METHODS AND SYSTEMS FOR PROVISIONING MOBILE DEVICES WITH PAYMENT CREDENTIALS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a non-provisional application of, and claims priority to U.S. Provisional App. No. 61/863,878, filed on August 8, 2013, titled "METHODS AND SYSTEMS FOR PROVISIONING MOBILE DEVICES WITH PAYMENT CREDENTIALS", and U.S. Provisional App. No. 61/898,428, filed on October 31, 2013, titled "METHODS AND SYSTEMS FOR PROVISIONING MOBILE DEVICES WITH PAYMENT CREDENTIALS", and U.S. Provisional App. No. 61/866,514, filed on August 15, 2013, titled "REMOTE MOBILE PAYMENT TRANSACTION WITH MOBILE APPLICATION USING SECURE ELEMENT", and U.S. Provisional App. No. 61/868,487, filed on August 21, 2013, titled "TRANSACTION ALERT SYSTEM INCORPORATING ENCRYPTION", and U.S. Provisional App. No. 61/978,172, filed on April 10, 2014, titled "TRANSACTION ALERT AND TRANSACTION HISTORY DELIVERY SYSTEM INCORPORATING ENCRYPTION", and U.S. Provisional App. No. 61/870,153, filed on August 26, 2013, titled "TRANSACTION LOG PAYMENT APPLICATION", the entire contents of which are herein incorporated by reference for all purposes.

FIELD

[0002] Aspects of the disclosure relate to computing technologies. In particular, aspects of the disclosure relate to device provisioning technologies, such as systems, methods, apparatuses, and computer-readable media for provisioning mobile devices with payment credentials.

BACKGROUND

[0003] With the continuing development and use of mobile technology, more and more features are being integrated into mobile devices. For example, global positioning system (GPS) applications, mobile office products, messaging systems, video cameras, and even compass functionalities have been incorporated into

mobile devices, which has led to their widespread adoption in both business and personal contexts.

[0004] To further utilize mobile technology to better cater to a user's daily needs, some attempts have been made to utilize technology enabled by mobile devices to replace conventional physical wallets. For example, one way to provide mobile wallet functionality has been realized by provisioning a card issuer's account information directly onto a secure element (SE) of a mobile device that may be equipped with Near Field Communication (NFC) chipset. A SE may be a smart card chip that is capable of storing multiple applications and/or account specific information that may not be easily accessed by external parties. NFC technology is commonly used for contactless short-range communications based on radio frequency identification (RFID) standards using magnetic field induction to enable communication between electronic devices. This short-range high frequency wireless communications technology allows devices to exchange data over a short distance (e.g., a few centimeters). Such mobile devices may thus use a mobile wallet application that, like a conventional physical wallet, may "contain" payment cards (e.g., credit cards, debit cards, prepaid cards), member cards, transportation cards, loyalty cards, etc.

[0005] To this end, user financial credentials (e.g., a Primary Account Number (PAN) of an account, an expiry date, etc.) may be provisioned onto mobile devices. Once these financial credentials have been provisioned onto the mobile device, an NFC-enabled device may transact with (e.g., transfer information, make payments to) another NFC-enabled device by placing the devices near each other. Additionally, mobile devices with provisioned accounts may also be used to perform transactions with other remote systems (e.g., such as a website of a merchant) using other wireless protocols, such as via a cellular or wireless (e.g., IEEE 802.11) network.

[0006] Although the benefits from integrating wallet functionality into mobile devices are significant and still being developed, the prevailing technology still lacks effective and safe processes and means to securely and efficiently provision financial credentials to user devices. Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0007] Typical payment credential provisioning processes require multiple messages between a third party wallet provider and a provisioning server. Additionally, unnecessary delay is often encountered while user accounts are authenticated during provisioning. Accordingly, there is a need to speed the process for provisioning payment accounts on mobile devices (e.g., on secure elements) and provide more efficient methods for provisioning large numbers of card instances on secure elements. Additionally, there is a need for enhanced authentication services during provisioning processes as some legitimate consumers may have questionable initial authentication results. Accordingly, there is a need for additional authentication processes that do not interrupt or delay the provisioning process.

[0008] Embodiments of the present invention are directed at optimizing the provisioning of payment account credentials to mobile devices utilizing mobile wallets. According to some embodiments, a provisioning scheme from multiple provisioning paths may be selectively chosen for payment account credential provisioning based upon a determined risk involved with a particular provisioning request.

[0009] In some embodiments, a low risk provisioning request may result in an immediate commencement of provisioning, whereas a high risk provisioning request may result in the provisioning request being denied. In some embodiments, those provisioning requests of medium risk will cause an additional user authentication to be completed before the payment account provisioning is finalized. In some embodiments, the additional user authentication includes communicating with the user via a separate communication channel than a channel in which the provisioning request was received. The communication may include sending the user a one-time password over the second communication channel, which may be a SMS message, email, or HTTP message sent by an issuer to the user.

[0010] In some embodiments, a medium risk request will cause payment account credentials to be provisioned to a mobile device in an inactive state that does not allow the payment credentials to be utilized, and upon completion of the authentication process, the provisioned inactive credentials may be activated for use.

[0011] According to an embodiment, a method performed by a service provider for provisioning account credentials includes receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device. The first payment credential is associated with a first account of a first user. A first risk level associated with the first provisioning request is determined. Responsive to the first risk level being within a predetermined risk threshold range, the method includes causing an authentication process to be performed with the first user. Responsive to a successful performance of the authentication process, the first payment credential is provisioned onto the first mobile device. The method further includes receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device. The second payment credential is associated with a second account of a second user. The method further includes determining a second risk level associated with the second provisioning request, and responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device. In an embodiment, a non-transitory computer readable medium stores instructions that when executed by a processor of a server cause the server to perform this method. In an embodiment, a server computer is described that includes a processor and the described non-transitory computer readable medium. In an embodiment, a payment account credential provisioning system is described that includes this server computer, and one or more of an issuer computer, a wallet provider server computer, and a mobile device.

[0012] Embodiments of the present invention are directed at optimizing secure element (“SE”) application provisioning on mobile devices with mobile wallets that have a consumer enrollment process. Some embodiments are directed at provisioning card data on a secure element by generating and delivering multiple possible personalization scripts for implementing multiple provisioning outcomes in one communication. Accordingly, an embodiment optimizes secure element application provisioning by providing all possible provisioning scripts to a wallet provider or other payment account manager before card data activation is completed, so that the eventual activation of a provisioned card account on a secure account requires less communication and/or computational resources at the time of

activation. Accordingly, card application data may be provisioned on a secure element of a mobile device while only requiring a single provisioning message from a provisioning system, which can minimize the number of messages between a mobile wallet server and a payment processing network service provider.

[0013] Thus, embodiments of the invention provide efficient provisioning processes that can selectively provide enhanced authentication of a user in a single, efficient process.

[0014] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. 1 illustrates a block diagram including entities in a payment transaction system.

[0016] FIG. 2 illustrates a block diagram including entities in an account provisioning system according to some embodiments of the present invention.

[0017] FIG. 3 illustrates a combined sequence and flow diagram depicting account provisioning, including low risk and high risk provisioning, in an account provisioning system according to some embodiments of the present invention.

[0018] FIG. 4 illustrates a combined sequence and flow diagram depicting medium risk account provisioning in an account provisioning system with respect to FIG. 2 according to some embodiments of the present invention.

[0019] FIG. 5 illustrates a flow in a server computer for account provisioning according to some embodiments of the present invention.

[0020] FIG. 6 illustrates a combined sequence and flow diagram depicting two dynamic verification value validation configurations in an account provisioning system according to some embodiments of the present invention.

[0021] FIG. 7 illustrates a combined sequence and flow diagram depicting consumer-specific encryption key provisioning and the secure message transmission through a wallet provider according to some embodiments of the present invention.

[0022] FIG. 8 illustrates a combined sequence and flow diagram depicting the use of unique transaction identifiers for transaction log updates according to some embodiments of the present invention.

[0023] FIG. 9 illustrates a high level block diagram of a computer system that may be used to implement any of the entities or components described herein.

DETAILED DESCRIPTION

[0024] Typical payment credential provisioning processes require multiple messages between a third party wallet provider and a provisioning gateway. Additionally, unnecessary delay is often encountered while user accounts are authenticated during provisioning. Accordingly, there is a need to speed the process for provisioning payment accounts on secure elements and providing more efficient methods of provisioning (potentially large numbers of) card instances on secure elements.

[0025] Additionally, there is a need for enhanced authentication services during provisioning processes as some legitimate consumers may have questionable initial authentication results. Accordingly, there is a need for additional authentication processes that do not interrupt or delay the provisioning process.

[0026] Embodiments of the present invention are directed at optimizing the provisioning of payment account credentials to mobile devices utilizing mobile wallets. According to some embodiments, a provisioning scheme from multiple provisioning paths may be selectively chosen for payment account credential provisioning based upon a determined risk involved with a particular provisioning request.

[0027] In some embodiments, a low risk provisioning request may result in an immediate commencement of provisioning, whereas a high risk provisioning request may result in the provisioning request being denied. In some embodiments, those provisioning requests of medium risk will cause an additional user authentication to be completed before the payment account provisioning is finalized. In some embodiments, a medium risk request will cause payment account credentials to be provisioned to a mobile device in an inactive state that does not allow the payment

credentials to be utilized, and upon completion of the authentication process, the provisioned inactive credentials may be activated for use.

[0028] Embodiments of the present invention are directed at optimizing secure element ("SE") application provisioning on mobile devices with mobile wallets that have a consumer enrollment process. Some embodiments are directed at provisioning card data on a secure element by generating and delivering multiple possible personalization scripts for implementing multiple provisioning outcomes in one communication. Accordingly, an embodiment optimizes secure element application provisioning by providing all possible provisioning scripts to a wallet provider or other payment account manager before card data activation is completed, so that the eventual activation of a provisioned card account on a secure account requires less communication and/or computational resources at the time of activation. Accordingly, card application data may be provisioned on a secure element of a mobile device while only requiring a single provisioning message from a provisioning system, which can minimize the number of messages between a mobile wallet server and a payment processing network service provider.

[0029] Thus, embodiments of the invention provide efficient provisioning processes that can selectively provide enhanced authentication of a user in a single, efficient process.

I. TERMINOLOGY

[0030] Prior to discussing embodiments of the invention, a description of some terminology is presented to assist with understanding this disclosure.

[0031] As used herein, the term "comprising" is not intended to be limiting, but may be a transitional term synonymous with "including," "containing," or "characterized by." The term "comprising" may thereby be inclusive or open-ended and does not exclude additional, non-recited elements or method steps when used in a claim. For instance, in describing a method, "comprising" indicates that the claim is open-ended and allows for additional steps. In describing a device, "comprising" may mean that a named element(s) may be essential for an embodiment, but other elements may be added and still form a construct within the scope of a claim. In contrast, the transitional phrase "consisting of" excludes any element, step, or

ingredient not specified in a claim. This is consistent with the use of the term throughout the specification.

