SYSTEMS AND METHODS FOR MAPPING A MOBILE CLOUD ACCOUNT TO A PAYMENT ACCOUNT

RELATED APPLICATIONS

[0001] This application claims the priority benefit of commonly assigned U.S. Provisional Application No. 61/605,588, filed March 1, 2012, entitled "Systems and Methods for Mapping a Mobile Cloud Account to a Payment Account," by Theresa L. Smith et al., which is herein incorporated by reference in its entirety.

FIELD

[0002] The present disclosure relates to the mapping of a mobile cloud account to a payment account, specifically using a mobile cloud account to conduct contactless payment transactions without modification to legacy issuer processing systems.

BACKGROUND

[0003] Advances in mobile and communication technologies have created tremendous opportunities, one of which is providing users of mobile computing devices, such as smart phones, the ability to conduct payment transactions using their mobile computing device. One approach to enable mobile computing devices to conduct payment transactions is through the use of near field communication (NFC) technology to securely transmit payment credentials from the mobile device to a contactless terminal. In many instances, a secure element chip included as part of the mobile device is utilized.

[0004] However, many payment account issuers utilize systems that are not configured to process contactless payment transactions. As a result, many payment account holders who possess NFC-capable mobile devices may not be able to take advantage of the convenient NFC technology. This may negatively affect not only the account holder, who is unable to conduct a contactless transaction using their mobile device, but also the account

issuer, who may lose the business of the account holder should he or she choose to switch to an issuer capable of processing contactless transactions.

[0005] Thus, there is a need for a technical solution to facilitating the conducting of contactless payment transactions on a mobile device that does not require significant changes to legacy issuer processing systems.

SUMMARY

[0006] The present disclosure provides a description of systems and methods for mapping a mobile cloud account to a payment account, and the processing of financial transactions based therein.

[0007] A method for mapping a payment account to a mobile cloud account number includes: generating, by a generating device, an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key; generating, by the generating device, an ICC master key based on at least a master key identifier; transmitting, by a transmitting device, the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device for storage in a secure element; receiving, by a receiving device, a real card account number (RCA) corresponding to a payment account; identifying, by a processing device, attributes of the RCA; identifying, by the processing device, a mobile cloud account number (MCA) based on the attributes of the RCA; receiving, by the receiving device, an issuer private key and an issuer private key certificate; generating, by the generating device, an ICC public key certificate based on certification of the ICC public key by the issuer private key; creating, by the processing device, a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, wherein the mobile cloud account data includes at least the issuer public key certificate, the MCA, and the ICC public key certificate; transmitting, by the transmitting device, the created post issuance script to the mobile device; and storing, in a mapping

database, a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA.

[0008] A method for processing a financial transaction includes: storing, in a mapping database, a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA), and wherein the MCA is based on attributes of the RCA; receiving, by a receiving device, transaction data related to a financial transaction, wherein the transaction data includes at least an MCA and a payment cryptogram; validating, by a validation device, the payment cryptogram; identifying, in the mapping database, a specific mapping record, wherein the specific mapping record includes the MCA included in the received transaction data; and transmitting, by a transmitting device, at least the RCA included in the specific mapping record and a validation result indicating a success or failure of the validation of the payment cryptogram.

[0009] A method for providing payment credentials for a financial transaction includes: receiving, by a receiving device, personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier; storing, in a first location of a secure element of a mobile device, the received personalization data; receiving, by a receiving device at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA); storing, in a database not included in the secure element, the received at least one post issuance script; receiving, by an input device, an indication of an MCA included in a specific post issuance script of the received at least one post issuance script; and executing, by a processing device, the specific post issuance script,

wherein the MCA is based on attributes of a real card account number (RCA).

[0010] A system for mapping a payment account to a mobile cloud account includes a mapping database, a generating device, a transmitting device, a receiving device, and a processing device. The generated device is configured to generate an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key; generating, by the generating device, an ICC master key based on at least a master key identifier. The transmitting device is configured to transmit the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device for storage in a secure element. The receiving device is configured to receive a real card account number (RCA) corresponding to a payment account. The processing device is configured to identify attributes of the RCA and identify a mobile cloud account number (MCA) based on the attributes of the RCA. The receiving device is further configured to receive an issuer private key and an issuer private key certificate. The generating device is further configured to generate an ICC public key certificate based on certification of the ICC public key by the issuer private key. The processing device is further configured to create a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, wherein the mobile cloud account data includes at least the issuer public key certificate, the MCA, and the ICC public key certificate. The transmitting device is further configured to transmit the created post issuance script to the mobile device. The mapping database is configured to store a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA.

[0011] A system for processing a financial transaction includes a mapping database, a receiving device, a validation device, a processing device, and a transmitting device. The mapping database is configured to store a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card

account number (RCA), and wherein the MCA is based on attributes of the RCA. The receiving device is configured to receive transaction data related to a financial transaction, wherein the transaction data includes at least an MCA and a payment cryptogram. The validation device is configured to validate the payment cryptogram. The processing device is configured to identify, in the mapping database, a specific mapping record, wherein the specific mapping record includes the MCA included in the received transaction data. The transmitting device is configured to transmit at least the RCA included in the specific mapping record and a validation result indicating a success or failure of the validation of the payment cryptogram.

[0012] A mobile device for providing payment credentials for a financial transaction includes an input device, a secure element, a database not included in the secure element, a receiving device, and a processing device. The receiving device is configured to receive personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier. The processing device is configured to store, in a first location of the secure element of the mobile device, the received personalization data. The receiving device is further configured to receive at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA). The processing device is further configured to store, in the database, the received at least one post issuance script. The input device is configured to receive an indication of an MCA included in a specific post issuance script of the received at least one post issuance script. The processing device is further configured to execute the specific post issuance script, wherein the MCA is based on attributes of a real card account number (RCA).

[0013] A non-transitory computer readable recording medium records program instructions stored therein that causes a processor of a mobile computing device to execute a method for providing payment credentials for a financial transaction, wherein the method includes: receiving, by a receiving device, personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier; storing, in a first location of a secure element of a mobile device, the received personalization data; receiving, by a receiving device at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA); storing, in a database not included in the secure element, the received at least one post issuance script; receiving, by an input device, an indication of an MCA included in a specific post issuance script of the received at least one post issuance script; and executing, by a processing device, the specific post issuance script, wherein the MCA is based on attributes of a real card account number (RCA).

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0014] 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:

[0015] FIG. 1 is a high level architecture illustrating a system for the mapping of mobile cloud accounts to payment accounts and processing of contactless payment transactions using a mobile cloud account in accordance with exemplary embodiments.

[0016] FIG. 2 is a block diagram illustrating data stored in the mobile device of FIG. 1 for the conducting of contactless payment transactions accordance with exemplary embodiments.

[0017] FIG. 3 is a process flow illustrating a method for the over-the-air provisioning of a master key identifier to a mobile device in accordance with exemplary embodiments.

[0018] FIGS. 4A and 4B are a process flow illustrating a method for the provisioning of mobile cloud account data to a mobile device in accordance with exemplary embodiments.

