CLOUD-BASED TRANSACTIONS METHODS AND SYSTEMS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority to U.S. Provisional Application No. 61/918,643, filed on December 19, 2013, U.S. Provisional Application No. 61/941,227, filed on February 18, 2014, U.S. Provisional Application No. 61/982,169, filed on April 21, 2014, and U.S. Provisional Application No. 61/983,635, filed on April 24, 2014, which are all herein incorporated by reference in their entirety for all purposes.

BACKGROUND

[0002] Advances in the capabilities of portable communication devices have allowed portable communication devices such as smart phones to be used as payment instruments to conduct contactless transactions. For example, a portable communication device can be placed in proximity to an access device such as a point-of-sale (POS) terminal to transfer account information from the portable communication device to the access device to conduct a transaction. To provide a secure operating environment to securely store account information on a portable communication device, a secure element such as subscriber identity module (SIM) card, specialized integrated chip embedded into the portable communication device, or specialized component provided as aftermarket solution is used. At the time of a transaction, the secure element communicates directly with a contactless interface (e.g., a near-field communication (NFC) transceiver) of the portable communication device to pass payment data to a contactless reader of the access device. A secure element is considered secure because account information is stored in tamper-resistant hardware, which protects the account information from malware or viruses that may have infected the operating system or an application running on the portable communication device.

[0003] However, a secure element used in a portable communication device is typically not under the control of a financial institution, but is instead under the control of a mobile network operator (MNO). As a result, an issuer and/or payment processor may not have direct access to a secure element to provision it with account credentials and payment functionalities. In order to gain access to a secure element, an issuer and/or payment processor may have to establish commercial agreements and technical connectivity with the party controlling the secure element to perform over-the-air (OTA) personalization of the secure element. This is both a cumbersome and complex process. Furthermore, incorporating a secure element adds to the manufacturing cost of the portable communication device, and increases the cost of the finished portable communication device.

[0004] Thus, in some cases, it would be desirable to use a portable communication device that does not have a secure element to make payments. Or, if the portable communication device does have a secure element, it may be desirable not to rely on the use of the secure element. However, because a secure element is not used, transaction security will be a concern.

[0005] Embodiments of the present invention address these and other problems individually and collectively. Specifically, embodiments of the invention address the problem of security concerns with conducting payment transactions with a mobile communication device that does not have or does not rely on a secure element.

BRIEF SUMMARY

[0006] Embodiments of the present invention provide techniques for enhancing the security of a communication device (e.g., a portable communication device) when conducting a transaction using the communication device. The techniques described herein can be used with a communication device that may or may not have a secure element, because the techniques do not require the use of a secure element to safeguard account credentials. Embodiments of the invention instead utilize limited-use account parameters that may have a limited lifespan, and once expired, may no longer be used to conduct a transaction until the limited-use account parameters are replenished from the cloud (e.g., a remote computer). Hence, transactions conducted using the techniques described herein may be referred to as "cloud-based transactions."

[0007] According to an aspect, there is provided a method for enhancing the security of a communication device when conducting a transaction using the communication device that may include receiving, from a remote computer, a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limits usage of the LUK, wherein the LUK is usable for more than one transaction; generating, by the communication device, a transaction cryptogram using the LUK, sending, by the communication device to an access device, a token instead of a real account identifier and the transaction cryptogram to conduct the transaction, wherein the transaction can be authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds, sending, to the remote computer, a replenishment request for a second LUK, the replenishment request including transaction log information derived from a transaction log stored on the communication device, the transaction log storing transaction data for a plurality of transactions conducted using the first LUK, and receiving, from the remote computer, the second LUK when the transaction log information in the replenishment request matches transaction log information at the remote computer.

[0008] Disclosed herein is a communication device that may include a processor; and a memory coupled to the processor and storing a mobile application that performs operations for enhancing security of the communication device when conducting transactions using the communication device. The operations may include receiving a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limits usage of the LUK, generating a transaction cryptogram using the LUK, and sending a token instead of a real account identifier and the transaction cryptogram to conduct the transaction. The transaction may be authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds.

[0009] Disclosed herein is a method for enhancing the security of a communication device when conducting a transaction using the communication device that may include encrypting, by a computer, account information with a first encryption key to generate a second encryption key, and encrypting key index information using the second key to generate a limited-use key (LUK), where the key index information includes a key index having information pertaining to generation of the LUK. The method may also include providing the LUK and the key index to the communication device to facilitate generation of a transaction cryptogram for a transaction conducted using the communication device. The transaction can be authorized based on the LUK and the transaction cryptogram.

[0010] Disclosed herein is a computer for enhancing the security of a communication device when conducting a transaction using the communication device that may include a processor, and a memory storing computer readable code, which when executes by the processor, causes the computer to encrypt account information with a first encryption key to generate a second encryption key, encrypting key index information using the second key to generate a limited-use key (LUK), and provide the LUK and the key index to the communication device to facilitate generation of a transaction cryptogram for a transaction conducted using the communication device. The key index information may include a key index having information pertaining to generation of the LUK. The transaction can be authorized based on the LUK and the transaction cryptogram.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 illustrates a block diagram of an example of a cloud-based transaction system, according to some embodiments.

[0012] FIG. 2 illustrates a communication flow diagram of an example of an enrollment and provisioning process, according to some embodiments.

[0013] FIG. 3 illustrates a communication flow diagram of an example of executing an integrated chip based transaction, according to some embodiments.

[0014] FIG. 4 illustrates a communication flow diagram of an example of executing a magnetic stripe based transaction, according to some embodiments.

[0015] FIG. 5 illustrates an example of a transaction verification log, according to some embodiments.

[0016] FIG. 6 illustrates a communication flow diagram of an example of a post-payment verification process, according to some embodiments.

[0017] FIG. 7 illustrates a communication flow diagram of an example of an account parameters replenishment process, according to some embodiments.

[0018] FIG. 8 illustrates an example of a process for generating a transaction cryptogram, according to some embodiments.

[0019] FIG. 9 illustrates an example of an encryption function, according to some embodiments.

[0020] FIG. 10 illustrates a flow diagram of an example of a method for enhancing the security of a portable communication device, according to some embodiments.

[0021] FIG. 11 illustrates a flow diagram of an example of another method for enhancing the security of a portable communication device, according to some embodiments.

[0022] FIG. 12 illustrates a block diagram of an example of a portable communication device, according to some embodiments.

[0023] FIG. 13 illustrates a state diagram of an example of a mobile application in manual mode, according to some embodiments.

[0024] FIG. 14 illustrates a state diagram of an example of a mobile application in always-on mode, according to some embodiments.

[0025] FIG. 15 illustrates a state diagram of an example of a mobile application in always-on mode with on-device verification, according to some embodiments.

[0026] FIG. 16 illustrates a block diagram of an example of a computer system, according to some embodiments.

DETAILED DESCRIPTION

[0027] Embodiments of the present invention provide for methods, devices, and systems for cloud-based transactions that can be performed by a communication devices with or without a secure element. The techniques described herein can utilize card emulation technology (e.g., Host Card Emulation (HCE), etc.) to emulate a smartcard on a communication device (e.g., a portable communication device) to allow a mobile application running on the portable communication device to conduct contactless transactions. In the card emulation environment, a mobile application can access the contactless interface (e.g., a near-field communication (NFC) transceiver) of the portable communication device via the operating system (OS) of the portable communication device without involving a secure element. As compared to secure element implementations, the card emulation approach reduces the technical and commercial complexities for issuers and/or payment processors, because issuers and/or payment processors can provision account credentials and payment functionalities to a mobile application on a portable communication device

without having to obtain access to a secure element through a mobile network operator.

[0028] By removing the control of payment functionalities and account credentials from the confines of a secure element, the tamper-resistant hardware based security provided by a secure element can no longer be relied on to safeguard account information. Without the requirement that a secure element be present, account credentials may be stored in a memory of the portable communication device that is not part of a secure element, such as the general memory of the portable communication device. As such, the account credentials may be susceptible to access by malware or viruses that may have infected an application or operating system of the portable communication device.

[0029] To enhance the security of a portable communication device when conducting transactions without utilizing a secure element, instead of using stagnant account credentials stored on a portable communication device which may be valid for the lifetime of an account, the cloud-based techniques described herein provision a portable communication device with limited-use account parameters that have a limited usage or lifespan. When the limited usage or lifespan of the limited-use account parameters is exhausted, the same set of limited-use account parameters may no longer be used to conduct further transactions. In order to conduct further transactions using the portable communication device, new limited-use account parameters are replenished to the portable communication device. The limited-use account parameters provided to the portable communication device can be renewed or replenished from the network (also be referred to as the "cloud") repeatedly during the lifetime of an account. By managing the delivery and lifecycle of the limited-use account parameters between a set of network based capabilities and the portable communication device, the compromise of mobile application software and/or account credentials stored on a portable communication device becomes only a limited security risk, because stolen limited-use account parameters can at most be used for only a small number of transactions or limited monetary amount.

[0030] Prior to discussing the details of some embodiments of the present invention, description of some terms may be helpful in understanding the various embodiments.

[0031] A "communication device" may be a device that includes one or more electronic components (e.g., an integrated chip) that can communicate with another device. A "portable communication device" be a communication device that can be transported and operated by a user. A portable communication device may provide remote communication capabilities to a network. The portable communication device can be configured to transmit and receive data or communications to and from other devices. A portable communication device may be in the form of a mobile device such as a mobile phone (e.g., smart phone, cellular phone, etc.), tablets, portable media player, personal digital assistant devices (PDAs), wearable computing device (e.g., watch), electronic reader device, etc., or in the form of a card (e.g., smart card) or a fob, etc. Examples of portable communication devices may also include portable computing devices (e.g., laptops, netbooks, ultrabooks, etc.).

[0032] A "server computer" may include a powerful computer or 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. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0033] An "issuer" may typically refer to a business entity (e.g., a bank) that maintains an account for a user that is associated with a portable communication device such as an account enrolled in a mobile application installed on a portable communication device. An issuer may also issue account parameters associated with the account to a portable communication device. An issuer may be associated with a host system that performs some or all of the functions of the issuer on behalf of the issuer.

[0034] A "merchant" may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0035] An "acquirer" may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers.

[0036] An "access device" may be any suitable device for communicating with a merchant computer or payment processing network, and for interacting with a payment device, a user computer apparatus, and/or a user mobile device. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a portable communication device. In some embodiments, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a portable communication device.

[0037] An "authorization request message" may be an electronic message that is sent to request authorization for a transaction. The authorization request message can be sent to a payment processing network and/or an issuer of a payment card. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include information that can be used to identify an account. An authorization request message may also comprise additional data elements such as one or more of a service code, an expiration date, etc. An authorization request message may also comprise 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 information that identifies the access device that generated the authorization request message, information about the location of the access device, etc.

[0038] An "authorization response message" may be an electronic message reply to an authorization request message. The authorization response message can be generated by an issuing financial institution or a payment processing network. 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 a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant computer that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0039] The term "authentication" and its derivatives may refer to a process by which the credential of an endpoint (including but not limited to applications, people, devices, processes, and systems) can be verified to ensure that the endpoint is who they are declared to be.

[0040] The term "verification" and its derivatives may refer to a process that utilizes information to determine whether an underlying subject is valid under a given set of circumstances. Verification may include any comparison of information to ensure some data or information is correct, valid, accurate, legitimate, and/or in good standing.

[0041] A "token" may include a substitute identifier for some information. For example, a payment token may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For instance, a token may include a series of alphanumeric characters that may be used

as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction. The token may also be used to represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0042] A "real account identifier" may include an original account identifier associated with a payment account. For example, a real account identifier may be a primary account number (PAN) issued by an issuer for a card account (e.g., credit card, debit card, etc.). For instance, in some embodiments, a real account identifier may include a sixteen digit numerical value such as "4147 0900 0000 1234." The first six digits of the real account identifier (e.g., "414709"), may represent a real issuer identifier (BIN) that may identify an issuer associated with the real account identifier.

[0043] "Account parameters" may refer to information relating to an account that can be used to conduct a transaction on the account. Examples of account parameters may include information that can be used to identify an account of the user (e.g., real account identifier, alternate account identifier, token, etc.), data or information relating to the status of the account, one or more keys that are used to generate cryptographic information, data or information relating to the one or more keys, etc. An account parameter can be semi-static or dynamic. A dynamic account parameter may be an account parameter that has a limited lifespan, and which once expired, can no longer be used to conduct a transaction until the account parameter is replenished, refreshed, or renewed. A dynamic account parameter may be replenished frequently during the lifetime of an account. A semi-static account parameter may be an account parameter that has an extended lifespan that is longer

than a dynamic account parameter, and can be replenished less frequently than a dynamic account parameter or not at all during the lifetime of the account.

[0044] A "key" may refer to a piece of information that is used in a cryptographic algorithm to transform input data into another representation. A cryptographic algorithm can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc.

[0045] A "cryptogram" may refer to an encrypted representation of some information. A cryptogram can be used by a recipient to determine if the generator of the cryptogram is in possession of a proper key, for example, by encrypting the underlying information with a valid key, and comparing the result to the received cryptogram.

[0046] A "limited-use threshold" may refer to a condition that limits the usage of a piece of information. A limited-use threshold may be exceeded or exhausted when the underlying condition is met. For example, a limited-use threshold may include a time-to-live that indicates an amount of time for which a piece of information is valid, and once that amount of time has elapsed, the limited-use threshold is exceeded or exhausted, and the piece of information may become invalid and may no longer be used. As another example, a limited-use threshold may include a number of times that a piece of information can be used, and once the piece of information has been used for that number of times, the limited-use threshold is exceeded or exhausted, and the piece of information may become invalid and may no longer be used.

[0047] Details of some embodiments of the present invention will now be described.

[0048] I. ACCOUNT PARAMETERS

[0049] The cloud-based transactions system according to some embodiments provides a set of functionalities to manage the deployment and usage of account parameters for transactions conducted using a portable communication device. Account parameters (may also be referred to as "account credentials") are

information relating to an account (e.g., a financial account, bank account, payment account, etc.) associated with a user that can be used to conduct transactions on the user's account. The account parameters can be provided or provisioned to a portable communication device to enable the portable communication device to conduct transactions on the user's account (e.g., by placing the portable communication device in proximity to a contactless reader of an access device such as a point-of-sale (POS) terminal).

[0050] Account parameters may include a semi-static set of data and a dynamic set of data, and some or all of the account parameters may be limited-use account parameters. The semi-static set of data may include an identifier that can be used to identify an account associated with the user (e.g., an account identifier such as a primary account number (PAN), an alternate account identifier such as an alternate PAN, or a token that is a substitute for an account identifier, etc.), an expiry date, and/or other account details or data that does not necessarily change for an extended period of time, or in some embodiments, for the lifetime of the account. The dynamic set of data may include one or more keys, information associated with the one or more keys, and/or other dynamic data that has a limited lifespan, and are repeatedly refreshed or replenished during the lifetime of an account. The dynamic set of data can be used for or relates to on-device generation of dynamic transaction cryptograms, or represent dynamic transaction data during payment transactions.

[0051] The dynamic set of data may be limited-use in the sense that the dynamic set of data can be used for only a limited time or a limited number of transactions, and may need to be renewed, refreshed, updated, or replenished when the dynamic set of data has exhausted its limited usage. For example, the dynamic set of data may include a limited-use key (LUK) that is used as an encryption key to generate a transaction cryptogram during a transaction. The LUK may be associated with a set of one or more limited-use thresholds that limits the usage of the LUK, where once the usage of the LUK has exhausted or exceeded the set of one or more limited-use thresholds, a further transaction conducted using that LUK will be declined even if the underlying account is still in good standing. The set of one or more limited-use thresholds to enforce can be determined, for example, by an issuer of the account or by a cloud-based payments platform that provides the cloud-based transaction service.

[0052] The set of one or more limited-use thresholds may include at least one of a time-to-live indicating the duration of time for which the LUK is valid, a predetermined number of transactions for which the LUK is valid, and/or a cumulative transaction amount indicating the total transaction amount summed across one or more transactions for which the LUK is valid, or any combination thereof. For example, a LUK may be valid for a time-to-live of five days, and a transaction conducted using that LUK after five days have elapsed since the LUK was generated may be declined. As another example, a LUK may be valid for a predetermined number of five transactions, and a sixth transaction (and any subsequent transaction) conducted using that LUK may be declined. As a further example, a LUK may be valid for a cumulative transaction amount of five hundred dollars, and a transaction conducted using the LUK after that LUK has already been used for transactions totaling more than five hundred dollars may be declined.

[0053] It should be understood that the limited usage values described above are just examples, and that other usage limits can be used. For example, the number of transactions usage limit can be set to a number in the range of 2 to 10 transactions, or a number in the range of 5 to 50 transactions, etc., and the cumulative transaction amount can be set to a value in the range of $100 to $5,000, or a value in the range of $10 to $1000, etc.

[0054] It should also be noted that in some embodiments, the number of transactions limited-use threshold can be set to one transaction such each LUK is valid for only one transaction. However, in some embodiments, the network bandwidth available to a portable communication device may be limited, or the portable communication device may not always have uninterrupted network connectivity. As such, the number of transactions limited-use threshold can be set to more than one transaction (e.g., five transactions) in some embodiments, for example, to reduce the frequency and amount of LUK replenishments over time, and hence reduce the amount of network traffic used by the portable communication device over time.

[0055] In some embodiments, the set of one or more limited-use thresholds may also include an international usage threshold and a domestic usage threshold indicating separate limits for international transactions versus domestic transactions.

For example, the number of transactions that a LUK may be valid for can be higher for domestic transactions than for international transactions, if international transactions are deemed to be more risky. The set of one or more limited-use thresholds may also include a low value transaction threshold and a high value transaction threshold indicating separate limits for low value transactions versus high value transactions. For example, the number of transactions that a LUK may be valid for can be higher for low value transactions (e.g., LUK valid for ten transactions under $20) than for high value transactions (e.g., LUK valid for five transactions over $20) such that low value transactions will trigger replenishment of the LUK less frequently than high value transactions.

[0056] In some embodiments, the set of one or more limited-use thresholds associated with an account may change when the LUK is replenished such that a new LUK replacing a previous LUK may have one or more different usage limits than the previous LUK. This may occur, for example, based on changes in the consumer spending habits, the location of the portable communication device, or the time of the year, etc. For example, a new LUK may have a higher usage limit if the user has a recent pattern of conducting many high value transactions, or when it is during the holiday season when transaction activity is expected to increase. As another example, a new LUK may have a lower usage limit if the location of the portable communication device indicates that the user may have traveled to a high risk country where fraud is prevalent.

