG. 15

IPR2025-01145
Apple EX1074 Page 41

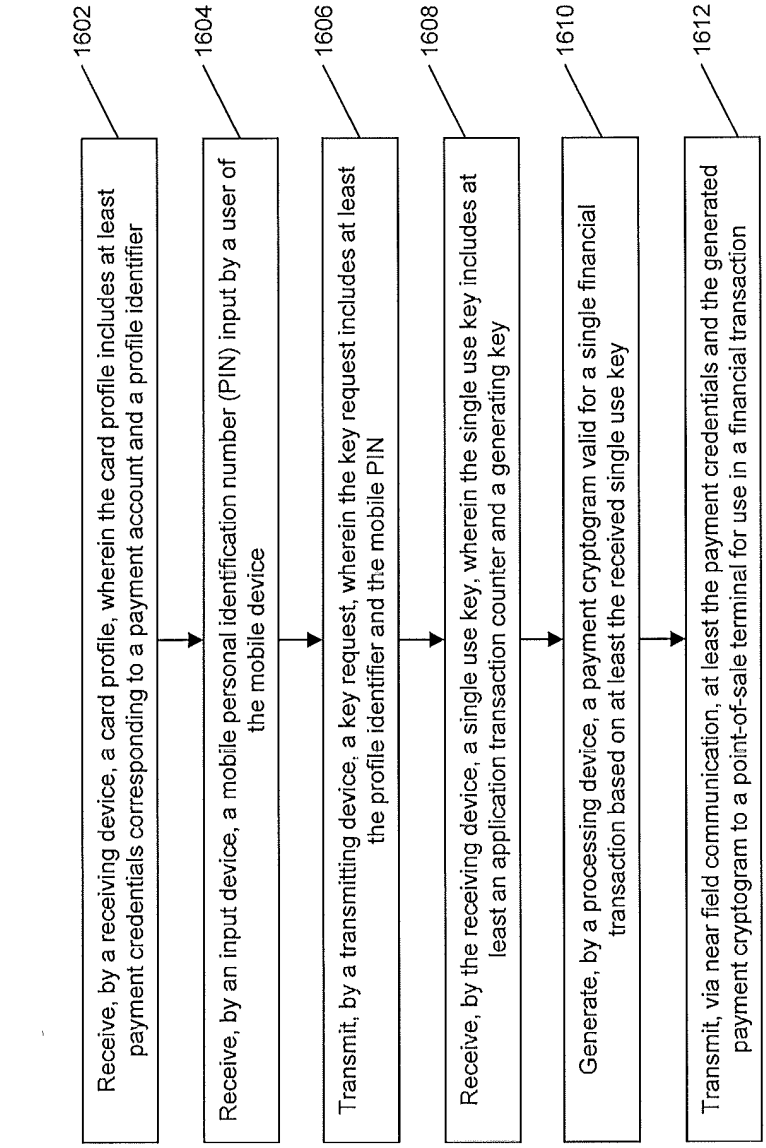
1600
1602
Receive, by a receiving device, a card profile, wherein the card profile includes at least payment credentials corresponding to a payment account and a profile identifier
1604
Receive, by an input device, a mobile personal identification number (PIN) input by a user of the mobile device
1606
Transmit, by a transmitting device, a key request, wherein the key request includes at least the profile identifier and the mobile PIN
1608
Receive, by the receiving device, a single use key, wherein the single use key includes at least an application transaction counter and a generating key
1610
Generate, by a processing device, a payment cryptogram valid for a single financial transaction based on at least the received single use key
1612
Transmit, via near field communication, at least the payment credentials and the generated payment cryptogram to a point-of-sale terminal for use in a financial transaction