[0019] FIG. 5 is a flow chart illustrating a high-level method for the processing of an authorization request for a contactless payment transaction funded via a mobile cloud account in accordance with exemplary embodiments.

[0020] FIG. 6 is a process flow illustrating a method for the processing of contactless payment transaction funded via a mobile cloud account in accordance with exemplary embodiments.

[0021] FIG. 7 is a block diagram illustrating the provisioning of mobile cloud accounts to a mobile device in accordance with exemplary embodiments.

[0022] FIG. 8 is a block diagram illustrating the provisioning of mobile cloud account data to a secure element of a mobile device in accordance with exemplary embodiments.

[0023] FIG. 9 is a process flow illustrating a method for the mapping and cryptography of mobile cloud account data in accordance with exemplary embodiments.

[0024] FIG. 10 is a flow chart illustrating an exemplary method for the mapping of a payment account to a mobile cloud account in accordance with exemplary embodiments.

[0025] FIG. 11 is a flow chart illustrating an exemplary method for the processing of a financial transaction in accordance with exemplary embodiments.

[0026] FIG. 12 is a flow chart illustrating an exemplary method for providing payment credentials for a financial transaction in accordance with exemplary embodiments.

[0027] FIG. 13 is a block diagram illustrating a computer system architecture in accordance with exemplary embodiments.

[0028] 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

[0029] 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.

[0030] 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.

[0031] 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. Payment cards may also include real card accounts having associated real card account numbers (RCAs) and mobile cloud accounts having associated mobile cloud account numbers (MCAs) as discussed in more detail herein.

System for Mapping and Processing Mobile Cloud Accounts

[0032] FIG. 1 is a high level diagram illustrating a system 100 for the mapping of mobile cloud accounts to payment accounts and the processing of financial transactions funded via mobile cloud accounts.

[0033] The system 100 may include a mobile device 102. The mobile device 102 may be any type of mobile computing device 102 suitable for performing the functions as disclosed herein as will be apparent to persons having skill in the relevant art, such as a cellular phone, smart phone, table computer, etc. The mobile device 102 may include a secure element. A secure element may be a tamper-resistant platform capable of securely storing data, such as a hardware chip. The secure element may store a master key identifier, which may be provisioned to the secure element at the time of the manufacture of the mobile device 102, or via an over-the-air (OTA) provisioning method, such as discussed in more detail below.

[0034] The mobile device 102 may also include data related to one or more mobile cloud accounts. A mobile cloud account may include a mobile cloud account number (MCA), which may be associated with a real card account number (RCA). The RCA may correspond to a payment account issued to the user by an issuer 112. The MCA may be mapped to the RCA such that the user may conduct a financial transaction using the MCA for funding of the financial transaction, and the funds may be supplied by the payment account corresponding to the RCA. As a result, the user may be able to conduct a payment transaction using the mobile device 102 without storing the RCA, thereby reducing the potential for fraud.

[0035] The user may indicate, using the mobile device 102, one of the MCAs to be used to fund a financial transaction while at a merchant. The mobile device 102 may execute a post issuance script, discussed in more detail below, configured to transmit mobile cloud account data into the secure element of the mobile device 102. The mobile device may then transmit payment credentials for the indicated mobile cloud account to a contactless point-of-sale terminal 104 via near field transaction. Methods and systems for the transmission of payment credentials via near field transaction will be apparent to persons having skill in the relevant art.

[0036] The contactless terminal 104 may transmit the payment credentials and other transaction information to an acquirer 106, such as an acquiring bank, operating as or on behalf of the merchant, who may then submit an authorization request for the financial transaction with the MCA included for funding of the transaction. The submission of authorization requests for a financial transaction will be apparent to persons having skill in the relevant art. The authorization request may be submitted to, and received by, a payment network 108.

[0037] The payment network 108 may identify the MCA included in the authorization request and may, based on attributes of the MCA, such as an issuer identification number (IIN) or bank identification number (BIN), route the authorization request to a mobile cloud service provider 110. The

service provider 110 may include a mapping database 116 configured to store a plurality of mapping records, each of which may include at least a master key identifier, an MCA, and the corresponding RCA. The service provider 110 may identify the MCA included in the authorization request and then may identify the corresponding mapping record included in the mapping database 116. The service provider 110 may then transmit the corresponding RCA back to the payment network 108. It will be apparent to persons having skill in the relevant art that the service provider 110 may be any service, server, manager, system, etc. configured to perform the functions as disclosed herein. In some embodiments the service provider 110 may be included as part of the payment network 108 or may be operated by or on behalf of the issuer 112.

[0038] The payment network 108 may receive the RCA corresponding to the MCA supplied by the mobile device 102, and may forward the authorization request including the RCA to the issuer 112 for authorization. The issuer 112 may then authorize the financial transaction for funding by the payment account corresponding to the RCA and submit an authorization response to the payment network 108. The payment network 108 may then replace the RCA included in the authorization response with the MCA, and forward the authorization response to the acquirer 106, which may forward the response to the merchant for finalization of the transaction.

[0039] Following the finalization of the financial transaction, the acquirer 106 may post the financial transaction for clearing with a clearing service 114. In an exemplary embodiment, the clearing service 114 may transmit the posted transaction to the service provider 110. The service provider 110 may identify the RCA corresponding to the MCA included in the posted transaction using the mapping database 116, and may return the identified RCA to the clearing service 114. The clearing service 114 may then clear the transaction using the RCA with the issuer 112 using systems and methods apparent to persons having skill in the relevant art.

[0040] The use of the MCA may enable the user of the mobile device 102 to more securely conduct a contactless payment transaction without using an RCA. In addition, the issuer 112 may be able to process the financial transaction via the RCA without being required to significantly change their existing processing systems. In some embodiments, the service provider 110 may pre-validate the payment transaction based on the MCA and/or additional payment credentials. In such an embodiment, if the validation of the MCA fails, the service provider 110 (e.g., via the payment network 108) may transmit an authorization response to the acquirer 106 indicating denial of the transaction, and notify the issuer 112 of the failed validation. This may allow the transaction to be conducted without requiring any processing by the issuer 112. Conversely, if validation succeeds, the authorization may reach the issuer 112 pre-validated, which may enable the issuer 112 to approve or deny the transaction without being required to perform validation. Such a system may then not only enable the issuer 112 to process contactless payment transactions, but may also improve the efficiency of transaction processing.

Mobile Device

[0041] FIG. 2 illustrates data stored in the mobile device 102 for use in conducting contactless payment transactions via a mobile cloud account. The mobile device 102 may include a mobile wallet 202. The mobile wallet 202 may be an electronic wallet configured to store and transmit payment credentials for one or more mobile cloud accounts. The use of electronic wallets for the storage and transmission of payment credentials will be apparent to persons having skill in the relevant art. The mobile account credentials may include at least the MCA for each mobile cloud account and one or more security key certificates, as discussed in more detail below.