[0057] In embodiments in which a LUK is associated with more than one limited-use thresholds, the usage of the LUK can be exhausted when any one of the limited-use thresholds is exceeded, or when some combination of the limited-use thresholds is exceeded. Hence, replenishment of the LUK may be triggered when any one of the limited-use thresholds is exceeded or is about to be exceeded, or when some combination of the limited-use thresholds is exceeded or is about to be exceeded.

[0058] In some embodiments, a limited-use threshold associated with a LUK of an account may have different usage limits configured in different components or entities of the cloud-based transaction system. In other words, different components or entities may have different usage limits for a particular limited-use threshold to trigger replenishment of the LUK. The components or entities that may be

configured with different usage limits may include, for example, the portable communication device of the user, the cloud-based service provider, and/or the issuer/host system. According to some embodiments, the usage limit at the portable communication device can be set lower than the usage limit at cloud-based service provider, and the usage limit at the cloud-based service provider can be set lower than the usage limit at the issuer. For example, a LUK may have a time-to-live limited-use threshold, and the on-device usage limit to trigger replenishment of the LUK at the portable communication device can be set at 2 days, the service provider usage limit at the cloud-based service provider can be set at 4 days, and the issuer usage limit at the issuer can be set at 5 days. In this example, the portable communication device would normally initiate replenishment of the LUK after 2 days. However, if the portable communication device is turned off or has lost network connectivity, the cloud-based service provider can initiate replenishment of the LUK after 4 days, or the issuer can initiate the replenishment after 5 days, if the LUK has not been renewed prior to that to ensure the LUK does not remain stale.

[0059] In some embodiments, the different components or entities of the cloud-based transaction system may be configured with different limited-use thresholds that may trigger LUK replenishment. For example, the on-device set of one or more limited-use thresholds configured on the portable communication device may include a time-to-live and a number of transactions that will trigger LUK replenishment initiated by the portable communication device, while the cloud-based service provider and/or the issuer/host system may additionally or alternatively be configured with a cumulative transaction amount to trigger LUK replenishment initiated by the cloud-based service provider and/or the issuer/host system. In other words, different components or entities may monitor different types of conditions or limited-use thresholds to trigger replenishment of the LUK.

[0060] In some embodiments, the set of one or more limited-use thresholds may be account specific (e.g., where different accounts may have different usage limits), portable communication device specific (e.g., where different portable communication devices of the user may have different usage limits even if the underlying account is the same), and/or mobile application specific (e.g., where different mobile applications may have different usage limits even if the mobile applications are installed on the same portable communication device and/or if the

underlying account is the same). In some embodiments, the LUK may also have other use restrictions such as which type of merchant, which particular merchant, or which geographical location where the LUK can be used. The particular rules or risk parameters for triggering the LUK replenishment and/or for setting the limited-use thresholds can be determined by the issuer or cloud-based transactions provider.

[0061] The dynamic set of data may also include a key index that is associated with the LUK. The key index may include information pertaining to the generation of the LUK. For example, the key index may be used as a seed to generate its corresponding LUK. The key index may include time information (e.g., a timestamp) indicating when the LUK is generated, and/or may include a replenishment counter value indicating the number of times that the LUK has been renewed or replenished for a particular account, mobile application, or portable communication device. In some embodiments, the replenishment counter value may indicate the number of times the LUK has been replenished within a predetermined time period, and the replenishment counter value may reset when each predetermined time period elapses. This predetermined time period may correspond, for example, to the smallest unit of time determinable from the time information, although other predetermined time periods can be used. As an example, if the time information included in the key index indicates down to which hour the current LUK is generated, the counter value may indicate the number of times the LUK has been replenished in the hour. In some embodiments, the LUK may include an application transaction counter value indicating the number of transactions that has been previously conducted by a mobile application of the portable communication device at the time the LUK is generated, or may include a pseudo random number generated by a cloud-based transaction service provider or by a suitable entity such as an issuer involved in processing the transaction. It should be understood that the key index may include one or more pieces of information pertaining to the generation of the LUK, and that one or more or all pieces of information included in the key index may be used as a seed to generate the LUK.

[0062] In some embodiments, the semi-static set of data may also include limited-use account parameters that have their own set of limited-use thresholds and/or own set of use restrictions. Although in some embodiments, an account identifier such as a PAN can be used and stored on the portable communication device, a PAN may

be valid for the lifetime of an account and may be used for a wide range of different types of transactions (e.g., card present transactions, online transactions, etc.). As such, to further enhance the security of the portable communication device and to reduce the impact if the account parameters are compromised, in some embodiments, instead of using and storing a PAN in the portable communication device, an alternate account identifier (e.g., an alternate PAN) or a token that is a substitute for an account identifier may be used.

[0063] An account may have one or more alternate account identifiers and/or tokens associated with the account. Each alternate account identifier or token may be restricted to the type of transactions in which the alternate account identifier or token can be used. For example, an account may be associated with a first token that can only be used for online transactions and a second token that can only be used for cloud-based transactions, and an online transaction conducted using the cloud-based token will be declined. Other types of use restrictions may include restrictions on what type of merchant or which merchant and/or which geographical location that the alternate account identifier or token can be used.

[0064] An alternate account identifier or a token may also have its own set of limited-use thresholds (e.g., time-to-live, number of transactions, and/or cumulative transaction amount, etc.). In some embodiments, the limited-use thresholds of an alternate account identifier or a token may have higher usage limits than those of the dynamic set of data (e.g., LUK) such that the replenishment of the alternate account identifier or token occurs less frequently. For example, an alternate account identifier or a token may have a time-to-live of a year whereas the time-to-live of a LUK may be five days. As another example, an alternate account identifier or a token may be valid for up to two thousand transactions whereas a LUK may be valid for up to five transactions. It should be understood that in some embodiments, the usage limits of the alternate account identifier or token can also be set to be the same as those of the dynamic set of data (e.g., LUK), such that replenishment of the alternate account identifier or token occurs at the same time as the dynamic set of data.

[0065] II. CLOUD-BASED TRANSACTION SYSTEM OVERVIEW

[0066] In the cloud-based transaction system, issuers of accounts may configure service portfolio characteristics to define the risk parameters and hence the limited-use thresholds of account parameters for accounts belonging to a particular portfolio. The limited-use thresholds can be used to manage the triggers for refreshing or replenishing account parameters on a provisioned portable communication device. To ensure that the cloud-based transactions are processed according to the risk parameters specified in the service profile for an account, several core functions are implemented in the system to manage the deployment and usage of the account parameters. These functions may include provisioning, active account management, verification for payment, transaction processing, lifecycle management, and post-payment processing.

[0067] Provisioning may entail taking an enrolled account, creating account parameters such as an identifier to identify the enrolled account for cloud-based transactions (e.g., an alternate account identifier such as an alternate PAN or token) and an initial dynamic set of data to ensure the account parameters have only limited use after delivery to the portable communication device, and inheriting the service profile (e.g., limited-used thresholds) that has been established for the portfolio that the enrolled account belongs to. Depending on the type of transactions supported, the dynamic set of data may include a LUK and/or other dynamic data such as a key index. The LUK, for example, can be used by the portable communication device during a transaction to calculate a transaction cryptogram or limited-use dynamic data such as a verification value to support legacy transactions that use verification values (e.g., dynamic card verification value (dCVV)).

[0068] After an account is provisioned onto the portable communication device, the relevant service profile details (e.g., limited-use thresholds) can be shared with the transaction processing software and entities in the system to ensure transaction authorization decisions are handled properly. Additionally, the service profile details (e.g., limited-use thresholds) can be provided to the on-device cloud-based transaction software of the mobile application installed on the portable communication device to ensure that the account parameters are managed appropriately on the portable communication device. As discussed above, different

usage limits for triggering account parameters replenishment can be set at the different entities in the cloud-based transaction system, and thus the service profile may define different usage limits of each limited-use threshold to be set at the different entities that may initiate account parameters replenishment (e.g., portable communication device, cloud-based service provider, issuer, etc.).

[0069] After provisioning, the cloud-based transaction system may perform active account management to initiate the renewal or replenishment of the account parameters. The active account management processes can be triggered by transaction processing activity or initiated by the mobile application running on the portable communication device. If the service profile parameters for a particular account indicate that the account parameters on the device should be replaced (e.g., have exhausted their usage limits), the active account management capability recognizes this and attempts to connect to the portable communication device to replenish the account parameters. Additionally or alternatively, if the on-device service profile parameters managed by the mobile application indicate that account parameter replenishment is needed or is close to be being needed, then the mobile application can request account parameter replenishment.

[0070] To provide verification for payments, the cloud-based transaction system also has a capability to provide on-device verification functionalities to the payment processing network prior to or during a transaction to provide some level of verification that the transaction was initiated and intended by a proper user of the portable communication device. The on-device verification may include cardholder verification methods (CVMs) that can be used as verification for payment for provisioned accounts. As part of the service profile for a portfolio, specific rules for what can be used as CVM (e.g., screen lock, application passcode, etc.) can be established and shared with the provisioning, active account management, and transaction processing capabilities.

[0071] After an account is provisioned, the transaction processing capability of the system can provide awareness that a transaction being conducted is performed using a cloud-based account. When a cloud-based account is identified, the transaction processing capability of the cloud-based transaction system can ensure that the service profile parameters (e.g., limited-use thresholds) are verified, applied,

and communicated to the issuer in transaction processing messages. This capability also ensures that any necessary active account management actions are initiated. For example, account identifying information provided during a transaction can be used to identifying an account as a cloud-based account if the account identifying information corresponds to an account identifier range (e.g., a PAN range) that is dedicated for cloud-based transactions, or if the account identifying information corresponds to an alternate PAN or token that is used only for cloud-based transactions.

[0072] After an account has been provisioned for cloud-based transactions, the lifecycle management functionality may allow the user or the issuer to manage the lifecycle of the provisioned account. Lifecycle management events such as suspension or deletion of an account may be consumer-initiated. For example, reporting a lost or stolen portable communication device and/or an associated card by the consumer may trigger suspension or deletion of an account from a portable communication device, or a user may elect to remove a provisioned account from the portable communication device. Lifecycle management events can also be issuer-initiated, for example, based on risk management or account reissuance activities. In some embodiments, other parties that may be involved in the processing of cloud-based transactions or managing cloud-based accounts, including merchants or multi-issuer mobile wallet providers, may also initiate lifecycle actions.

[0073] FIG. 1 illustrates a cloud-based transaction system 100, according to some embodiments. The core components of system 100 may include a cloud-based payments platform (CBPP) 180 and a mobile application platform (MAP) 170 to manage cloud-based transactions conducted using portable communication device 101. CBPP 180 may be referred to as a remote computer, and may be implemented using one or more computing devices or computers, such as one or more server computers, and can be associated with or be operated by a cloud-based service provider such as an issuer, payment processor, and/or other suitable entities. CBPP 180 may manage cloud-based accounts, provide verification functions for cloud-based transactions, manage lifecycle messages from issuer/host system 172 or MAP 170, as well as initiate lifecycle management events. CBPP 180 may also assist issuer/host system 172 with post payment functionalities to mitigate the risk

against counterfeit account parameters, and limit the exposure on account parameters stored on the device. For example, CBPP 180 can be used to facilitate issuer/host system 172 requests for periodic post payment verification of payment transactions and/or validation of account parameters replenishment requests using post payment information.

[0074] CBPP 180 may also implement a set of key management functions that manages issuer master derivation keys (MDKs) from which the limited-use keys (LUKs) for cloud-based transactions are derived. CBPP 180 may implement a set of provisioning functions that manages the preparation and delivery of cloud-based account parameters (e.g., alternate account identifier or token, initial LUK and associated key index, etc.) to MAP 170 for the initial setup of the mobile application 112 on portable communication device 110. CBPP 180 may also manage the cloud-based accounts for processing by issuer/host system 172, and may perform active account management functions such as functions to generate account parameters based on requests or the risk profile of the cloud-based account per CBPP 180 risk management parameters. CBPP180 may also maintain the account status for each cloud-based account, and manage the replenishment or refreshing of the account parameters.

[0075] In some embodiments, CBPP 180 may also implement or be provided with access to a token service 182 and/or a token vault 184. Token service 182 can be used to generate, process, and maintain tokens, which are substitute identifiers for account identifiers. During a transaction, instead of using a real account identifier (e.g., a primary account number (PAN)) to identify the account of the user, a token can be used instead to identify the account. By using a token as a substitute for an account identifier, the risk of comprising real account information can be mitigated. As indicated above, a token may have its own set of use restrictions, and token service 182 may manage the deployment and usage of the tokens according to their use restrictions. Token service 182 may be in communication with token vault 184 where the generated tokens are stored. Specifically, token vault 184 may maintain a mapping between a token and the real account identifier (e.g., PAN) represented by the token. During transaction processing, token vault 184 may be queried to retrieve the real account identifier or PAN associated with the token.

[0076] MAP 170 is used to facilitate communications between mobile application 112 executing on portable communication device 101 and other entities in cloud-based transactions system 100 such as CBPP 180 and/or issuer/host system 172, etc. MAP 170 may communicate with portable communication device 101 via a communications network 192 such as the Internet. In some environments, portable communication device 101 may not always have constant network connectivity, and thus one of the primary roles of MAP 170 is to intermediate requests between mobile application 112 and the other entities in the cloud-based transactions system 100 to ensure that requests and responses involving mobile application 112 are fulfilled as soon as network connectivity to portable communication device 101 is established. MAP 170 may be referred to as a remote computer, and may be implemented using one or more computing devices or computers such as one or more server computers, and can be associated with or be operated by the provider of mobile application 112. The provider of mobile application 112 can be, for example, an issuer, a bank, a third-party mobile wallet provider, a merchant, or other suitable entities. In some embodiments, MAP 170 can be associated with or be operated by the same entity as CBPP 180, or they can be separate. Although MAP 170 is illustrated as a separate logical entity in FIG. 1 because CBPP 180 is not expected to communicate directly with portable communication devices, it should be understood that in some embodiments, some or all of the functionalities of MAP 170 may be integrated as part of CBPP 180. Examples of MAP 170 may include mobile banking platforms and mobile wallet platforms.

[0077] In some embodiments, MAP 170 may implement authentication functionalities to authenticate portable communication device 101 when portable communication device 101 communicates with the other entities in cloud-based transaction system 100 via MAP170. The authentication functionalities may ensure that a portable communication device communicating with the system is an authorized portable communication device and/or a portable communication device that has not been hacked, infected with malware or virus, or otherwise been compromised. For example, MAP 170 may perform, request, or facilitate a device fingerprint of portable communication device 101 to capture the state of portable communication device 101 when portable communication device 101 communicates with MAP 170. The device fingerprint may, for example, capture information about

portable communication device 101 such as the operating system and version, applications installed on portable communication device 101, memory usage, whether portable communication device 101 has been jail-broken, device identifiers such as a portable communication device identifier, and/or other suitable device characteristics.

[0078] MAP 170 may verify the device fingerprint of portable communication device 101 for each communication session established with portable communication device 101 or periodically (e.g., once every five communication sessions, once a month, etc.). If the device fingerprint of a portable communication device indicates that the portable communication device is not an authorized device for an account (e.g., the portable communication device requesting replenishment of account parameters is a different device than the original device that was used to enroll the account), or if the device fingerprint indicates that the portable communication device may potentially be hacked, MAP 170 may prevent the portable communication device from communicating with the system and alert the issuer that the portable communication device may have been compromised.

[0079] MAP 170 may perform enrollment functions to enroll a mobile cardholder into a cloud-based transactions program, and a set of provisioning functions that facilitates the preparation and delivery of the account parameters, configuration, and cloud-based payments device threshold parameters to mobile application 112. MAP 170 may perform account parameters replenishment functions to facilitate the account parameter replenishment process for the cloud-based account provisioned on portable communication device 101, and lifecycle management functions that manage lifecycle messages from issuer/host system 172, CBPP 180, and/or mobile application 112. MAP 170 may also perform post-payment functions to mitigate the risk against counterfeit account parameters, and to limit the exposure on account parameters stored on portable communication device 101, such as facilitating periodic post payment verification of payment transactions or the use of post payment information to validate account parameters replenishment requests.

[0080] In cloud-based transactions system 100, portable communication device 101 can be used to conduct cloud-based transactions facilitated by CBPP 180 and/or MAP 170. The components in portable communication device 101 may include

device hardware 103, a mobile operating system (OS) 114, and an applications environment 110 in which mobile application 112 may reside. Device hardware 104 may include a contactless interface 108 that can interact with a contactless reader 162 of an access device 160. Examples of contactless interface 108 may include one or more radio frequency (RF) transceivers that can send and receive communications using near-field communications (NFC), or other radio frequency or wireless communication protocols such as Bluetooth, Bluetooth low-energy (BLE), Wi-Fi, iBeacon, etc. In some embodiments, contactless interface 108 may include an optical interface (e.g., a display screen) to present payment information in the form of an image such as a quick response (QR) code, or bar code, etc. to contactless reader 162 of access device 160 when contactless reader 162 includes an optical code scanner or reader.

[0081] Applications environment 110 of portable communication device 101 may host a mobile application 112 provided by a mobile application provider. For example, if the provider of mobile application 112 is an issuer, mobile application 112 may be a mobile banking application or a separate mobile payment application. If the provider is a mobile wallet provider such as a mobile network operator or third-party wallet provider that supports multiple issuers, mobile application 112 may be a mobile wallet application. For merchants, mobile application 112 may be a merchant's own mobile application from which consumers can conduct e-commerce or point of sale transactions with that merchant, or may be a mobile wallet application that supports multiple merchants.

[0082] According to some embodiments, mobile application 112 may include on-device cloud-based transaction software 113 (e.g., can be in the form of a software developer kit (SDK)) integrated into mobile application 112 to support cloud-based transaction functionalities. The on-device cloud-based transaction software 113 may perform functions to facilitate cloud-based transactions such as to take the account parameters (e.g., LUK and associated key index), generate transaction cryptograms, and deliver them to mobile operating system 114 for transmission over contactless interface 108. The on-device cloud-based transaction software 113 may also manage the initial service profile parameters (e.g., limited-use thresholds) that are provided after an account has been provisioned to ensure that requests for account

parameter replenishment and other account parameter management activities are initiated.