[0032] In the following description and claims, the terms “coupled” and “connected,” may be used. The term “coupled” may be used to indicate that two or more elements, which may or may not be in direct physical or electrical contact with each other, co-operate or interact with each other. The term “connected” may be used to indicate the establishment of communication between two or more elements that are coupled with each other.

[0033] As used herein, a “mobile device” may comprise any electronic and/or communication device that may be transported and operated by a user, which may also provide remote communication capabilities with resources via one or more networks. Examples of mobile devices include mobile phones (e.g., cellular phones), personal digital assistants (PDAs), tablet computers, laptop computers (e.g., netbooks), personal music players, hand-held electronic reading devices, wearable computing devices, etc.

[0034] A “server computer” may be a powerful computer or combination of two or more computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit such as a cluster. In one example, the server computer may be a database server coupled to a web server. Server computers often execute server applications that act as a server in client-server interactions, including but not limited to database server applications, web server applications, application server applications, etc.

[0035] As used herein, a “communications channel” may refer to any suitable path for communication between two or more entities. Suitable communications channels may be present directly between two entities such as a payment processing network and a merchant or issuer computer, or may include a number of different entities. Any suitable communications protocols may be used for generating a communications channel. A communication channel may in some instance comprise a “secure communication channel,” which may be established in any known manner, including the use of mutual authentication and a session key and establishment of a Secure Sockets Layer (SSL) session. However, any method of creating a secure channel may be used. By establishing a secure channel, sensitive

information related to a payment device (such as account number, Card Verification Value (CVV) values, expiration dates, etc.) may be securely transmitted between the two entities to facilitate a transaction.

[0036] As used herein, a “risk score” may include an arbitrary designation or ranking that represents the risk associated that a transaction may be fraudulent. The risk score may be represented by a number (and any scale), a probability, or in any other relevant manner of conveying such information. The risk score may comprise an aggregation of information about a transaction, including transaction information, account information, and verification information as defined above. The risk score may be used by any authorizing entity (such as a merchant or an issuer) in determining whether to approve a transaction. The risk score may comprise and/or utilize both current transaction information and past transaction information, and may weight such information in any suitable manner.

[0037] As used herein, a “payment account” (which may be associated with one or more payment devices) may refer to any suitable payment account including a credit card account, a checking account, a prepaid account, etc.

[0038] As used herein, “identification information” may include any suitable information associated with an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (Primary Account Number or “account number”), user name, expiration date, CVV (Card Verification Value), dCVV (Dynamic Card Verification Value), CVV2 (Card Verification Value 2), CVC3 card verification values, etc.. CVV2 is generally understood to be a static verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors).

II. PAYMENT SYSTEMS

[0039] FIG. 1 illustrates a block diagram including entities in a payment transaction system 100. This depicted payment transaction system 100 includes a

user 107, a payment device 108, a mobile device 101, an access device 102, a merchant computer 103, an acquirer computer 104, a payment processing network 105, and an issuer computer 106.

[0040] The system 100 comprises a user 107 who may operate a mobile device 101. The user 107 may use mobile device 101 to conduct a financial transaction (e.g., a payment transaction) at an access device 102 connected to a merchant computer 103. The user 107 may also use a payment device 108 at the access device 102 to conduct the financial transaction. Merchant computer 103 may be connected to acquirer computer 104. Acquirer computer 104 may be connected to issuer computer 106 via payment processing network 105. Of course, some or all of these entities depicted as connected may be connected across one or more communication networks or may be directly connected.

[0041] As used herein, a “merchant” is typically an entity that engages in transactions and may sell goods and/or services. An “issuer” may typically refer to a business entity (e.g., a bank) that maintains financial accounts for users and may issue payment credentials to be stored on a mobile device 101 (e.g., a cellular telephone, smart card, tablet, laptop, etc.) of a user. An "acquirer" is typically a business entity (e.g., a bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions, and some embodiments may encompass such single entity issuer-acquirers. Each of the entities (e.g., merchant computer 103, acquirer computer 104, payment processing network 105, and issuer computer 106) may comprise one or more computer apparatuses to enable communications or to perform one or more of the functions described herein.

[0042] As used herein, a “payment device” 108 may refer to any device that may be used to conduct a financial transaction, such as to provide payment information to a merchant. A payment device may be in any suitable form. For example, suitable payment devices include, but are not limited to, smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, 2-D barcodes, an electronic or digital wallet, and the like. Such devices can operate in either a contact

or contactless mode. In some configurations, a payment device 108 directly interacts with an access device 102 (i.e., without the use of any other device and/or network), but in some configurations payment device 108 communicates with the access device 102 using an intermediary device and/or a communication network. Mobile device 101 is a mobile device (as described above) that may in some embodiments be thought of as a type of payment device (e.g., payment device 108). For example, a mobile device 101 may include, but is not limited to, cellular phones, laptops, tablets, wearable computing devices, etc., and may interact with an access device 102 (e.g., using NFC) and/or merchant computer 103 (e.g., via the Internet to access a website or utilize an application provided by merchant computer 103) to initiate and/or conduct a financial transaction.

[0043] The payment processing network 105 may include data processing subsystems, networks, and operations used to support and deliver certificate authority services, authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, digital wallet transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) that processes authorization requests and a Base II system that performs clearing and settlement services. In some embodiments, payment processing network 105 may conduct transactions in substantially real-time (e.g., in fewer than a few seconds or fractions of a second). The payment processing network 105 may include one or more server computers (as described above). The payment processing network 105 may use any suitable wired or wireless network, including the Internet.

[0044] In an exemplary purchase transaction, the user 107 purchases a good or service at from a merchant using a mobile device 101 (e.g., a mobile phone). The user's mobile device 101 can interact with an access device 102 at a merchant associated with merchant computer 103. For example, the user 107 may tap the mobile device 101 against an NFC reader in the access device 102. Alternatively, the user 107 may indicate payment details to the merchant electronically, such using a digital wallet or in through an online transaction. In some purchase transactions the mobile device 101 may not utilize an access device 102, and may directly interact

with a merchant computer 103 (e.g., a computing system providing a merchant website or “backend” services for a merchant application 208A executing on the mobile device 101). In these examples, the merchant computer 103 may be thought of as implementing a virtual access device.

[0045] To cause the financial transaction to be performed, an authorization request message is generated by the access device 102 (or virtual access device, which may be at merchant computer 103) and is forwarded to the acquirer computer 104. The acquirer computer 104 is a system of an acquirer (as discussed above) providing an account of the merchant, which will ultimately receive the funds for the transaction from an issuer providing the user’s 107 account. Such an “authorization request message” may be an electronic message that is sent to a payment processing network 105 and/or an issuer of a payment card (e.g., issuer computer 106) to request authorization for a transaction. An authorization request message, according to some embodiments, may comply with a message type defined by the International Organization for Standardization (ISO) 8583 standard, which is a standard for systems that exchange electronic transaction information associated with payments made by users using a payment device 108 (which could be a mobile device 101) or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to “identification information” including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc. An authorization request message may also include “transaction information,” such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction. The authorization request message may also include other information, such as an identifier of the access device 102 that generated the authorization request message, information about the location of the access device 102, etc.

[0046] Typically, an authorization request message will include a field for a primary account number (PAN) associated with an account of the user 107 that was provided by the mobile device 101 (or payment device 108). After receiving the

authorization request message, the acquirer computer 104 will send the authorization request message to the payment processing network 105. The payment processing network 105 then forwards the authorization request message to an issuer computer 106 associated with the issuer of the user's account. The PAN included in the authorization request message may be used by the payment processing network 105 to identify the appropriate issuer computer 106 for the purpose routing or processing (e.g., determining a risk of the authorization request, which may be based upon known rules of the involved issuer) the message.

[0047] After the issuer computer 106 receives the authorization request message, the issuer computer 106 sends an authorization response message back to the payment processing network 105 to indicate whether or not the current transaction is authorized. An "authorization response message" may be an electronic message reply to an authorization request message generated by an issuing financial institution or a payment processing network, and may comply with the ISO 8583 standard. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that an issuer returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device 102 (e.g. POS equipment) that indicates an approval of a transaction, and may serve as proof of authorization.

[0048] The payment processing network 105 receives the authorization response message from the issuer computer 106 and transmits the authorization response message back to the acquirer computer 104. The acquirer computer 104 then sends the authorization response message back to the merchant computer 103, where the merchant can determine whether to proceed with the transaction. In some embodiments, such as when a fraud rule is triggered at payment processing network 105, payment processing network 105 may decline a transaction previously authorized by issuer computer 106. After the merchant computer 103 receives the authorization response message, the access device 102 may then provide an authorization response message for the user 107. The response message may be

displayed by a display device (e.g., a display device that is part of or coupled to the access device 102), printed out on a receipt, communicated to the user's mobile device 101, etc. Alternately, if the transaction is an online transaction (e.g., via a website or application), the merchant computer 103 may provide a web page, display module, or other indication of the authorization response message to the mobile device 101.

[0049] At the end of the day, a normal clearing and settlement process can be conducted by the payment processing network 105. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a user's payment account and reconciliation of the user's settlement position. However, it should be noted that embodiments of the invention are not limited to a single settlement process.

III. SYSTEM FOR PROVISIONING CARD CREDENTIALS USING PRE-GENERATED SCRIPTS

[0050] In some scenarios, a user 107 with a mobile device 101 may desire to have the mobile device 101 be "provisioned" with payment credentials (e.g., payment credentials 207) to be used with merchants (e.g., with merchant computer 103, typically via an application 208 such as a merchant application 208A, web browser 208B, third-party application, etc.) or for other transactions. The payment credentials 207 may be for an account maintained by an issuer 240. Thus, in some embodiments, mobile device 107 may need to be first provisioned with personalization data, such as payment information and information regarding a user 107. FIG. 2 shows an example of a system 200 that may be used to conduct device provisioning according to some embodiments of the invention. System 200 comprises mobile device 107, an application provider 209 (e.g., a wallet provider 210) server computer 211, a service provider 230 (e.g., a payment processing network 105) server computer 212, and an issuer 240 server computer 106. Each of mobile device 101 and server computers 211, 212, and 106 may be implemented using one or more computing devices. In some embodiments, the mobile device 101 includes a secure element 202, which may be where the payment credentials 207 are provisioned to, and may optionally also include a secure payment application

206 and/or a transaction log 204 (both of which may exist at mobile device 101 outside of secure element 202).

[0051] Application provider 209 server computer 211 may be a server computer or another computing device operated by or on behalf of an application provider 209. An application provider 209 may be any entity that provides an application (e.g., an application 208) to a user 107. One example of an application provider 209 may be a digital wallet provider 210 (e.g., Visa Checkout™ or Google™ Wallet). The digital wallet provider 210 may maintain digital wallets for users, each digital wallet comprising payment data for one or more payment accounts. An application provider 209 may be associated with an application installed on mobile device 101. For example, a Visa Checkout application on mobile device 101 may be configured to connect to an application provider 209 server computer 211 operated by Visa.