[0042] The mobile device 102 may also include a payment user interface (UI) 204. The payment UI 204 may include an interface provided for the user for management of a payment application 208. The payment

application 208 may be an application program stored on the mobile device 102 and executed by a processor of the mobile device. The payment application 208 may provide security for the functions performed by the mobile device 102 as disclosed herein, and may also facilitate communication between the internal components of the mobile device 102 as well as external communications, such as with the service provider 110. The payment UI 204 and/or the payment application 208 may be downloaded and/or installed to the mobile device using methods and systems that will be apparent to persons having skill in the relevant art, such as the downloading of application data from an application store via the Internet.

[0043] The mobile device 102 may also include a secure element 210. As discussed above, the secure element 210 may be a tamper-resistant platform, such as a hardware chip. The secure element 210 may store at least a master key identifier and a mobile cardlet. In an exemplary embodiment, the master key identifier and the mobile cardlet may be stored in separate portions of the secure element 210. The master key identifier may be a value that is unique to the mobile device 102, such as a sixteen or nineteen digit number. Values suitable for use as the master key identifier will be apparent to persons having skill in the relevant art.

[0044] The master key identifier may be provisioned to the secure element 210 by the manufacturer of the mobile device 102 at the time of the manufacture of the mobile device 102. In some instances, the master key identifier may be provisioned to the mobile device 102 and stored in the secure element 210 via over-the-air (OTA) processing, as discussed in more detail below. The mobile cardlet may be similarly provisioned to the secure element 210 physically or via OTA processing. In some embodiments the mobile cardlet and master key identifier may be provisioned to the secure element 210 simultaneously.

[0045] The mobile cardlet may be configured to store mobile cloud account data for the transmission of payment credentials including the mobile cloud

account data to the contactless terminal 104 for the conducting of a payment transaction. When a mobile cloud account is selected by the user for the funding of the payment transaction, the mobile device 102 may execute a post issuance script, discussed in more detail below, which may transmit payment credentials for the selected mobile cloud account to the secure element 210 (e.g., to the mobile cardlet). The user may then initiate transmission of the payment credentials from the mobile cardlet to the contactless terminal 104 to initiate the transaction.

[0046] In some embodiments, the payment UI 204 may include additional functionality 206. The additional functionality 206 may be configured to provide the user of the mobile device 102 with additional functions, such as the application of coupons to contactless transactions conducted using the mobile device 102, participation in a loyalty program, receiving of offers or discounts, etc. Additional functions will be apparent to persons having skill in the relevant art, such as the inControl™ platform by MasterCard®. Details regarding inControl™ may be found in U.S. Patent No. 6,636,833, issued October 21, 2003; U.S. Patent No. 7,136,835, issued November 14, 2006; U.S. Patent No. 7,571,142, issued August 4, 2009; U.S. Patent No. 7,567,934, issued July 28, 2009; U.S. Patent No. 7,593,896, issued September 22, 2009; U.S. Patent Application No. 12/219,952, filed July 30, 2008; U.S. Patent Application No. 12/268,063, filed November 10, 2008; and U.S. Patent Application No. 12/359,971, filed January 26, 2009; each of which are herein incorporated by reference in their entirety.

Provisioning of Master Key Identifiers and MCAs to the Mobile Device

[0047] FIG. 3 is a process flow illustrating a method for the OTA provisioning of a master key identifier to the mobile device 102 for storage in the secure element 210.

[0048] In step 306, a user 302 may request to use the mobile cloud service on a mobile device 102 that lacks a master key identifier in a secure element 210 of the mobile device 102. The request may be submitted to the service

provider 110 via a mobile network operator (MNO) 304. The service provider 110 may receive the request and may, in step 308, verify that the mobile device 102 does not already include a master key identifier. In an instance where, in step 308, the service provider 110 may identify that the mobile device 102 already includes a master key identifier in the secure element 210 (e.g., if the master key identifier was provisioned by the MNO or a third party (e.g., the mobile device manufacturer, secure element issuer, etc.) at the manufacture of the mobile device 102), the method may proceed to step 316, if applicable, or step 320 where the mobile device 102 may be ready to receive MCAs.

[0049] In step 310, the service provider 110 may generate a master key identifier and a mobile cardlet for provisioning to the mobile device 102. The master key identifier may be any unique value suitable for the identification of the mobile device 102 and/or the secure element 210. In an exemplary embodiment, the master key identifier may be a sixteen or nineteen digit number. In another exemplary embodiment, the master key identifier may be identified in outside of possible RCA account ranges such that the master key identifier may not correspond to a RCA. In a further embodiment, the first digit of a generated master key identifier may be zero. The mobile cardlet may be configured to store payment credentials for transmission to the contactless terminal 104 via near field communication. In an exemplary embodiment, the mobile cardlet may contain no payment credentials upon provisioning to the mobile device 102.

[0050] In step 312, the service provider 110 may push (e.g., transmit) the generated master key identifier and mobile cardlet to the mobile device 102 via the MNO 304. The mobile device 102 may receive the data and may, in step 314, install (e.g., store) the master key identifier and mobile cardlet into the secure element 210. In an exemplary embodiment, the master key identifier and mobile cardlet may be stored in separate portions of the secure element 210.

[0051] In step 316, the service provider 110 may identify (e.g., generate) personalization data and forward the personalization data to the mobile device 102. The personalization data may be data uniquely associated with the user 302 and/or the mobile device 102, as discussed in more detail below. In step 318, the mobile device 102 may receive and install the personalization data in the secure element 210. Then, in step 320, the mobile device 102 may be ready to receive MCAs for use in conducting contactless payment transactions.

[0052] FIGS. 4A and 4B are a process flow illustrating a method for the provisioning of a mobile cloud account to the mobile device 102.

[0053] In step 402, the MNO 304 may provision the master key identifier to the mobile device 102. It will be apparent to persons having skill in the relevant art that, in some embodiments, the master key identifier may be provisioned to the mobile device 102 over the air, such as using the method illustrated in FIG. 3. In step 404, the mobile device 102 may receive the master key identifier and store the master key identifier in the secure element 210.

[0054] In step 406, the user 302 may receive the mobile device 102, such as by purchasing the mobile device 102, or may otherwise be in possession of the mobile device 102 with the master key identifier included in the secure element 210. In step 408, the user 302 may perform a service discovery to identify any RCAs associated with the user 302 that are eligible for use with the mobile cloud service. The service discovery may be performed by the MNO 304, in step 410, by identifying those RCAs associated with the user 302 eligible for the mobile cloud service. In some embodiments, the method may include step 412, where the issuer 112 may provide real card account information to the MNO 304 for use in the determination of eligible RCAs. For example, the MNO 304 may request specific card or issuer system details to determine if an RCA may be used in the mobile cloud service. In one embodiment, the identification of eligible RCAs may be performed by the service provider 110.

[0055] In step 414, the MNO 304 may transmit the eligible RCAs to the mobile device 102, for display to the user 302 at step 416 (e.g., via the payment UI 204). It will be apparent to persons having skill in the relevant art that steps 408 and 416 may be performed via a computing device other than the mobile device 102, such as a computer where the user 302 may initiate the service discovery and view eligible RCAs via a webpage.

