AUTOMATED ACCOUNT PROVISIONING

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims benefit under 35 U.S.C. §119(e) to U.S. Provisional Patent Application No. 61/906,378 filed November 19, 2013 and entitled "Issuer Initiated Account Provisioning", the disclosure of which is incorporated by reference herein in their entirety for all purposes.

BACKGROUND

[0002] Mobile communication devices are becoming increasingly popular for conducting various types of transactions. A mobile communication device can store financial account information or other information associated with a user, for example, information associated with credit cards, debit cards, coupons, rewards, receipts, concert tickets, and the like. The mobile communication device may be linked to a user's payment account credentials as well as personal information. Using mobile communication devices for payment transactions reduce the need to enter payment credentials or present a physical card each time a payment transaction is conducted. Often, a provisioning system (i.e. a provisioning service provider computer) is required to provision the financial account information of the user on the user's mobile communication device.

[0003] Current provisioning systems typically require the users to request provisioning of accounts from the mobile communication device. However, this can be onerous and difficult for some accountholders who are not technically savvy. Furthermore, issuers may wish to provision payment accounts for some customers (e.g., VIPs) or accountholders who indicate an interest in the provisioning while in a branch office. However, issuers do not have access to all of the mobile device information, such as information associated with a secure element of the mobile device, necessary to provision the financial account on the mobile device. In addition, conventional systems require interaction with a third party (e.g. the mobile network operator) to obtain the secure element information. These communications are extensive in nature, and require cooperation between different entities with

different data transfer protocols. Accordingly, there is a need for a system that allows an account issuer to initiate a provisioning request on behalf of the user.

[0004] Embodiments of the invention address these and other problems, individually and collectively.

SUMMARY

[0005] Embodiments of the invention are directed to systems, apparatuses, and methods related to initiating the provisioning of financial accounts on mobile devices by an issuer and without user interaction. Provisioning a financial account on a mobile device includes secure communication of financial account information into a secure element or other secure data storage element of the mobile device. The financial account information or credentials may be accessed by authorized applets or mobile payment applications on the mobile device to initiate and complete transactions with access devices, server computers, and any other components or systems in a transaction processing system.

[0006] Embodiments of the present invention allow an issuer to initiate account provisioning on a mobile device without requiring interaction with or input from an accountholder (i.e. user). For example, the issuer may initiate the process by sending a provisioning information request message to a mobile device with a secure element (i.e. secure memory). The operating system of the mobile device may recognize the provisioning request message and gather the requisite provisioning information without requiring user input. The provisioning information may include, for example, information associated with the secure element of the mobile device. The mobile device may then send a provisioning request message to a provisioning system (i.e. provisioning service provider computer). In some exemplary embodiments, the mobile device may send the provisioning request message to the issuer, which may, in turn, send the provisioning request message to the provisioning system. The provisioning request message may include the requisite provisioning information to allow the provisioning system to provision the financial account on the secure element of the mobile device.

[0007] In some embodiments, the issuer may include an authorization code in the provisioning information request message. The authorization code may be forwarded to the provisioning system as part of the provisioning request message. The provisioning system may validate the authorization code to ensure the mobile device is authorized by the issuer for provisioning of the account.

[0008] One embodiment of the invention is directed to a method comprising receiving, by a mobile communication device, an information request message from an issuer server computer. The mobile communication device automatically determines provisioning information associated with a secure memory in response to the information request message and without input of a user operating the mobile communication device. The method further includes generating, by the mobile communication device, a provisioning request message including the provisioning information. The mobile communication device sends the provisioning request message including the provisioning information to a provisioning system or the issuer server computer and receives a provisioning response message including provisioning data from the provisioning system. The provisioning data is generated using the provisioning information associated with the secure memory. The method also includes storing, by the mobile communication device, the provisioning data in the secure memory. The provisioning data associates the mobile communication device with a payment account.

[0009] Another embodiment of the invention is directed to a method comprising authenticating, by an issuer server computer, a user associated with a user payment account. The issuer server computer receives a mobile device identifier identifying a mobile device of the user and generates a provisioning information request message without interacting with the user. The provisioning information request message includes at least the mobile device identifier and a provisioning information request identifier. The provisioning information request identifier automatically causes the mobile device to gather provisioning information. The method further includes sending, by the issuer server computer, the provisioning information request message to the mobile device of the user. The provisioning

information request message initiates provisioning of the user payment account on the mobile device of the user.

[0010] Yet another embodiment of the invention is directed to an issuer computer server computer comprising a processor and a non-transitory computer readable medium coupled to the processor. The computer readable medium comprises code, that when executed by the processor, causes the processor to send an information request message to a mobile communication device. The information request message requests provisioning information associated with a secure memory of the mobile communication device. The code, when executed by the processor, further causes the processor to receive a response message including the provisioning information from the mobile communication device. The provisioning information is automatically gathered by the mobile communication device in response to the information request message and without input of a user operating the mobile communication device. The code, when executed by the processor, further causes the processor to send a provisioning request message to a provisioning system such that provisioning data can be sent to the mobile communication device for associating the mobile communication device with a payment account. The provisioning request message includes the provisioning information, and one or more of an account identifier and a mobile device identifier associated with the mobile communication device. In certain embodiments, the code, when executed by the processor, causes the processor to generate an authorization code indicating that the provisioning request message associated with the authorization code is authorized and authenticated by the issuer server computer, and include the authorization code in the provisioning request message.

[0011] Other embodiments include a mobile communication device comprising a processor, a server computer comprising a processor and computer readable media configured to complete the methods described above. Further, other embodiments may include systems, server computers, and methods for completing the functionality disclosed herein.