FIG. 16

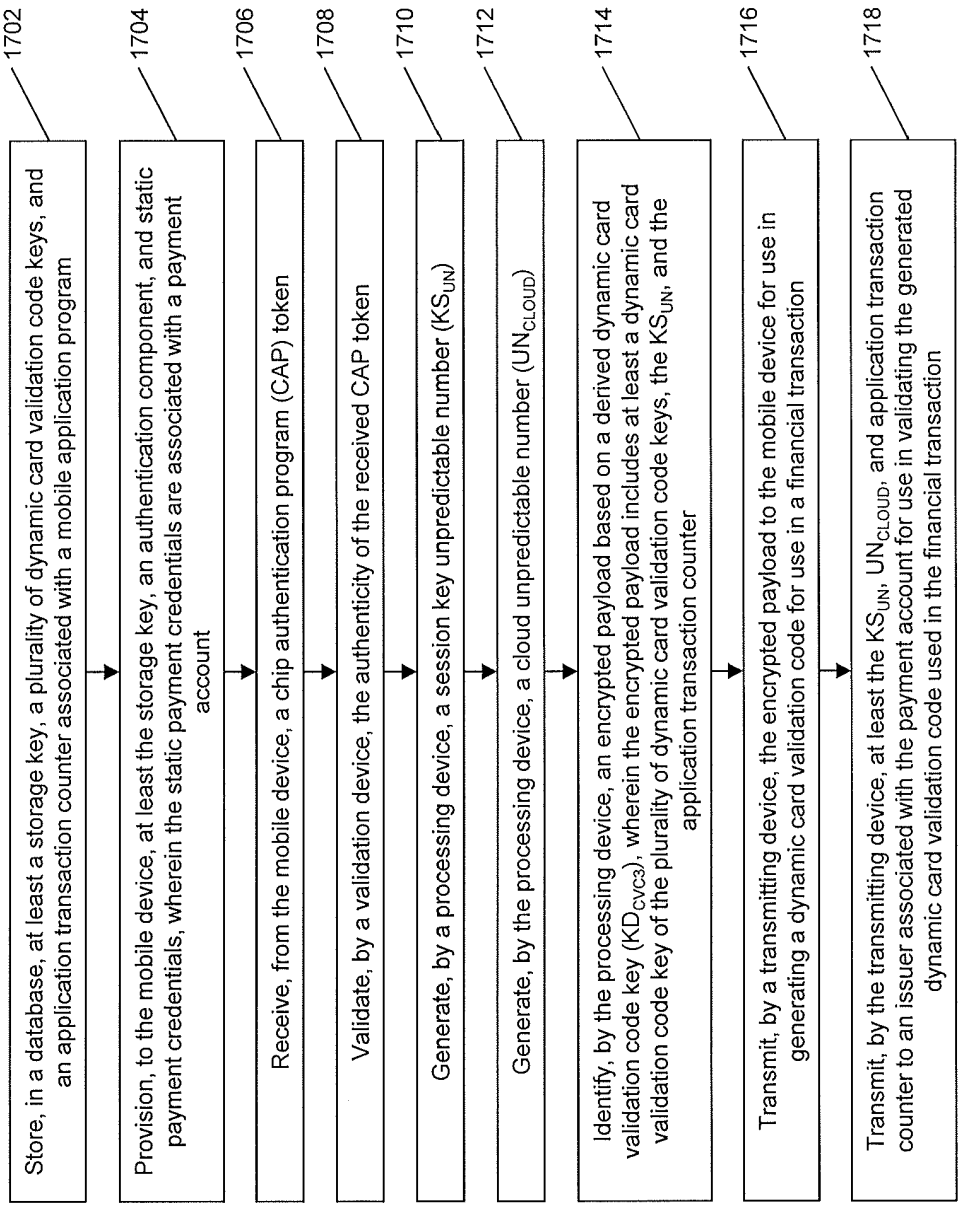
1700
1702
Store, in a database, at least a storage key, a plurality of dynamic card validation code keys, and an application transaction counter associated with a mobile application program
1704
Provision, to the mobile device, at least the storage key, an authentication component, and static payment credentials, wherein the static payment credentials are associated with a payment account
1706
Receive, from the mobile device, a chip authentication program (CAP) token
1708
Validate, by a validation device, the authenticity of the received CAP token
1710
Generate, by a processing device, a session key unpredictable number (KS_{UN})
1712
Generate, by the processing device, a cloud unpredictable number (UN_{CLOUD})
1714
Identify, by the processing device, an encrypted payload based on a derived dynamic card validation code key (KD_{CVC3}), wherein the encrypted payload includes at least a dynamic card validation code key of the plurality of dynamic card validation code keys, the KS_{UN}, and the application transaction counter
1716
Transmit, by a transmitting device, the encrypted payload to the mobile device for use in generating a dynamic card validation code for use in a financial transaction
1718
Transmit, by the transmitting device, at least the KS_{UN}, UN_{CLOUD}, and application transaction counter to an issuer associated with the payment account for use in validating the generated dynamic card validation code used in the financial transaction

FIG. 17

1800
1802
Receive, by a receiving device, at least a storage key, an authentication component, and static payment credentials
1804
Receive, by an input device, at least one additional credential
1806
Generate, by a processing device, a chip authentication program (CAP) token, wherein the CAP token is based on at least the authentication component and the at least one additional credential
1808
Transmit, by a transmitting device, the generated CAP token
1810
Receive, by the receiving device, an encrypted payload, wherein the encrypted payload includes at least a supplied dynamic card validation code, session key unpredictable number, and application transaction counter
1812
Decrypt, by the processing device, the encrypted payload using at least the received storage key
1814
Receive, via near field communication, a reader unpredictable number from a point-of-sale terminal
1816
Generate, by the processing device, a payment dynamic card validation code based on at least the supplied dynamic card validation code, the session key unpredictable number, the application transaction counter, and the reader unpredictable number
1818
Transmit, via near field communication, the generated payment dynamic card validation code and the application transaction counter to the point-of-sale terminal for including in an authorization request for a financial transaction