[0056] In step 418, the user 302 may request an MCA for a real card account. The request may be submitted to the service provider 110. The service provider 110 may then request the master key identifier from the secure element 210 of the mobile device 102. The mobile device 102 may identify the master key identifier in the secure element 210 and transmit it to the service provider 110 in step 422. The service provider 110 may then, in step 424, request details for the real card account identified by the user 302 from the issuer 112. The issuer 112 may identify the real card account in step 426 and then may, in step 428, provide the requested RCA details back to the service provider 110.

[0057] In step 430, the service provider 110 may identify an MCA to correspond to the RCA, may map the MCA to the RCA, and store a mapping record in the mapping database 116. Identification of the MCA is discussed in more detail below with respect to FIG. 9. In some embodiments, step 430 may be an optional step. In such an embodiment, the MCA may be identified by the issuer 112 and supplied directly to the service provider 110. The service provider 110 may validate the payment credentials for the MCA supplied by the issuer 112, but the issuer 112 may perform any necessary mapping as part of the processing of the financial transaction.

[0058] In step 432, the service provider 110 may generate a post issuance script. The post issuance script may be configured to cause the mobile device 102 to transmit mobile cloud account data for a selected MCA from a database or storage in the mobile device 102 to the mobile cardlet inside of the secure element 210. Data that may be included in the mobile cloud

account data may include the MCA and additional information discussed in more detail below.

[0059] In step 434, the service provider 110 may transmit the post issuance script and related data to the mobile device 102, which may receive the script and data in step 436. In step 438, the user 302 may (e.g., via the display UI 204), select an MCA for use in funding a contactless payment transaction. Once the MCA is selected, the mobile device 102 may execute the corresponding post issuance script. The execution of the script may cause the mobile device 102 to transmit the corresponding mobile cloud account data into the mobile cardlet in the secure storage 210. In some embodiments, the transmitted mobile cloud account data may overwrite an existing mobile cloud account data in the mobile cardlet such that the mobile cardlet may include data for only a single mobile cloud account at any given time. In step 442, the mobile device 102 may be ready for the contactless payment transaction (e.g., ready to transmit payment credentials to the contactless terminal 104 via near field communication).

Processing Authorization Requests in Mobile Cloud Account Contactless Transactions

[0060] FIG. 5 is a high level flow diagram illustrating a method for processing an authorization request for a contactless payment transaction funded via an MCA initiated by the mobile device 102.

[0061] In step 502, the mobile device 102 may transmit the MCA and related payment credentials from the mobile cardlet in the secure storage to the contactless terminal 104 via near field communication. Methods suitable for the secure transmission of payment credentials via near field communication will be apparent to persons having skill in the relevant art. The contactless terminal 104 may receive the MCA and payment credentials and may, in step 504, forward the information to the acquirer 106. The acquirer 106 may then generate an authorization request using systems and

methods apparent to persons having skill in the relevant art, wherein the authorization request includes the MCA and payment credentials.

[0062] The authorization request may be submitted by the acquirer to the payment network 108 in step 506. The payment network 108 may then, in step 508, forward at least the MCA to the service provider 110. The service provider 110 may receive the MCA and perform cryptography to validate the MCA using methods apparent to persons having skill in the relevant art. The service provider 110 may also, using the mapping database 116, identify an RCA corresponding to the MCA. The service provider 110 may then, in step 510, forward the identified RCA to the payment network 108.

[0063] In instances where validation of the MCA fails, the service provider 110 may return an indication of the failure of the validation to the payment network 108 and/or directly to the acquirer 106. In some embodiments, if verification fails, the service provider 110 may transmit a notification to the issuer 112. In a further embodiment, the issuer 112 may request to the service provider 110 to not be notified of any failed verifications. In one embodiment, the service provider 110 may still forward the RCA to the payment network 108 for forwarding to the issuer 112 if mapping succeeds but cryptography validation of payment credentials (e.g., a payment cryptogram) fails.

[0064] The payment network 108 may receive the RCA from the service provider 110 and may, in step 512, replace the MCA in the authorization request with the RCA and forward the authorization request to the issuer 112. In embodiments where the issuer 112 provides the MCA directly to the service provider 110 (e.g., such that the service provider 110 does not generate the MCA), the payment network may submit the authorization request including the MCA and the indication of the successful validation performed by the service provider 110, and the issuer 112 may map the MCA to the corresponding RCA. Once the issuer 112 has the authorization request and the RCA, the issuer 112 may approve or deny the financial transaction using systems, methods, and practices that will be apparent to

persons having skill in the relevant art. The issuer 112 may then, in step 514, submit an authorization response to the payment network 108 indicating whether the transaction is approved or denied.

[0065] The payment network 108 may then replace the RCA in the authorization response with the MCA and forward the modified authorization response to the acquirer 106 for finalization of the transaction. In some embodiments, the payment network 108 may forward the authorization response including the RCA to the service provider 110 for replacement with the MCA via the mapping database 116.

[0066] FIG. 6 is a process flow illustrating a more detailed method for the authorization of a contactless payment transaction funded via a mobile cloud account.

[0067] In step 602, the user 302 may "tap" the contactless terminal 104 using the mobile device 102 with payment credentials loaded into the mobile cardlet in the secure storage 210. The term "tapping" may refer to the transmission of payment credentials via near field communication from the mobile device 102 to the contactless terminal 104 due to the close proximity of the mobile device 102 to the terminal 104, which sometimes may result in the mobile device 102 physically tapping the terminal 104. The payment credentials may include a payment cryptogram, such as an authorization request cryptogram or dynamic card validation code, generated based on at least a portion of the mobile cloud account data stored in the secure element 210. The contactless terminal 104 may forward the payment credentials, including the MCA and payment cryptogram, to the acquirer 106, who may then submit an authorization request including the MCA and payment credentials to the payment network 108 in step 604.

[0068] In some embodiments, the mobile device 102 may also transmit additional credentials to the contactless terminal. For example, the credentials may include a mobile personal identification number (PIN), which may be a number input by the user 302 into the mobile device 102 prior or subsequent to indication of an MCA for use in the payment transaction. In

another example, the credentials may include an online PIN, which may be input by the user 302 into the contactless terminal 104. In some instances, the contactless terminal 104 may prompt the user 302 to input the online PIN subsequent to the transmission of the payment credentials to the contactless terminal 104 and prior to the transmission of data to the acquirer 106.

[0069] In step 606, the payment network 108 may route the authorization request based on the MCA. For example, the number may indicate that the transaction is to be funded by an MCA, which the payment network 108 may identify needs to be mapped by the service provider 110 and accordingly forward the relevant information to the service provider 110. In some embodiments, the authorization request may originate from a different payment network, but may be forwarded to the payment network 108 and/or the service provider 110 for validation/verification and/or mapping. In a further embodiment, the verified and/or mapped credentials may be forwarded on to the issuer 112 for authorization, and then returned to the originating payment network. The processing of payment transactions across multiple payment networks will be apparent to persons having skill in the relevant art.