[0012] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 shows a block diagram of an exemplary secure element account provisioning system, according to an embodiment of the invention.

[0014] FIG. 2 shows components of, and interactions between, an issuer, a mobile device and a provisioning system for provisioning a financial account on a secure element of the mobile device, according to an embodiment of the invention.

[0015] FIG. 3 shows an exemplary flow diagram for an issuer initiated account provisioning process where provisioning information is sent directly from a mobile device to a provisioning system, according to an embodiment of the present invention.

[0016] FIG. 4 shows another exemplary flow diagram for an issuer initiated account provisioning process where provisioning information is sent indirectly from a mobile device to a provisioning system, according to an embodiment of the present invention.

[0017] FIG. 5 shows exemplary steps performed by a mobile device for provisioning a financial account on a secure element of the mobile device, according to an embodiment of the invention.

[0018] FIG. 6 shows exemplary steps performed by an issuer for initiating the provisioning of a financial account on a mobile device, according to an embodiment of the invention.

[0019] FIG. 7 shows an exemplary financial transaction system, according to an embodiment of the invention.

[0020] FIG. 8 shows an exemplary computer system according to embodiments of the present invention.

DETAILED DESCRIPTION

[0021] Embodiments of the present invention allow an issuer to initiate account provisioning on a mobile device without interaction with or input from a user. For example, the issuer may initiate the process by sending a provisioning

information request message to a mobile device with a secure element (i.e. secure memory). The operating system of the mobile device may recognize the provisioning request message and gather the requisite provisioning information without requiring user input. The provisioning information may include, for example, information associated with the secure element of the mobile device. The mobile device may then send a provisioning request message to a provisioning system. In some exemplary embodiments, the mobile device may send the provisioning request message to the issuer, which may, in turn, send the provisioning request message to the provisioning system. The provisioning request message may include the requisite provisioning information to allow the provisioning system to provision the financial account on the secure element of the mobile device.

[0022] In some embodiments, the issuer may include an authorization code in the provisioning information request message. The authorization code may be forwarded to the provisioning system as part of the provisioning request message. The provisioning system may validate the authorization code to ensure the mobile device is authorized for provisioning of the account.

[0023] Thus, embodiments of the present invention may be used in connection with transaction processing systems or may use data generated during transaction processing through a transaction processing system. Such embodiments may involve transactions between accountholders and merchants using the mobile communication device of the accountholders. For example, once an account has been successfully provisioned onto the secure element of the mobile communication device of the accountholder (i.e. user), the accountholder may use the provisioned account information to initiate and complete transactions with transaction processing systems, as further described below in connection with FIG. 7.

[0024] Before discussing specific embodiments and examples, some descriptions of terms used herein are provided below.

[0025] As used herein, a “mobile device” may comprise any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication

capabilities include using a mobile phone (wireless) network, wireless data network (*e.g.* 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (*e.g.* cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, etc. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (*e.g.* when a device has remote access to a network by tethering to another device - *i.e.* using the other device as a modem – both devices taken together may be considered a single mobile device). A mobile device may also comprise secured hardware or software component within the mobile device and/or one or more external components that may be coupled to the mobile device. A detailed description of an exemplary mobile device is provided below.

[0026] A "secure element" may include any secure memory device such that the data contained on the secure element cannot easily be hacked, cracked, or obtained by an unauthorized entity. For example, the secure element may be an integrated circuit device that is implemented within a near field communications (NFC) enabled mobile communication device. The secure element may contain embedded smart card-grade applications (e.g., payment, transport, etc.). The secure element may be used by the mobile communication device to host and store data and applications that require a high degree of security. For example, the secure element may be encrypted and may store payment account information. The secure element may be provided to the mobile communication device by the secure element owner, who may also be the mobile network operator (MNO), original equipment manufacturer (OEM), mobile device manufacturer (MDM), or any other suitable entity. Additionally, the secure element may be either embedded in the handset of the mobile communication device or in a subscriber identity module (SIM) card that may be removable from the mobile communication device. The secure element can also be included in an add-on device such as a micro-Secure Digital (microSD) card or the like.

[0027] An "issuer" may typically refer to a business entity (*e.g.*, a bank) that maintains financial accounts for a user and often issues a credit or debit card to the user. An issuer can include a payment account issuer or other service provider that provisions and personalizes mobile payment applications on a secure element of a mobile device. During provisioning, issuers (and issuer trusted service managers) may ensure that the mobile device is properly configured to allow accountholder purchases using mobile payment applications on the secure element. The issuer may be responsible to make a credit limit available to account holders and may also be responsible for sending payments to merchants for purchases made with payment accounts issued by the issuer.

[0028] As used herein, a "payment account" or a "financial account" (which may be associated with one or more payment devices) may include any suitable payment account including a credit card account, a checking account, a savings account, a merchant account assigned to a accountholder, or a prepaid account.

[0029] A "server computer" or a "server" can be a powerful computer or a cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0030] As used herein, "provisioning information" may include information specific to a memory (e.g., a secure element) of a mobile device that is used by a provisioning system to provision payment account credentials on the mobile device. For example, the provisioning information may include algorithms and/or encryption keys stored by the secure element, a secure element identifier assigned to the secure element, information associated with a secure domain of the secure element, network operator information, user information, trusted service manager information, etc.

[0031] As used herein, "provisioning request message" may include a message sent from a mobile device directly or indirectly to a provisioning system to request provisioning of payment account credentials on the mobile device. The payment account credentials associate the mobile device with a payment account, thereby enabling the mobile device to initiate payment transactions. The

provisioning request message may include provisioning information that would enable the provisioning system to provision payment account credentials on the mobile device.