[0052] Service provider 230 server computer 212 may be a server computer or another computing device operated by or on behalf of a service provider 230. A service provider 230 may be any entity that provides provisioning or personalization services. For example, a service provider 230 computer may maintain a personalization database (not illustrated herein) with information about users, and may be configured to communicate with one or more issuers 240 to determine personalized payment data for users 107. The service provider 230 server computer 212, via its provisioning service module 225, may provide “provisioning as a service” to one or more application provider 209 server computers 211, wherein the application provider 209 server computer 211 utilizes an application programming interface (API) to communicate with the service provider 230 server computer 212.

[0053] The service provider 230 – such as a payment processing network 105 – may, as part of its server computer(s) 212, provides a provisioning service module 225 and/or a device provisioning consumer authentication system (DPCAS) 214. The DPCAS 214 may operate as an authentication server that provides authentication services, and may include an access control server 216 (e.g., to determine whether an account is eligible for or participates in particular services) and/or a directory server 218 (e.g., that identifies, for an account, the associated issuer 240 and/or ACS 216). In some embodiments, DPCAS 214 may verify user 107 authentication information, such as user-identifying information, one-time

passwords, challenge-response information, etc. In other embodiments, parts or all of DPCAS 214 may be associated with (or provided by) an issuer 240 or another entity. For example, in some embodiments, ACS 216 may be provided by issuer 240. In some embodiments, DPCAS 214 is simply configured to determine an appropriate authentication system to be used for authentication, which may be implemented by the service provider 230, an issuer, a wallet provider, or another third party.

[0054] Additionally, the service provider 230 may provide additional services, including but not limited to an alert service 220 (e.g., via one or more processes executing at/by server computer 212) that can generate and provide alerts to a user 107 based upon transactions occurring with the user's 107 account. For example, alert service 220 may analyze one or more transactions of an account of user 107 using a set of one or more alert rules that may be configured by the user 107, and if any of the rules have conditions that are met (i.e., one or more rules are "triggered"), the alert service 220 may provide an alert message to the user 107 indicating and/or describing the triggering of the rules. As one example, a user 107 may configure a rule to be triggered (and thus, an alert message to be provided) when any transactions occur on their account having a value exceeding a defined threshold value. The service provider 230 may also provide a token service 222 that can generate and/or store a "token" (e.g., a first data value) that is associated with another, potentially sensitive second data value. For example, token service 222, may generate a token value for a Primary Account Number (PAN) of an account, and provide the token value while keeping a stored association (or mapping) between the token value and the PAN, such that only the token service 222 (or a limited set of entities) is able to "translate" the token value back to the actual PAN, providing enhanced security. Additionally, server computer 212 – such as when it is operated by a payment processing network 105, may maintain/store a transaction log 224 of financial transactions that it processes.

[0055] In some embodiments, issuer computer 106 may provide to service provider 230 server computer 212 personal information regarding users 107 associated with issuer computer 106. For example, issuer computer 106 may provide payment information, user information, account information, etc. In some embodiments, service provider 230 server computer 212 may provide to issuer computer 106 data relating to the provisioning process. For example, if during a

provisioning process a payment token was generated for a user's 107 account (e.g., by token service 222), this payment token may be provided to the account's issuer 240 by service provider 230 server computer 212.

[0056] Thus, in one use case of system 200, a user 107 may operate mobile device 101 to initiate a request for provisioning of a mobile application (e.g., a digital wallet application, which can be payment application 208C and/or secure payment application 206). The request for provisioning may be sent to application provider 209 server computer 211. Application provider 209 server computer 211 may forward the request to service provider 230 server computer 212, and in particular, to provisioning service module 225. The provisioning service module 225 may generate provisioning scripts (e.g., one or more of a partial personalization script, an activation script, a deletion script, etc.) using personalization data determined from issuer computer 106 and/or one or more databases, and transmit these scripts to application provider 209 server computer 211. Application provider 209 server computer 211 may then initiate execution one or more of the scripts at mobile device 101. For example, application provider 209 server computer 211 may cause a partial personalization script to be executed by mobile device 101. At a same or different time, service provider 230 server computer 212 (e.g., provisioning service module 225) may authenticate the user, perhaps using its DPCAS 214. Once the partial provisioning script has been executed and the user 107 has been authenticated, provisioning service module 225 may instruct application provider 209 server computer 211 to cause an activation script to be executed on mobile device 101 to complete a provisioning, thereby completely an "installation" of a set of payment credentials 207 onto the mobile device 101 for use.

[0057] In various embodiments, the authentication processes are selectively utilized to avoid their use when additional authentication is not necessary but to efficiently incorporate them when additional authentication is helpful.

[0058] It should be noted that any of server computers 211, 212, and/or 106 may be operated by or otherwise associated with a same or different entity. For example, in one embodiment, server computer 212 may be operated by payment processing network 105, and in some embodiments, the DPCAS 214 may be operated by a third-party entity not illustrated herein or by issuer 240, for example.

A. PAYMENT CREDENTIAL PROVISIONING

[0059] To assist in understanding the depicted entities of FIG. 2, an exemplary flow for provisioning payment account credentials 207 according to some embodiments is described. A user 107 may send a request for provisioning by use of a mobile application 208 running on mobile device 101. For example, in a payment application 208C (e.g., digital wallet application), the user 107 may request provisioning of an account, credit card, or any other payment credentials for mobile device 101. The request for provisioning message may include device information such as a mobile device 101 identifier, secure element 202 identifier, a secure element key identifier (or key), a user identifier (to identify a user or account), and user authentication information (e.g., a cryptogram such as a CVV2 for card verification based authentication processes, a ZIP code for geographic verification, etc.). The application provider 209 server computer 211 receives the request for provisioning message, and may perform a risk check or risk analysis for the requesting user 107, account, mobile device 101, or any other data that is present in the received request for provisioning message, or is tied to a user's account associated with the request for provisioning message. For example, the risk check may involve determining how many times the user's account has been provisioned and how many accounts are provisioned on mobile device 101. The risk check may, for example, indicate the likelihood that the request for provisioning is fraudulent. if the risk check indicates that the risk of provisioning is acceptable, then application provider 209 server computer 211 may send the request for provisioning to provisioning service module 225 executing at service provider 230 server computer 212. The request for provisioning message may include any of the information included in the message received from mobile device 101, and may include additional information determined by application provider 209 server computer 211, such as a primary account number (PAN) associated with the user's account and a reference number associated with the request for provisioning.

[0060] The provisioning service module 225 may then attempt to verify the provided user authentication information. For example, if the request for provisioning included a PAN and a cryptogram, provisioning service module 225 may retrieve a master encryption key, use the master encryption key to decrypt the cryptogram, and ensure that the decrypted value is an expected value (e.g., corresponding to

received value of the PAN). The provisioning service module 225 may then generate a payment token to provision onto the mobile device using token service 222. The payment token represents a PAN or other account number to be provisioned on the mobile device, and may comprise the actual PAN provided in the provisioning request, a generated token, the PAN together with a PAN sequence number, or another item of payment information to identify the account when used through the mobile payment application 208C. The payment token may be included in the personalization data later stored onto the mobile device 101.

[0061] The provisioning service module 225 may then generate a partial personalization script, an activation script, and a deletion script, and send these "provisioning scripts" to application provider 209 server computer 211 in a provisioning script message. The partial personalization script (or "perso" script) may be operable to store personalization data onto mobile device 101, the activation script may be operable to activate or enable access to the personalization data, and the deletion script may be operable to delete or otherwise remove the personalization data from mobile device 101. The provisioning script message may also include device information (which may allow application provider 209 server computer 211 to identify which mobile device 101 is associated with the provisioning scripts), a reference identifier (for a similar purpose), and card art (which may be provided to mobile device 101 as a graphical representation of the account to be provisioned). In some embodiments, the provisioning scripts may be encrypted such that only mobile device 101 or the secure element 202 of mobile device 101 may decrypt the scripts. For example, the original request for provisioning sent by the mobile device 101 may include a public key (or a shared key) of the secure element 202 that allows other entities to use this public key to encrypt messages that can in turn only be decrypted by the secure element 202 using a corresponding private key.

[0062] When the provisioning script message is received by application provider 209 server computer 211, it may initiate execution of the partial personalization script on mobile device 101. The execution may be initiated by, for example, sending a partial personalization script message to mobile device 101 that comprises the partial personalization script and instructions (i.e., a command) to execute the script. Once received, a mobile application 208, secure element 202, or another suitable

element in mobile device 101 may cause its processor to execute the partial personalization script.

[0063] The mobile device 101 may then send, to application provider 209 server computer 211, a partial personalization confirmation message indicating whether the partial personalization script was successfully installed, which may be forwarded to the provisioning service module 225 of the service provider 230 server computer 212.

[0064] At an earlier or later point in time, the provisioning service module 225 may utilize the DPCAS 214 to authenticate the user 107. For example, provisioning service module 225 may send an authentication request message to DPCAS 214. The authentication request message may include user authentication information provided by mobile device 101 or application provider 209 server computer 211, such as a PAN, and may also include a reference identifier and device information. The DPCAS 214 may then conduct a further risk assessment and authentication process and determine whether the user is authenticated and authorized to provision mobile device 101, which may include performing detailed checks such as whether the user's 107 account was previously flagged as compromised or an analysis of past transactions (e.g., using transaction log 224). Thus, DPCAS 214 may determine that the user 107 is authenticated, not authenticated, or may seek additional information from the user 107. For example, DPCAS 214 may cause an authentication request message to be sent to mobile device 101 requesting additional user authentication data, and then receive an authentication response message in return. Some examples of additional user authentication information may include answers to a challenge question, security question, a one-time password, etc. Eventually, the DPCAS 214 may provide an authentication response message back to the provisioning service module 225 to indicate a result of the authentication.

[0065] When provisioning service module 225, for example, has determined that it has received a partial personalization confirmation message and that it has made an authentication decision, the provisioning service module 225 may send an activation message or a deletion message to application provider 209 server computer 211. For example, provisioning service module 225 may send an activation message if the partial personalization confirmation message indicated a successful

execution of the script and the authentication result indicates a successful authentication of the user. Similarly, provisioning service module 225 may send a deletion message if either the partial personalization confirmation message or authentication result indicates a failure. The application provider 209 server computer 211, then, may initiate the execution of the activation script or the deletion script by the mobile device 101, depending on whether an activation message or deletion message was received, respectively. The initiation of the execution of the activation script / deletion script may be performed in a similar manner to initiation of the partial personalization script, as described above.

[0066] Upon the execution of the script, the mobile device 101 may then send a provisioning confirmation message to application provider 209 server computer 211 indicating whether the activation or deletion was successfully performed, and this message may be returned to the provisioning service module 225. With a successful verification that the account has been provisioned and activated on the device, service provider 230 server computer 212 may fully activate the account provisioned on the account by informing issuer computer 106 of the activation. For example, if a payment token was previously generated for the payment account, provisioning service module 225 may send a token linkage message comprising the payment token and the account PAN to issuer computer 106 instructing that the token and PAN to be linked.