[0083] Mobile application 112 may perform functions to manage the risk profile of the cloud-based account, maintain the account status, and replenish account parameters for each cloud-based account based on the on-device threshold management parameters. Mobile application 112 may also manage lifecycle messages from issuer/host system 172 or lifecycle messages from MAP 170. Mobile application 112 may perform a set of functions to enroll a mobile cardholder into a cloud-based transactions program, and a set of functions that manages the receiving and configuration of the cloud-based account parameters and cloud-based payments device threshold parameters received from MAP 170. Mobile application 122 may also provide consumer device cardholder verification method (CDCVM) functions for cloud-based transactions, and perform a set of functions that processes and responds to messages in support of post-payment processing to limit the exposure of account parameters stored on the portable communication device. For example, post-payment processing may include periodic post-payment verification of payment transactions or using post-payment information to validate account parameters replenishment requests.

[0084] In secure element based implementations, a contactless application (e.g., a mobile wallet or payment application for contactless transactions) using a contactless interface to communicate with a contactless reader of an access device would have to be coded for and be executed on a secure element in order to gain access to the contactless interface. In some embodiments, portable communication device 101 may include a mobile operating system (OS) 114 that implements a set of card emulation application programming interfaces (APIs) 116 such as host card emulation (HCE) APIs to allow mobile application 112 to gain access to contactless interface 108 without requiring the use of a secure element. For example, card emulation APIs 116 may be coded for and be executed from mobile OS 114 of portable communication device 101, and may include programming function calls to allow mobile application 112 to receive, process, and respond to transaction communications such as Application Protocol Data Unit (ADPU) commands sent from contactless reader 162. In this manner, portable communication device 101 is

able to conduct contactless transactions without requiring access to a secure element on portable communication device 101.

[0085] Once portable communication device 101 and mobile application 112 have been provisioned with the account parameters, portable communication device 110 can conduct cloud-based transactions by interacting with contactless reader 162 of access device 160 (e.g., at a merchant point-of-sale (POS) location). Contactless reader 162 may include one or more RF transceivers that can send and receive communications using NFC or other radio frequency or wireless communication protocols such as Bluetooth, BLE, Wi-Fi, iBeacon, etc. In some embodiments, contactless reader 162 may include an optical code scanner or reader to conduct transactions using QR codes, bar codes, etc. Access device 160 may also include a POS acceptance device 164 and/or electronic cash register 166.

[0086] To conduct a cloud-based transaction, a user of portable communication device 101 may place portable communication device 101 in proximity to contactless reader 162 of access device 160, or display an image such as a QR code or bar code on a screen of portable communication device 101 for scanning by contactless reader 162 of access device 160. Portable communication device 101 may provide access device 160 with an identifier (e.g., an account identifier such as a PAN, an alternate account identifier such as an alternate PAN, or a token, etc.) to identify the account of the user and additional information such as the limited-use account parameters or information derived from the limited-use account parameters (e.g., transaction cryptograms generated from an LUK). For example, in some embodiments, an account identifier or token, and additional information (e.g., a transaction cryptogram, account parameters, etc.) can be transmitted to access device 160 in APDU responses that are responsive to a series of APDU commands received from access device 160. In some embodiments, an account identifier or token, and the additional information can be encoded in a QR code or bar code that is scanned and processed by access device 160 to retrieve the encoded information. Access device 160 or a merchant computer coupled to access device 160 may then generate an authorization request message including the account identifier or token, and additional information such as a transaction cryptogram and other transaction data, and forward the authorization request message to acquirer 174 associated with

the merchant. The authorization request message can then be sent by acquirer 174 to payment processing network 194.

[0087] Payment processing network 194 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, transaction scoring 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, may include a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0088] Upon receiving the authorization request message, payment processing network 194 may forward the authorization request message received from acquirer 174 to the corresponding issuer/host system 172 of the account of the user of portable communication device 101. After issuer/host system 172 receives the authorization request message, the authorization request message may be parsed, and the information in the authorization request message may be verified. For example, issuer/host system 172 may verify that the transaction cryptogram was generated by a valid LUK, and that the set of one or more limited-use thresholds associated with the LUK has not been exceeded. In some embodiments, some or all of the information in the authorization request message can also be sent to CBPP 180 for verification and processing. For example, if issuer/host system 172 does not have the capability to verify the transaction cryptogram, the payment processing network 194 or issuer/host system 172 may forward the transaction cryptogram to CBPP 180 for verification.

[0089] An authorization response message is then sent back to payment processing network 194 to indicate whether the current transaction is authorized (or not authorized). Payment processing network 194 then forwards the authorization response message back to acquirer 174. In some embodiments, payment processing network 194 may decline the transaction even if issuer/host system 172 has authorized the transaction, for example, depending on a value of a fraud risk score or depending if limited-use account parameters are verified by CBPP 180.

Acquirer 174 then sends the authorization response message to the merchant computer and/or access device 160. The authorization response results, which may include transaction data for the transaction can be displayed by access device 160, or be printed out on a physical receipt.

[0090] At the end of the day, a clearing and settlement process can be conducted by payment processing network 194. A clearing process is a process of exchanging financial details between an acquirer and an issuer to facilitate posting to a user's payment account and reconciliation of the user's settlement position. It should be understood that any of the acquirer 174, payment processing network 194, issuer/host system 172, CBPP 180, and/or MAP 170 may be referred to as a remote computer, and may include one or more computing devices such as one or more computers or server computers to enable the entity to communicate with the other entities in system 100, and/or to perform one or more of the functions described herein.

[0091] III. ENROLLMENT AND PROVISIONING

[0092] FIG. 2 illustrates a communication flow diagram of an example enrollment and provisioning process, according to some embodiments. The enrollment and provisioning process can be initiated from portable communication device 201 installed with a mobile application programmed with cloud-based transaction capabilities. The mobile application may be pre-installed on portable communication device 201 during manufacturing or by a retailer, or by a user downloading the mobile application from an application store or from an issuer or cloud-based transaction service provider and installing the mobile application on portable communication device 201. The user may launch the mobile application and initiate an enrollment request 222 from the mobile application to add an account to the cloud-based transaction service. Enrollment request 222 is sent from portable communication device 201 to MAP 270, and may include information that can be used to identify the user and the account of the user, as well as device information about portable communication device 201.

[0093] According to some embodiments, to facilitate communications with portable communication device 201, MAP 270 (or issuer/host system 272, or CBPP 280) may generate a device identifier from the device information or assign a device

identifier to portable communication device 201 during the enrollment and provisioning process. The device identifier is provided to the mobile application on portable communication device 201, and can be used by the mobile application to identify portable communication device 201 to the other entities in the cloud-based transaction system in subsequent interactions with the system.

[0094] When MAP 270 receives enrollment request 222, MAP 270 may process the request, capture the device information about portable communication device 201, and route enrollment request 224 with the relevant information to issuer/host system 272. Issuer/host system 272 may perform identification and verification (ID&V) of the user and the user's account, and send a provisioning request 226 to CBPP 280. Provisioning request 226 may include account identifying information such as a PAN to identify the user's account. In embodiments in which an alternate account identifier or a token is used, CBPP 280 or issuer/host system 272 may generate an alternate account identifier, or invoke a token service to generate a token that is used as a substitute for an account identifier. Upon receiving provisioning request 226, CBPP 280 may use a master derivation key (MDK) associated with issuer/host system 272 to generate the initial set of account parameters (e.g., LUK) for provisioning to portable communication device 201. In some embodiments, issuer/host system 272 may provide CBPP 180 with the MDK if the MDK is maintained or managed by issuer/host system 272, or issuer/host system may generate the LUK and provide CBPP 180 with the generated LUK. In either case, whether the LUK is generated by CBPP 180 or by issuer/host system 272, the LUK can be generated based on a key index that acts as a seed for the generation of the LUK, and the key index can be shared between CBPP 180 and issuer/host system 272 to facilitate processing of transactions using the LUK.

[0095] CBPP 280 then packages provisioning data 228, which may include an alternate account identifier or a token, an initial set of account parameters such as a LUK and key index, and other information relevant for executing and/or processing of a transaction (e.g., set of one or more limited-use thresholds associated with the LUK), and sends provisioning data 228 to MAP 270. MAP 270 can then forward the information as provisioning data 330 to portable communication device 201. The mobile application then stores the account parameters and relevant information on

portable communication device 201 to enable portable communication device 201 to be used for conducting contactless transactions on the user's account.

[0096] In should be noted that in some embodiments, the different entities in the system (e.g., portable communication device 201, CBPP 280, and issuer/host system 272) can be provided with different usage limits for the set of one or more limited-use thresholds during the enrollment and provisioning process, and the respective entities can trigger subsequent account parameters replenishment at different usage limits.

[0097] Once provisioning data 330 has been successfully provisioned onto portable communication device 201, portable communication device 201 may send an acknowledgement or confirmation 332 to MAP 270. MAP 270 may also send a confirmation 334 to CBPP 280, which in turn forwards confirmation 336 to issuer/host system 272 to complete the enrollment and provisioning process.

[0098] It should be understood that the enrollment and provisioning process described above is just an example, and that the messaging sequence in some embodiments may have different variations. In some embodiments, the roles of CBPP 280 and issuer/host system 272 can be interchanged. For example, CBPP 280 may receive enrollment request 324 from MAP 270 and send provisioning request 326 to issuer/host system 372. As another example, MAP 270 may send confirmation 334 to issuer/host system 272, and issuer/host system may send confirmation 336 to CBPP 280.

[0099] IV. TRANSACTION EXECUTION

[0100] Once a portable communication device has been provisioned with the appropriate account parameters, the portable communication device can be used to execute a contactless transaction, for example, by placing portable communication device in proximity to a contactless reader of an access device. Depending on the capabilities of the access device, a contactless transaction conducted using the techniques described herein can be processed as if the transaction is being performed with an integrated chip card (referred to as "integrated chip based transaction"), or as if the transaction is being performed with a magnetic stripe card (referred to as "magnetic stripe based transaction"). In some embodiments, the contactless transaction times using the card emulation techniques described herein

may be similar to those of secure element based implementations. For example, according to some embodiments, a contactless transaction using card emulation may take less than 500 milliseconds to complete.

[0101] In some embodiments, execution of a contactless transaction using a portable communication device can be carried out by providing or exchanging messages (e.g., Application Protocol Data Unit (APDU) messages) between a mobile application running on the portable communication device and a contactless reader of an access device over a contactless medium such as radio frequency waves. The messages can be in the form of APDU commands sent from the contactless reader to the portable communication device, and APDU responses sent from the mobile application to the contactless reader in response to the APDU commands. To provide additional security, the mobile application may be configured to only respond to APDU commands received from the contactless interface or contactless controller of the portable communication device. In other words, the mobile application can be configured to ignore or reject APDU commands received from other applications or components, and/or ADPU commands that the mobile application does not recognize. In some embodiments, if the mobile application receives an unrecognized APDU command from the contactless interface or contactless controller of the portable communication device, the mobile application can respond to the command with a default status word.

[0102] In some embodiments, when the mobile application interacts with an external entity (e.g., MAP, CBPP or issuer/host system via the MAP, or a contactless reader of an access device) for which the mobile application may change its state or its stored information, the mobile application processes the interaction in an atomic manner. In other words, the mobile application may process either all of the functions required by the interaction or none of them. In this manner, the mobile application may keep a recognized state as seen from external entities.

[0103] During installation of the mobile application, the mobile application may register its proximity payment system environment (PPSE) name as well as all Application Identifiers (AIDs) covered by the mobile application to ensure that transactions using those AIDs are routed to the mobile application (e.g., this can be achieved through a declaration in the manifest of the mobile application to the mobile

operating system). For example, in some embodiments, the mobile application can be registered to receive APDU commands for one or more AIDs of a PPSE with a name such as "2PAY.SYS.DDF01."

[0104] In some embodiments, the mobile application can be registered to receive and process APDU commands for multiple AIDs (e.g., AIDs defined for a particular issuer, payment processor or processing network, service provider, etc.), and in some scenarios, the multiple AIDs can be associated with a single account. A single account may have multiple AIDs associated with it, for example, if a transaction conducted on that account can be processed by different payment processing networks and/or if the account can have different services, features, product-types, and payment capabilities associated with the account. For example, a single account may have a common debit AID and a payment processing network specific AID (e.g., a Visa AID) associated with the single account. As another example, a single account may support different payment products, and each payment product can have its own AID. The multiple AIDs can be communicated to the access device to allow an access device to select a preferred AID to choose how the transaction is processed (e.g., which payment processing network) and/or what services or features to associate with or provide for the transaction. The multiple AIDs can be populated in the directory entry for the PPSE, and communicated to an access device for this purpose.

[0105] The mobile application on the portable communication device may receive, store, and/or support generation of information related to the account to enable the mobile application to respond with the necessary information to a contactless reader as well as provide cardholders with information about the account via the portable communication device's user interface. Some or all of this information can be provided to the mobile application during the enrollment and provisioning process. The account related information may include card art or other visuals that identifies the account to the consumer, account identifying information that can identify the account to the user (e.g. nickname or last 4 digits of the account), the state of the account (e.g. active, suspended etc.), account configuration information, transaction flow parameters (e.g., information that is provided to a contactless reader during a transaction), the current set of account parameters (e.g., LUK and key index) and its associated set of one or more limited-use thresholds and corresponding usage limits,

and a transaction verification log, etc. The account configuration information may include the AID(s) of the account, which consumer verification method(s) (CVM(s)) (e.g., online PIN, consumer device CVM, signature, etc.) are supported by the account (or by the respective AID if multiple AIDs are present) and their priority, whether the account supports magnetic stripe based transactions, and a derivation key index (DKI) associated with the issuer master key used during verification of the transaction cryptograms. For mobile applications supporting multiple accounts for the same or different account AIDs, the mobile application may also support the concept of which account is currently the active account and be able to populate responses to the contactless reader with the data according to the currently active account.

[0106] The mobile application may also implement one or more counters to track the transaction activity of the mobile application. For example, the mobile application may implement a sequence counter (SC) to count how many times the mobile application has successfully requested new account parameters for a specific account. The mobile application may also implement an application transaction counter (ATC) to count how many times the mobile application has been used to initiate a transaction.

[0107] During a transaction, the mobile application may receive, store, and/or dynamically build information such as transaction flow parameters related to the contactless transaction in order to return the necessary information to the contactless reader for the transaction to be successfully executed. Some of the transaction flow parameters may be received, stored, and/or built before the contactless transaction is initiated, while some transaction flow parameters (e.g., transaction cryptogram) can be dynamically built at the time of transaction. For mobile applications supporting multiple AIDs, different transaction flow parameters can be stored and/or generated per AID. Example details of the transaction flow parameters (e.g., including the transaction processing information and/or account data referred to below), and example details of the communication exchanges between the mobile application and the contactless reader will be described with reference to FIG. 3 for an integrated chip based transaction, and with reference to FIG. 4 for a magnetic stripe based transaction.

[0108] INTEGRATED CHIP BASED TRANSACTION

[0109] FIG. 3 illustrates an example communication flow between a portable communication device 301 and an access device 360 during an integrated chip based transaction, according to some embodiments. In some embodiments, the communications can be in the form of ADPU commands and responses. However, it should be understood that other messages, messaging protocols, or formats can be used to exchange the relevant information to conduct the transaction. The communications can be carried out between a mobile application running on portable communication device 301 and a contactless reader of access device 360. In some embodiments, the mobile application may communicate with the contactless reader using card emulation APIs of the mobile operating system of portable communication device 301, and thus the transaction can be carried out without requiring the use of a secure element (although a secure element can be used).

[0110] When access device 360 detects the presence of portable communication device 301 in proximity to a contactless reader of access device 360, access device 360 may initiate a transaction by sending an available applications request 302 to portable communication device 301 to request information on which payment application(s) (e.g., a list of AID(s)) may be available on the mobile application of portable communication device 301. In some embodiments, the available application(s) request 302 may be in the form of a select PPSE command. The available applications request 302 may include a payment environment identifier (e.g., a PPSE name such as "2PAY.SYS.DDF01") to identify the payment environment supported by access device 360 and the mobile application.

[0111] Upon receiving the available applications request 302, the mobile application of portable communication device 301 may identify and process the request by recognizing the payment environment identifier (e.g., PPSE name) included in the request, and respond by sending an available applications response 304 back to access device 360. The available applications response 304 may include a list of available AIDs, and may include the payment environment identifier (e.g., PPSE name) as the dedicated file name. In some embodiments, the available applications response 304 may be in the form of a select PPSE response and may include PPSE file control information (FCI). For example, the available applications

response 304 may include a directory entry for each available AID. If the mobile application supports only one AID (irrespective of the number of accounts related to that AID), the mobile application may respond with a single directory entry for the supported AID. If the mobile application supports an account with multiple AIDs, the mobile application may respond with a directory entry for each of the supported AIDs. Each directory entry may include information such as the AID, an application label associated with the AID (e.g., a mnemonic associated with the AID), an application priority indicator indicating the priority of the AID, a kernel identifier indicating the application's kernel preference, and/or additional information relating to the particular AID. The available application(s) response 304 may also include other data such as FCI issuer discretionary data.

[0112] When access device 360 receives the available applications response 304, access device 304 may select a suitable application from the list of applications received in the available applications response 304 (e.g., by selecting an AID from the available AID(s) received in the available application(s) response 304). In some embodiments, the selected AID can be the highest priority AID available on the mobile application that is supported by access device 360. Access device 360 may send an application selection 306 with the selected AID to the mobile application of portable communication device 301 to continue the transaction. In some embodiments, the application selection 306 can be in the form of a select AID command.

[0113] Upon receiving the application selection 306, the mobile application of portable communication device 301 may send a terminal transaction data request 308 to request transaction data from access device 360 which may be needed to execute the transaction using the selected application/AID. In some embodiments, the terminal transaction data request 308 may be in the form of a select AID response and may include AID file control information (FCI) with the selected AID as the dedicated file name. The terminal transaction data request 308 may include a list of transaction data identifiers to request the appropriate data from access device 360, and the list of transaction data identifiers can be in the form of a processing options data object list (PDOL). The transaction data requested by the mobile application for the transaction may include terminal transaction qualifiers (TTQ), authorized amount, other amount, terminal country code, terminal verification results,

transaction currency code, transaction data, transaction type, and/or an unpredictable number. The terminal transaction data request 308 may also include other data such as FCI issuer discretionary data, application program identifier, and language preference.