[0032] As used herein, "provisioning data" may include information that is configured to be installed on a device to allow the device to perform a service or set of functionality. In some embodiments, the provisioning data may be installed on a memory of a device. Further, in some embodiments, the memory may include a secure memory (e.g., a secure element). For example, provisioning data may include data that has been encrypted with a secure element key that may allow a secure element or other secure data to receive and install the data. Alternatively or additionally, the provisioning data may include data that is ready to be provisioned to the secure element. For example, the provisioning data may include application data and a secure element key that may allow a mobile application on the device or the secure element to install or store the application data onto the secure element.

[0033] As used herein, "provisioning response message" may be message sent from a provisioning system to a mobile device to enable provisioning of payment account credentials on the mobile device. The payment account credentials associate the mobile device with a payment account, thereby enabling the mobile device to initiate payment transactions. The provisioning response message may include provisioning data that would enable the mobile device to install the or store the payment account credentials on the secure element.

I. Issuer-Initiated Secure Element Account Provisioning

[0034] Embodiments of the present invention allow an issuer to initiate account provisioning on a secure element of a mobile device without interacting with a user. FIG. 1 shows a block diagram of an exemplary secure element account provisioning system 100 that may be used in connection with issuer-initiated secure element account provisioning described herein. The secure element account provisioning system 100 may include, among other elements, a mobile device 110 (also referred to as a "mobile communication device"), a payment processing network 130 associated with a provisioning service provider computer 120, a device provisioning accountholder authentication system (DPCAS) 140, one or more access

control servers 150, and an issuer server computer 160. The entities may comprise any suitable hardware or software, for example such as those illustrated in FIG. 8, and may communicate with one another through any series of communications networks.

[0035] The mobile device 110 may include any electronic device comprising a secure element or other secure data storage memory that is configured to receive and store secure data. For example, the mobile device 110 may include a smart phone, a tablet device, a smartcard, a cellular phone, or any other device that may be portable, configured to communicate with one or more entities within the transaction processing system (as shown in FIG. 7) as well as the secure element account provisioning system 100, and may be configured to store secure payment credentials for initiating and conducting payment transactions.

[0036] The wallet provider server 120 may include any server computer that may manage, facilitate, and otherwise interact with the mobile device 110 as well as any mobile wallets provided on the mobile device 110, and the payment processing network 130 in order to manage the use and maintenance of a wallet system. For example, the wallet provider server 120 may comprise a secure element trusted service manager (SE TSM) for devices associated with the wallet provider server 120.

[0037] The payment processing network 130 may include data processing subsystems, networks, and operations used to support and deliver 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, and other types of commercial transactions. VisaNet™, in particular includes a Visa Integrated Payments (VIP) system which processes authorization requests and a Base II system which performs clearing and settlement services. Furthermore, the payment processing network 130 may include a server computer and may use any suitable wired or wireless telecommunications network, including the Internet.

[0038] The payment processing network 130 may include or be associated with a provisioning service provider computer 120 (also referred to as a "provisioning system"). The provisioning service provider computer 120 may include any number of systems that may allow the payment processing network 130 to provide provisioning services to merchants, accountholders, mobile devices, etc. The payment processing network 130 and the provisioning service provider computer 120 may provision a financial account on the mobile device 110 upon, for example, the issuer server computer 160 initiating the provisioning of the financial account via communication with the mobile device 110.

[0039] The device provisioning accountholder authentication system (DPCAS) 140 may include any computer or series of computers configured to determine the appropriate authentication system to be implemented for authenticating a provisioning request. According to various embodiments, the provisioning request may be sent by the mobile device 110 in response to a provisioning initiating message sent from the issuer server computer 160 to the mobile device 110. The DPCAS 140 may be configured to return a response to the payment processing network 130 indicating that a provisioning request is approved, declined, or that the authentication server is not sure whether the accountholder is authentic and would like to perform further authentication processes to be sure.

[0040] The DPCAS 140 may be in communication with one or more access control servers 150 to authenticate the accountholder. The one or more access control servers may include any number of different authentication systems that may be operated by the payment processing network 130, the issuer server computer 160, the wallet provider server 120, or any other third party. The different authentication systems that may be implemented may include on-behalf-of (OBO) issuer authentication system, existing accountholder authentication system, or an authentication system that uses the issuer's access control server (ACS).

[0041] The on-behalf-of Issuer authentication service (OBO AS) server may be implemented by the payment processing network 130 and may provide risk-based authentication, using device activation specific rules. These rules may or may

not be issuer-specific, and may be used for issuers that do not have an approved ACS for device activation authentication requests.

[0042] The accountholder authentication system may be implemented from authentication services related to issuer issued accounts (e.g., Verified by Visa (VbV)) payment authentication requests. The accountholder authentication system can allow issuers to specify customized rules for the authentication of accountholders.

[0043] The ACS 150 may be implemented such that the payment processing network 130 may establish new specifications that may be required for the ACS 150 to support device activation authentication requests. An ACS 150 may be selected by the issuer server computer 160 for performing the device activation authentication function.

[0044] Elements of the secure element account provisioning system 100 may interact to provision a financial account (e.g. a payment account) on the secure element of the mobile device 110. FIG. 2 shows the interactions between the issuer server computer 160, the mobile device 110 and the provisioning service provider computer 120 for provisioning the financial account on the secure element of the mobile device 110, according to an embodiment of the invention. The actions of the elements illustrated in FIG. 2 are illustrated in greater detail in FIGs. 3 and 4. Specifically, FIG. 3 shows an exemplary flow diagram for an issuer initiated account provisioning process and FIG. 4 shows another exemplary flow diagram for an issuer initiated account provisioning process, according to embodiments of the present invention. Accordingly, method steps illustrated in FIGs. 3 and 4 are discussed below in connection with FIG. 2.