[0070] In step 608, the service provider 110 may receive the MCA and additional payment credentials if applicable and may verify (e.g., validate) the MCA and/or payment cryptogram or other credentials using cryptography methods and systems apparent to persons having skill in the relevant art. If the verification of the credentials fails, then, in step 610, the payment network 108 may receive an indication from the service provider 110 to deny the authorization. The payment network 108 may then submit an authorization response denying the transaction, which may then be forwarded to the contactless terminal in step 612. In some embodiments, the service provider 110 may submit a notification to the issuer 112 of the failed verification of the credentials. In a further embodiment, the service provider 110 may map the MCA used in the failed verification to identify the corresponding RCA and include the corresponding RCA in the notification.

[0071] If the credentials are successfully verified, then, in step 614, the service provider 110 may identify the RCA corresponding to the MCA via the mapping database 116. It will be apparent to persons having skill in the relevant art that, in some embodiments, step 614 may be an optional step. In such an embodiment, the service provider 110 may return only an indication of the successful validation of the credentials. If the mapping is performed by the service provider 110, then, in step 616, the service provider 110 may return the corresponding RCA to the payment network 108.

[0072] In step 618, the payment network 108 may route the authorization request with the RCA in place of the MCA to the issuer 112. In step 620, the issuer 112 may approve and process the financial transaction using methods apparent to persons having skill in the relevant art. In embodiments where the service provider 110 does not generate and map an MCA, the authorization response routed to the issuer 112 may include the MCA, and step 620 may further include identifying the RCA corresponding to the MCA. In step 622, the issuer 112 may submit a response to the payment network 108 approving the financial transaction.

[0073] In step 624, the payment network 108 may replace the RCA included in the authorization response with the corresponding MCA. In some embodiments, replacing the RCA may include step 626, where the service provider 110 may remap the RCA to the corresponding MCA and transmit the MCA to the payment network 108. The payment network 108 may transmit the authorization response including the MCA to the acquirer 106, who may then forward the authorization response to the contactless terminal 104 for finalization of the transaction.

Provisioning of Mobile Cloud Account Data to the Mobile Device

[0074] FIGS. 7 and 8 illustrate the provisioning of mobile cloud account data to the mobile device 102 and subsequently into the secure element 210

for transmission to the contactless terminal 104 for use in funding a contactless payment transaction.

[0075] As illustrated in FIG. 7, the issuer 112 may issue a plurality of real card accounts 702 to the user 302. Each real card account may include an RCA corresponding to the account. Using methods disclosed herein and discussed in more detail below, the service provider 110 may identify and/or generate an MCA to correspond to each RCA. The MCA may be included in a mobile cloud account 704 provisioned to the wallet 202 of the mobile device 102. The wallet 202 may store the mobile cloud account 704 and related data (e.g., MCA, post issuance scripts, etc.) for selection by the user 302 for use in a contactless payment transaction.

[0076] The mobile device 102 may also include the secure element 210. The secure element 210 may include the master key identifier 706 stored in a first portion of the secure element 210.

[0077] As illustrated in FIG. 8, each mobile cloud account 704 may include mobile cloud account data 802, such as the MCA, an issuer public key certificate, and ICC public key certificate, discussed in more detail below. When the user 302 indicates a particular mobile cloud account 704 for use in funding a payment transaction, the mobile device 102 may execute the corresponding post issuance script. The post issuance script may cause the mobile device 102 to execute an update command 804. The update command 804 may cause the mobile device 102 to transmit the mobile cloud account data 802 to the secure element 210.

[0078] The mobile cloud account data 802 may be stored in the secure element 210 in a second portion of the secure element 210 separate from the master key identifier 706, such as the mobile cardlet. The storage of the mobile cloud account data 802 in a separate portion of the secure element 210 may provide for additional security to prevent misappropriation or unauthorized access to the master key identifier 706 or other information. It will be apparent to persons having skill in the relevant art that the data included in the mobile cloud account data 802 as illustrated in FIG. 8 is

provided as an illustration, and that the mobile cloud account data 802 may include different data or information.

Generation and Mapping of Mobile Cloud Account Numbers and Data

[0079] FIG. 9 is a process flow illustrating a detailed method for the generation of mapping and cryptography data for a mobile cloud account.

[0080] In step 902, the service provider 110 may generate (e.g., create) an integrated circuit card (ICC) RSA key pair, which may include an ICC public key and an ICC private key. Methods for generating key pairs using RSA will be apparent to persons having skill in the relevant art. In step 904, the service provider 110 may create ICC master keys, such as an ICC master data encryption service (DES) key, based on the master key identifier sequence number and master key identifier domain issuer master keys.

[0081] In step 906, the service provider 110 may create personalization data. The personalization data may include data personalized to a specific user 302 and/or mobile device 102. In an exemplary embodiment, the personalized data may include at least an ICC DES master key, the ICC private key, the ICC public key and master key identifier and sequence number, and any additional information as applicable, such as card risk management information. In step 908, the personalization data may be transmitted to the mobile device 102 for storage in the secure element (e.g., in the mobile cardlet). In embodiments where the secure element does not already include the mobile cardlet (e.g., such as during OTA processing), step 906 may further include creating the mobile cardlet for installation in the secure storage 210 in step 908.

[0082] In step 910, the mobile device 102 may transmit the mobile key identifier and ICC public key stored in the secure element 210 to the service provider 110. In step 912, the issuer 112 may send the RCA to which an MCA is requested to the service provider 110. It will be apparent to persons having skill in the relevant art that steps 910 and 912 may be performed concurrently, in an alternate order, or at varying points in time. It will be

further apparent to persons having skill in the relevant art that step 910 may be optional, as the service provider 110 may retain the mobile key identifier and ICC public key utilized and/or created in previous steps. In some embodiments, step 912 may occur prior to step 902 such that step 902 is triggered by the receipt of the RCA for the identification and mapping of a corresponding MCA.

[0083] In step 914, the service provider 110 may generate an MCA corresponding to the RCA. The MCA may be generated to include one or more attributes of the RCA. In one embodiment, the MCA may include one or more attributes of the RCA including at least one of: brand, product, country code, region, account level management participation, and Durbin indicator. In some embodiments, the MCA may include at least a portion of the RCA. In a further embodiment, the portion may be at least the last four digits of the RCA. In such an embodiment, the payment UI 204 may display the mobile cloud account for the MCA to the user 302 in the form of an image of a payment card with first twelve digits of the MCA obscured (e.g., replaced by asterisks) and the last four digits displayed, such that the user 302 may readily recognize which MCA corresponds to which RCA based on the last four digits. It will be apparent to persons having skill in the relevant art that other indicators may be used, such as a similar graphical image (e.g., a graphical representation of a physical payment card), a nickname or other notation provided by the user 302, etc.

[0084] In some embodiments, the MCA may be identified such that there is a 1:1 relationship between an RCA account range and an MCA account range. In a further embodiment, an MCA account range may correspond to a particular issuer 112. In an exemplary embodiment, the first digit of the identified MCA may be zero, which may indicate that the MCA corresponds to an RCA (e.g., for routing by a payment network 108). In some embodiments, multiple MCAs may be mapped to correspond to a single RCA, such as in an instance where multiple payment cards may be issued for a single RCA (e.g., family cards, corporate cards, etc.).