[0114] After receiving the terminal transaction data request 308, access device 360 may send, to the mobile application of portable communication device 301, the terminal transaction data 310 requested by the mobile application. In some embodiments, the terminal transaction data 310 may be sent in the form of a get processing options (GPO) command, and may include the requested terminal transaction data in a processing options data object list (PDOL). In some embodiments, the terminal transaction data 310 (e.g., terminal transaction qualifiers (TTQ)) may include a transaction type indicator indicating whether access device 360 supports integrated chip based transactions or magnetic stripe based transactions. Thus, in the integrated chip based transaction illustrated in FIG. 3, access device 360 may send a transaction type indicator in the terminal transaction data 310 to indicate that access device 360 supports integrated chip based transactions. In some embodiments, the terminal transaction data 310 (e.g., terminal transaction qualifiers (TTQ)) may also include a consumer verification method (CVM) requirement indicator to indicate whether a CVM is required by access device 360 for the transaction, and also one or more CVM type indicators indicating the types of CVM supported by access device 360. Examples of CVMs that may be supported by access device 360 can include online PIN, signature, and/or consumer device CVM (CDCVM) such as a passcode used on portable communication device 301 to unlock the screen or mobile application.

[0115] Once the mobile application of portable communication device 301 receives terminal transaction data 310, the mobile application may increment its Application Transaction Counter (ATC), generate dynamic transaction processing information using at least some of the received terminal transaction data 310, and send a set of transaction processing information 312 including the generated dynamic transaction processing information to access device 360. In some embodiments, the transaction processing information 312 can be sent in the form of a GPO response. In some embodiments, the transaction processing information 312 may include one or more application file locators (AFLs) that can be used as file

address(es) by access device 360 to read account data stored on portable communication device 301, and an application interchange profile (AIP) that can be used to indicate the capabilities of the mobile application.

[0116] For an integrated chip based transaction, the transaction processing information 312 may include a transaction cryptogram dynamically generated using the LUK, track-2 equivalent data, and addition data such as issuer application data (IAD), form factor indicator (FFI), card transaction qualifiers (CTQ), cryptogram information data (CID), the updated ATC, and/or an application PAN sequence number (PSN). In some embodiments, the issuer application data (IAD) may include a length indicator indicating the length of the IAD, cryptogram version number (CVN) indicating the version of the transaction cryptogram, a derived key indicator (DKI) that can be used to identify a master key (e.g. a master key associated with the issuer used in generation of the LUK), card verification results (CVR), a wallet provider ID, and/or derivation data such as the key index that was used in the generation of the LUK.

[0117] The card verification results (CVR) may include information about the CVM verifying entity and the CVM verified type for the transaction. The CVM verifying entity is used to indicate which entity is performing the verification of the CVM for the transaction. The verification entity may be the access device (or terminal), a co-residing secure application, a trusted execution environment application, the mobile application itself, a remote server or computer (e.g., the cloud), or the mobile operating system. The CVM verified type is used to indicated the CVM method used for the transaction. The CVM method may be a passcode, biometric (e.g., fingerprint), pattern lock (e.g., for a screen lock), signature, or online PIN. In some embodiments, if the terminal transaction data 310 received from access device 360 indicates that the CVM supported by access device 360 is an online PIN or a signature, the CVM verifying entity in the CVR can be set to the access device (or terminal) to indicate that access device 360 is the verifying entity, and the CVM verified type can be set accordingly (e.g., online PIN or signature).

[0118] If the terminal transaction data 310 received from access device 360 indicates that the CVM supported by access device 360 is a CDCVM, the CVM verifying entity and the CVM verified type can be set according to the configuration

parameters of the account. For example, if the account supports CVM using a passcode that is verified by the mobile operating system of portable communication device 301, the CVM verifying entity can be set to the mobile operating system, and the CVM verified type can be set to indicate that the CVM is a passcode. In some embodiments, a CDCVM performed indicator can be included in the card transaction qualifiers (CTQ) to indicate whether the CVM verifying entity has successfully verified the user using the CDCVM indicated by the CVM verified type.

[0119] If the terminal transaction data 310 received from access device 360 indicates that a CVM is not required, the CVM verifying entity and the CVM verified type can be set to indicate that no CVM was verified. In some embodiments, the CVR may include additional data such as a threshold indicator that indicates whether one or more limited-use thresholds associated with the LUK has been exceeded.

[0120] The form factor indicator (FFI) may include information about portable communication device 301, such as a form factor indicator version number indicating the version of the form factor indicator being used, a consumer payment device form factor indicator indicating the device type of portable communication device 301, and consumer payment device features indicators indicating what payment features are supported by portable communication device 301. The consumer payment device form factor may indicate that portable communication device 301 is a standard card (e.g., ID-1 card type as specified in ISO 7811), a mini-card, a non-card form factor (e.g., key fob, watch, wristband, ring, sticker, etc.), or a mobile phone. The consumer payment device features indicators may indicate whether portable communication device 301 is capable of using a passcode (can be separate from a PIN that is used during transactions), has a signature panel, has a hologram, has support for card verification values (e.g., CVV2), capable of two-way messaging to exchange identifying information between the issuer and the user, and/or has support for using cloud-based credentials (e.g., LUK, token, etc.). The form factor indicator (FFI) may also include a payment transaction technology indicator indicating that portable communication device 301 supports contactless transactions (e.g., NFC).

[0121] It should be understood that in some embodiments, the transaction processing information 312 being sent from portable communication device 301 to

access device 360 may include some or all of the information describe above, and in some embodiments, may include additional information not specifically described.

[0122] After access device 360 receives the transaction processing information 312, access device 360 may send an account data request 314 to the mobile application of portable communication device 301 to read additional account data that may be stored on portable communication device 301. In some embodiments, the account data request 314 may be in the form of a read record command, and may include an application file locator (AFL) indicating the location of the account data that access device 360 is attempting to read. The AFL included in the account data request 314 may correspond to an AFL in the transaction processing information 312 that was provided to access device 360 from portable communication device 301.

[0123] After access device 360 receives the transaction processing information 312, access device 360 may send an account data request 314 to the mobile application of portable communication device 301 to read additional account data that may be stored on portable communication device 301. In some embodiments, the account data request 314 may be in the form of a read record command, and may include an application file locator (AFL) indicating the address or location of the account data that access device 360 is attempting to read. The AFL included in the account data request 314 may correspond to an AFL in the transaction processing information 312 provided from portable communication device 301.

[0124] In response to receiving the account data request 314 from access device 360, portable communication device 301 may send the account data 316 stored at the location indicated by the AFL to access device 360. In some embodiments, the account data 316 may be sent in the form of a read record response. The account data 316 may include, for example, application usage control that indicates the issuer's restrictions on the usage and services allowed for the application, the cardholder's name, customer exclusive data, issuer country code, token requester ID (e.g., if a token is used), and/or other account related data that is accessible at the AFL location.

[0125] It should be understood that in some embodiments, the account data 316 being sent from portable communication device 301 to access device 360 may

include some or all of the information describe above, and in some embodiments, may include additional information not specifically described.

[0126] In some embodiments, there can be more than one pair of account data request 314 and account data 316 communication exchange between access device 360 and portable communication device 301, for example, if additional account related data stored is needed by access device 360 to complete the transaction. Once access device 360 has received the requisite data from the transaction processing information 312 and/or one or more account data 316 transmissions, some or all of the data elements in the transaction processing information 312 and/or one or more account data 316 transmissions can be used by access device 360 to generate a transaction authorization request message to request authorization of the transaction from the issuer. For example, in some embodiments, the transaction authorization request message may include at least the track-2 equivalent data and the transaction cryptogram generated with the LUK, and the transaction can be authorized based on at least verifying that the transaction cryptogram was generated correctly and that the LUK used in generation of the transaction cryptogram has not exhausted the LUK's set of one or more limited use thresholds.

[0127] MAGNETIC STRIPE BASED TRANSACTION

[0128] FIG. 4 illustrates an example communication flow between a portable communication device 401 and an access device 460 during a magnetic stripe based transaction, according to some embodiments. In some embodiments, the communications can be in the form of ADPU commands and responses. However, it should be understood that other messages, messaging protocols, or formats can be used to exchange the relevant information to conduct the transaction. The communications can be carried out between a mobile application running on portable communication device 401 and a contactless reader of access device 460. In some embodiments, the mobile application may communicate with the contactless reader using card emulation APIs of the mobile operating system of portable communication device 401, and thus the transaction can be carried out without requiring the use of a secure element (although a secure element can be used).

[0129] For a magnetic stripe based transaction, the available applications request 402, the available application response 404, the application selection 406, and the

terminal transaction data request 408 communications and the relevant data elements included in the communications are similar to that of an integrated chip card based transaction as described above with reference to FIG. 3, and thus a detailed description of which need not be repeated.

[0130] In response to receiving the terminal transaction data request 408 from the mobile application of portable communication device 401, access device 460 may send the requested terminal transaction data 410 to portable communication device 401. The terminal transaction data 410 provided to portable communication device 401 in a magnetic stripe based transaction is similar to that of the integrated chip card based transaction as described above with reference to FIG. 3, with the exception that the transaction type indicator provided in the terminal transaction data 410 (e.g., terminal transaction qualifiers (TTQ)) may indicate that access device 360 supports magnetic stripe based transactions.

[0131] Once the mobile application of portable communication device 401 receives terminal transaction data 410 and determines that access device 460 supports magnetic stripe based transactions, the mobile application may increment its Application Transaction Counter (ATC), and send a set of transaction processing information 412 to access device 360. In some embodiments, the transaction processing information 412 can be sent in the form of a GPO response. In some embodiments, the transaction processing information 412 may include one or more application file locators (AFLs) that can be used as file address(es) by access device 460 to read account data stored on portable communication device 401, and an application interchange profile (AIP) that can be used to indicate the capabilities of the mobile application. In some embodiments, the one or more AFLs provided to access device 460 during a magnetic stripe based transaction can be different than the AFL(s) provided during an integrated chip based transaction such that the mobile application maintains different locations to store separate sets of data for use in magnetic stripe based transactions versus integrated chip based transactions. The mobile application may also generate dynamic transaction processing information that may or may not use at least some of the received terminal transaction data 410, and store the generated information at a location accessible by the one or more application file locators (AFLs). The dynamic transaction processing information may include, for example, a transaction cryptogram generated by using the LUK.

[0132] After access device 460 receives the transaction processing information 412, access device 460 may send an account data request 414 to the mobile application of portable communication device 401 to read account data that may be stored on portable communication device 301. In some embodiments, the account data request 414 may be in the form of a read record command, and may include an application file locator (AFL) indicating the location of the account data that access device 460 is attempting to read. The AFL included in the account data request 414 may correspond to an AFL in the transaction processing information 412 that was provided to access device 460 from portable communication device 401.

[0133] In response to receiving the account data request 414 from access device 460, portable communication device 401 may send the account data 416 stored at the location indicated by the AFL to access device 460. In some embodiments, the account data 416 may be sent in the form of a read record response. The account data 416 may include, for example, track-2 equivalent data and the cardholder name, etc. In some embodiments, for a magnetic stripe based transaction, the transaction cryptogram generated by using the LUK and/or the key index associated with the LUK can be embedded in the track-2 equivalent data.

[0134] It should be understood that in some embodiments, the account data 416 being sent from portable communication device 401 to access device 460 may include some or all of the information describe above, and in some embodiments, may include additional information not specifically described.

[0135] In some embodiments, there can be more than one pair of account data request 414 and account data 416 communication exchange between access device 460 and portable communication device 401, for example, if additional account related data stored is needed by access device 460 to complete the transaction. Once access device 460 has received the requisite data from the transaction processing information 412 and/or one or more account data 416 transmissions, some or all of the data elements in the transaction processing information 412 and/or one or more account data 416 transmissions can be used by access device 460 to generate a transaction authorization request message to request authorization of the transaction from the issuer. For example, in some embodiments, the transaction authorization request message may include at least the track-2 equivalent data and

the transaction cryptogram generated with the LUK, and the transaction can be authorized based on at least verifying that the transaction cryptogram was generated correctly and that the LUK used in generation of the transaction cryptogram has not exhausted the LUK's set of one or more limited use thresholds.

[0136] TRACK-2 EQUIVALENT DATA

[0137] According to some embodiments, depending on the type of transaction being execute (e.g., integrated chip based transaction or magnetic stripe based transaction), different data elements can be included in the track-2 equivalent data provided from the mobile application of the portable communication device to the access device. Table 1 shows an example of a track-2 equivalent data format with an embedded transaction cryptogram that can be used in either a magnetic stripe based transaction or an integrated chip based transaction.

Data Element
Account Identifier (e.g., PAN, alternate PAN, token)
Field Separator = 'D'
Expiry Date
Service Code
Key Index
Transaction Cryptogram
Padding 'F'

Table 1: Track-2 equivalent data with embedded transaction cryptogram

[0138] The key index is associated with the LUK that was used in the generation of the transaction cryptogram for the particular transaction, and may include information pertaining to the generation of the LUK as described herein. For example, the key index may be a seed that was used to generate the LUK, and may include time information (e.g., a timestamp) indicating when the LUK was generated, and/or may include a replenishment counter value indicating the number of times that the LUK has been renewed or replenished for a particular account, mobile application, or portable communication device. In some embodiments, the key index may include an application transaction counter value indicating the number of transactions that has been previously conducted by a mobile application of the portable communication device at the time the LUK is generated, or may include a pseudo random number generated by a cloud-based transaction service provider or by a suitable entity such as an issuer involved in processing the transaction.

[0139] The transaction cryptogram embedded in the track-2 equivalent data may be a cryptogram generated by using the LUK as an encryption key. In some embodiments, the transaction cryptogram that is embedded in the track-2 equivalent data may be different than the transaction cryptogram that is provided in the transaction processing information 312 (e.g., GPO response). For example, the transaction cryptogram embedded in the track-2 equivalent data (may be referred to as a "decimalized transaction cryptogram") may have a reduced-length (e.g., reduced to six digits), and/or may be generated by encrypting a static data (e.g., a predetermined numeric string) instead of terminal transaction data.

[0140] In some embodiments in which the transaction is conducted using an optical contactless interface, an optical image such as a QR code or a bar code can be generated to encode the track-2 equivalent data format shown in Table 1, and the optical image encoding the track-2 equivalent data can be displayed on a portable communication device, and be presented to an optical scanner or reader of an access device to conduct the transaction.

[0141] Table 2 shows an example of a track-2 equivalent data format without an embedded transaction cryptogram that can be used in an integrated chip based transaction.

Data Element
Account Identifier (e.g., PAN, alternate PAN, token)
Field Separator = 'D'
Expiry Date
Service Code
PIN Verification Field
Track 2 Discretionary Data
Padding 'F'

Table 2: Track-2 equivalent data without embedded transaction cryptogram

[0142] For an integrated chip based transaction, a transaction cryptogram is already provided to the access device in the transaction processing information 312 (e.g., GPO response), and thus it may be unnecessary to include a transaction cryptogram in the track-2 equivalent data for an integrated chip based transaction. Hence, the track-2 equivalent data format shown in Table 2 can be used for an integrated chip based transaction, although the track-2 equivalent data format shown in Table 1 may also be used.

[0143] In some embodiments, the key index associated with the LUK can be embedded in the track-2 discretionary data in the track-2 equivalent data format shown in Table 2. The key index, for example, may include time information and/or a replenishment counter value, an application transaction counter value, or a pseudo random number, or any of the examples described herein. In some embodiments, the key index may act as a seed for generating the transaction cryptogram. By including the seed in the track-2 discretionary data that is passed to the issuer, the issuer can verify the seed, and in some embodiments, regenerate the transaction cryptogram using the seed to verify the transaction cryptogram.

[0144] It should be understood that the track-2 equivalent data formats describe above are examples, and that in some embodiments, the track-2 equivalent data may omit some of the data elements, and/or may include additional data elements not specifically shown.

[0145] V. TRANSACTION VERIFICATION LOG

[0146] According to some embodiments, the mobile application may update a transaction verification log maintained by the mobile application at the end of a transaction to include information about the transaction in the transaction verification log. The mobile application may recognize the end of a transaction by recognizing that all transaction processing information and/or account data that may be needed by the access device to complete the transaction has been provided to the access device (e.g., recognizing that the last record defined in the AFL has been returned successfully or if no AFL, when the GPO response has been returned successfully).

[0147] FIG. 5 illustrates examples of data elements that can be include in a transaction verification log, according to some embodiments. The mobile application may maintain a transaction verification log per LUK or per set of account parameters. In some embodiments, the portable communication device may maintain a number of transaction verification logs for several LUKs or sets of account parameters, or optionally, once the current LUK or account parameters have been renewed or replenished, the transaction verification log corresponding to the previous LUK or account parameters can be deleted to save memory space on the portable communication device.

[0148] The transaction verification log may be associated with and/or may include the key index corresponding to the LUK or set of account parameters used in the logged transactions, and a sequence counter value associated with the key index or set of account parameters indicating the number of times the LUK or set of account parameters have been replenished. For each transaction conducted using the particular LUK or particular set of account parameters, the transaction verification log may include a transaction timestamp indicating the time of the corresponding transaction, an unpredictable number (UN) provided from the access device during the transaction (if available), an application transaction counter (ATC) value associated with the corresponding transaction (e.g., a value indicating the number of transactions that has been conducted using the mobile application at the time of the transaction), and a transaction type indicator indicating whether the corresponding transaction was conducted as an integrated chip based transaction or a magnetic stripe based transaction. The transaction timestamp may be the UTC time as determined by the portable communication device at the time of the transaction. In some embodiments, additional information such as the location of the portable communication device at the time of the corresponding transaction can be included in the transaction verification log. It should be understood that in some embodiments, the transaction verification log may include fewer data elements, and/or may include other data elements not specifically shown.

[0149] The transaction verification log can be used for various purposes such as post payment verification and account parameters replenishment. FIG. 6 illustrates a communication flow diagram of an example of a post-payment verification process, according to some embodiments. The post-payment verification process can be initiated by an issuer/host system 672 when issuer/host system 672 decides to check the account, for example, when a transaction flagged as being suspicious or potentially fraudulent is received, or when issuer/host system 672 checks the account randomly or periodically as a fraud-prevention measure.

[0150] Issuer/host system 672 may initiate the post-payment verification process by sending, to CBPP 680, a transaction log request 622 to request the transaction verification log associated with an account. The transaction log request 622 may include information such as an account identifier that can be used by CBPP 680 to identify the account. CBPP 680 may identify the account in question and the mobile

application that the account is registered to, and forward this information as transaction log request 624 to MAP 670. MAP 670 may identify and authenticate the portable communication device associated with the account and mobile application, and send transaction log request 626 to the identified mobile application of portable communication device 601.