[0045] Before the exemplary method shown in FIG. 2 may be initiated, the issuer server computer 160 may engage in some transaction or otherwise communicate with an accountholder or someone who has authorization to provide a mobile device identifier to the issuer server computer 160 on behalf of the accountholder. The issuer server computer 160 may receive an identifier for a mobile communication device that allows the issuer server computer 160 to identify and communicate with the mobile device 110 associated with the requested account.

The mobile device identifier may include one or more of a telephone number, a unique device number, such as an international mobile station equipment identity (IMEI) number, a unique serial number (i.e. integrated circuit card identifier (ICCI)) of a subscriber identification module (SIM) card, and a unique international mobile subscriber identity (IMSI) identifier. In some embodiments, the accountholder (e.g. the user) may register their mobile device identifier with the issuer server computer 160 at any time (i.e. irrespective of, and unrelated to, the provisioning of a payment account). The accountholder may perform any other suitable steps to inform the issuer server computer 160 of their mobile communication device identifier. For instance, an authorized person that is not the accountholder (e.g., a spouse) may inform a teller at the bank that their spouse may wish to have their account provisioned on their device and may provide a mobile device identifier to allow the issuer server computer 160 to contact the mobile device 110.

[0046] According to various embodiments, the mobile device 110 may be used to conduct transactions using the accountholder's financial account. In order to do so, the account is provisioned on the mobile device 110. Embodiments of the present application allow the issuer server computer 160 to initiate the provisioning process without any interaction with or input from the accountholder. For example, an executive of the issuer, a customer service representative, a business unit manager or other entity may determine that the financial account is part of a determined accountholder base that should have their account credentials provisioned onto their mobile devices. Based on that determination, the issuer server computer 160 may initiate the provisioning of the financial account on the mobile device 110.

[0047] The issuer server computer 160 may include, among other elements, a provisioning module 212. The provisioning module 212 may generate a provisioning information request message (step 302 of FIG. 3 and step 402 of FIG. 4). The provisioning information request message may include one or more of a provisioning information request message identifier (e.g., a header, a flag, a particular formatting, or any information that allows the mobile device 110 to identify the message as a provisioning information request message), an account identifier (e.g., a primary

account number (PAN), a PAN substitute, a payment token, a pseudo-PAN, or any other credential associated with the accountholder's account), additional account credentials (e.g., CVV, track 2 data, etc.), an authorization code , and a mobile device identifier (e.g., a phone number, SMS text address, an IP address, a MSISDN, or any other information that may be used to identify and contact the mobile device 110 to be provisioned). The mobile device identifier may also include a unique device number, such as an international mobile station equipment identity (IMEI) number, a unique serial number (i.e. integrated circuit card identifier (ICCI)) of a subscriber identification module (SIM) card, or a unique international mobile subscriber identity (IMSI). The issuer server computer 160 may send the provisioning information request message to the mobile device 110 via, for example, an external communication interface 216 (step 304 of FIG. 3 and step 404 of FIG. 4).

[0048] The authorization code in the provisioning information request message may be a re-creatable code that the provisioning service provider computer may use to validate that the provisioning request is authorized and authenticated by, for example, the issuer server computer 160.

[0049] According to various embodiments, the issuer server computer 160 may include an authentication module 212 that authenticates the accountholder prior to generating the provisioning information request message using the provisioning module 214. Upon authenticating the accountholder, the authentication module 212 may generate the authorization code which may be used by the provisioning service provider computer 120 to validate that the provisioning request is authorized and authenticated by the issuer server computer 160. The issuer server computer 160 may also include a system memory 218 and a processor 219 to perform one or more of the actions described herein. An exemplary memory and processor is discussed below in connection with FIG. 8.

[0050] The mobile device 110 illustrated in FIG. 2 may include a secure element 222 that may securely store account credentials to allow the user of the mobile device 110 to securely initiate and process transactions from the mobile device 110 with NFC point-of-sale devices or through e-commerce merchant servers, etc. When the mobile device 110 receives the provisioning information

request message from the issuer server computer 160, the operating system 226 of the mobile device 110 may identify the provisioning information request message indicator included in the provisioning information request message. The identification may occur through any suitable method. For example, the operating system 226 may comprise an identification module that is configured to allow the operating system 226 to identify the provisioning information request message identifier (e.g. a header, a flag, some specific pre-determined message string or content, the specific address of the issuer server computer 160 that sends the provisioning information request message, or any other associated information) indicating that the received message is a provisioning information request message.

[0051] In response to the provisioning information request message, the operating system 226 may gather provisioning information associated with the secure element 222. For example, the operating system 226 may request secure domain information from the secure element 222 for an available domain on the secure element 222. In addition, the operating system 226 may gather or determine accountholder information associated with the mobile device 110, network operator information stored on a system memory 228, trusted service manager (TSM) information, unique derived key (UDK) or other encryption key information, and any other information that may be useful for a provisioning system to provision an account on the secure element 222 of the mobile device 110. Accordingly, the provisioning information may include any data (e.g., secure element identifier, UDK identifier, etc.) that may be provided by the mobile device 110 during a request to provision an account on the mobile device 110. Additional details regarding the provisioning information as well as the other information provided during provisioning requests may be found in U.S. Patent Application No. 13/713,938, filed December 13, 2012, by Makhotin, *et al.*, which is hereby incorporated by reference in its entirety for all purposes.