IV. DIFFERENTIATED RISK-BASED AUTHENTICATION FOR CREDENTIAL PROVISIONING

[0067] As described earlier, typical account credential provisioning processes require multiple messages between a wallet provider 210 and a provisioning service module 225 (or service provider 230 server computer 212). Additionally, unnecessary delay is often encountered while user accounts are authenticated during provisioning, and thus there is a need to speed the process for provisioning payment accounts on mobile devices (e.g., using secure elements) and providing more efficient ways to provision large numbers of payment accounts on large numbers of mobile devices 101. Additionally, there is a need for enhanced authentication services during provisioning processes, as some legitimate consumers may have questionable initial authentication results, or may not be able

to easily use typical authentication schemes. Accordingly, there is a need for additional authentication processes that do not interrupt or delay the provisioning process.

[0068] Embodiments of the invention address these problems, individually and collectively, through in part the use of differentiated risk-based provisioning. FIG. 3 illustrates a combined sequence and flow diagram 300 depicting account provisioning, including low risk and high risk provisioning, in an account provisioning system according to some embodiments of the present invention. As used herein, the terms “account provisioning”, “payment account provisioning”, “card provisioning”, “credential provisioning” and the like may be used interchangeably to refer to the process of putting (or “installing”) information associated with the user 107 and/or user account onto a mobile device 101 such that the mobile device 101 can utilize the account for performing a financial transaction, except where it is made clear from the usage of the term and/or its surrounding context that a difference is being referenced.

[0069] The depicted sequence and flow diagram 300 depicts messages sent between and actions performed by a set of entities. The set of entities includes a mobile device 101, wallet provider 210, service provider 230, and issuer 240. In some embodiments, one or more computing devices (e.g., server computers) implement each of entities 210, 230, and 240. Thus, the actions and messages presented herein are described with reference to higher-level entities to provide ease of understanding. Additionally, in some embodiments more entities are involved in performing this set of actions, and in some embodiments fewer entities are utilized to perform this set of actions. Accordingly, this representation is merely illustrative of one possible embodiment and is not intended to be exhaustive or limiting.

[0070] The depicted process begins when initially user 107 logs into an electronic wallet application (e.g., payment application 208C and/or secure payment application 206) on their mobile device 101 at block 302 to initially request a provisioning of an account, credit card, or any other payment credentials for the mobile device 101.

[0071] However, in some embodiments, payment credentials 207 may be installed before the user even tries to activate, use, or otherwise provision the cards to the mobile device. Thus, the process described below may occur automatically

without the user knowing. At some point, the user may request that the card credentials be provisioned on the mobile application, and at that time, no further data may need to be sent to the mobile device and the provisioned account may be nearly immediately accessible by the user. Accordingly, embodiments may complete a provisioning process for card credentials before a consumer even requests provisioning of a card instance on a mobile device. For example, a user 107 may download a mobile wallet application on their mobile device 101 and may enter their user name, identifier, cards registered, etc. At that time, the wallet provider 210 may initiate this described process for all of the cards registered with the mobile wallet. Accordingly, embodiments may apply provisioning scripts to user devices before a user even asks to provision a specific card.

[0072] However, upon the user 107 providing the wallet credentials to the mobile device 101 at block 302, the mobile device 101 (e.g., at the request of a mobile payment application) transmits the credentials 350 to the wallet provider 210. In the depicted embodiment, upon affirming that the credentials 350 are correct and for a valid account, will transmit a check account message 352 (e.g., make an API call for a card eligibility request) for one or more accounts of the user 107 to the service provider 230. In some embodiments, this check account message 352 includes one or more PANs of accounts of the user (or other types of account identifiers), which may have been provided by the user 107 (e.g., to the wallet provider) at an earlier time, or may have been provided by the user 107 along with the credentials (i.e., at block 302) and sent with the wallet credentials message 350.

[0073] The service provider 230, for the PAN (or for one or more of the one or more PANs provided in, identified by, or otherwise associated with the check account message 352) verifies the eligibility of the associated account for which credentials are to be provisioned. In some embodiments, the service provider 230 verifies the eligibility at block 304, but in some embodiments the service provider 230 transmits an account eligibility request message 354 to the issuer 240, and the issuer 240 will then verify the eligibility at block 306 and return an account eligibility response message 356 indicating the eligibility of the account(s). In some embodiments, the account eligibility request message 354 may include a risk value indicating a risk associated with the request, as generated by the service provider

230 or wallet provider 210, which allows the issuer 240 an additional factor to consider when verifying an eligibility of the request.

[0074] For example, for a particular PAN, block 304 may include identifying the issuer 240 of the account (e.g., based upon a bank identification number (BIN) of the PAN, for example) and then determining whether that issuer 240 allows for this provisioning to occur. Block 304 may also include utilizing a database of eligible and/or ineligible accounts (e.g., existing in an exception file listing those accounts that have been lost, stolen, or blocked), which may be provided by the issuer 240. In some embodiments, this verification in block 304 may include performing a check digit calculation using the PAN based upon the issuer check digit scheme, determining whether the account has already been provisioned to a device (a same or different device), etc. Similarly, issuer 240 may verify the eligibility of the account at block 306 according to a variety of ways left to configuration preference, such as allowing all accounts to have credentials be provisioned, allowing no accounts to have credentials be provisioned, or allowing only some accounts have credentials be provisioned – which may be based upon an account history, a history of the user's other accounts at the issuer 240, whether the account has previously been provisioned, etc.

[0075] At some point, whether via block 304 or block 306, the service provider 230 will have determined the eligibility of the account(s), and will transmit an account eligibility response message 358 (e.g., send an API response message) to the wallet provider 210 identifying one or more accounts and indicating, for these accounts, whether the respective account is eligible for credential provisioning.

[0076] At block 308, if an account is not eligible, the wallet provider 210 may transmit an ineligibility message 360 to the mobile device 101, which may cause a message to be presented to the user 107 (e.g., via a display device) to indicate that the account is ineligible. Then, at block 310, the flow ends, and the user 107 may optionally attempt to begin the flow again for a different account.

[0077] If, at block 308, an account is eligible, the flow continues with the wallet provider 210 sending an enable payments query message 362 indicating that the account is eligible, and the user 107 and/or wallet application may, in response, cause another enable payments query response message 362 to be sent back to the

wallet provider 210 to indicate that the user 107 does seek to “enable” the provisioning of the payment credential 207 associated with the account to the mobile device 101 (i.e., “add” their account to the mobile device 101). The enable payments query message 362 may cause the mobile device 101 to also present a set of terms and conditions to the user during this service activation phase, which the user must accept to continue.

[0078] The wallet provider 210 then transmits a CVV2 prompt message 264 to the mobile device 101 seeking the entry of further card information (e.g., a CVV2 or CVV value of a credit card, for example) of the account, which may cause the mobile device 101 to prompt the user 107 for this information. Upon receipt of this card information (e.g., a CVV2 value) from the user 107 at block 312, the mobile device 101 transmits a provision request message 366, which may include the provided card information value (e.g., CVV2 value).

[0079] The provisioning request message 366, in some embodiments, includes device information (to identify the mobile device 101 and secure element 202, and may include any unique identifier for the device to identify the secure element keys necessary), consumer identifier or login information/credentials (to identify the user 107), account credentials (e.g., a PAN and/or a card verification value (e.g., CVV2 for card verification based authentication processes)), and/or a zip code (for geographic based authentication processes). The provisioning request message 366 is sent by the mobile device 101 to wallet provider 210, which may generate a risk score (or perform a “risk check” or “risk analysis” to generate risk assessment data) at block 313 based upon the provisioning request message 366. This risk analysis may occur based upon the requesting user 107, account, card, mobile device 101, or any other data that is present in the provisioning request message 366 (e.g., a CVV2 value, ZIP Code, User Identifier, etc.) or is tied to the account of the user 107 submitting the provisioning request (e.g., previously registered/provisioned card data, determining how long the account has been open, how many cards the consumer uses in total or has used, a number of purchases in the past, etc.).

[0080] Assuming that the determined risk is not too high, the wallet provider 210 sends a provisioning request 368 to service provider 230 (e.g., provisioning service module 225). The provisioning request may include device information, a primary

account number (PAN) associated with the account attempting to be provisioned, an expiration date, a user-entered CVV2 value, a ZIP code, a time-sensitive token (i.e., that can expire if a period of time passes) returned with the account eligibility response message 358, or any other information that may be associated with a user account, and a reference identifier for the provisioning request.

[0081] In some embodiments, the provisioning request 352 may include a reference identifier (ID) of the PAN (or token)but not the PAN itself. This reference ID, in some embodiments, is preconfigured (or otherwise agreed upon) by both the wallet provider 210 and the service provider 230 so that both are aware of the mapping (or can otherwise translate) between the reference identifier and the PAN.

[0082] In some embodiments, the risk of the request is determined (or "assigned") by the service provider 230 at block 314 (e.g., based upon rules and/or data provided by the issuer 240 at an earlier time) to yield a token activation response 372A. However, in some embodiments the service provider 230 identifies the issuer 240 of the account (e.g., based upon the PAN), transmits a token activation request message 370 (which may include a risk value indicating the service provider assigned risk 314 and/or a risk value generated by the wallet provider 210) to the issuer 240 such that the issuer 240, at block 316, will determine/assign its own risk and return a token activation response message 372B back to the service provider 230.

[0083] Similar to the verification of account eligibility described above with respect to blocks 304/306, the assignment of risk at block(s) 314/316 may be performed according to preferences of the implementing entities, and thus can be based upon a variety of factors including, but not limited to, whether the provided CVV2 value exists and is verified as correct, whether an earlier-provided token was included in the provisioning request 352, whether the requested account is already provisioned on the mobile device 101 or another device, if a provided address can be verified as correct, account configuration data provided earlier by the user 107, wallet provider data (e.g., a risk value), device information such as its available hardware or software capabilities, fingerprint or other identifier, etc.

[0084] In some embodiments, the service provider 230, after sending the token activation request message 370, may be configured to only wait for the

corresponding token activation response message 372B for a period of time. In some of these embodiments, if the period of time expires, the service provider 230 may use its own generated risk assignment 314 outcome (i.e., a token activation response 372A) to continue the flow, and may optionally (not illustrated) transmit another message to the issuer 240 to identify what risk assignment 314 outcome it assigned and/or how the service provider 230 chose to proceed. This embodiment allows the process to continue proceeding an efficient, highly-responsive manner to avoid keeping the user 107 waiting.

[0085] Regardless of the exact risk assignment formulation of blocks 314/316, the token activation response message 372A/372B may indicate a level of risk. In some embodiments, at least three levels of risk may be generated, including a “low” risk where the provisioning request is unconditionally approved, a “medium” risk where the provisioning request is conditionally approved, and a “high” risk where the provisioning request is declined. The depicted flow varies based upon which of these levels of risk were generated.

[0086] At block 318, the service provider 230 determines which level of risk was determined. As depicted, block 318 indicates identifying whether the level of risk was “High,” “Medium,” or “Low.” Of course, although in some embodiments the levels of risk may be explicitly categorical (and thus uniquely identify which risk category is determined), in other embodiments the levels of risk may be in other formats (e.g., a risk score is generated that is an integer between 0 and 100, for example, and thus the determination of the risk category may include determining if the risk score is within a range of values, meets or exceeds a value, is below a value, etc.).