[0151] Upon receiving the transaction log request 626, the mobile application of portable communication device 601 may retrieve the transaction verification log from the memory of the portable communication device, and package the data into transaction log information 628 for transmission to issuer/host system 672. The transaction log information 628 is derived from the transaction verification log stored on the portable communication device, and may include some or all of the information contained in the transaction verification log such as the per transaction details for each transaction such as the transaction timestamp, application transaction counter value, transaction type indicator, unpredictable number if available, and/or any combination thereof; the key index associated with the LUK or account parameters used for the transactions; the sequence counter associated with the LUK or account parameters; and/or any combination thereof. Alternatively or additionally, the transaction log information derived from the transaction verification log may include an authentication code (e.g., a message authentication code, hash value, etc.) computed over some or all of the information in the transaction verification log. For example, the authentication code may be computed over the per transaction details, or over the key index and/or sequence counter together with the per transaction details. In some embodiments, the authentication code can be generated by using the LUK as an encryption key.

[0152] After deriving the relevant transaction log information 628 from the transaction verification log, the mobile application on portable communication device 601 sends the transaction log information 628 to MAP 670. MAP 670 forwards the information as transaction log information 630 to CBPP 680, and CBPP 680 forwards the information as transaction log information 632 to issuer/host system 672. In some embodiments, CBPP 680 may perform verification of the received transaction log information, for example, if CBPP 680 tracks the transaction activity of the account, and may additionally or alternatively provide the verification result in the transaction log information 632 transmitted to issuer/host system 672.

[0153] When issuer/host system 672 receives the transaction log information 632, issuer/host system 672 may compare the information against the suspicious transaction, and/or compare the information against the transaction activity for the current LUK or set of account parameters. If the transaction log information 632 indicates the suspicious transaction was conducted by the mobile application of portable communication device 601 and/or the transaction log information 632 matches the transaction activity, issuer/host system 672 completes the post-payment verification process and maintains the account in active status.

[0154] If the transaction log information 632 indicates the suspicious transaction did not originate from the mobile application of portable communication device 601 or if the transaction log information 632 does not match the transaction activity at the issuer, issuer/host system 672 may suspend the account, and send a suspend notification to CBPP 680. CBPP 680 may suspend the account in its own system and forward the suspend notification to MAP 670. MAP 670 then forwards the suspend notification to the mobile application of portable communication device 601. In response to receiving the suspend notification, the mobile application may delete the current set of account parameters from the mobile application and display a message to request the user to contact the issuer.

[0155] VI. ACCOUNT PARAMETERS REPLENISHMENT

[0156] When a set of account parameters (e.g., LUK) expires due to the age of the account parameters or usage of the account parameters exhausting the associated set of one or more limited-use thresholds, a subsequent transaction conducted using the expired set of account parameters may be declined. In order to be able to continue to conduct transactions using the mobile application of the portable communication device, the mobile application may need to update, renew, refresh, or replenishment the set of account parameters available to the mobile application. In some embodiments, the transaction verification log may also be used during the account parameter replenishment process to verify that the mobile application or portable communicate device requesting new account parameters is the same application or device that had previously received and used the prior set of account parameters.

[0157] To facilitate the account parameters replenishment process, the mobile application of the portable communication device may track the usage of the set of account parameters (e.g., LUK), and maintain an account parameters status that indicate whether one or more limited-use thresholds associated with the account parameters or LUK has been exhausted or is about to be exhausted. For example, the mobile application may track how many transactions have been conducted using the set of account parameters or LUK, how much time has elapsed since the set of account parameters or LUK was generated, and/or the cumulative transaction amount over all transactions that were conducted using the set of account parameters or LUK. At the end of each transaction, the mobile application may update the usage of the set of account parameters or LUK being tracked by the mobile application, and compare the usage against the on-device set of one or more limited-use thresholds. In some embodiments, if the mobile application determines that the usage of the current set of account parameters or LUK has exhausted the on-device set of one or more limited-use thresholds or used beyond the usage limit, the mobile application may initiate an account parameters replenishment request. In some embodiments, the mobile application may initiate an account parameters replenishment request if the mobile application determines that the next transaction conducted using the current set of account parameters or LUK will exhaust the set of one or more limited-use thresholds. This can be done, for example, to help ensure that a valid set of account parameters or LUK is constantly available to the mobile application such that the next transaction conducted with the mobile application does not get declined.

[0158] FIG. 7 illustrates a communication flow diagram of an example of an account parameters replenishment process, according to some embodiments. In the example shown in FIG. 7, the account parameters replenishment process is initiated by the mobile application of portable communication device 701, and may be referred to as a replenishment pull process. When the mobile application determines that the set of one or more limited-use thresholds associated with the current set of account parameters have been exhausted or is about to be exhausted, the mobile application of portable communication device 701 may send an account parameters replenishment request 722 to MAP 770 to replenish the set of account parameters or LUK available to the mobile application.

[0159] The account parameters replenishment request 722 may include information identify the relevant account, mobile application, and/or portable communication device 701, and may include transaction log information derived from the transaction verification log stored on the portable communication device. The transaction log information provided in the account parameters replenishment request 722 may include some or all of the information contained in the transaction verification log such as the per transaction details for each transaction conducted using the current set of account parameters or LUK (e.g., transaction timestamp, application transaction counter value, transaction type indicator, unpredictable number if available, and/or any combination thereof). The transaction log information may include the key index associated with the current set of account parameters or LUK, and/or the sequence counter associated with the current set of account parameters or LUK. Alternatively or additionally, the transaction log information derived from the transaction verification log and provided in the account parameters replenishment request 722 may include an authentication code (e.g., a message authentication code, hash value, etc.) computed over some or all of the information in the transaction verification log. For example, the authentication code may be computed over the per transaction details, or over the key index and/or sequence counter together with the per transaction details. In some embodiments, the authentication code can be generated by using the LUK as an encryption key.

[0160] When MAP 770 received the account parameters replenishment request 722, MAP 770 forwards the request as account parameters replenishment request 724 to CBPP 780. Upon receiving the account parameters replenishment request 724, CBPP 780 may verify the transaction log information or request issuer/host system 772 to verify the transaction log information. If the transaction log information matches the transaction activity at CBPP 780 or issuer/host system 772, CBPP 780 may then generate a new set of account parameters (e.g., new key index and new LUK) to replenish the current set of account parameters at the mobile application. CBPP 780 may send a replenishment notification 726 to issuer/host system 772 to notify the issuer that a new set of account parameters is being replenished to the mobile application. In some embodiments, the replenishment notification 726 may include the new set of account parameters (e.g., new key index and new LUK) such that issuer/host system 772 may perform its own update.

Issuer/host system 772 may respond by sending an acknowledgment 728 to CBPP 780.

[0161] After the new set of account parameters are generated, CBPP 780 may send the new set of account parameters 730 to MAP 770. The new set of account parameters 730 may include a new key index, a new LUK, etc., and in some embodiments, may also include a new set of one or more limited-use thresholds associated with the account parameters or LUK that may have different usage limits than the previous thresholds. MAP 770 then forwards the data as the new set of account parameters 732 to the mobile application of portable communication device 701.

[0162] When the mobile application of portable communication device 701 receives the new set of account parameters (e.g., new LUK and new key index associated with the LUK), the mobile application delete the previous set of account parameters and associated transaction verification log details and usage tracking, and store the new set of account parameters. If the new set of account parameters has different usage limits for the set of one or more limited-use thresholds, the one or more limited-use thresholds can be updated with the new usage limits. The mobile application also increments the sequence counter for each successful account parameters replenishment. Once the mobile application has updated the set of account parameters, the mobile application of portable communication device 701 may send a confirmation 734 to MAP 780, and MAP 780 may forward this as confirmation 736 to CBPP 770 to confirm that the account parameters replenishment process was successful.

[0163] In some embodiments, if issuer/host system 772 is responsible for account parameters generation, instead of sending the replenishment notification 726 to issuer/host system 772, CBPP 780 may forward account parameters replenishment request 724 to issuer/host system 772, and have issuer/host system 772 generate the new set of account parameters. (e.g., new key index and new LUK) In such embodiments, issuer/host system 772 may provide the new set of account parameters to CBPP 780 and/or to MAP 770 for forwarding to the mobile application on portable communication device 701.

[0164] According to some embodiments, the account parameters replenishment process can be initiated by CBPP 770 and/or issuer/host system 772. An account parameters replenishment process that is not initiated by the mobile application may be referred to as a replenishment push process. For example, the account parameters replenishment process can be triggered by transaction activity monitored by CBPP 770 and/or issuer/host system 772. In some embodiments, CBPP 770 and/or issuer/host system 772 may maintain their own set of one or more limited-use thresholds, which may or may not have the same usage limits as the on-device limited-use thresholds maintained at the mobile application. CBPP 770 and/or issuer/host system 772 may track the usage of the current set of account parameters (e.g., LUK).

[0165] When CBPP 770 determines that the set of one or more limited-use thresholds at the CBPP 770 associated with the current set of account parameters have been exhausted or is about to be exhausted, CBPP 770 may send a push message to MAP 780 to request the mobile application to replenish its current set of account parameters. When issuer/host system 772 determines that the issuer set of one or more limited-use thresholds associated with the current set of account parameters have been exhausted or is about to be exhausted, issuer/host system 772 may send a push message to CBPP 770 and/or MAP 780 to request the mobile application to replenish its current set of account parameters.

[0166] Upon receiving a push message to replenish the set of account parameters from CBPP 770 or issuer/host system 772, MAP 780 may forward the push message to the mobile application of portable communication device 701. In some scenarios, portable communication device 701 may be powered off or the mobile application may not be active at portable communication device 701 at the time CBPP 770 and/or issuer/ host system 772 initiates the replenishment process. In such scenarios, MAP 780 may queue the push message for deliver to the mobile application at a later time, and may periodically attempt to reach the mobile application until MAP 780 establishes communication with the mobile application. When the mobile application receives the push message requesting the mobile application of portable communication device 701 to replenish the account parameters (e.g., LUK and associated key index), in response, the mobile application of portable communication device 701 may send an account parameters

replenishment request with the relevant transaction log information to MAP 780. The replenishment process may continue in a similar manner as the replenishment push process described above with reference to FIG. 7. In some embodiments, CBPP 770 and/or issuer/host system 772 may generate the new set of account parameters and provide them to MAP 780 together with the push message such that MAP 780 may provide the new set of account parameters to the mobile application when communication with the mobile application is established.

[0167] Although the above description of the account parameters replenishment process may have been described with reference to replenishing the LUK and the key index associated with the LUK, it should be understood that the account parameters replenishment process can be used, for example, to replenish other account parameters or related information such as to replenish a token that is used as a substitute for an account identifier. In some embodiments, a token can be replenished at the same time as the LUK and key index, or separately from the LUK and key index.

[0168] VII. CRYPTOGRAMS FOR TRANSACTIONS

[0169] According to some embodiments, because no secure element is required to be present to protect account credentials stored on the potable communication device, the account parameters for conducting cloud-based transactions may have a limited lifespan such that even if a given set of account parameters is compromised, the stolen account parameters would be of little use as they may have expired or will expire shortly. For example, instead of using a static key stored in a secure element to generate cryptograms during transactions as in some secure element implementations, the cloud-based transaction system uses limited-use keys in the generation of transaction cryptograms.

[0170] In some embodiments, two types of transaction cryptogram may be used – one for track-2 data used in magnetic stripe based transactions, and one for integrated chip based transactions. For both types of transaction cryptogram, the transaction cryptogram is generated using a limited use key (LUK). The difference between the two types of transaction cryptograms is the input data used for generating the cryptogram and/or the final format of the transaction cryptogram that is transmitted to the access device to conduct the transaction. For an integrated chip

based transaction, the input data used to generate the cryptogram may include dynamic data (e.g., data that changes for each transaction) received from the contactless reader of an access device during the transaction (e.g., terminal transaction data), while the input data for a magnetic stripe based transaction may be static data (e.g., data that does not change from one transaction to another such as a predetermined numeric string). This means that in some embodiments, for a magnetic stripe based transaction, either the CBPP or the mobile application itself can generate the transaction cryptogram as the generation of the transaction cryptogram does not rely on data from the contactless read of an access device; and for an integrated chip based transaction, the mobile application provides generation of the transaction cryptogram.

[0171] It should also be noted that in some embodiments, the input for generating the transaction cryptogram in a magnetic stripe based transaction can alternatively or additionally include dynamic data received from the contactless reader of an access device during the transaction (e.g., terminal transaction data). Furthermore, the input for generating the transaction cryptogram in an integrated chip based transaction can alternatively or additionally include static data.

[0172] In addition to being used in transaction cryptogram generation, in some embodiments, the LUK can be used to generate an authentication code when the mobile application communicates with the other components or entities of the cloud-based transaction system. For example, an authentication code or hash code can be generated over the transaction verification log details using the LUK as a key during the account parameters replenishment process.

[0173] FIG. 8 illustrates a block diagram of an example of a process 800 for generating a transaction cryptogram, according to some embodiments. Any one of the encryption functions 806, 812, 818, and/or 824 can be the same or be different than any of the other encryption functions. For example, any one of the encryption functions 806, 812, 818, and/or 824 may be implemented as triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), or other suitable encryption algorithms.

[0174] Process 800 can be divided into two parts – the first part relates to the LUK generation (blocks 802 to 814), and the second part relates to the transaction

cryptogram generation (blocks 816-828). The first part relating to the LUK generation can be performed once to generate a LUK (e.g., by CBPP or issuer/host system), and the second part relating to the transaction cryptogram generation can be performed multiple times using the LUK generated from the first part (e.g., by the mobile application) until the LUK has exceeded its set of one or more limited-use thresholds, at which time, the first part relating to the LUK generation can be performed again to replenish, renew, or refresh the LUK.

[0175] Process 800 may begin by encrypting account information 804 with a first encryption key 802 using an encryption function 806 to generate a second encryption key 808. The first encryption key 802 may be a base key that is associated with the issuer of the user's account, and the base key may be associated with a group of accounts. For example, the first encryption key 802 may be associated with a group of accounts within a BIN or PAN range designated for the cloud-based transaction service. In some embodiments, the first encryption key 802 may be a master derivation key (MDK) associated with the issuer of the account associated with the account information 804, and the first encryption key 802 can be maintained at the CBPP or at the issuer/host system.

[0176] The account information 804 may include account identifying information such as an account identifier (e.g., a PAN), an alternate account identifier (e.g., an alternate PAN), or a token that is a substitute for an account identifier, and may additionally include user identifying information such as a sequence number (e.g., a PAN sequence number (PSN)) that identifies the particular user of the account (e.g., when multiple users use the same account). For example, the account information 804 that is used as the input to encryption function 806 can be a concatenation of the account identifying information and the user identifying information, or an inverted version of the concatenation.

[0177] In some embodiments, the second encryption key 808 being generated from the account information 804 may include multiple portions that are each generated from different variations of the account information 804. For example, the second encryption key 808 may be divided into two portions. The first portion of the second encryption key 808 may be generated by encrypting the account information 804 using the first encryption key 802. The second portion of the second encryption

key 808 may be generated by inverting the account information 804 and encrypting the inverted account information using the first encryption key 802. The encryption function 806 used to generate the second encryption key 808 may be, for example, triple data encryption standard (TDES) or other suitable encryption algorithms, and may use an initial chaining vector of binary zeros. In some embodiments, the second encryption key 808 generated from the account information 804 may correspond to a unique derivation key (UDK) for the account.

[0178] Process 800 may continue by encrypting key index information 810 with the second encryption key 808 using an encryption function 812 to generate the limited-use key (LUK) 814. The key index information 810 may be derived from a key index that includes information pertaining to the generation of the LUK 814, and that may be used as a seed to generate LUK 814. For example, the key index may include time information indicating when the LUK 814 is being generated. In some embodiments, the time information can be represented as the numeric string 'YHHHH', where 'Y' (0-9) represents the least significant digit of the current year, and 'HHHH' (0001-8784) represents the number of hours since the start of January 1st of the current year expressed as digits (e.g., first hour of January 1st = 0001). In some embodiments, the key index may also include a replenishment counter value indicating the number of times that the LUK 814 has been renewed or replenished in a predetermined time period (e.g., number of times LUK 814 has been generated in each hour). For example, the replenishment counter value can be represented as the numeric string 'CC' (00-99). At the beginning of each hour, 'CC' starts at 00 and is incremented by 1 each time LUK 814 is generated. In some embodiments, the key index may include an applications transaction counter value, or a pseudo random number generated by the CBPP or the issuer.

[0179] According to some embodiments, the key index information 810 that is provided as input to the encryption function 812 may be generated by padding the key index with one or more numeric values. For example, the key index can be padded with a numeric value (e.g., 1 or 2 shown as 'm' or 'n' in FIG. 8) at the beginning of the key index and/or a numeric value (e.g., 80000000 shown as 'xxxxxxxx' in FIG. 8) at the end of the key index. In some embodiments, the LUK 814 being generated from the key index information 810 may include multiple portions that are each generated from different variations of the key index

information 810. For example, the LUK 814 may be divided into two portions. The first portion of LUK 814 may be generated by padding the key index with a first value to generate a first padded key index (e.g., 1YHHHHCC80000000), and encrypting the first padded key index using the second encryption key 808. The second portion of LUK 814 may be generated by padding the key index with a second value to generate a second padded key index (e.g., 2YHHHHCC80000000), and encrypting the second padded key index using the second encryption key 808. The encryption function 812 used to generate the LUK 814 may be, for example, TDES or other suitable encryption algorithms, and may use an initial chaining vector of binary zeros. It should be understood that the numeric values described herein are just examples, and that in some embodiments, other numeric values can be used.

[0180] After the LUK 814 is generated (e.g., by the CBPP or the issuer), the LUK 814 and the key index that includes information pertaining to the generation of LUK 814 may be provided to a portable communication device to facilitate generation of transaction cryptograms for transactions conducted using the portable communication device. The LUK may be associated with a set of one or more limited-use thresholds that limit the number of transactions that can be conducted using the LUK 814, such as those described herein. During execution of a transaction, the transaction cryptogram and/or the key index can be provided from the portable communication device to an access device, and the transaction may be authorized based on verification of the transaction cryptogram and whether the LUK 814 used to generate the transaction cryptogram has exceeded one or more of the LUK's limited-use thresholds.