[0052] After the operating system 226 gathers the provisioning information, the provisioning module 224 of the mobile device 110 may generate a provisioning request message including the provisioning information (step 306 of FIG. 3 and step 406 of FIG. 4). The provisioning request message may also include one or more of

the authorization code, the account identifier, the additional account credentials and the mobile device identifier provided to the mobile device 110 by the issuer server computer 160. The mobile device 110 may send the provisioning request message to the provisioning service provider computer 120 via the external communication interface 227 (step 308 of FIG. 3). The mobile device 110 may also include a processor 229 to perform one or more of the actions described herein. An exemplary processor is discussed below in connection with FIG. 8.

[0053] In some embodiments, the mobile device 110 may send the provisioning request message or just the provisioning information to the issuer server computer 160 in response to the provisioning information request message (step 408 of FIG. 4). The issuer server computer 160 may then send the provisioning information along with one or more of the authorization code, the account identifier, the additional account credentials and the mobile device identifier to the provisioning server provider 120 via the external communication interface 216 (step 409 of FIG. 4).

[0054] According to various embodiments, the provisioning service provider computer 120 may be located in the payment processing network 130 illustrated in FIG. 1 or may include a separate third party provisioning system such as a TSM associated with the mobile network operator, mobile device manufacturer, the issuer server computer 160, or any other third party, or any combination thereof. The provisioning service provider computer 120 may be configured to receive the provisioning request message from the mobile device 110 or the issuer server computer 160 and complete the provisioning process. Any suitable combination of components or systems that are configured to provision the requested account onto the secure element 222 of the mobile device 110 may be included in the provisioning service provider computer 120.

[0055] Upon receiving the provisioning request message, the provisioning service provider computer 120 may authenticate the accountholder information using a validation module 232 (step 310 of FIG. 3 and step 410 of FIG. 4). For example, the validation module 232 may validate the authorization code generated by the authentication module 212 of the issuer server computer 160 to ensure that the

mobile device 110 is authorized by the issuer server computer 160 to be provisioned. In some embodiments, the DPCAS 140 and ACS controllers 150 shown in FIG. 1 may be used to implement an advanced authentication of the accountholder. If the validation module 232 determines that the authorization code, the account identifier or the additional account credentials do not match with the information stored and/or accessed by the provisioning service provider computer 120, the provisioning process may be terminated. Similarly, if some risk data at the provisioning service provider computer 120 requires advanced authentication of the accountholder, the provisioning process may be paused or terminated. Details regarding the advanced authentication process and other exemplary methods of provisioning account data onto a mobile communication device may be found in U.S. Patent Application No. 14/455,600, filed August 8, 2014, by Karpenko, *et al.*, which is hereby incorporated by reference in its entirety for all purposes.

[0056] The generation of and subsequent validation of the authentication code may occur in any suitable manner. For example, an authentication code may be generated by the authentication module in the issuer server using a number of data inputs and a hashing algorithm to obtain the authorization code. The validation module of the provisioning service provider computer can then create the authentication code using the data inputs. Such data inputs may be associated with the transaction or the account. Exemplary data inputs may include an account number, a CVV, home address, date, time, phone identifier information such as a SIM card number, IMEI number, etc., and name, as well as other data elements in this application. In another example, the issuer server and the provisioning service provider computer may share a secret encryption key. The issuer server may concatenate and encrypt data inputs such as those above using the encryption key and an encryption algorithm to form the authentication code. The authentication code could be decrypted by the provisioning service provider computer using the secret encryption key and the associated encryption algorithm.

[0057] If the provided information is validated by the validation module 232, the provisioning service provider computer 120 may provision the accountholder's payment account on the secure element 222 of the mobile device 110 (step 312 of

FIG. 3 and step 412 of FIG. 4). For example, the provisioning service provider computer 120 may send a provisioning response message to the mobile device 110 via an external communication interface 236. The provisioning response message may provision the accountholder's payment account on the secure element 222 of the mobile device 110 (step 314 of FIG. 3 and step 414 of FIG. 4). As illustrated in FIG. 2, the provisioning service provider computer 120 may also include a system memory 238 and a processor 239 to perform one or more of the actions described herein. An exemplary memory and processor is discussed below in connection with FIG. 8.

[0058] Additional details regarding some potential implementations of the provisioning service provider computer 120 and details of the provision information, provisioning data, encryption steps, and key management can be found in U.S. Patent Application No. 13/713,938, filed December 13, 2012, by Makhotin, *et al.*, which is hereby incorporated by reference in its entirety for all purposes.

II. Exemplary Methods

[0059] FIG. 5 shows an exemplary method 500 performed by a mobile device for provisioning a financial account on a secure element of the mobile device, according to an embodiment of the invention. At 502, the mobile device comprising the secure element receives a provisioning information request message from an issuer. In some embodiments, the provisioning information request message may be encrypted with an issuer provisioning service key or other shared encryption key pair to ensure that the provisioning information request message may not be intercepted by a malicious third party. If the message is encrypted, the mobile device may decrypt the message upon receipt. The provisioning information request message may include one or more of an authorization code, an account identifier and a mobile device identifier. The mobile device may receive the provisioning information request message using any communication network or communication protocol. For example, the provisioning information request message may include a text message, an email, an over-the-air (OTA) communication message, or any other message that the mobile device may receive. In some embodiments, the provisioning information request message may include an identifier. An operating

system of the mobile device may identify that the received message is a provisioning information request message based on the identifier and without the user (or the accountholder) having to identify the message as such. According to various embodiments, the mobile device may not even display the provisioning information request message to the user.