[0085] In step 916, the service provider 110 may create an ICC public key certificate. In some embodiments, the ICC public key certificate may be created by the certification of the ICC public key by an issuer private key received from the issuer 112. In a further embodiment, the ICC public key may be received by the service provider 110 from the secure element 210 of the mobile device 102. In step 918, the issuer 112 may transmit an issuer public key certificate to the service provider 110.

[0086] In step 920, the service provider 110 may generate mobile cloud account data 802 corresponding to the generated MCA. The mobile cloud account data 802 may include at least the issuer public key certificate, the ICC public key certificate, and the MCA. In some embodiments, the generated MCA may include an expiration date, which may be further included in the mobile cloud account data 802. In one embodiment, the mobile cloud account data 802 may further include static track data and initialization vectors.

[0087] In step 922, the service provider 110 may generate a post issuance script configured to transmit the mobile cloud account data 802 from the wallet 202 of the mobile device 102 to the mobile cardlet in the secure storage 210. The service provider 110 may transmit the post issuance script to the mobile device 102, which may, in step 924, receive and store the post issuance script in the wallet 202. In step 926, the service provider 110 may save a mapping record for the generated MCA in the mapping database 116. The mapping record may include at least the master key identifier 706, the MCA, and the RCA.

Exemplary Method for Mapping a Payment Account to a Mobile Cloud Account Number

[0088] FIG. 10 illustrates a method 1000 for mapping a payment account (e.g., the real card account 702) to a mobile cloud account number.

[0089] In step 1002, an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key may be generated by a generating

device (e.g., included in the service provider 110). In step 1004, the generating device may generate an ICC master key based on at least a master key identifier (e.g., the master key identifier 706). In one embodiment, the master key identifier may be a sixteen or nineteen digit number.

[0090] In step 1006, a transmitting device may transmit at least the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device (e.g., the mobile device 102) for storage in a secure element (e.g., the secure element 210). In step 1008, a receiving device may receive a real card account number (RCA) corresponding to a payment account 702.

[0091] In step 1010, attributes of the RCA may be identified by a processing device. In one embodiment, the attributes of the RCA may include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator. In step 1012, the processing device may identify a mobile cloud account number (MCA) based on the identified attributes of the RCA. In one embodiment, identifying the MCA may include receiving, by the receiving device, the MCA from an issuer (e.g., the issuer 112) associated with the RCA. In some embodiments the identified MCA may include at least a portion of the RCA. In a further embodiment, the portion of the RCA may include at least the last four digits.

[0092] In step 1014, the receiving device may receive an issuer private key and an issuer private key certificate. In step 1016, the generating device may generate an ICC public key certificated based on certification of the ICC public key by the issuer private key. In step 1018, the processing device may create a post issuance script configured to store mobile cloud account data (e.g., the mobile cloud account data 802) in the secure element 210 of the mobile device 102, wherein the mobile cloud account data 802 includes at least the issuer public key certificate, the MCA, and the ICC public key certificate.

[0093] In step 1020, the transmitting device may transmit the created post issuance script to the mobile device 102. In step 1022, a mapping record may be stored in a mapping database (e.g., the mapping database 116), wherein the mapping record includes at least the master key identifier 706, the MCA, and the RCA.

Exemplary Method for Processing a Financial Transaction

[0094] FIG. 11 illustrates a method 1100 for processing a contactless financial transaction using a mobile cloud account.

[0095] In step 1102, a plurality of mapping records may be stored in a mapping database (e.g., the mapping database 116), wherein each mapping record includes at least a master key identifier (e.g., the master key identifier 706), a mobile cloud account number (MCA), and a real card account number (RCA), and wherein the MCA is based on attributes of the RCA. In one embodiment the MCA may include at least a portion of the RCA. In a further embodiment, the portion of the RCA may include at least the last four digits of the RCA. In some embodiments, the attributes of the RCA may include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator. In one embodiment, the master key identifier 706 may be a sixteen or nineteen digit number.

[0096] In step 1104, a receiving device may receive transaction data related to a financial transaction, wherein the transaction data may include at least an MCA and a payment cryptogram. In one embodiment, the received transaction data may be included in an authorization request for the financial transaction. In some embodiments, the payment cryptogram may be one of: a dynamic card validation code and an authorization request cryptogram. In step 1106, a validation device may validate the payment cryptogram.

[0097] In step 1108, a specific mapping record may be identified in the mapping database 116, wherein the specific mapping record includes the MCA included in the received transaction data. In step 1110, a transmitting device may transmit at least the RCA included in the specific mapping record

and a validation result indicating a success or failure of the validation of the payment cryptogram.

[0098] In embodiments where the transaction data may be included in an authorization request, the method 1100 may further comprise: receiving, by the receiving device, an authorization response from an issuer (e.g., the issuer 112) associated with the RCA, the authorization response including at least the RCA included in the specific mapping record and an indication of approval or denial of the financial transaction; and transmitting, by the transmitting device, an authorization response including the MCA included in the specific mapping record in response to the authorization request.

Exemplary Method for Providing Payment Credentials for a Financial Transaction

[0099] FIG. 12 illustrates a method 1200 for providing payment credentials for a mobile cloud account from a mobile device for a contactless payment transaction.

[0100] In step 1202, personalization data may be received by a receiving device, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier (e.g., the master key identifier 706). In step 1204, the received personalization data may be stored in a first location of a secure element (e.g., the secure element 210) of a mobile device (e.g., the mobile device 102).

[0101] In step 1206, at least one post issuance script may be received by a receiving device, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element 210 of the mobile device 102, mobile cloud account data (e.g., the mobile cloud account data 802), the mobile cloud account data 802 including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA), and wherein the MCA is based on attributes of a real card account number (RCA). In one embodiment, the MCA may include

at least a portion of the RCA. In a further embodiment, the portion of the RCA may include at least the last four digits of the RCA. In some embodiments, the attributes of the RCA may include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator. In one embodiment, the master key identifier 706 is a sixteen or nineteen digit number.

[0102] In step 1208, the received at least one post issuance script may be stored in a database (e.g., the wallet 202) not included in the secure element 210. In step 1210, an indication of an MCA included in a specific post issuance script of the at least one post issuance script may be received by an input device. In one embodiment the input device may include at least one of: a mouse, keyboard, click wheel, scroll wheel, and touch screen. In step 1212, the specific post issuance script may be executed by a processing device.

[0103] In one embodiment, the method 1200 may further include: generating, by a generating device, a payment cryptogram based on at least a portion of the mobile cloud account data 802; and transmitting, via near field communication, at least the generated payment cryptogram and the indicated MCA. In a further embodiment, the payment cryptogram may be one of: a dynamic card validation code and an authorization request cryptogram.

Computer System Architecture

[0104] FIG. 13 illustrates a computer system 1300 in which embodiments of the present disclosure, or portions thereof, may be implemented as computer-readable code. For example, mobile device 102, the contactless terminal 104, the acquirer 106, the payment network 108, the service provider 110, the issuer 112, and the clearing service 114 of FIG. 1 may be implemented in the computer system 1300 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. 3-7 and 9-12.

[0105] 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.