[0181] As discussed above, in some embodiments, two types of transaction cryptograms can be generated. For a magnetic stripe based transaction, the transaction cryptogram 828 may be a reduced-length transaction cryptogram (may also be referred to as a decimalized transaction cryptogram). Transaction cryptogram 828 may be generated by encrypting static data 822 (e.g., can be a predetermined numeric string such as '0000000000000001') using the LUK 814 as an encryption key in encryption function 824 to form an encrypted static data or encrypted numeric string represented in hexadecimals (0-F). The encryption function 824 may be, for example, TDES or other suitable encryption algorithms, and may use an initial chaining vector of binary zeros. The encrypted static data (or

encrypted numeric string) may then be decimalized by using decimalize function 826 to generate the transaction cryptogram 828.

[0182] In some embodiments, the transaction cryptogram 828 may be divided into two data blocks. The decimalize function 826 used to generate the two data blocks of the transaction cryptogram 828 may include extracting numeric digits (0-9) from the encrypted static data or encrypted numeric string to form the first data block; and for the second data block, extracting hexadecimal digits (A-F) from the encrypted static data or encrypted numeric string, and converting each extracted hexadecimal digit into a numeric digit by subtracting ten from the corresponding hexadecimal digit to form the second data block. The first data block is then concatenated with the second data block to form the transaction cryptogram 828. In some embodiments, the decimalized transaction cryptogram 828 may have six digits, and may be embedded with the key index (e.g., 'YHHHHCC') in the track-2 equivalent data provide in a transaction authorization request message to request authorization for a transaction from the issuer.

[0183] For an integrated chip based transaction, the transaction cryptogram 820 may be generated by encrypting dynamic transaction data 816 using the LUK 814 as an encryption key in encryption function 818. The dynamic transaction data 816 may include, for example, some or all of the terminal transaction data 310 provided from the access device to the mobile application of the portable communication device during execution of the transaction. In some embodiments, the dynamic transaction data 816 may include the following data elements: authorized amount, other amount, terminal country code, terminal verification results, transaction currency code, transaction date, transaction type, and unpredictable number; and/or may include the application interchange profile (AIP), application transaction counter (ATC), and issuer application data (IAD). In some embodiments, some data elements may be omitted, and/or additional data elements not specifically described can be included. The data set that makes up the dynamic transaction data 816 is provided as input to the encryption function 818. In some embodiments, the transaction cryptogram 820 can be generated by enciphering the dynamic transaction data 816 using a first portion of the LUK 814, deciphering the enciphered dynamic transaction data using a second portion of the LUK 814, and then re-enciphering the deciphered dynamic transaction data using the first portion of the LUK 814.

[0184] It should be noted that according to some embodiments, in addition to the transaction cryptogram 820, the decimalized transaction cryptogam 828 can also be used and generated in an integrated chip based transaction, and the decimalized transaction cryptogram 828 can be inserted into the track-2 equivalent data.

[0185] FIG. 9 illustrates a block diagram of an example of encryption function 900, according to some embodiments. In some embodiments, encryption function 900 can be used as encryption function 818. For example, the data set that makes up the dynamic transaction data 816 may be concatenated together (e.g., in the order described above), and then divided into a set of data blocks D_1 to D_N of equal length (e.g., 8-byte data blocks). If the dynamic transaction data 816 does not divide equally into the length of the data blocks, the missing least significant bits in the last data block D_N can be zero filled. The first key KA may correspond to a first portion of the LUK 814 (e.g., most significant 8 bytes), and the second key KB may correspond to a second portion of the LUK 814 (e.g., least significant 8 bytes) An iterative enciphering process may be applied to the set of data blocks D_1 to D_N. The iterative enciphering process may include encrypting a first data block D_1 using key KA as the encryption key in a data encryption algorithm (DEA(e)). The result of the encryption is then exclusive-ORed with the next data block D_2. The result of the exclusive-OR operation is then used as the input for the next iteration of the enciphering process. The enciphering process continues until all data blocks D_1 to D_N has been processed, and the output I_N of the last exclusive-OR operation with the last data block D_N is encrypted to form the output of the iterative enciphering process O_N. The output of the of the iterative enciphering process O_N may then be deciphered using key KB as the decryption key in data decryption algorithm (DEA(d)). The output of the deciphering process O_{N+1} is then re-enciphered using key KA as the encryption key in a data encryption algorithm (DEA(e)) to generate the output O_{N+2}. According to some embodiments, the output O_{N+2} can be used as the transaction cryptogram 820.

[0186] It should be noted that in some embodiments, the encryption function 900 described with reference to FIG. 9 can be used to generate the authentication code that is used in the post-payment verification process and/or the account parameters replenishment process, for example, by applying the encryption function 900 over at least the transaction verification log stored on the portable communication device. In

some embodiments, the encryption function 900 described with reference to FIG. 9 can also be used for any of the encryption functions 806, 812, 818, and/or 824.

[0187] VIII. EXEMPLARY METHODS

[0188] FIG. 10 illustrates an exemplary flow diagram of a method 1000 for enhancing the security of a communication device (e.g., a portable communication device) when conducting a transaction using the communication device, according to some embodiments. Process 1000 can be performed, for example, by a mobile application executing on a portable communication device, and can be performed without using a secure element (although a secure element can be used in some embodiments).

[0189] At block 1002, a communication device may receive a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limits the usage of the LUK. The LUK may be received from a remote computer (e.g., a remote computer associated with MAP, CBPP, or issuer/host system). In some embodiments, the set of one or more limited-use thresholds may include at least one of a time-to-live indicating a time duration that the LUK is valid for, a predetermined number of transactions that the LUK is valid for, and/or a cumulative transaction amount indicating the total transaction amount that the LUK is valid for. In some embodiments, the set of one or more limited-use thresholds may include an international usage threshold and a domestic usage threshold.

[0190] According to some embodiments, the communication device may also receive, with the LUK, a key index that includes information pertaining to generation of the LUK. For example, the key index may include time information indicating when the LUK is generated, a replenishment counter value indicating the number of times the LUK has been replenished, a pseudo-random number that is used as a seed to generate the LUK, a transaction counter value indicating the number of transactions that has been previously conducted by a mobile application of the communication device at the time the LUK is generated, and/or any combination thereof.

[0191] At block 1004, a transaction (e.g., a payment transaction, access transaction, or other transaction that is performed using an account) can be initiated, for example, by placing the communication device in proximity to a contactless

reader of an access device such as a POS terminal. At block 1006, the communication device may generate a transaction cryptogram using the LUK. At block 1008, the communication device may send the transaction cryptogram to the access device to conduct the transaction. In some embodiments, the commination device may also send a token (e.g., a substitute for an account identifier) instead of a real account identifier to the access device to conduct the transaction. In some embodiments, process 1000 does not use a secure element to store the token or the LUK in the communication device. The transaction can be authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds and/or verification of the transaction cryptogram.

[0192] At block 1010, after conducting the transaction, process 1000 may determine if the set of one or more limited-use thresholds associated with the LUK has been exhausted or exceeded (or is about to be exhausted or exceeded). If it is determined that the set of one or more limited-use thresholds associated with the LUK has not been exhausted or exceeded (or is not about to be exhausted or exceeded), process 1000 may continue to block 1004 to conduct another transaction.

[0193] If it is determined that the set of one or more limited-use thresholds associated with the LUK has been exhausted or exceeded (or is not about to be exhausted or exceeded), the communication device may send a replenishment request for a new LUK to the remote computer at block 1012. The replenishment request may be sent in response determining that the set of one or more limited-use thresholds associated with the LUK has been exhausted, or in response to determining that a next transaction conducted with the LUK will exhaust the set of one or more limited-use thresholds. In some embodiments, the replenishment request may be sent in response to receiving a push message requesting the communication device to replenish the LUK

[0194] The replenishment request may include transaction log information derived from a transaction log (e.g., a transaction verification log) stored on the communication device. In some embodiments, the transaction log stored on the communication device may include, for each transaction conducted using the LUK, a transaction timestamp indicating the time of the corresponding transaction, an

application transaction counter value associated with the corresponding transaction, and/or a transaction type indicator indicating whether the corresponding transaction is a magnetic stripe based transaction or an integrated chip based transaction. In some embodiments, the transaction log information sent to the remote server or computer may include an authentication code computed over at least the transaction log using the LUK. If the transaction log information in the replenishment request matches the transaction log information at the remote computer, process 1000 may continue to block 1002, and communication device may receive a new LUK and a new key index associated with the new LUK.

[0195] FIG. 11 illustrates an exemplary flow diagram of a method 1100 for enhancing the security of a communication device when conducting a transaction using the communication device, according to some embodiments. Process 1100 can be performed, for example, by a computer associated with CBPP or issuer.

[0196] At block 1102, account information associated with an account is encrypted using a first encryption key to generate a second encryption key. In some embodiments, the account information may include an account identifier such as a PAN, an alternate account identifier such as an alternate PAN, or a token that is a substitute for an account identifier. In some embodiments, the first encryption key may be a master derivation key associated with the issuer of the account. According to some embodiments, encrypting the account information to generate the second encryption key may include encrypting the account information using the first encryption key to generate a first portion of the second encryption key, inverting the account information, and encrypting the inverted account information using the first encryption key to generate a second portion of the second encryption key. In some embodiments, the second encryption key may be a unique derivation key for the account

[0197] At block 1104, key index information is encrypted using the second encryption key to generate a limited-use key (LUK). The key index information may include a key index having information pertaining to generation of the LUK. For example, the key index information may include a counter value indicating the number of times that the LUK has been renewed or replenished in a predetermined time period and/or time information indicating when the LUK is generated. In some

embodiments, encrypting the key index information to generate the LUK may include padding the key index with a first value to generate a first padded key index information, and encrypting the first padded key index information to generate a first portion of the LUK. Encrypting the key index information to generate the LUK may also include padding the key index with a second value to generate a second padded key index information, and encrypting the second padded key index information to generate a second portion of the LUK.

[0198] At block 1106, process 1100 associates the LUK with a set of one or more limited-use thresholds that limits the usage of the LUK. At block 1108, the LUK and the key index are provided to a communication device (e.g., a portable communication device) to facilitate the generation of a transaction cryptogram for a transaction conducted using the communication device. The transaction may be authorized based on the LUK and the transaction cryptogram (e.g., whether usage of the LUK has exceeded the set of one or more limited-use thresholds and/or verification of the transaction cryptogram).

[0199] In some embodiments, when the transaction is an integrated chip based transaction, the transaction cryptogram may be generated by enciphering transaction information (e.g., dynamic transaction information such as terminal transaction data received from an access device during a transaction) using a first portion of the LUK, deciphering the enciphered transaction information using a second portion of the LUK, and re-enciphering the deciphered transaction information using the first portion of the LUK.

[0200] When the transaction is a magnetic stripe based transaction, the transaction cryptogram may be generated by encrypting a predetermined numeric string using the LUK, and decimalizing the encrypted predetermined numeric string. In some embodiments, decimalizing the encrypted predetermined numeric string may include extracting numeric digits from the encrypted predetermined numeric string to form a first data block, extracting hexadecimal digits from the encrypted predetermined numeric string and converting each extracted hexadecimal digit into a numeric digit to form a second data block, and concatenating the first data block and the second data block to form the transaction cryptogram. The transaction

cryptogram and/or the key index can be embedded in track-2 equivalent data of an authorization request message.

[0201] IX. CLOUD-BASED PAYMENTS PLATFORM (CBPP)

[0202] This section describes additional details of some of the functionalities that can be performed by the cloud-based payments platform (CBPP) (e.g., CBPP 180). In some embodiments, these functionalities may include key management, active account management and account parameters replenishment, payment and payment transaction processing, verification for payment, provisioning, lifecycle management, and post-payment verification. Communications between CBPP and mobile application platform (MAP) can be established using secure channels such as those adhering to transport level security (TLS) protocol, time bound secure sockets layer (SSL) protocol, or hypertext transfer protocol secure (HTTPS) protocol. Communications between CBPP and the issuer/host system can be established using secure channels adhering to the security requirements of issuer.

[0203] KEY MANAGEMENT

[0204] The issuer of an account may use a dedicated set of keys (e.g., MDKs) per bank identification number (BIN) range or per primary account number (PAN) range for cloud-based payment transactions in order to avoid situations where the same keys are used for both secure element based and cloud-based transactions. A MDK can be used as a base key to generate the LUKs that are provided to a portable communication device. In some embodiments, CBPP may provide its own set of issuer MDK keys (specific for the cloud-based environment) which are stored in its own hardware security modules. In some embodiments, instead of using its own set of MDKs to generate LUKs, CBPP may make calls to the issuer/host system to retrieve LUKs stored in hardware security modules of the issuer/host system.

[0205] ACTIVE ACCOUNT MANAGEMENT AND ACCOUNT PARAMETER REPLENISHMENT

[0206] The cloud-based payments techniques described herein do not require the use of a secure element to securely store data such as a unique derived key (UDK). As such, the portable communication device may not have access to all the capabilities associated with a secure element, such as the capability to generate

application cryptogram (AC) for transactions using only securely stored information. In order to mitigate the risk of account parameters being compromised, limited-use account parameters can be generated by CBPP periodically and replenished in the mobile application of the portable communication device as well as refreshed in the issuer/host system in order to maintain the account in the active state.

[0207] For the active account management process to be initiated, CBPP may receive a request for account parameters generation from MAP or the issuer/host system. For example, MAP may request a new set of account parameters such as a limited-use key and associated key index from CBPP in response to a request for account parameters data update from the mobile application. As another example, the issuer/host system may check, during transaction processing, if the current set of account parameters is still valid (e.g., being used within its limited-use thresholds such as the number of allowed transactions, the time-to-live, etc.). In case the threshold for a given risk setting gets exceeded, the issuer/host system may alert CBPP that a new set of account parameters is to be updated in the mobile application.

[0208] In response to a request, CBPP may generate a set of account related data. The account related data may include semi-static account information and dynamic account parameters that changes with each replenishment such as a LUK that may be used by the mobile application to generate a transaction cryptogram (e.g., an application cryptogram (AC)) when the portable communication device is presented to contactless reader of access device. The account parameters may be account specific (e.g., different account parameters for different accounts of the user), portable communication device specific (e.g., different account parameters for different portable communication devices of the user, even when the underlying account is the same), and/or mobile application specific (e.g., different account parameters for different mobile applications, even when the different mobile applications are within the same portable communication device).

[0209] The set of account related data may also include risk management parameters (e.g., limited-use thresholds such as number of consecutive transactions allowed and time-to-live) that will indicate to issuer/host system how it is supposed to use the transaction data. The risk parameters may be account specific (e.g., all

cloud-based transactions conducted with an account are consolidated for assessment of risk parameters), portable communication device specific (e.g., all cloud-based transactions conducted with a particular portable communication device are consolidated for assessment of risk parameters), mobile application specific (e.g., all cloud-based transactions conducted via a particular mobile application are consolidated for assessment of risk parameters), and/or account parameters specific (e.g., each set of account parameters has its own set of risk parameters).

[0210] In some embodiments, the issuer/host system may implement its own set of risk limits or limited-use thresholds that is applied per account to have a consolidate view of all transactions performed on the account, because the same account can be provisioned in different mobile applications which may have their own risk limits, while all transactions conducted by the different mobile applications using that account may be authorized by the same issuer/host system. The risk management parameters can be pre-defined in both the mobile application and the issuer/host system, or can be managed separately by other systems, so that CBPP may not need to generate them. The set of account related data may also include device threshold management parameters that are used to trigger the update of account parameters in the mobile application as well as to update risk management parameters the in issuer/host system when possible.

[0211] The mobile application may store or receive from the cloud a number of risk management parameters (e.g., limited-use thresholds) that trigger the update of the current set of account parameters. When account parameters are close to the point when they become out of date (e.g., when it is that a next transaction conducted with the LUK will exhaust the set of one or more limited-use thresholds), the mobile application may request an update from CBPP via MAP to replenish account parameters. The device threshold management parameters monitored by the mobile application may include, for example, a number of transactions with a given set of account parameters that can be performed before the account parameters need to be updated (e.g., five transactions). Mobile application may send an alert to the mobile wallet platform before this limit gets exceeded in order to let portable communication device be used for one or more transactions before they start to get declined (e.g., the alert can be sent after four transactions to allow portable communication device to be used for one more transaction). Hence, if the

account parameters are valid for a predefined number of transactions in the CBPP risk management parameters, then the number of transactions for the on-device threshold management parameters managed by mobile application can be configured with a threshold lower than the value in CBPP to trigger replenishment.

[0212] The device threshold management parameters may also include a time-to-live for a given set of account parameters before they need to be updated (e.g., five days). Mobile application 114 can notify the mobile wallet platform before this limit gets depleted in order to request a new set of account parameters (e.g., after four days). Hence, if account parameters have an expiration time in the CBPP, then the value of the time-to-live for on device threshold management parameters managed by mobile application can be configured with a threshold before that specified time in the CBPP to trigger replenishment. In some embodiments, the device threshold management parameters may also include but not limited to: a use transaction amount for the mobile application to make a decision whether account parameters should be updated or not (e.g., smaller transaction amounts may not require an immediate update of the account parameters); a cumulative transaction amount as the trigger for account parameters update based on the sum of individual transaction amounts; and/or a domestic versus international risk settings in order to trigger updates for international transactions more often in case they are considered more risky.

[0213] Since the account parameters are intended for limited use, additional risk management parameters specific to the cloud-based environment may be implemented and performed by the issuer/host system. These risk management parameters can either be provided to the issuer/host system by CBPP during active account management process, or they can be defined and managed separately. For example, the issuer/host system may verify that the current set of account parameters (e.g., LUK and associated key index) can be used for only a limited number of times (e.g., five times) before the issuer/host system raises an alert to request CBPP to generate a new set of account parameters to be replenished in the mobile application. The issuer/host system may also check that the current set of account parameters can only be used for a limited period of time (e.g., five days) before a new set of account parameters need to be generated by CBPP and sent to the mobile application.

[0214] Additional risk management parameters checks such as individual transaction amounts and cumulative total transaction amounts can also be performed by the issuer/host system. For example, smaller transaction amounts may not require an immediate update of the account parameters while high value transactions may require updates more often. As another example, when the cumulative total transaction amount based on the sum of individual transaction amounts gets exceeded, issuer/host system may notify CBPP that a new set of account parameters needs to be generated and replenished in mobile application. Domestic versus international risk settings may also be checked to trigger updates for international transactions more often in case they are considered more risky.