[0060] Once the mobile device identifies the provisioning information request message, the operating system of the mobile communication device may gather or determine provisioning information associated with the secure element and the mobile communication device without the input of the user operating the mobile device (step 504). At step 506, the mobile device generates a provisioning request message including the gathered/determined provisioning information. The provisioning request message may also include one or more of the authorization code, the account identifier and a mobile communication device identifier (e.g., phone number, MSISDN, etc.) that may allow a provisioning system to determine the appropriate mobile communication device and the associated secure element on which to provision the account credentials. Further, the provisioning request message may be encrypted with an encryption service key to ensure that the provisioning request may not be intercepted by a malicious third party.

[0061] At step 507, the mobile device may send the provisioning request message to the issuer or to a provisioning system (i.e. provisioning service provider computer). If the provisioning request message is sent to the issuer in response to the provisioning information request message, the issuer may send the provisioning request message to the provisioning system.

[0062] When the provisioning system receives the provisioning request message including the authorization code, the provisioning information, and the accountholder account credentials (e.g., PAN, payment token, CVV, any other track 1 or track 2 data associated with the payment account, etc.), the provisioning system may validate the authorization code to ensure the mobile device is authorized to be provisioned by the issuer. The validation of the authorization code may be completed in any suitable manner. For example, in some embodiments, the provisioning system and the issuer server computer may share a unique secret key

or secret algorithm that allows the provisioning system to generate another authorization code and compare the received authorization code to the generated authorization code to ensure they are the same and thus, that the authorization code must have come from the issuer server computer as the issuer is the other party that knows the unique secret key or secret algorithm. Alternatively, the provisioning system may contact the issuer server computer to obtain authorization and/or validate the authorization code is associated with the mobile device requesting the account provisioning. Any other suitable validation technique may be implemented to allow the provisioning system to ensure that the provisioning request message is associated with the correct account, the correct mobile device, and that the issuer server computer has requested or initiated the account provisioning.

[0063] Once the authorization code has been validated to confirm that the mobile device is authorized to have the payment account credentials provisioned onto the secure element of the mobile device, the provisioning system uses the received provisioning information, mobile communication device identifier, account credentials, and any other information associated with the request to generate a provisioning response message including account provisioning data. The account provisioning data may be traditional provisioning data that one of ordinary skill in the art may recognize. The provisioning system may send the provisioning response message to the mobile device.

[0064] At step 510, the mobile device may receive the provisioning response message including the provisioning data. In some embodiments, the account provisioning data may be generated using a unique derived key (UDK) or other encryption key that is associated with a mobile payment application stored on the secure element such that the secure element or the mobile payment application may decrypt the account provisioning data and store the account provisioning data onto the secure element. One or more software modules or applets on the mobile device and/or the secure element may identify the provisioning data as being a provisioning response directed at the secure element and may operate to provision the provisioning data onto the secure element. Accordingly, the secure element may now comprise the payment account credentials associated with the payment account

and may be configured to initiate and complete transactions using an NFC communications chip, e-commerce transactions, or any other secure payment processes from the mobile device.

[0065] Accordingly, the payment account that may be used in a payment transaction is provisioned on the mobile device without any user input, knowledge, or affirmative action by the mobile device operator. In some embodiments, the accountholder or mobile communication device operator may be notified as to the status of the process or that the process is being completed, but such notification is optional and in other embodiments, no such notification may be given. Embodiments of the present invention enable an issuer to automatically and seamlessly provision a payment account onto an authorized mobile device.

[0066] FIG. 6 shows exemplary steps performed by the issuer for initiating the provisioning of a financial account on a mobile device, according to an embodiment of the invention. At step 602, the issuer authenticates a user associated with a user payment account. At step 604, the issuer may receive a mobile device identifier associated with a mobile device of the user. As provided above, the mobile device identifier may include one or more of a telephone number, a unique device number, such as an international mobile station equipment identity (IMEI) number, a unique serial number (i.e. integrated circuit card identifier (ICCI)) of a subscriber identification module (SIM) card, and a unique international mobile subscriber identity (IMSI) identifier.

[0067] The issuer may not have access to provisioning information associated with a secure element of the mobile device. Without the provisioning information, the issuer cannot provision (or request a provisioning service to provision) the financial account on the mobile device. According to various embodiments, the issuer may request the provisioning information from the mobile device instead of a third party such as a mobile network operator. The issuer may either request the provisioning information from the mobile device and send the provisioning information to a provisioning system, or automatically cause the mobile device to determine/gather the provisioning information and send the provisioning information directly to the provisioning system.

[0068] At step 606, the issuer server computer generates a provisioning information request message to the accountholder's mobile device without interacting with the accountholder. The provisioning information request message may include one or more of an authorization code, an account identifier, the mobile device identifier and a provisioning information request identifier (e.g. a header) that identifies the message to the recipient mobile device as a provisioning information request message. In some embodiments, the provisioning information request message may be encrypted with an issuer provisioning service key or other shared encryption key pair to ensure that the provisioning request may not be intercepted by a malicious third party.

[0069] At 608, the issuer may send the provisioning information request message to the mobile device of the user to initiate the provisioning of the payment account on the mobile device. According to various embodiments, the provisioning information request message may be sent using any communication network or communication protocol. For example, the provisioning information request message may include a text message, email, over-the-air (OTA) communication message, or any other message that the mobile device may receive.

III. Exemplary Systems

[0070] Provided below is a description of an exemplary system in which embodiments provided herein may be utilized. Although some of the entities and components may be depicted as separate, in some instances, one or more of the components may be combined into a single device or location (and vice versa). Similarly, although certain functionality may be described as being performed by a single entity or component within the system, the functionality may in some instances be performed by multiple components and/or entities (and vice versa). Communication between entities and components may comprise the exchange of data or information using electronic messages and any suitable electronic communication medium and method, as described below. The system may be used to perform a process for using a mobile device with a provisioned account identifier such as a PAN or a payment token. The process for using a mobile device with a

provisioned account identifier is discussed subsequently to the discussion of the system.