[0087] FIG. 3 depicts how flow continues for the “high” and “low” risk levels, and FIG. 4 illustrates how flow continues for “medium” risk levels, as indicated by the line leading to the bottom of the page and labeled “TO FIG. 4” next to circle ‘A’.

[0088] If, at block 318, the risk level is identified as “high,” the service provider 230 may transmit a provision request denial message 374 indicating that the provision request message 368 is denied. In response, the wallet provider 210 may transmit a denial message 376 to the mobile device 101, which presents a message to the user 107 indicating the denial and/or instructing the user 107 to contact the

issuer of the account (e.g., to ask the issuer to enable the account for account provisioning). At this point, the “high risk” flow ends at block 320.

[0089] If, at block 318, the risk level is identified as “low,” the service provider 230 may acquire a token 322. In an embodiment, this token acquisition 322 includes the provisioning service module 225 requesting, from token service module 222 (which may be a part of server computer 212 – as illustrated – or part of another device), a token for a PAN by sending the PAN to the token service module 222. The token service module 222 may then, using a variety of transformation techniques, generate and return a token, and may store a mapping between the token and the PAN for future translations. For example, in an embodiment, the token may be created with a same size as the PAN (e.g., having a same number of digits), have a same BIN value (or another BIN value within a range of associated BIN values) as the PAN, etc. The token service module 222 (and/or the provisioning service module 225) may store a sequence number (e.g., 0 for a first time token creation for the PAN) of the token, an expiration date of the token (e.g., to be 24 or 36 months from the request date, for example), and set the token to be an “active” token at block 324, perhaps by setting a value within its records, or perhaps may modifying the token value itself.

[0090] At block 326, the provisioning service module 225 prepares and sends a message 376 to the wallet provider 210 including the token (received from the token service module 222) along with a set of one or more provisioning scripts. In some embodiments, the this message 376 includes one or more of the token (which may be encrypted), a token expiration date, a portion of the associated PAN (e.g., the last four digits), a portion of the token itself (e.g., the last four unencrypted digits), the associated card metadata, a token reference identifier, a PAN reference identifier, a token to be returned with further messages, and/or the personalization scripts. Then, the wallet provider 210 may forward, in another message 378 back to the mobile device 101, some or all of the information from message 376 (e.g., the provisioning scripts and the token, for example) to cause the token for the account to be provisioned onto the mobile device 101 (by executing the scripts at block 328). In some embodiments, the set of provisioning scripts includes a partial personalization script and an activation script, although in some embodiments the functionality provided by the partial personalization script and the activation script is consolidated into one (or more) scripts.

[0091] At block 379, the service provider 230 may transmit a token notification message 379 to the issuer 240 that includes some or all of the information from the message 376, including but not limited to the token, token expiration, a portion or all of the PAN, etc., which serves to notify the issuer 240 of the generated token.

[0092] Upon execution of the provisioning scripts received by the mobile device 101 in message 378, the mobile device 101 may return a token activation results message 380 to the wallet provider to confirm and/or deny whether the token (i.e., payment credential 207) was successfully provisioned (i.e., installed). This message 380 may be forwarded on by the wallet provider 210 to the service provider 230 in token activation results message 381, which may further forward the message on as message 382 to the issuer 240. At block 324, the “low” risk flow ends.

[0093] Going back to block 318, if the assigned risk value is deemed to be “medium” risk, flow continues to the bottom of the figure and leads to FIG. 4. FIG. 4 illustrates a combined sequence and flow diagram 400 depicting medium risk account provisioning in an account provisioning system with respect to FIG. 2 according to some embodiments of the present invention.

[0094] Circle ‘A’ indicates a beginning to the “medium” risk flow, and the service provider 230 acquires a token at block 402 in a similar manner to the token acquisition described above with respect to block 322 in the “low” risk flow. Accordingly, the service provider 230 may generate a token, retrieve a stored token, or ask another entity for a token (e.g., a third party token provider service). At block 404, the token is set to inactive, which may include modifying the token (e.g., encrypting it), and/or modifying a provisioning script to cause the token to be placed as inactive (i.e., unavailable for payment use by the mobile device 101 for the present time), such as by setting a flag within a memory location of the mobile device 101 (e.g., setting a protection flag within a memory of a secure element 202), etc. At block 406, the service provider 230 prepares one or more provisioning scripts, which in some embodiments includes personalization scripts but not activation scripts.

[0095] The provisioning scripts and the inactive token are sent in a message 450 to the wallet provider 210. The message 450 may include some or all of the items as described with respect to message 376 in the “low” risk flow of FIG. 3, and in particular, may include an indicator that the token is inactive and/or that the wallet

provider 210 is to acquire a dynamic verification value delivery choice from the user 107 (described later herein). The provisioning scripts and the inactive token are then forwarded on by wallet provider 210 in a message to the mobile device 101, where the scripts are executed at block 407 to cause the inactive token to be installed. Similar to message 379, the service provider 230 may transmit a token notification message 453 to the issuer 240 to inform the issuer 240 of the generated token and its mapping to the PAN.

[0096] In some embodiments, the mobile device 101 transmits (not illustrated) a message to the wallet provider 210 to indicate whether the installation of the inactive token was a success, and in response, the wallet provider 210 will transmit a device provisioning results message 454 back to service provider 230, which in turn may forward the device provisioning results message 454 as message 456 back to the issuer 240.

[0097] At this point, the wallet provider 210, based upon the indicator that the token is inactive and/or that the wallet provider 210 is to acquire a dynamic verification value delivery choice from the user 107 (from message 450), will send a query message 458 to seek the user's selection as to a preferred way for the user to receive a dynamic verification value (DVV). In some embodiments, this DVV serves as an element of an additional (or "stepped-up") user verification procedure that can be used to increase the confidence that an ultimate provisioning of a credential is proper and thus, is much less likely to be fraudulent. In these examples, a DVV that is a one-time password is discussed; however, many other verification methods may be employed, including but not limited to performing a challenge/response test with the user via mobile device 101 (e.g., based upon information the legitimate user previously provided or is likely to know), having the user call a telephone number (of a customer service center of the issuer, as one example) to pass a set of challenge/response tests, having the user click on a link within an email sent to an email address on file for the user, having the user submit a voice sample or other biometric sample (e.g., fingerprint impression, iris scan, facial image, etc.) for recognition, or another known authentication technique.

[0098] As an example, a set of delivery options for the DVV may be presented to the user, including but not limited to receipt through the mobile payment application,

receipt of a text message (e.g., Short Message Service (SMS) or other similar messaging service message), placing or receiving a telephone call to acquire the DVV (e.g., to a call center), receipt of the DVV within an email sent to an email address on file for the user, etc. The user 107 may select one of these options and thus the mobile device 101 will receipt the user's selected DVV delivery choice at block 408, and transmit a message 460 including the selected delivery choice to the wallet provider 210, which will forward the delivery choice on in another message 462 (e.g., in a "send OTP" message) to the service provider 230. Further, some or all of the delivery options may include obfuscated information, such as a partially hidden/obscured telephone number (alongside one or more erroneous telephone numbers) or email address, for example.

[0099] The service provider 230, in some embodiments, will verify the message 462 by performing one or more of verifying whether a token reference ID passed in the request is valid, whether a token-to-PAN mapping is known to exist, whether that token has previously been provisioned, whether the token is currently in an inactive state, whether a maximum number of OTP code attempts (as allowed by the issuer) has been met or exceeded, etc.

[0100] At this point, several configurations exist for generating and/or validating an entry of a DVV. A first DVV variant 420 is illustrated here in FIG. 4, although two other variations are presented later herein in FIG. 6. However, in the first DVV variant 420, the service provider 230 will generate a DVV at block 410, which may include generating a length of random characters/numbers/values. For example, in an embodiment a DVV is a randomly generated four digit number. The generation at block 410 may further include setting an expiration date/time for the generated DVV, and/or setting a "retry count" indicating how many times the user may attempt to provide the DVV, both of which may be sent and/or stored.

[0101] In this first variant 420, the service provider 230 transmits a consumer authentication request message 464 (including the user-selected DVV delivery choice and the generated DVV) to the issuer 240. In some embodiments, if the issuer 240 does not respond with a consumer authentication response message within a configured timeout period of time, the service provider 230 may transmit an

error message to the wallet provider 210 indicating that the wallet provider 210 should send another message (e.g., message 462) after a particular amount of time.

[0102] After receipt of the consumer authentication request message 464, the issuer 240 contacts the user 107 via the selected delivery choice mechanism (see message 466) to provide the user 107 with the generated DVV. Thus, the selected delivery choice mechanism may be thought of utilizing a second “channel” of communication with the user (e.g., via SMS), as opposed to the first “channel” from the user’s mobile device 101 through the wallet provider 210 to the service provider 230.

[0103] At some point, the DVV is provided to the user 107 according to the selected delivery mechanism, and the user may input the DVV into the mobile device 101 (e.g., via the mobile wallet application), which receives the entry of the DVV at block 412, and transmits the DVV in a DVV message 468 to the wallet provider 210.

[0104] At this point, the wallet provider 210 may transmit a Resume Account message 470, which includes the entered-DVV (from message 468) along with an identifier of the respective account (e.g., a PAN, a reference ID, the inactive token, etc.). The service provider 230 may verify the Resume Account message 470 by performing one or more of the following: verifying whether a token reference ID in the message 470 is valid, whether a token-to-PAN mapping is known, whether the token has previously been issued to the wallet provider 210, whether the token is in the inactive state, etc.

[0105] At block 414, the service provider 230 then validates the DVV based upon a stored copy of the DVV (from when it was generated in block 410) or by generating a copy of the DVV (e.g., in an embodiment where the DVV is generated based upon a defined and can be re-generated). In some embodiments, the service provider 230 also verifies that the DVV has not expired based upon its submission time and/or verifies the number of user attempts to submit the DVV does not exceed a configured allowable number of attempts.

[0106] If, at block 414, the DVV is not validated, there are several (not illustrated) options for proceeding depending upon the needs of the system implementer. In some embodiments, one of the DVV variants (e.g., first DVV variant 420) may be performed one or more additional times until the DVV is validated or a number of

attempts has been satisfied. In other embodiments, the service provider 230 simply transmits an error code to the wallet provider 210.

[0107] However, when (at block 414) the DVV is validated, the service provider 230 may update its records to indicate that the token is now active (e.g., update a status maintained by token service module 222 for the token), and may generate and/or provide an activation script to the wallet provider 210 in message 472, which is forwarded to the mobile device 101 as message 474. The mobile device 101 may then activate the token at block 416 by executing the token activation script, which may cause a protection flag of the token (e.g., within secure element 102) to be disabled (at block 418), or may decrypt the previously-encrypted token (at block 419). In some embodiments, the mobile device 101 reports back to the wallet provider 210 an indicator of whether the token activation was successful (not pictured, and may include an identifier of the account / token and a yes/no or other description of the success or lack thereof of the token activation), and the wallet provider 210 then transmits the token activation results message 476 to the service provider 230, which may forward the results on to the issuer 240. At this point, the "medium" flow terminates at block 422.