[0215] After CBPP receives a request for account parameters to be updated from either the MAP or the issuer/host system, CBPP can proceed with data generation for a given account. CBPP may use its own set of issuer MDK keys (specific for cloud-based environment) which it stores in its own hardware security modules and generate the LUK derived from the MDK using a newly generated key index, or CBPP may retrieve LUKs derived from the MDK using the newly generated key index from issuer/host system's hardware security modules.

[0216] After generating or otherwise retrieving the new set of account parameters, CBPP may send the account parameters to the entities that have requested it. MAP may receive the new set of account parameters and device threshold management parameters, and further send it to the mobile application. In some embodiments, the set of risk parameters or limited-use thresholds for a given account may change over time, and the new set of account parameters may have different thresholds than the previous set of account parameters. The threshold limits may change, for example, based on consumer spending habits, or if the consumer is travelling abroad. The issuer/host system may also receive the new set of account parameters from CBPP. In some embodiments, CBPP may be disconnected from the issuer/host system or may not be real-time connected. In this case, the issuer/host system may use a time stamp in the authorization message to determine when the data has been generated. In particular, the key index may be generated to contain the notion of the date when the account parameters were generated.

[0217] After MAP and the issuer/host system receive the new set of account parameters and device threshold management parameters from CBPP, they may perform certain actions. MAP may deliver and apply the new set of account parameters to the mobile application over a communication network. After the set of account parameters gets replenished in the mobile application, the old set of set of account parameters becomes obsolete and can be deleted from the mobile application. If MAP is unable to communicate to the mobile application immediately, it may keep trying to do so until communication to the mobile application is established; otherwise the issuer/host system may start declining transactions that are performed with the old set of account parameters from that point of time. In some embodiments, MAP may receive a confirmation from the mobile application that the account parameters have been updated in order to notify the issuer/host system to start using the new set of account parameters. The issuer/host system may also update risk management parameters for a given set of account parameters as soon as it gets an update. In case the issuer/host system received an update from CBPP directly real-time or with a certain delay, it may refresh risk management parameters for the new set of account parameters, for example, if the issuer/host system receives a confirmation form CBPP that the new set of data has been successfully applied to the mobile application. In case the issuer/host system doesn't receive an update directly from CBPP, the issuer/host system may receive the new set of account parameters in the first transaction conducted with portable communication device after the update. At that moment, the processing authorization system may activate the new risk management parameters for the new set of account parameters and apply a different policy or obsolete the old set of account parameters.

[0218] The issuer/host system may operate in sync with CBPP and consequently with MAP to ensure that the transaction data processing process is synchronized with the account parameters generation process. The data generation system and data host processing system may also use algorithms, time stamps and other mechanisms to ensure that the data in the issuer/host system and the mobile application are consistent, up to date, and abide by the same risk model.

[0219] PAYMENT AND PAYMENT TRANSACTION PROCESSING

[0220] When the payment transaction is initiated at an access device and then processed by the processing authorization system, the mobile application and the issuer/host system may take additional actions to process the cloud-based transaction. When the payment transaction occurs, and the portable communication device and contactless reader exchange data, the mobile application may use the LUK or together with it associated key index stored in the mobile application to generate a transaction cryptogram (e.g., an application cryptogram (AC)). From the reader perspective, the transaction may look like a regular contactless transaction. For an integrated chip based transaction, the access device map provide an unpredictable number (UN) that is used for the transaction cryptogram generation. For a magnetic stripe based transaction, the transaction cryptogram may be generated by the mobile application without using input from access device. In some embodiments, a dynamic card verification value (dCVV) may be omitted.

[0221] After the mobile application sends the transaction cryptogram and other transaction data to the access device, the mobile application may check that the account parameters are still valid by checking the on-device threshold management parameters (e.g., on-device limited-use thresholds). The mobile application may alert MAP when the device threshold management parameters are exceeded and request a new set of account parameters from CBPP. The mobile application may check that even if the account parameters have not been updated in the mobile application, that the old set of account parameters can still be used in subsequent transactions in order to let the issuer/host system makes the authorization and risk decision.

[0222] After the interaction between the mobile application and the access device takes place, the transaction data is passed by the merchant and acquirer to the issuer/host system. When the issuer/host system receives the transaction data in the authorization request message, the issuer/host system may validate the transaction cryptogram and other transaction data, convert an alternate account identifier or token assigned into a real account identifier (e.g., a real PAN) if necessary, perform risk parameter checks, and verify the account is in a good standing. The issuer/host system may verify that the data in particular the

transaction cryptogram and key index are still valid for a given account by checking risk management parameters. CBPP may be alerted when risk management parameters are exceeded and request a new set of account parameters from CBPP to be replenished in mobile application via the MAP. Even if the account parameters have not been updated in the mobile application, the issuer/host system may verify that the old set of account parameters can still be used in the subsequent transactions in case the issuer believes that this risk is acceptable for a given account, BIN or PAN range or specific transaction environment (e.g., domestic vs. international).

[0223] Although the account parameters may have been exceeded from the point of view of the issuer/host system because they haven't been updated in the mobile application, the issuer/host system may allow the transaction and provide some level of tolerance. CBPP may be notified that the issuer/host system may start declining further transactions if the account parameters are not updated in mobile application. Thresholds are set for each of the risk management parameters in the issuer/host system such as the number of transactions and time to live that would allow CBPP to be notified in advance before the actual risk management parameters are exceeded. This may give additional time to CBPP to generate a new set of account parameters and let MAP to replenish the account parameters in mobile application.

[0224] VERIFICATION FOR PAYMENT

[0225] To conduct a transaction, the consumer may activate the portable communication device before presenting portable communication device to contactless reader in order to proceed with the transaction. In some embodiments, activation of the portable communication device may involve the consumer entering input for a consumer device cardholder verification method (CDCVM) on the user interface of the portable communication device. Depending on the mobile application configuration, the CDCVM may be at the device level (e.g., screen lock) or at the mobile application level (e.g., application password/passcode). The mobile application may be set up to use a CDCVM on every transaction, or on every transaction greater than a certain transaction amount. If the mobile application is configured to use the CDCVM, the consumer may be prompted to enter an input corresponding to the CDCVM for authentication before or during the mobile payment

transaction. If a CDCVM is used on a transaction and the CDCVM was obtained before presentment of the portable communication device to contactless reader, the transaction may proceed to completion. If a CDCVM is used on a transaction and the CDCVM was not obtained before presentment of the portable communication device to the contactless reader, the transaction process may depend upon the merchant access device version.

[0226] CBPP may provide a set of functions where issuer can set the CDCVM, and this CDCVM configuration information (e.g., screen lock, passcode, etc.) is provisioned to the mobile application. CBPP may support the issuer CDCVM requirements, and allow the issuer to configure the CDCVM data in the provisioning data. In some embodiments, the issuer/host system may determine if an input corresponding to a CDCVM was entered. Where an input corresponding to a CDCVM is captured by the device, the result can be passed to the issuer/host system in the authorization message for transaction processing.

[0227] PROVISIONING

[0228] CBPP may provide a set of provisioning functions that allow cloud-based account data to be sent to MAP. CBPP may manage the data per cloud-based account and ensure the data is sent to MAP per request. CBPP may perform data preparation before sending to MAP, and support a provision function where an issuer could initiate a request to replenish or update the cloud-based account data. CBPP may provide a provisioning function to provision account parameters data to MAP per account holder, and prepare and package the data before sending to MAP. For example, CBPP may provide a function to provision the semi-static data portion (e.g., account identifier or token) and the dynamic data portion (e.g., LUK and key index) to MAP. CBPP may maintain a state machine per account and provide push or pull functionality to/from MAP for initiating a provisioning/replenishment request. CBPP may provide a replenishment function to provision account parameter data to MAP per account holder. CBPP may provide a provisioning/replenishment functionality with push features from the issuer. CBPP may provide provisioning/replenishment functionality that supports a single account which could be initiated by MAP or the issuer/host system. In some embodiments, CBPP may

provide updated account parameters as part of a provisioning/replenishment request only if invoked by the mobile application.

[0229] LIFE CYCLE MANAGEMENT

[0230] Lifecycle management is a set of functions which perform account lifecycle events. CBPP may receive and process lifecycle event messages from MAP or from the issuer/host system. For some cases, the lifecycle request can be initiated by the consumer as in the case of deleting an account from the mobile application or blocking an account from the issuer to handle fraud activity. CBPP 180 may perform lifecycle management functions per account, and provide account lifecycle events such as adding, deleting, suspending, and resuming suspended accounts. In some embodiments, account lifecycle events may include replacing or blocking accounts, and/or managing lost or stolen accounts. CBPP may provide an interface for MAP and/or the issuer/host system to perform a lifecycle update of a consumer account. The query may trigger provisioning or replenishment of new account parameters. In some embodiments, CBPP may act on the lifecycle events such as deleting or suspending accounts upon such a request immediately. CBPP may provide notification of all lifecycle events to impacted systems, such as the issuer/host system and MAP.

[0231] POST-PAYMENT PROCESSING

[0232] Post payment verification may mitigate the risk against counterfeit account parameters. It may also reduce the exposure on account parameters stored on the portable communication device, e.g. the issuer/host system can perform periodic verification, which limits the exposure associated with account parameters stored on the portable communication device. CBPP may define a protocol to exchange post payment verification messages. The post payment verification protocol may be based on real time interfaces and may follow transport level security (TLS). Either issuer/host system and/or CBPP can trigger the post payment verification message exchange. CBPP may provide options for issuers to configure the post payment verification parameters, which triggers the post payment verification message exchange with CBPP. For example, an issuer may configure the parameters such that CBPP triggers the post payment verification on transactions above a threshold (e.g., $100). Issuer may configure the parameters such that CBPP triggers the post

payment verification on every renewal of account parameters or after a number of renewals (e.g. after five renewals). In some embodiments, an issuer may configure the parameters such that the issuer/host system initiates the post payment verification. In this case, CBPP facilitates messages exchange between the issuer/host system and the mobile application.

[0233] In some embodiments, CBPP may refrain from taking any action based on the results of verification, and may instead informs the issuer/host system about suspicious activity. The issuer/host system may decide an appropriate action based on their process and risk profile of the account. CBPP may support post-payment processing handling using a transaction verification log to verify whether the appropriate device made a payment. CBPP may support post-payment processing handling using the transaction verification log to verify whether the appropriate device is initiating the request for account parameters replenishment, e.g., by verifying that the transaction log for a given set of account parameters stored on the portable communication device matches the transactions at the issuer/host system. CBPP may provide options to configure thresholds to triggers post payment verification messages from CBPP. CBPP may take life cycle management action based on the results of post payment verification. If verification fails, then CBPP may inform the issuer/host system about the suspicious activity. CBPP may provide additional information, such as location information about a transaction or unique device identifiers, in the transaction verification log.

[0234] X. MOBILE APPLICATION PLATFORM (MAP)

[0235] This section describes additional details of some of the functionalities that can be performed by the mobile application platform (MAP) (e.g., MAP 170). According to some embodiments, MAP may manage the mobile application and intermediate communications between CBPP and the mobile application. MAP may support cloud-based payment interactions such as enrolling into a cloud-based payment service, provisioning cloud-based payment accounts, active account management (i.e., account parameter replenishment, account lifecycle management, and post payment transaction verification log requests. MAP and CBPP may communicate using a secure transport channel such as time bound SSL or HTTPS.

MAP and CBPP may exchange secure web service message by using Web Services Security (WSS).

[0236] To communicate with the mobile application, MAP may authenticate the user, the portable communication device, and/or the mobile application using single or multifactor authentication to establish a secure channel between the mobile application and MAP. In support of this, MAP may establish an account with the consumer with a unique username and password. The password can be stored and verified by MAP. The consumer can create their mobile application credential (username/password) via the enrollment process. In some embodiments, this username and password may be different or the same as the portable communication device verification or CDCVM.

[0237] ENROLLMENT AND ACCOUNT PROVISIONING

[0238] MAP may forward account and consumer enrollment data received from the mobile application to CBPP or the issuer/host system for validating enrollment requests and performing issuer defined identification and verification processes. The issuer may be involved in the enrollment process (e.g., the issuer makes the accept/decline enrollment decision or delegates the decision to a third party under pre-defined conditions). In both cases, the issuer may be in control of the criteria and specifically defines account verification methods and the consumer authentication methods. MAP may support the receipt of an enrollment request and associated enrollment data from the mobile application.

[0239] MAP may route the enrollment request and associated data to CBPP and/or the issuer/host system. Upon successful enrollment, MAP may initiate a provisioning request with CBPP. If provisioning is successful by CBPP, MAP may receive the data from CBPP to configure the new cloud-based payment account in the mobile application. MAP may receive a provisioning confirmation or failure notification from the mobile application. MAP may route the confirmation or failure notification from the mobile application to CBPP and/or the issuer/host system. If provisioning is not successful by CBPP, MAP may receive an enrollment failure notification from CBPP, and MAP may route the provisioning failure notification to the mobile application. The mobile application may display an appropriate message to the consumer.

[0240] ACTIVE ACCOUNT MANAGEMENT

[0241] In order to mitigate the risk of the account parameters being compromised, account parameters are periodically generated by CBPP (or by the issuer/host system) and replenished in the mobile application as well as refreshed in the issuer/host system in order to maintain the account in the active state. For the active account management process to be initiated, CBPP may receive a replenishment request for new account parameters from the mobile application through MAP. CBPP may also act upon a replenishment request received from the issuer/host system. MAP acts as a broker and routes the communications to and from the mobile application and to and from CBPP for active account management interactions.

[0242] In a pull implementation, MAP receives an account parameter replenishment request from the mobile application. Before initiating the request message exchange from the mobile application, MAP may establish a secure communication channel. After receiving the replenishment request, MAP forwards the replenishment request message to CBPP. After processing the replenishment request, CBPP sends new account parameters to MAP, which then forwards them to the mobile application. If necessary, MAP may re-establish a secure connection with mobile application. If MAP is not successful in sending the account parameters replenishment response from CBPP to the mobile application after a pre-determined number of attempts in a time window, MAP may notify CBPP that the account parameter replenishment delivery attempt was not successful.

[0243] In a push implementation, CBPP (or the issuer/host system) initiates the process to update the account parameters. CBPP sends a push message to MAP to initiate the replenishment push. MAP then sends the push message to the mobile application. The mobile application then generates the account parameter replenishment request per the pull flow described above. Before initiating the exchange of sensitive information, MAP may perform user, portable communication device, and/or application level authentication per security requirements. If MAP is not successful in sending the account parameters replenishment response from CBPP to the mobile application after a pre-determined number of attempts in a

specified time window, MAP may notify CBPP that the account parameter replenishment attempt was not successful.

[0244] Upon the mobile application receiving and processing the new set of account parameters from either the push or pull implementations, mobile application may generate a status or confirmation notification to MAP, which then forwards the status or confirmation notification to CBPP.

[0245] LIFECYCLE MANAGEMENT

[0246] When a consumer initiates account deletion, MAP may facilitate a delete message exchange from the mobile application to CBPP and the issuer/host system. MAP may delete the account data associated with the account from its database, and forward the delete message from the mobile application to the CBPP.

[0247] When an issuer initiates account deletion, MAP may facilitate a delete message exchange from CBPP or the issuer/host system to the mobile application. The issuer/host system may send a delete request to CBPP or to MAP. MAP may forward the delete message from the issuer/host system or CBPP to mobile application. MAP may send an acknowledgement to CBPP or the issuer/host system after receiving the acknowledgment from mobile application. MAP may ensure that account delete request is sent to the appropriate mobile application installed on the appropriate portable communication device. MAP may delete the data associated with the deleted account from its records to ensure that the previously provisioned account for the particular consumer's mobile application profile is no longer an active cloud-based payments account.

[0248] When the issuer/host system or CBPP initiates account suspension, MAP may facilitate a suspend message exchange from CBPP or the issuer/host system to mobile application. The issuer/host system may send a suspend request to CBPP or to MAP. MAP may forward the suspend message from the issuer/host system or CBPP to mobile application. MAP may send an acknowledgement to CBPP or the issuer/host system after receiving the acknowledgment from the mobile application. MAP may ensure that account suspend request is sent to the appropriate mobile application installed on the appropriate portable communication device.

[0249] When the issuer/host system or CBPP initiates account resumption, MAP may facilitate a resume message exchange from CBPP or the issuer/host system to the mobile application. The issuer/host system may send a resume request to CBPP or directly to MAP. MAP may forward the resume message from the issuer/host system or CBPP to the mobile application. MAP may send an acknowledgement to CBPP or the issuer/host system after receiving the acknowledgment from the mobile application. MAP may ensure that an account resume request is sent to the appropriate mobile application installed on the appropriate portable communication device.

[0250] POST-PAYMENT PROCESSING

[0251] Post payment interactions can help issuers mitigate the risk of account parameters being compromised and hence can help limit the exposure of the account parameters stored on the portable communication device. MAP may support the receipt of information that gets captured from the on-device transaction verification log (e.g., corresponding to a particular the key index) for the purposes of ensuring the veracity of account parameters replenishment requests. The issuer/host system working in conjunction with CBPP has the option of initiating a request, through MAP, for transaction verification log data captured and stored by the mobile application. The mobile application may respond, via MAP, to the request with the requested transaction verification log data. This data can then be verified by the issuer/host system in order to confirm if a particular transaction was originated by the queried portable communication device. Examples of the data elements that may be used for this purpose may include, for each transaction conducted using the set of account parameters, the transaction time (e.g., contactless interaction time), application transaction counter (ATC) that counts the number of transactions conducted from mobile application, transaction amount, and/or terminal unpredictable number (UN) received from the access device during the transaction.

[0252] For the purposes of using transaction verification log to ascertain whether a transaction was conducted from a certain portable communication device, MAP may receive a request for mobile application transaction verification log data from the CBPP originated by the issuer/host system. For the purposes of using the transaction verification log to provide a degree of assurance to CBPP that the

request is originating from the appropriate portable communication device, MAP may use information provided from the transaction verification log in account parameter replenishment requests from the mobile application. MAP may identify and authenticate the portable communication device before transmitting or receiving post payment interaction messages to and from the mobile application.