[0106] 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 1318, a removable storage unit 1322, and a hard disk installed in hard disk drive 1312.

[0107] Various embodiments of the present disclosure are described in terms of this example computer system 1300. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the present disclosure using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0108] Processor device 1304 may be a special purpose or a general purpose processor device. The processor device 1304 may be connected to a communication infrastructure 1306, 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 1300 may also include a main memory 1308 (e.g., random access memory, read-only memory, etc.), and may also include a secondary memory 1310. The secondary memory 1310 may include the hard disk drive 1312 and a removable storage drive 1314, such as a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, etc.

[0109] The removable storage drive 1314 may read from and/or write to the removable storage unit 1318 in a well-known manner. The removable storage unit 1318 may include a removable storage media that may be read by and written to by the removable storage drive 1314. For example, if the removable storage drive 1314 is a floppy disk drive, the removable storage unit 1318 may be a floppy disk. In one embodiment, the removable storage unit 1318 may be non-transitory computer readable recording media.

[0110] In some embodiments, the secondary memory 1310 may include alternative means for allowing computer programs or other instructions to be loaded into the computer system 1300, for example, the removable storage unit 1322 and an interface 1320. 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 1322 and interfaces 1320 as will be apparent to persons having skill in the relevant art.

[0111] Data stored in the computer system 1300 (e.g., in the main memory 1308 and/or the secondary memory 1310) 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.

[0112] The computer system 1300 may also include a communications interface 1324. The communications interface 1324 may be configured to allow software and data to be transferred between the computer system 1300 and external devices. Exemplary communications interfaces 1324 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 1324 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 1326, 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.

[0113] Computer program medium and computer usable medium may refer to memories, such as the main memory 1308 and secondary memory 1310, which may be memory semiconductors (e.g. DRAMs, etc.). These computer program products may be means for providing software to the computer system 1300. Computer programs (e.g., computer control logic) may be stored in the main memory 1308 and/or the secondary memory 1310. Computer programs may also be received via the communications interface 1324. Such computer programs, when executed, may enable computer system 1300 to implement the present methods as discussed herein. In particular, the computer programs, when executed, may enable

processor device 1304 to implement the methods illustrated by FIGS. 3-7 and 9-12, as discussed herein. Accordingly, such computer programs may represent controllers of the computer system 1300. Where the present disclosure is implemented using software, the software may be stored in a computer program product and loaded into the computer system 1300 using the removable storage drive 1314, interface 1320, and hard disk drive 1312, or communications interface 1324.

[0114] Techniques consistent with the present disclosure provide, among other features, systems and methods for mapping mobile cloud accounts to payment accounts and the processing of financial transactions funded thereof. 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. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the disclosure, without departing from the breadth or scope.

CLAIMS:

1. A method for mapping a payment account to a mobile cloud account number, comprising:

generating, by a generating device, an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key;

generating, by the generating device, an ICC master key based on at least a master key identifier;

transmitting, by a transmitting device, the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device for storage in a secure element;

receiving, by a receiving device, a real card account number (RCA) corresponding to a payment account;

identifying, by a processing device, attributes of the RCA;

identifying, by the processing device, a mobile cloud account number (MCA) based on the attributes of the RCA;

receiving, by the receiving device, an issuer private key and an issuer private key certificate;

generating, by the generating device, an ICC public key certificate based on certification of the ICC public key by the issuer private key;

creating, by the processing device, a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, wherein the mobile cloud account data includes at least an issuer public key certificate, the MCA, and the ICC public key certificate;

transmitting, by the transmitting device, the created post issuance script to the mobile device; and

storing, in a mapping database, a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA.

2. The method of claim 1, wherein identifying a MCA based on the attributes of the RCA includes receiving, by the receiving device, the MCA from an issuer associated with the RCA.

3. The method of claim 1, wherein the identified MCA includes at least a portion of the RCA.

4. The method of claim 3, wherein the portion of the RCA includes at least the last four digits of the RCA.

5. The method of claim 1, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

6. The method of claim 1, wherein the master key identifier is a sixteen or nineteen digit number.

7. A computer-implemented method for processing a financial transaction initiated by a secure element of a mobile device, comprising:

storing, in a mapping database of a mobile cloud service provider, a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA), wherein (i) the mobile cloud service provider is configured to bi-directionally communicate with point-of-sale (POS) devices of merchants, via associated acquirers and/or issuers; (ii) the master key identifier is a value unique to the mobile device and is provisioned to the secure element of the mobile device, and (iii) the MCA is based on attributes of the RCA;

receiving, by a receiving device of the mobile cloud service provider, from a contactless POS terminal of a merchant, transaction data related to a financial transaction,

receiving, by the receiving device of the mobile cloud service provider, from a mobile device via the contactless POS terminal of the merchant, at least an MCA and a payment cryptogram, wherein the transaction data, the MCA, and the payment cryptogram are received as a first authorization request;

performing, by the mobile cloud service provider, cryptography to validate the MCA and the payment cryptogram received from the mobile device via the contactless POS terminal of the merchant;

when the MCA and payment cryptogram are successfully validated, (i) identifying, in the mapping database of the mobile cloud service provider, a specific mapping record, wherein the specific mapping record includes the MCA included in the first authorization request, and (ii) electronically transmitting, by a transmitting device of the mobile cloud service provider, a second authorization request comprising at least the RCA included in the specific mapping record and the transaction data to a computer system of an issuer associated with the RCA, via a payment network; and

when the MCA and payment cryptogram are not successfully validated, transmitting by the transmitting device of the mobile cloud service provider, an indication of failure of the validation to the contactless POS terminal of the merchant via the payment network without communicating with an issuer computer system.

8. The method of claim 7, further comprising:

provisioning, to a secure element of the mobile device, the MCA.

9. The method of claim 8, further comprising:

receiving, by the receiving device of the mobile cloud service provider, an authorization response from the issuer associated with the RCA, wherein the authorization response includes at least the RCA included in the specific mapping record and an indication of approval or denial of the financial transaction; and

transmitting, by the transmitting device of the mobile cloud service provider, an authorization response including the MCA included in the specific mapping record in response to the authorization request.

10. The method of claim 7, wherein the MCA includes at least a portion of the RCA.

11. The method of claim 10, wherein the portion of the RCA includes at least the last four digits of the RCA.

12. The method of claim 7, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

13. The method of claim 7, wherein the master key identifier is a sixteen or nineteen digit number.

14. The method of claim 7, wherein the payment cryptogram is one of: a dynamic card validation code and an authorization request cryptogram.

15. A method for providing payment credentials for a financial transaction, comprising:

receiving, by a receiving device, personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier;

storing, in a first location of a secure element of a mobile device, the received personalization data;

receiving, by the receiving device, at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA);

storing, in a database not included in the secure element, the received at least one post issuance script;

receiving, by an input device, an indication of an MCA included in a specific post issuance script of the received at least one post issuance script; and

executing, by a processing device, the specific post issuance script,

wherein the MCA is based on attributes of a real card account number (RCA).