[0108] FIG. 5 illustrates a flow 500 in a server computer for account provisioning according to some embodiments of the present invention. In some embodiments, the operations of flow 500 may be performed by a service provider 230 server computer 212, and in some embodiments the operations of flow 500 are performed by provisioning service module 225.

[0109] Flow 500 includes, at block 502, receiving, over a first communication channel, a provisioning request to provision a payment credential 207 of an account of a user to a mobile device. The first communication channel may comprise a connection from the service provider 230 server computer 212 to the wallet provider 210. The provisioning request may include a PAN of the account, and in some embodiments may include a reference identifier of the PAN but not the actual PAN itself. The account may be a credit card account, debit card account, checking or savings account, prepaid account, etc. The payment credential 207 may include one or more of an account number of the account, a token associated with the account, an expiration date of the token or account number, personal information associated

with the account, a public and/or private key to be used to encrypt and/or decrypt information associated with transactions with the account, card art (e.g., an image such as a depiction of an actual credit card or payment device) for the account, an identifier and/or name of a user associated with the account, an identifier and/or name of an issuer associated with the account, etc.

[0110] At block 504, the flow 500 includes determining a risk level associated with the provisioning request. This determination of the risk level may include performing a risk check or risk analysis for the requesting user, account, card, mobile device, or any other data that is present in the received provisioning request (e.g., the CVV2 value, a ZIP Code, a user identifier, etc.) or is tied to the consumer's account associated with the provisioning request (e.g., previously registered/provisioned card data, etc.). The model used for the risk analysis may be configured according to the desires of the operator, and may take into consideration historical information provided by the wallet provider in each request (e.g., how long the account has been opened, how many cards the consumer used, a number or amount of purchases in the past, etc.). The model may also combine payment processing network data regarding spending patterns on the account and network level fraud trends (e.g. data compromise trends, common merchants/ categories of spend).

[0111] At decision block 506, the flow 500 includes a determination of whether the risk level is below, within, or above a predetermined risk threshold range. In some embodiments, the risk level is set to be "high" (i.e., above the risk threshold range), "medium" (i.e., within the risk threshold range), or "low" (i.e., below the risk threshold range). In some embodiments, the risk threshold range defines a range of values that delineate at least three categories of risk values. For example, in an embodiment where generated risk values are numbers between 0 and 100, the predetermined risk threshold range may be configured as [25, 50], and thus, any generated risk value score that is greater than or equal to 25 and less than or equal to 50 will be considered "medium" risk, and any risk score above that range (i.e., greater than 50) is considered "high" risk, and any risk score below that range (i.e., less than 25) is considered "low" risk. Of course, other predetermined risk threshold ranges may be configured using other ranges/cutoff points, and may be configured according to different types of generated risk scores (e.g., integers, real numbers, letters, etc.) and schemes.

[0112] In the depicted embodiment, if the risk level is deemed below the predetermined risk threshold range (i.e., is “low” risk), the flow 500 includes causing, at block 508, the payment credential 207 to be provisioned to the mobile device. In some embodiments, this includes transmitting a set of one or more provisioning scripts to be executed by the mobile device to cause the payment credential 207 to be provisioned in an activated state. In some embodiments, this transmission is made with the wallet provider as the destination, and the wallet provider then forwards on the set of provisioning scripts to the mobile device for execution. In some embodiments, the set of provisioning scripts includes a personalization script including account provisioning data and an activation script that, when executed, causes the provisioned account credential 207 to be provisioned in the active state (i.e., is able to be used by the mobile device for payment transactions). In other embodiments, the set of provisioning scripts includes just one script that provisions the account credential(s).

[0113] In the depicted embodiment, if the risk level is deemed to be above the predetermined risk threshold range (i.e., is “high” risk), the flow 500 includes at block 510, transmitting a provisioning request denial message indicating that the provisioning request is denied. In some embodiments, the provisioning request denial message is transmitted to a wallet provider, which then forwards on the provisioning request denial message to the mobile device of the user or otherwise transmits a message to the mobile device to indicate that the provisioning request has been denied.

[0114] If, in the depicted embodiment, the risk level is deemed to be within the predetermined risk threshold range (i.e., is “medium” risk), the flow 500 continues with an optional optimization at block 512 of transmitting a set of provisioning scripts to be executed by the mobile device to cause the payment credential 207 to be stored on the mobile device in an inactive state. In some embodiments, the set of provisioning scripts includes a personalization script that, when executed, provisions the payment account credentials 207 in an inactive state that cannot be used by the mobile device. For example, in some embodiments the provisioned token is obfuscated (e.g., encrypted or otherwise transformed) to be invalid, in some embodiments a protection flag is set (e.g., within a mobile device 101 secure element 202) such that the mobile device 101 cannot access the payment credential

207. In some embodiments, the performance of block 512 allows for some credential-provisioning work to be performed “early” (i.e., before a time the credential is actually allowed to be activated), which can distribute the required workload from a time perspective by allowing these potentially relatively computationally expensive steps to be performed early and just using a relatively computationally lightweight script to be executed later on (e.g., at block 530) to activate the pre-provisioned but inactive account credentials. However, in some embodiments this block 512 is not performed, and all payment account credential provisioning occurs later at block 526.

[0115] At block 514, the flow 500 includes causing an authentication process to be performed with the user 107. In some embodiments, this authentication process comprises, at block 516, causing a dynamic verification value (DVV) to be provided to the user via a second communication channel. In some embodiments, the second communication channel includes a communication between an issuer 240 of the account with the user 107, and may not include any direct communication between the service provider 230 and the user 107 or between the service provider 230 and wallet provider 210. In some embodiments, this communications channel includes the issuer transmitting an SMS message, an email, placing or receiving a telephone call with the user, transmitting a webpage to the user, etc. In some embodiments, the DVV comprises a one-time password (OTP). The OTP, in some embodiments, is generated by the service provider 230, and in some embodiments is generated by the issuer 240. In some embodiments, the service provider 230 server computer 212 generates (or acquires) the OTP and provides it (at block 518) to the issuer computer 106 managing the user’s account for delivery to the user. In some embodiments, the issuer computer 106 generates the OTP and transmits the OTP to both the user 107 (via the second communications channel) as well as to the service provider 230 server computer 212 to enable the server computer 212 to later validate a user’s entry of the OTP. However, in some embodiments the issuer computer 106 generates the OTP but does not need to provide the OTP to the service provider 230 server computer 212. For example, issuer computer 106 may generate the OTP according to a determined algorithm so that the OTP can be verified by the service provider 230 server computer 212 based upon the server computer 212 generating the OTP again using the same algorithm, for example. Thus, at some point after the user 107 is provided with the DVV via the second communications channel, the user

107 may provide the DVV back via the mobile device 101. This may cause the mobile device 101 to send the entered DVV to the wallet provider 210, which in turn may generate and transmit a consumer verification response message including the entered DVV to the service provider 230 server computer 212 at block 520.

[0116] At block 522, the flow 500 includes determining whether the authentication process was successful. For example, the determining may include a determination of whether the user-entered DVV within the consumer verification response message is the "correct" dynamic verification value. In some embodiments, this determination comprises looking up a stored copy of the DVV (e.g., generated by the service provider 230, issuer 240, or third-party) and comparing it to the received DVV to determine if they are the same. In some embodiments, this determination comprises using a DVV-generation algorithm (e.g., that was previously used to generate the DVV) to generate the DVV and compare the generated DVV to the received user-entered DVV. In some embodiments, when the user-entered DVV within the consumer verification response message is not the same as the "correct" DVV, the authentication process is deemed to have failed, and flow continues at block 524, where an error message is sent. In some embodiments, this message is transmitted to the wallet provider 210 and/or issuer computer 106.

[0117] However, in some embodiments when the authentication process is deemed to have succeed (e.g., the user-provided DVV is the same as the "correct" DVV), the flow 500 continues with block 526, which includes causing the payment credential 207 to be provisioned onto the mobile device. In some embodiments, this includes causing the payment credential 207 (previously) provisioned onto the mobile device to be switched from the inactive state to an active state, which may include decrypting/deobfuscating a token of the account, changing a data protection flow (e.g., within a secure element 202), etc. In some embodiments, this provisioning includes at block 530 transmitting an activation script to be executed by the mobile device. In some embodiments, the activation script is sent to wallet provider 210, which in turn provides the activation script to the mobile device 101, causing the activation script to be executed and thus the payment credentials 207 installed/activated. In some embodiments, the service provider 230 server computer 212 also receives a token activation result message 381 from wallet provider 210 indicating whether the provisioning was successful, and may forward this message

382 on to the issuer 240. In some embodiments, the service provider 230 server computer 212 may also transmit a token notification message 379 to the issuer 240 to inform the issuer 240 of the token and the account that it is associated with.

V. VARIANTS FOR GENERATING AND VERIFYING DYNAMIC VERIFICATION VALUES

[0118] FIG. 6 illustrates a combined sequence and flow diagram depicting two dynamic verification value validation configurations 600A-600B in an account provisioning system according to some embodiments of the present invention. In some embodiments, the first DVV variant 420 of FIG. 4 is replaced with one of second DVV variant 600A or third DVV variant 600B. However, these are just a few DVV variants possible, and other variants may be utilized that may or may not include features from these variants. Both the second and third DVV variants 600A-600B begin after the service provider 230 server computer 212 has received a DVV delivery choice message 462 from the wallet provider 210.

[0119] The second DVV variant 600A includes – instead of generating a DVV as in block 410 of FIG. 4 – transmitting a DVV request message 650 (including the delivery choice indicated in the DVV delivery choice message 462) to the issuer 240, which itself will generate the DVV at block 602, provide the DVV to the user at block 466 according to the delivery choice over the second communications channel, and return the generated DVV in message 652 to the service provider 230. The service provider 230 may store this DVV at block 604. After the user has received the DVV over the second communications channel, the user will enter the DVV into the mobile device 101 (e.g., using a mobile wallet application), which will send the entered-DVV in a message 468 to the wallet provider 210. The wallet provider 210 will then transmits a resume account message 470 including the DVV to the service provider 230, which can determine the validity of the authentication by validating the DVV at block 606, which includes comparing the stored DVV (from block 604) with the received user-entered DVV (from message 470). If the values match or are otherwise deemed equivalent, the DVV is validated and thus the authentication succeeds; otherwise, the DVV is not validated and the authentication fails.