FIG. 18

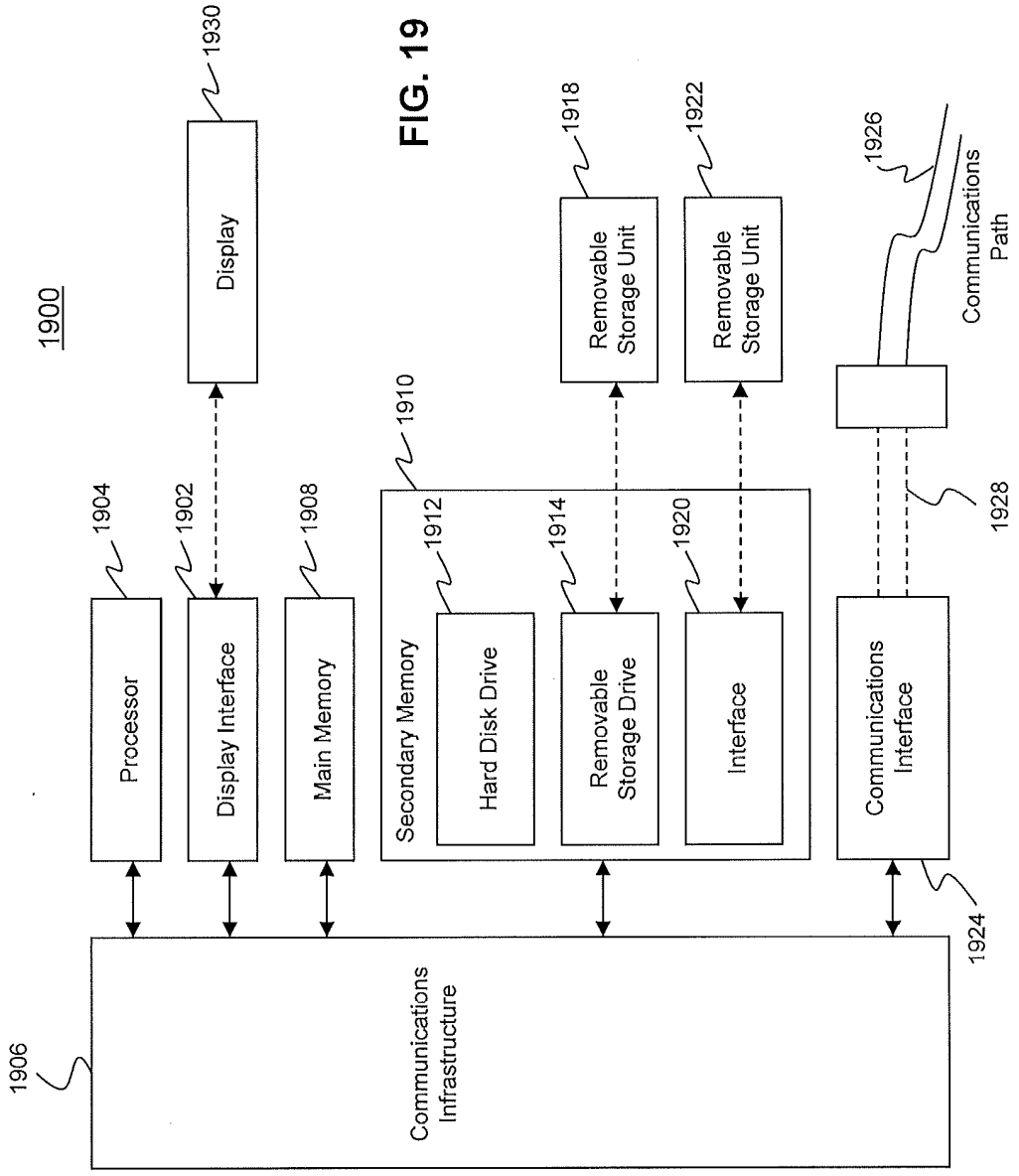
1900
1930
Display
1904
Processor
1902
Display Interface
1908
Main Memory
1910
Secondary Memory
1912
Hard Disk Drive
1914
Removable Storage Drive
1920
Interface
1918
Removable Storage Unit
1922
Removable Storage Unit
1926
Communications Path
1928
Communications Interface
1924
1906
Communications Infrastructure

FIG. 19

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 61619095 **[0001]**
- US 61639248 **[0001]**
- US 61735383 **[0001]**
- US 61762098 **[0001]**
- US 82704213 **[0001]**
- US 2008040285 A **[0006]**

IPR2025-01145
Apple EX1074 Page 46