16. The method of claim 15, further comprising:

generating, by a generating device, a payment cryptogram based on at least a portion of the mobile cloud account data; and

transmitting, via near field communication, at least the generated payment cryptogram and the indicated MCA.

17. The method of claim 16, wherein the payment cryptogram is one of: a dynamic card validation code and an authorization request cryptogram.

18. The method of claim 15, wherein the MCA includes at least a portion of the RCA.

19. The method of claim 18, wherein the portion of the RCA includes at least the last four digits of the RCA.

20. The method of claim 15, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

21. The method of claim 15, wherein the master key identifier is a sixteen or nineteen digit number.

22. A system for mapping a payment account to a mobile cloud account number, comprising:

a mapping database;

a generating device configured to generate an integrated circuit card (ICC) RSA key pair including an ICC public key and an ICC private key, and an ICC master key based on at least a master key identifier;

a transmitting device configured to transmit the ICC public key, the ICC private key, the ICC master key, and the master key identifier to a mobile device for storage in a secure element;

a receiving device configured to receive a real card account number (RCA) corresponding to a payment account; and

a processing device configured to identify attributes of the RCA and identify a mobile cloud account number (MCA) based on the attributes of the RCA, wherein

the receiving device is further configured to receive an issuer private key and an issuer private key certificate,

the generating device is further configured to generate an ICC public key certificate based on certification of the ICC public key by the issuer private key,

the processing device is further configured to create a post issuance script configured to store mobile cloud account data in the secure element of the mobile device, the mobile cloud account data including at least an issuer public key certificate, the MCA, and the ICC public key certificate,

the transmitting device is further configured to transmit the created post issuance script to the mobile device, and

the mapping database is configured to store a mapping record, wherein the mapping record includes at least the master key identifier, the MCA, and the RCA.

23. The system of claim 22, wherein the processing device is configured to identify the MCA by causing the receiving device to receive the MCA from an issuer associated with the RCA.

24. The system of claim 22, wherein the identified MCA includes at least a portion of the RCA.

25. The system of claim 24, wherein the portion of the RCA includes at least the last four digits of the RCA.

26. The system of claim 22, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

27. The system of claim 22, wherein the master key identifier is a sixteen or nineteen digit number.

28. A system for processing a financial transaction initiated by a secure element of a mobile device, comprising:

a mapping database of a mobile cloud service provider configured to store a plurality of mapping records, wherein each mapping record includes at least a master key identifier, a mobile cloud account number (MCA), and a real card account number (RCA), wherein (i) the mobile cloud service provider is configured to bi-directionally communicated with point-of-sale (POS) devices of merchants, via associated acquirers and/or issuers, (ii) the master key identifier is a value unique to a mobile device and is provisioned to a secure element of the mobile device, and (iii) the MCA is based on attributes of the RCA;

a receiving device of the mobile cloud service provider, configured to receive:

from a contactless POS terminal of a merchant, transaction data related to a financial transaction, and

from a mobile device via the contactless POS terminal of the merchant, at least an MCA and a payment cryptogram,

wherein the transaction data, the MCA and the payment cryptogram are received as a first authorization request;

a validation device of the mobile cloud service provider configured to perform cryptography to validate the MCA and payment cryptogram received from the mobile device via the contactless POS terminal of the merchant;

a processing device of the mobile cloud service provider; and

a transmitting device of the mobile cloud service provider,

wherein when the MCA and payment cryptogram are successfully validated, (i) the processing device is configured to identify, in the mapping

database of the mobile cloud service provider, a specific mapping record, said specific mapping record including the MCA included in the first authorization request, and (ii) the transmitting device is configured to transmit a second authorization request comprising at least the RCA included in the identified specific mapping record and transaction data to a computer system of an issuer associated with the RCA, via a payment network, and

when the MCA and payment cryptogram are not successfully validated, (i) the transmitting device, of the mobile cloud service provider, is configured to transmit an indication of failure of the validation to the contactless POS terminal of the merchant via the payment network without communicating with an issuer computer system.

29. The system of claim 28, wherein the MCA is stored in a secure element of the mobile device.

30. The system of claim 29, wherein

the receiving device of the mobile cloud service provider is further configured to receive an authorization response from the issuer associated with the RCA, the authorization response including at least the RCA included in the specific mapping record and an indication of approval or denial of the financial transaction, and

the transmitting device of the mobile cloud service provider is further configured to transmit an authorization response including the MCA included in the specific mapping record in response to the authorization request.

31. The system of claim 28, wherein the MCA includes at least a portion of the RCA.

32. The system of claim 31, wherein the portion of the RCA includes at least the last four digits of the RCA.

33. The system of claim 28, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

34. The system of claim 28, wherein the master key identifier is a sixteen or nineteen digit number.

35. The system of claim 28, wherein the payment cryptogram is one of: a dynamic card validation code and an authorization request cryptogram.

36. A mobile device for providing payment credentials for a financial transaction, comprising:

an input device;

a secure element;

a database not included in the secure element;

a receiving device configured to receive personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier; and

a processing device configured to store, in a first location of the secure element, the received personalization data, wherein

the receiving device is further configured to receive at least one post issuance script, each of the at least one post issuance script configured to cause the processing device to store, in a second location of the secure element, mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA),

the processing device is further configured to store the received at least one post issuance script in the database,

the input device is configured to receive an indication of an MCA included in a specific post issuance script of the received at least one post issuance script,

the processing device is further configured to execute the specific post issuance script, and

the MCA is based on the attributes of a real card account number (RCA).

37. The system of claim 36, further comprising:

a generating device configured to generate a payment cryptogram based on at least a portion of the mobile cloud account data, wherein

the transmitting device is further configured to transmit, via near field communication, at least the generated payment cryptogram and the indicated MCA.

38. The system of claim 37, wherein the payment cryptogram is one of: a dynamic card validation code and an authorization request cryptogram.

39. The system of claim 36, wherein the MCA includes at least a portion of the RCA.

40. The system of claim 39, wherein the portion of the RCA includes at least the last four digits of the RCA.

41. The system of claim 36, wherein the attributes of the RCA include at least one of: a brand, product, country code, region, account level management participation, and Durbin indicator.

42. The system of claim 36, wherein the master key identifier is a sixteen or nineteen digit number.

43. A non-transitory computer readable recording medium having program instructions stored therein that causes a processor of a mobile computing device to execute a method for providing payment credentials for a financial transaction, the method comprising:

receiving, by a receiving device, personalization data, wherein the personalization data includes at least an integrated circuit card (ICC) public key, an ICC private key, an ICC master key, and a master key identifier;

storing, in a first location of a secure element of a mobile device, the received personalization data;

receiving, by a receiving device, at least one post issuance script, wherein each of the at least one post issuance script is configured to store, in a second location of the secure element of the mobile device, mobile cloud account data, the mobile cloud account data including at least an issuer public key certificate, an ICC public key certificate, and a mobile cloud account number (MCA);

storing, in a database not included in the secure element, the received at least one post issuance script;

receiving, by an input device, an indication of an MCA included in a specific post issuance script of the received at least one post issuance script; and

executing, by a processing device, the specific post issuance script,

wherein the MCA is based on attributes of a real card account number (RCA).