[0120] The third DVV variant 600B is similar to the second DVV variant 600A aside from a few key differences. First, in the third DVV variant 600B, the issuer 240 does not report the generated DVV back to the service provider (see message 652 of the second DVV variant 600A). Instead, when the service provider 230 receives the resume account message 470 including the user-entered DVV, the service provider 230 may validate the DVV at block 608 according to an algorithm. In some embodiments, the issuer 240 generates the DVV 602 using a particular algorithm that is known to the service provider 230 such that the service provider 230 can either re-generate the DVV itself (using the same algorithm) or invert the algorithm such that it can “undo” the user-provided DVV value to arrive at a clear text value, and then test the clear text value to determine whether it formatted properly. For example, in an embodiment the issuer 240 may generate the DVV 602 by encrypting (with an issuer 240 private key) a clear text value that is based upon a value associated with the user (e.g., a PAN of the account, a user identifier, etc.) and further based upon a current date or time value, for example (of course, many other possibilities exist for creating clear text values, and this provided example is simply illustrative of one possible use case). Thus, the service provider 230 may have access to a public key of the issuer 240, decrypt the user-provided DVV, and determine whether the resulting clear text value includes the correct PAN and a correct date/time value.

VI. SECURE COMMUNICATIONS USING CONSUMER-SPECIFIC ENCRYPTION KEYS

[0121] Throughout many of the disclosed embodiments, information flows between the user 107 (and mobile device 101) to the service provider 230 or issuer 240 via wallet provider 210. However, consumers have significant privacy concerns and third parties (such as wallet provider 210) may often hold consumer data in transit as it passes from an information source to the consumer. For example, a significant amount of potentially-sensitive financial/transactional data of the user 107 flows through the wallet provider 210. Accordingly, where third party systems may route transaction alerts, transaction history, payment credentials, etc., to consumer devices (e.g., mobile device 101), there is a need for protection of sensitive data.

[0122] When the service provider 230 (e.g., payment processing network 105) does not directly communicate with the mobile communication device 101, providing an encryption key to the mobile communication device is a problem because the encryption key is passed through the third party computer (e.g., server computer 211) and the third party computer may gain access and use the key to decrypt future communications. As such, traditional methods of delivering transaction history data to the mobile device 101 via a third party server cannot be implemented to adequately protect the data using a TLS/SSL tunnel since it terminates at the third party server computers, thus giving third party server computers access to data in the clear.

[0123] However, by incorporating a unique, consumer-specific key into the provisioning scripts (described earlier with respect to payment credential provisioning) designed to be provisioned onto a user's mobile communication device 101, the encryption key may be protected from interception by the third party because the script may be encrypted with a secure element key associated with a secure memory area on a secure element 202 of the mobile communication device 101. Accordingly, the provisioning scripts are encrypted with keys that the third party computer does not have access to and the embedded consumer-specific key may be provisioned onto the secure element during a personalization process of a mobile payment application with a payment token or other payment credentials of a user. Thereafter, the unique consumer-specific encryption key may be accessed through communications with the mobile payment application on the mobile communication device and used to decrypt encrypted communication information received at the mobile communication device.

[0124] Accordingly, embodiments of the invention provide for better security for sensitive data (e.g., transaction alerts, other consumer data, transaction histories, etc.). For example, a third party with a specific consumer base may want to provide transaction alerts for its customers, but it may not be desirable for the third party to be able to view the data in the alert messages as the information could be considered confidential to the user and the third party may not want to have access to the transaction alert data. Embodiments of the invention may incorporate encryption keys at a data source (e.g., the service provider 230 / payment processor 105) and at the data destination (e.g., in the end users' mobile devices 101). Thus,

sensitive messages may pass from the service provider 230, through the third party computer systems (e.g., wallet provider 210 server computer 211), and to the users' mobile devices 101. The users' mobile devices 101 may include encryption keys so that they may decrypt the sensitive data.

[0125] FIG. 7 illustrates a combined sequence and flow diagram 700 depicting consumer-specific encryption key provisioning and the secure message transmission through a wallet provider according to some embodiments of the present invention. In this depicted embodiment, asymmetric cryptography techniques utilizing public/private key pairs are utilized for data protection, although in other embodiments other obfuscation techniques may similarly be utilized.

[0126] FIG. 7 illustrates a consumer-specific encryption key (CSEK) provisioning scheme 760 to securely provision the CSEK for use. In this embodiment, the mobile device 101 provides a secure element encryption key (SEEK) in message 750A that may be a public key allowing other entities to encrypt messages that can only be read (i.e., decrypted) by the secure element 202 of the mobile device 101 (e.g., using an associated private key). In other embodiments, this key is not associated with a secure element 202, however, and it is just a public key associated with a private key of the mobile device 101. The wallet provider 210 may forward the SEEK in message 750B to the service provider 230.

[0127] At block 702, the service provider 230 may acquire or generate a set of consumer-specific encryption keys. For example, the service provider 230 may generate a public key and a private key to be used for communications with the mobile device 101. The keys may be

[0128] The service provider 230 may then include the public CSEK with the provisioning scripts in a package at block 704, and encrypt this package using the SEEK originally provided by the mobile device 101. Thus, even though this package is routed / forwarded through the wallet provider 210 at messages 752A and 752B (and potentially computing devices of other entities), none of these entities can access the public CSEK or the provisioning scripts in the package, since only the mobile device 101 has the corresponding private SEEK to allow it to "open" the package. Of particular note is that this package (at messages 752A and 752B) – including the public CSEK -- may be what is sent when provisioning scripts are

generated/sent in any of FIGS. 3 and 4. For example, the preparation of provisioning scripts at block 326 (in “low” risk flow of FIG. 3) may comprise preparing a package that includes the scripts and the public CSEK. Similarly, the preparation of provisioning scripts at block 406 (in “medium” risk flow of FIG. 4) and/or the transmission of the token activation script (see message 472) may similarly comprise sending a public SEEK-encrypted package including the provisioning scripts and/or the public CSEK, for example. Of course, in some embodiments the public-SEEK encrypted package may not include the provisioning scripts (e.g., such as when they do not contain sensitive information) but may include other data such as the public CSEK.

[0129] Turning back to FIG. 7, after the CSEK provisioning scheme 760, the service provider 230 and the mobile device 101 are thus enabled, via the use of CSEK keys, to communicate securely without the wallet provider 210 or another entity becoming aware of the transmitted data. For example, at block 716 the service provider 230 may generate a message such as an account alert message (e.g., based upon a financial transaction event violating a configured rule) or a transaction history (e.g., detailing one or more previous transactions for the account of the user) message, for example. This message may then be encrypted, by the service provider 230 at block 718, using the private CSEK to yield an encrypted message. This encrypted message may be sent as message 754A from service provider 230 to wallet provider 210 to mobile device 101 (as message 754B). The mobile device 101 may then decrypt the encrypted message using the public CSEK at block 720, which it may have received in encrypted package 752B that was part of its receipt of the payment credential 207 provisioning scripts. The mobile device 101 may then utilize the message internally, and/or may display the message at block 722 to the user 107. Similarly, at some point in time the mobile device 101 may use the public CSEK at block 720 to encrypt a message for the service provider 230, and then may transmit the message securely toward the service provider 230.

[0130] In some embodiments, the encryption and/or decryption may occur at the secure element 202 of the mobile device 101 through a secure mobile payment application 206 that is embedded or installed on the secure element 202 of the mobile device 101. By performing the encryption/decryption at the secure element 202, the encryption keys and information received in the messages may be further

protected from malicious third parties that may install malicious software in the general purpose memory of the mobile device 101. Accordingly, more secure implementations of the encryption and decryption processes may be implemented in some embodiments.

VII. UNIQUE TRANSACTION IDENTIFIERS

[0131] Payment transactions originating from mobile devices 101 provide convenient payment options for consumers but can lead to incomplete and complex transaction processing and reporting issues. For example, mobile devices 101 may only have access to partial transaction data at the time a transaction is initiated and thus, mobile payment applications 208C, 206 located on the mobile device 101 may not have access to a full transaction details but may only have a partial transaction log 204. Additionally, payments initiated by a near-field communication (NFC) chip on a mobile device 101 may lead to a number of unsuccessful payment attempts due to complex radio frequency environments or outdated terminal software and/or hardware. However, when NFC payments are unsuccessful, information stored in a transaction log 204 on the mobile device 101 may not match transaction information stored at different entities (e.g., transaction log 224 at payment processing network 105, merchant 103, acquirer 104, issuer 240, etc.) within a transaction processing system. Accordingly, there is a need for a method for matching transactions received on the back-end of a transaction processing system with those transactions initiated at a mobile device 101. Additionally, there is a need for easily and efficiently identifying unique transactions between the front-end and the back-end of a transaction processing system. Embodiments of the invention address these and other problems, individually and collectively.

[0132] One embodiment is directed at a method for generating a unique transaction identifier on a mobile device 101 using a shared digest. The method comprises initiating a payment transaction from the mobile device 101. The method continues by selecting transaction elements associated with the payment transaction according to the shared digest, hashing the selected transaction elements according to a predetermined hashing algorithm, and concatenating the hashed transaction elements. The unique transaction identifier is then stored in a transaction log 204.

Another embodiment is directed at a method for matching transactions using a unique transaction identifier. The method comprises receiving an authorization request message for a transaction originating from a mobile device 101 and generating a unique transaction identifier for the transaction. The unique transaction identifier is generated using a shared digest and predetermined transaction elements in the authorization request message. The server computer (e.g., server computer 212) sends transaction matching information including the unique transaction identifier to the mobile device. The mobile device 101 searches a transaction log 204 for the transaction associated with the unique transaction identifier, identifies transaction information associated with the unique transaction identifier, and updates a transaction log with the transaction matching information. Further, other embodiments may be directed at using the transaction identification techniques described herein for a number of different uses including transaction reporting, loyalty program monitoring, and any other uses where matching transaction data between a front-end and back-end system is desirable.

[0133] To these ends, FIG. 8 illustrates a combined sequence and flow diagram 800 depicting the use of unique transaction identifiers for transaction log updates according to some embodiments of the present invention. The depicted embodiment is directed at providing full transaction information to a transaction log 204 located at a mobile device 101.

[0134] For example, at block 802 a transaction is initiated by a mobile device 101 using a payment application. At this point, the mobile device 101 may only have access to partial transaction information. At block 804, the mobile device 101 generates a first unique transaction identifier (UTI) for the transaction according to an algorithm. At block 806, the mobile device 101 stores the first UTI along with the partial transaction information of the transaction in a record of a transaction log 204, which may be stored in “general purpose” memory or in memory only accessible to a secure element 202.

[0135] Accordingly, a service provider 230 (e.g., payment processing network 105) server computer 212 receives, at block 808, an authorization request message or authorization response message. The service provider 230, at block 810, generates a second UTI for the transaction according to the algorithm, and the

second UTI will have the same value as the first UTI generated by the mobile device 101. The service provider 230 may update the transaction information of the mobile device 101 transaction log 204 by sending transaction matching information (e.g., the second UTI) to the mobile device 101 via messages 850 and 851 with the full transaction information (i.e., thus including “additional” transaction information not yet in the possession of the transaction log 204).

[0136] The mobile device 101, at block 814, can identify the record of the transaction log 204 for the transaction based upon the received second UTI. In an embodiment, the mobile device 101 will perform this identification by searching through the transaction log for a record having a stored UTI with a same value as the received second UTI. Upon finding a match, that record is selected as the transaction record, and the mobile device 101 may update the record based upon the additional transaction information at received in the message 851 at block 818. Thus, a service provider 230 may use a shared digest (or index) to generate a unique transaction identifier that both the service provider 230 and the mobile device 101 may use to identify the transaction associated with the transaction matching.