[0071] As used herein, an "issuer" may typically refer to a business entity (*e.g.*, a bank or other financial institution) that maintains financial accounts for the user and often issues a payment device such as a credit or debit card to the user. As used herein, a "merchant" may typically refer to an entity that engages in transactions and can sell goods or services to the user. As used herein, an "acquirer" may typically refer to a business entity (*e.g.*, a commercial bank or financial institution) that has a business relationship with a particular merchant or similar entity. Some entities can perform both issuer and acquirer functions.

[0072] An exemplary financial transaction system is shown in FIG. 7. The system 720 may include one or more merchants 722, one or more access devices 734, one or more acquirers 724, and one or more issuers 728. For example, the system 720 may include a merchant having a merchant computer 722 that comprises an external communication interface (*e.g.* for communicating with an access device 734 and an acquirer 724), system memory comprising one or modules to generate and utilize electronic messages, and a data processor (for facilitating a financial transaction and the exchange of electronic messages); an acquirer having an acquirer computer 724 that comprises an external communication interface (*e.g.* for communicating with a merchant computer 722 and a payment processing network 726), system memory comprising one or modules to generate and utilize electronic messages, and a data processor (for facilitating a financial transaction and the exchange of electronic messages); and an issuer having an issuer server computer 728 that comprises an external communication interface (*e.g.* for communicating with a payment processing network 726), system memory comprising one or modules to generate and utilize electronic messages, and a data processor (for facilitating a financial transaction and the exchange of electronic messages). The external communication interface of the merchant computer 722 may be coupled to an access device 734 (such that information may be received by the access device 734 and communicated to the merchant computer 722) or, in

some embodiments, the access device 734 may comprise a component of the merchant computer 722.

[0073] As used in this context, an "external communication interface" may refer to any hardware and/or software that enables data to be transferred between two or components of system 720 (*e.g.,* between devices residing at locations such as an issuer, acquirer, merchant, payment processing network 726, etc.). Some examples of external communication interfaces may include a modem, a network interface (such as an Ethernet card), a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. Data transferred via external communications interface may be in the form of signals which may be electrical, electromagnetic, optical, or any other signal capable of being received by the external communications interface (collectively referred to as "electronic signals" or "electronic messages"). These electronic messages that may comprise data or instructions may be provided between one or more of the external communications interface via a communications path or channel. As noted above, any suitable communication path or channel may be used such as, for instance, a wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, a WAN or LAN network, the Internet, or any other suitable method.

[0074] As would be understood by one of ordinary skill in the art, any suitable communications protocol for storing, representing, and transmitting data between components in the system 720 may be used. Some examples of such methods may include utilizing predefined and static fields (such as in core TCP/IP protocols); "Field: Value" pairs (*e.g.* HTTP, FTP, SMTP, POP3, and SIP); an XML based format; and/or Tag-Length-Value format.

[0075] As shown in the exemplary system 720 in FIG. 7, payment account information from mobile device 736 may be provided to access device 734, for example, through a contact or contactless interface . In some embodiments, the mobile device 736 may interact with the payment processing network 726 (or other entity in the system 720) via network 740 (such as the Internet).

[0076] A payment processing network 726 may be disposed between the acquirer computer 724 and the issuer server computer 728 in the system 720.

Furthermore, the merchant computer 722, the acquirer computer 724, the payment processing network 726, and the issuer server computer 728 may all be in operative communication with each other (*i.e.* although not depicted in FIG. 7, one or more communication channels may exist between each of the entities, whether or not these channels are used in conducting a financial transaction).

[0077] The payment processing network 726 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the payment processing network 726 may comprise a server computer, coupled to a network interface (*e.g.* by an external communication interface), and a database(s) of information. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The payment processing network 726 may use any suitable wired or wireless network, including the Internet.

[0078] Although many of the data processing functions and features of some embodiments may be present in the payment processing network 726 (and a server computer therein), it should be understood that such functions and features could be present in other components such as the issuer server computer 728, and need not be present in the payment processing network 726, or a server computer therein.

[0079] Using the mobile device 736 (which is provisioned with an account identifier such as a PAN or a payment token), the user may initiate a payment transaction with the merchant computer 722, through the access device 734. An illustrative method for an exemplary financial transaction is described below. The method described below is exemplary in nature, and are not intended to be limiting. Methods in accordance with some embodiments described herein may include (or omit) some or all of the steps described below, and may include steps in a different order than described herein.

[0080] A user presents his or her mobile device 736 to the access device 734 to pay for an item or service. The mobile device 736 and the access device 734 interact

such that information from the mobile device 736 (*e.g.* PAN, verification value(s), expiration date, etc.) is received by the access device 734 (*e.g.* via contact or contactless interface). The merchant computer 722 may then receive this information from the access device 734 via the external communication interface. The merchant computer 722 may then generate an authorization request message that includes the information received from the access device 734 (i.e. information received from the mobile device 736) along with additional transaction information (*e.g.* a transaction amount, merchant specific information, etc.). The merchant computer 722 may electronically transmit this information to the acquirer computer 724. The acquirer typically represents, and vouches for, the merchant in financial transactions (*e.g.* credit card transactions). The acquirer computer 724 may then receive (via its external communication interface), process, and forward the authorization request message to the payment processing network 726.