[0137] Using a similar scheme, embodiments of the invention also enable mobile devices 101 to report UTIs to the service provider 230. For example, another embodiment allows the service provider 230 to determine merchants with faulty or outdated terminals (e.g., access devices 102) by receiving information regarding unsuccessful transactions attempted by a mobile device 101. Accordingly, when a service provider 230 receives an authorization request messages in a transaction processing system, the server computer may be capable of generating a unique transaction identifier using a hashing algorithm on data elements in the authorization request message and may send the unique transaction identifier to a mobile device. The mobile device 101 may then identify the transaction associated with the received unique transaction identifier and may report any unsuccessful transactions since the last reported transaction to the service provider 230. Therefore, the service provider 230 may be able to determine the number of unsuccessful transactions, the merchants associated with those transactions, and any other relevant information from the transaction log.

VIII. EXEMPLARY COMPUTER SYSTEMS

[0138] The various participants and elements described herein may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in the above-described FIGS. 1-8, including any servers or databases, may use any suitable number of subsystems to facilitate the functions described herein.

[0139] Examples of such subsystems or components are shown in FIG. 9. The subsystems shown in FIG. 9 are interconnected via a system bus 902, which may comprise one or more buses. Additional subsystems such as a printer 910, keyboard 918, fixed disk 920 (or other memory comprising computer readable media, which may include a non-transitory computer readable storage medium), monitor 912 (or "display device"), which is coupled to display adapter 914, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 904 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as serial port 916 (or USB port, parallel port, etc.). For example, serial port 916 or external interface 922 can be used to connect the computer apparatus to a wide area network (WAN) such as the Internet, a mouse input device, or a scanner. The interconnection via system bus 902 allows the central processor 908 (which may comprise one or more processing units, processor cores, combinations thereof, etc.) to communicate with each subsystem and to control the execution of instructions from system memory 906 or the fixed disk 920, as well as the exchange of information between subsystems. The system memory 906 and/or the fixed disk 920 may embody a computer readable medium such as a non-transitory computer readable storage medium.

[0140] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++, C, Python, JavaScript, or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or

within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0141] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.

[0142] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0143] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0144] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

CLAIMS:

1. A method, comprising:

receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device, wherein the first payment credential is associated with a first account of a first user;

determining a first risk level associated with the first provisioning request;

responsive to the first risk level being within a predetermined risk threshold range, causing an authentication process to be performed with the first user;

responsive to a successful performance of the authentication process, causing the first payment credential to be provisioned onto the first mobile device;

receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device, wherein the second payment credential is associated with a second account of a second user;

determining a second risk level associated with the second provisioning request; and

responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device.

2. The method of claim 1, further comprising:

receiving, at the server computer via the first communication channel, a third provisioning request to provision a third payment credential to a third mobile device, wherein the third payment credential is associated with a third account of a third user;

determining a third risk level associated with the third provisioning request; and

responsive to the third risk level meeting or exceeding the predetermined risk threshold range, transmitting, by the server computer, a provisioning

request denial message indicating that the third provisioning request is denied.

3. The method of claim 1, further comprising:

further responsive to the first risk level being within the predetermined risk threshold range, transmitting a first set of provisioning scripts to be executed by the first mobile device to cause the first payment credential to be stored at the first mobile device in an inactive state, wherein the inactive state does not allow the first mobile device to utilize the first payment credential for financial transactions,

wherein said causing the first payment credential to be provisioned onto the first mobile device comprises transmitting, by the server computer, an activation script to be executed by the first mobile device to switch the first payment credential from the inactive state to an active state that allows the first mobile device to use the first payment credential for financial transactions.

4. The method of claim 3, wherein said activation script, when executed by the first mobile device, causes the first payment credential to be switched to the active state by one or more of:

disabling a protection flag associated with the first payment credential within a secure element of the first mobile device; and

decrypting the first payment credential.

5. The method of claim 1, wherein:

said causing the authentication process to be performed with the first user comprises causing a dynamic verification value to be provided to the first user via a second communication channel; and

said successful performance of the authentication process comprises receiving, at the server computer, a consumer verification response that includes the dynamic verification value.

6. The method of claim 5, wherein said causing the dynamic verification value to be provided to the first user via the second communication channel comprises:

generating, by the server computer, the dynamic verification value; and

transmitting, by the server computer, the dynamic verification value to an issuer computer of an issuer of the first account to cause the issuer to provide the dynamic verification value to the first user.

7. The method of claim 5, further comprising:

receiving, at the server computer, a message transmitted by the issuer computer that includes the dynamic verification value; and

comparing, by the server computer, the received dynamic verification value of the consumer verification response with a stored copy of the dynamic verification value received from the issuer computer,

wherein said causing the dynamic verification value to be provided to the first user via the second communication channel comprises transmitting, by the server computer to an issuer computer of an issuer of the first account, a request for the dynamic verification value.

8. The method of claim 5, further comprising:

determining, by the server computer, whether the received dynamic verification value of the consumer verification response has a same value as an output of a validation algorithm utilizing at least two input values, wherein the at least two input values comprise an account identifier of the first account and a time value,

wherein said causing the dynamic verification value to be provided to the first user via the second communication channel comprises transmitting, by the server computer, a request for the dynamic verification value to be generated and provided to the first user.

9. The method of claim 1, further comprising:

generating a set of one or more consumer-specific encryption keys;

causing at least one of the set of consumer-specific encryption keys to be provided to the first mobile device;

encrypting a communication message using one of the set of consumer-specific encryption keys to yield an encrypted communication message; and

transmitting the encrypted communication message to a wallet application provider, wherein the wallet application provider provides the encrypted

communication message to the first mobile device and does not have any of the set of consumer-specific encryption keys.

10. The method of claim 1, further comprising:

receiving, at the server computer, an authorization request message for a transaction involving the first account of the first user;

generating, by the server computer, a unique transaction identifier for the transaction; and

transmitting, by the server computer, the unique transaction identifier and additional transaction information for the transaction, wherein the first mobile device, upon receipt of the unique transaction identifier and the additional transaction information:

identifies a record of a transaction log based upon the unique transaction identifier, and

updates the record based upon the additional transaction information.

11. The method of claim 1, wherein the first provisioning request does not include a primary account number (PAN) of the first account but does include a reference identifier of the PAN, and wherein the method further comprises identifying, by the server computer, the first account using the reference identifier.

12. A non-transitory computer readable storage medium storing instructions which, when executed by one or more processors of a server computer, cause the server computer to perform operations comprising:

receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device, wherein the first payment credential is associated with a first account of a first user;

determining a first risk level associated with the first provisioning request;

responsive to the first risk level being within a predetermined risk threshold range, causing an authentication process to be performed with the first user;

responsive to a successful performance of the authentication process, causing the first payment credential to be provisioned onto the first mobile device;

receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device, wherein the second payment credential is associated with a second account of a second user;

determining a second risk level associated with the second provisioning request; and

responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device.

13. The non-transitory computer readable storage medium of claim 12, wherein the operations further comprise:

receiving, at the server computer via the first communication channel, a third provisioning request to provision a third payment credential to a third mobile device, wherein the third payment credential is associated with a third account of a third user;

determining a third risk level associated with the third provisioning request; and

responsive to the third risk level meeting or exceeding the predetermined risk threshold range, transmitting, by the server computer, a provisioning request denial message indicating that the third provisioning request is denied.

14. The non-transitory computer readable storage medium of claim 12, wherein the operations further comprise:

further responsive to the first risk level being within the predetermined risk threshold range, transmitting a first set of provisioning scripts to be executed by the first mobile device to cause the first payment credential to be stored at the first mobile device in an inactive state, wherein the inactive state does not allow the first mobile device to utilize the first payment credential for financial transactions,

wherein said causing the first payment credential to be provisioned onto the first mobile device comprises transmitting, by the server computer, an activation script to be executed by the first mobile device to switch the

first payment credential from the inactive state to an active state that allows the first mobile device to use the first payment credential for financial transactions.

15. The non-transitory computer readable storage medium of claim 12, wherein:

said causing the authentication process to be performed with the first user comprises causing a dynamic verification value to be provided to the first user via a second communication channel; and

said successful performance of the authentication process comprises receiving, at the server computer, a consumer verification response that includes the dynamic verification value.

16. The non-transitory computer readable storage medium of claim 12, further comprising:

generating a set of one or more consumer-specific encryption keys;

causing at least one of the set of consumer-specific encryption keys to be provided to the first mobile device;

encrypting a communication message using one of the set of consumer-specific encryption keys to yield an encrypted communication message; and

transmitting the encrypted communication message to a wallet application provider, wherein the wallet application provider provides the encrypted communication message to the first mobile device and does not have any of the set of consumer-specific encryption keys.

17. A server computer, comprising:

one or more processors; and

a non-transitory computer readable storage medium communicatively coupled with the one or more processors and storing instructions which, when executed by the one or more processors, cause the server computer to perform operations comprising:

receiving, at a server computer via a first communication channel, a first provisioning request to provision a first payment credential to a first mobile device, wherein the first payment credential is associated with a first account of a first user;

determining a first risk level associated with the first provisioning request;

responsive to the first risk level being within a predetermined risk threshold range, causing an authentication process to be performed with the first user;

responsive to a successful performance of the authentication process, causing the first payment credential to be provisioned onto the first mobile device;

receiving, at the server computer via the first communication channel, a second provisioning request to provision a second payment credential to a second mobile device, wherein the second payment credential is associated with a second account of a second user;

determining a second risk level associated with the second provisioning request; and

responsive to the second risk level being below the predetermined risk threshold range, causing the second payment credential to be provisioned onto the second mobile device.

18. The server computer of claim 17, wherein the operations further comprise:

receiving, at the server computer via the first communication channel, a third provisioning request to provision a third payment credential to a third mobile device, wherein the third payment credential is associated with a third account of a third user;

determining a third risk level associated with the third provisioning request; and

responsive to the third risk level meeting or exceeding the predetermined risk threshold range, transmitting, by the server computer, a provisioning request denial message indicating that the third provisioning request is denied.

19. The server computer of claim 17, wherein the operations further comprise:

further responsive to the first risk level being within the predetermined risk threshold range, transmitting a first set of provisioning scripts to be

executed by the first mobile device to cause the first payment credential to be stored at the first mobile device in an inactive state, wherein the inactive state does not allow the first mobile device to utilize the first payment credential for financial transactions,

wherein said causing the first payment credential to be provisioned onto the first mobile device comprises transmitting, by the server computer, an activation script to be executed by the first mobile device to switch the first payment credential from the inactive state to an active state that allows the first mobile device to use the first payment credential for financial transactions.

20. The server computer of claim 17, wherein:

said causing the authentication process to be performed with the first user comprises causing a dynamic verification value to be provided to the first user via a second communication channel; and

said successful performance of the authentication process comprises receiving, at the server computer, a consumer verification response that includes the dynamic verification value.