[0081] The payment processing network 726 may have an established protocol with each issuer on how the issuer's transactions are to be authorized. In some cases, such as when the transaction amount is below a threshold value, the payment processing network 726 may be configured to authorize the transaction based on information that it has about the user's account without generating and transmitting an authorization request message to the issuer server computer 728. In other cases, such as when the transaction amount is above a threshold value, the payment processing network 726 may receive the authorization request message via its external communication interface, determine the issuer associated with the payment account, and forward the authorization request message for the transaction to the issuer server computer 728 for verification and authorization. As part of the authorization process, the payment processing network 726 or issuer server computer 728 may analyze a verification value or other datum provided by the mobile device 736. The verification value may be stored at issuer server computer 728 or the payment processing network 726. Once the transaction is authorized, the issuer server computer 728 may generate an authorization response message (that may include an authorization code indicating the transaction is approved or declined) and transmit this electronic message via its external communication interface to the payment processing network 726. The payment processing network 726 may then

forward the authorization response message via a communication channel to the acquirer computer 724, which in turn may transmit the electronic message to comprising the authorization indication to the merchant computer 722.

[0082] 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. 1-7, including any servers or databases, may use any suitable number of subsystems to facilitate the functions described herein.

[0083] Examples of such subsystems or components are shown in FIG. 8. The subsystems shown in FIG. 8 are interconnected via a system bus 800. Additional subsystems such as a printer 808, keyboard 816, fixed disk 818 (or other memory comprising computer readable media), monitor 812, which is coupled to display adapter 810, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 802 (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 814. For example, serial port 814 or external interface 820 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 806 to communicate with each subsystem and to control the execution of instructions from system memory 804 or the fixed disk 818, as well as the exchange of information between subsystems. The system memory 804 and/or the fixed disk 818 may embody a computer readable medium.

[0084] 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++ 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.

[0085] 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.

[0086] 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.

[0087] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0088] 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.

WHAT IS CLAIMED IS:

1. A method comprising:

issuing, by an issuer server computer of an issuer, a user payment account to a user;

authenticating, by the issuer server computer, the user associated with the user payment account;

receiving, by the issuer server computer, a mobile device identifier identifying a mobile device of the user;

generating, by the issuer server computer, a provisioning information request message without interacting with the user, the provisioning information request message including at least the mobile device identifier and a provisioning information request identifier, wherein the provisioning information request identifier automatically causes the mobile device to gather provisioning information associated with a secure memory of the mobile device without interacting with the user; and

sending, by the issuer server computer, the provisioning information request message to the mobile device, wherein the provisioning information request message initiates provisioning of the user payment account on the mobile device of the user.

2. The method of claim 1, wherein the provisioning information request message further includes one or more of an authorization code and an account identifier.

3. The method of claim 1 or 2, further comprising:

generating, by the issuer server computer, an authorization code indicating that the user is authenticated by the server computer; and

incorporating the authorization code in the provisioning information request message.

4. The method of any one of claims 1 to 3, further comprising:

receiving, by the issuer server computer, the provisioning information from the mobile device;

generating, by the issuer server computer, a provisioning request message including at least the provisioning information and the mobile device identifier; and

sending, by the issuer server computer, the provisioning request message to a provisioning entity responsible for provisioning the user payment account on the mobile device of the user.

5. The method of claim 4, further comprising:

generating, by the issuer server computer, an authorization code indicating that the user is authenticated by the server computer; and

incorporating the authorization code in the provisioning request message.

6. An issuer server computer of an issuer that issued a payment account to a user comprising: a processor; and

a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code, that when executed by the processor, causes the processor to:

send an information request message to a mobile communication device, the information request message requesting provisioning information associated with a secure memory of the mobile communication device;

receive a response message including the provisioning information from the mobile communication device, wherein the provisioning information is automatically gathered by the mobile communication device in response to the information request message and without input of a user operating the mobile communication device; and

send a provisioning request message to a provisioning system such that provisioning data can be sent to the mobile communication device for associating the mobile communication device with a payment account, wherein the provisioning request message includes the provisioning information, and one or more of an account identifier and a mobile device identifier associated with the mobile communication device.

7. The issuer server computer of claim 6, wherein the provisioning information associated with the secure memory includes one or more of secure domain information, network operator information, user information, trusted service manager information and encryption key information.

8. The issuer server computer of claim 6, wherein the provisioning data includes a primary account number or a payment token.

9. The issuer server computer of claim 6, wherein the code, when executed by the processor, further causes the processor to:

generate an authorization code indicating that the provisioning request message associated with the authorization code is authorized and authenticated by the issuer server computer; and

include the authorization code in the provisioning request message.

10. A method comprising:

sending, by an issuer server computer of an issuer that issued a payment account to a user, an information request message to a mobile communication device, the information request message requesting provisioning information associated with a secure memory of the mobile communication device;

receiving, by the issuer server computer, a response message including the provisioning information from the mobile communication device, wherein the provisioning information is automatically gathered by the mobile communication device in response to the information request message and without input of a user operating the mobile communication device; and

sending, by the issuer server computer, a provisioning request message to a provisioning system such that provisioning data can be sent to the mobile communication device for associating the mobile communication device with the payment account, wherein the provisioning request message includes the provisioning information, and one or more of an account identifier and a mobile device identifier associated with the mobile communication device.

11. The method of claim 10, wherein the provisioning information associated with the secure memory includes one or more of secure domain

information, network operator information, user information, trusted service manager information and encryption key information.

12. The method of claim 10, wherein the provisioning data includes a primary account number or a payment token.

13. The method of claim 10, further comprising:

generating, by the server computer, an authorization code indicating that the provisioning request message associated with the authorization code is authorized and authenticated by the issuer server computer; and

including, by the issuer server computer the authorization code in the provisioning request message.