[0253] XI. MOBILE APPLICATION

[0254] This section describes additional details of some of the functionalities that can be performed by the portable communication device and the mobile application installed on the portable communication device used to conduct cloud-based transactions. FIG. 12 illustrates a detailed block diagram of a portable communication device 1201, according to some embodiments. Portable communication device 1201 may include device hardware 1204 and memory 1202. Device hardware 1204 may include a processor 1205, a communications subsystem 1209, a use interface 1206, a display 1207 (which may be part of user interface 1206), and a contactless interface 1208. Processor 1205 can be implemented as one or more integrated circuits (e.g., one or more single core or multicore microprocessors and/or microcontrollers), and is used to control the operation of portable communication device 1201. Processor 1205 can execute a variety of programs in response to program code or computer-readable code stored in memory 1202, and can maintain multiple concurrently executing programs or processes. Communications subsystem 1209 may include one or more RF transceivers and/or connectors that can be used by portable communication device 1201 to connect with external networks (e.g., communication network 192) and communicate with other devices. User interface 1206 can include any combination of input and output elements to allow a user to interact with and invoke the functionalities of portable communication device 1201. In some embodiments, display 1207 may be part of user interface 1206.

[0255] Contactless interface 1208 may include one or more RF transceivers to interact with a contactless reader of an access device. In secure element based implementations, only the secure element may have access to contactless interface 1208. In the cloud-based payments techniques described herein, contactless interface 1208 can be accessed by the mobile OS 1214 without requiring the user of

a secure element. In some embodiments, display 1207 can also be part of contactless interface 1208, and is used, for example, to perform transactions using QR codes, bar codes, etc.

[0256] Memory 1202 can be implemented using any combination of any number of non-volatile memories (e.g., flash memory) and volatile memories (e.g., DRAM, SRAM), or any other non-transitory storage medium, or a combination thereof media. Memory 202 may store a mobile OS 1214 and a mobile application environment 1210 where one or more mobile applications reside including mobile application 1212 (e.g., a mobile wallet application, mobile payment application, etc.) to be executed by processor 1205. Mobile OS 1214 may implement a set of card emulation APIs 1216 that can be invoked by mobile application 1212 to access contactless interface 208 to interact with an access device.

[0257] For cloud-based payments implementations, the payment system environment (e.g., PPSE) and mobile payment application functionalities are consolidated into mobile application 1212, whereas secure element based implementations may provide some or all of these functionalities from a secure element. Mobile application 1212 may include cloud-based payments logic 1250. Cloud-based payments logic 1250 may include contactless payment logic 1258, proximity payment system environment (PPSE) logic 1256, transaction verification log 1254, and account parameters thresholds 1252 (e.g., set of one or more limited-use thresholds associated with LUK 1242). Contactless payment logic 1258 may include functionalities that enable contactless communications to carried out to conduct a contactless transaction with a contactless reader of an access device. PPSE logic 1256 is used to inform the access device which payment product is available on mobile application 1212. The access device then uses this information to select the payment account to initiate a contactless transaction. Transaction verification log 1254 can be used for post-payment support. Mobile application 1212 may maintain transaction verification log 1254 (can be hidden from the consumer) retaining transaction details for transactions initiated from mobile application 1212. Mobile application 1212 may also use the transaction verification log 1254 to support active account management processes and post payment interactions. Account parameters thresholds 1252 (e.g., limited-user thresholds) are initially configured and can potentially be updated with different thresholds to inform mobile application 1212

when to initiate a request for updated account parameters (e.g., time-to-live, number of transactions, cumulative transaction amount, etc.).

[0258] Mobile application 1212 may also include account parameter storage 1240 and mobile application platform (MAP) communications logic 1246. Account parameter storage 1240 stores the account parameters (e.g., account identifier or alternate account identifier or token, LUK 1242, key index 1244, etc.) that are used to initiate a cloud-based payment transaction. MAP communications logic 1246 is used to enable secure communications with a mobile application platform (MAP) in order to request, send, and receive information to manage a user's cloud-based payment accounts. This may include logic to consume and process information for account management logic 1230.

[0259] Account management logic 1230 includes logic to process information for the cloud-based payments services such as enrollment logic 1232, provisioning logic 1233, active account management logic 1236, lifecycle management logic 1234, and post payment interactions logic 1238. Enrollment logic 1232 includes logic for a consumer to initiate the enrollment of an account to the cloud-based payment service. Provisioning logic 1233 includes logic to process the issuer data to configure the account into mobile application 1212, including the provisioning of the initial account parameters. Active account management logic 1236 can be used to initiate a request with MAP to update the account parameters when account parameter thresholds have been exceeded. Lifecycle management logic 1234 may include logic to initiate and process account lifecycle events such as consumer initiated delete, issuer-initiated delete, issuer-initiated suspend, and/or issuer-initiated resume, etc. Post payment interactions logic 1238 is used to support payment verification. Post payment interactions logic 1238 may include logic to receive and respond to requests from MAP for transaction verification log 1254. Post payment interactions logic 238 can also be used to support account parameters replenishment, and may include logic to extract required information from transaction verification log 1254 to send to MAP as part of an account parameter replenishment request.

[0260] Mobile application 1212 may also include mobile application features 1220. Mobile application features 1220 may include consumer verification methods (CVM)

logic 1224, payment modes 1222, and user settings 1226. CVM logic 1224 may include logic required to confirm a mobile application passcode or on-device verification method (e.g., screen lock), or other verification information method supported by mobile application 1212. Payment modes 1222 may include logic to support various ways of setting up mobile application 1212 and portable communication device 1201 to be ready to initiate a transaction, and may include support for Manual Mode and/or Always-On Mode.

[0261] Manual Mode is a state where mobile application 1212 is configured to be accessible for making a payment after the consumer has explicitly chosen to (1) open mobile application 1212, (2) entered user input for a consumer verification method if required, and (3) selected an account to make a contactless payment transaction and for a single transaction or limited time. For Manual Mode, a decision can be made whether a consumer device cardholder verification method (CDCVM) will be required prior to making payment. If a CDCVM is used, then the two-tap scenario for high-value transactions may not be necessary. Conversely, to reduce barriers to use, if an issuer decides to opt for not asking for a CDCVM in Manual Mode, then the consumer will be able to conduct transactions once the conditions for Manual Mode operation are met. In this latter scenario, mobile application 1212 may support entry of CDCVM if a CDCVM is requested during a high value payment.

[0262] Always-On Mode is a state where an account on portable communication device 1212 (a default account) is intended to be continuously accessible to a contactless reader. A portable communication device with an account set in this state allows a consumer to initiate a contactless payment transaction by the presentation of the portable communication device to a contactless reader. Always-On Mode may also support device verification (referred to below Always-On with On-Device Verification Mode). This setting allows for additional security. For example, the user may have to unlock the portable communication device's user interface or display screen before mobile application 1212 responds to a contactless reader attempting to initiate payment transaction.

[0263] FIGs. 13-15 illustrate the state machine of mobile application 1212 when mobile application 1212 is in Manual Mode (FIG. 13), Always-On Mode (FIG. 14),

and Always-On with On-Device Verification Mode (FIG. 15). The various states shown in FIGs. 13-15 are described below.

[0264] Downloaded: The consumer downloads the application. The downloaded state can be a transient state depending upon the application and OS design. If the consumer taps the portable communication device on a contactless reader in this state, then no information is exchanged between the portable communication device and the reader.

[0265] Installed: The consumer performs the installation. If the consumer taps the portable communication device on a contactless reader in this state, then no information is exchanged between the portable communication device and the reader.

[0266] Initialized: The consumer sets up an account with MAP but no payment card is added. If the consumer taps the portable communication device on a contactless reader in this state, then no information is exchanged between the portable communication device and the reader.

[0267] Active: The consumer adds a payment card and valid account parameters are provisioned in the mobile application. If the consumer taps the portable communication device on a contactless reader in this state, then the mobile application may respond per the Validate Processing Mode.

[0268] Ready-to-Pay (Manual-Mode): The consumer activates a payment card to make a payment. This is a transient state and the mobile application must set up a timer to exit from the state. The mobile application moves to payment Sent state if the transaction is made or moves to Active state if it times out, or moves to "CDCVM Input" if CDCVM input is required. If the consumer taps the portable communication device on a contactless reader in this state, then the mobile application initiates the contactless data exchange.

[0269] Ready-to-Pay (both Always-On Modes): The portable communication device is ready to initiate a transaction with a contactless reader. The consumer selects Always-On Mode in the mobile application. The mobile application moves to payment sent state if a transaction is made or moves to CDCVM input state if CDCVM is required. If the consumer taps the portable communication device on a

contactless reader in this state, then the mobile application initiates the contactless data exchange.

[0270] CDCVM Input: The contactless reader asks for a CDCVM. This is a transient state and the mobile application must set up a timer to exit from the state. The mobile application moves to the Second Tap state if the consumer enters a valid CDCVM, otherwise it moves to Active state (Manual Mode) or Ready-to-Pay (in both Always-On Modes) after the timer expires. If the consumer taps the portable communication device on a contactless reader in this state, then no information is exchanged between the portable communication device and the reader.

[0271] Second Tap: The portable communication device is ready for second tap to transmit CDCVM verification information to a contactless reader. This is a transient state and the mobile application may set up a timer to exit from the state. The mobile application moves to the Payment Sent state if the consumer taps the portable communication device on a contactless reader, otherwise it moves to Active state (Manual-Mode) or Ready-to-Pay (in both Always-On Modes) after the timer expires. If the consumer taps the portable communication device on a contactless reader in this state, then it sends a CDCVM verification flag to a contactless reader.

[0272] Payment Sent: The consumer sends the payment payload to a contactless reader. This is a transient state. If the consumer taps the portable communication device on a contactless reader in this state, then no information is exchanged between the portable communication device and the reader.

[0273] Background: The mobile application is running in the background. If the consumer taps the portable communication device on a contactless reader in this state, then the mobile application may respond per the Validate Processing Mode.

[0274] Not Running: The mobile application is not running on the portable communication device. If the consumer taps the device on a contactless reader in this state, then no information is exchanged between the portable communication device and the reader.

[0275] MOBILE APPLICATION SECURITY

[0276] To provide additional security, mobile application 1212 may obfuscate and protect stored keys by an accepted mechanism, such as key wrapping. Code and

data in the mobile application 1212 may be obfuscated in order to protect the code against reverse engineering. Communications between mobile application 1212 and MAP that contain sensitive information can be exchanged after the channel has been secured by MAP (e.g. using TLS). Mobile application 1212 may adhere to appropriate industry standards; such as FIPS-140-2. Error codes sent to the OS logging framework may disclose only information that will not be of aid to an attacker. Event logs and debugging information may avoid exposing directly or indirectly any credentials. Logged information can also be encrypted. Mobile application 1212 and MAP may provide mechanisms to detect, resist, and report if the portable communication device is in debug mode. Device state including jail breaking, rooting, malware, mobile application runtime integrity, etc. can be checked prior to personalization and provisioning of mobile application 1212, and when a new account parameter are sent to mobile application 1212. If any compromises are detected, mobile application 1212 can be deactivated, and the deactivation reason relayed back to MAP. The mobile application security capabilities can be inherently built in mobile application 1212, and dependencies on the portable communication device and OS platform security capabilities can be minimized. For a rooted or stolen device to gain access, device fingerprinting and tools that support device analysis and attestation can be used.

[0277] In some embodiments, MAP may authenticate the consumer and/or portable communication device 1201 using single or multifactor authentication. The storage/memory used to store the keys in mobile application 1212 may go through a certification process. For example, root credential can be generated. The input for generating root credential can be created from high entropy attributes such as hard to clone functions (UFs) resident on the portable communication device and time-bound attributes received and stored from backend system. Subsequent credentials hosted in key store can be extracted from a generated key encryption key (KEK). User credentials can be used as an input to generate a Root Credential and KEK. Obfuscated permutation logic can be provided as input to generating a Root Credential and KEK. Obfuscated permutation logic can be based on xx-morphic (polymorphic, metamorphic) mechanisms. Credential store can be time-bound and mutable. Extracted data-at-rest key from key store can be encrypted and decrypted from yet another KEK when resident as data-in-use. Binary attributes for application

logic processing the key can be provided as input (bind) to generate KEK for protecting data-in-use. Data-in-use keys can be scrubbed through application logic processing keys. The following Protection Profiles (PP) can be established: PPs for KEK1 protected Key Store, PPs for KEK1 & 2 generation logic, PPs for KEK2 protected data-in-use key, and/or PPs for data-in-use key scrubbing.

[0278] Code and data in mobile application 1212 can be obfuscated in order to protect the code against reverse engineering. The application logic that also drives key extraction can be certificated for tamper resistance for ensuring protection of keys. The application logic hosting credentials used to authenticate and the credentials themselves can be certificated for tamper resistance. Tamper resistance/detection mechanisms can be implemented to preserve the integrity of the code/application logic. User credentials can be used as an input to encrypting sensitive parts of code logic. Obfuscated permutation logic can be provided as input to generating a KEK. Obfuscated permutation logic can be based on xx-morphic (polymorphic, metamorphic) mechanisms. Code and application logic can be time-bound and mutable. The following Protection Profiles (PP) can be established: PPs for tamper resistance/detection, PPs for obfuscation generation logic, PPs for ensuring measured initialization, and/or PPs for update

[0279] MOBILE APPLICATION LAUNCH AND ACCOUNT PREPARATION

[0280] On each consumer-initiated manual launch (i.e., through a hard or soft key, or from the device's mobile application environment 1210), mobile application 1212 may check and report to MAP if portable communication device 1201 is in debug mode. Mobile application 1212 may check that the payment accounts provisioned in mobile application 1212 are active and available, and check if the account parameter thresholds 1252 have been exceeded and determine if an account parameter replenish request is required. Mobile application 1212 may check the device state, including jail breaking, rooting, malware, mobile application runtime integrity, and if new account parameters are sent to mobile application 1212. If device or application compromise is detected, mobile application 1212 may be deactivated and the deactivation reason relayed back to MAP.

[0281] If a payment account managed by mobile application 1212 is in a suspended state then the consumer can benefit from being presented with

information to take the necessary action or to contact their issuer. To make a payment account provisioned in mobile application 1212 ready for payment, the user may first select to pay using this payment account. This can be done in the following ways for each payment mode. In Manual Mode, the user launches mobile application 1212, selects the card or account to use for payment, navigates to payment screen for the selected card or account and selects to pay. In Always-On Mode, the user selects the card or account to be used for payment as the default payment account. For Always-On with On-Device Verification Mode, the user selects the card or account to be used for payment as the default payment account. Once a card or account is selected for payment, mobile application 1212 may configure PPSE 1256 with appropriate account details of the selected card or account. Once PPSE 1256 is configured, the selected card or account is ready for payment when the user taps portable communication device 1201 on an access device or otherwise communicate with the access device.

[0282] MOBILE APPLICATION USER VERIFICATION

[0283] In some embodiments, mobile application 1212 may support user verification when interacting with MAP and/or interacting with an access device. When interacting with MAP (e.g., provisioning or replenishment of account parameters stored in account parameters storage 1240), a unique username and password may be verified by MAP, depending on the context of that interaction and the requirements of the issuer. Mobile application 1212 may also provide a list of the cardholder verification methods supported by mobile application 1212 to an access device when interacting with the access device. Cardholder verification methods that are supported in the card environment, such as online PIN and signature, can also be supported by cloud-based payments.

[0284] Portable communication device 1201 may also have a specific category of cardholder verification methods, referred to as consumer device cardholder verification method (CDCVM). There are a number of different methods that can be used to provide the CDCVM for mobile application 1212, which can include the same username/password utilized in the authentication with MAP. The CDCVM method utilized by mobile application 212 may provide different levels of security.

[0285] Cloud-based CDCVM performed through connection to an online service may provide the highest level of security. This could be the same as the username/password used for authentication to MAP. However, if data connectivity is not present, this would result in a payment requiring CDCVM to fail. Hence, this option may be used in Manual Mode to prevent a payment transaction failing midway through the two-tap process due to no data connectivity

[0286] On-device CDCVM performed at the portable communication device level through the operating system may provide a better consumer experience. An example is the method required to unlock the portable communication device screen. Mobile application 1212 receives an indication from portable communication device 1201 when the CDCVM has been successfully entered. Mobile application 1212 has no capability to change the on-device CDCVM. Mobile application CDCVM can be performed on opening and launching mobile application 1212. An example is entering a numeric code to open mobile application 1212. As a software-based CDCVM may be less secure than the other options, this method may be used in combination with a more secure option, such as with a cloud-based CDCVM, where the mobile application CDCVM is used when there is no data connectivity available.

[0287] USER SETTINGS

[0288] Mobile application 1212 may receive these options, or a subset thereof, in a suitable manner or assume a default for one or more of these options. These options describe the general behavior of mobile application 1212. For example, user settings 1226 may include payment modes such as Manual, Always-On, or Always-On with On-Device Verification. User settings 1226 may include whether the consumer can make changes to these initial preferences, how much time a consumer has to make a payment in each mode, how much time a consumer has to enter password in a two tap transaction (may be applicable to higher value transaction scenarios), within what time period mobile application 1212 should shut down if there has been no interaction from the consumer, etc. User settings 1226 may also support password change. The user may populate the consumer's chosen mobile application password by invoking a password change process and provide the current or default password and the consumer's newly chosen password. The consumer may choose this option to change previously chosen passcode/password.

Mobile application 1212 may prompt the consumer to enter the current password and new password (depending on the implementation and the manner in which passwords are masked or not, the consumer may be prompted to input the new password twice to ensure correct entry). Mobile application 1212 may replace the old passcode/password with the new passcode/password. The location of the passcode/password may be stored remote or local to the device.

[0289] If the consumer has chosen to modify the Always-On Mode settings, the PPSE 1256 may be configured appropriately (e.g., the file control information (FCI) template can be updated with directory entry for the default payment account). This ensures that the default account is used when portable communication device 1212 is brought in proximity to an access device when conducting transactions.

[0290] If on-device verification setting is turned on, mobile application 1212 may ensure to not initiate a transaction until the verification method has been confirmed. The verification method in this case can be the one set by the user for unlocking the phone. Upon successful verification, the cardholder verification method (CVM) verified field in mobile application 1212 may be set. The successful verification in this setting is then conveyed to the access device and eventually to the issuer via the CVM verified field.

[0291] MOBILE APPLICATION INTERACTION EVENTS

[0292] The behavior of mobile application interaction events may depend on whether the mobile application 1212 is currently running when this event occurs, or whether the receipt of the event by the underlying mobile application environment 1210 is the trigger that caused mobile application 1212 to launch. Depending on the capabilities of the underlying mobile application environment 1210, mobile application 1212 may be able to differentiate between different events.

[0293] The receipt of a push notification by the underlying mobile application environment 1210 can be targeted towards mobile application 1212. Mobile application 1212 can be reached in band via MAP to replenish account parameters for the cloud-based account or push other data as may be deemed necessary by the issuer and/or MAP. The communication channel with MAP may also be used for issuers to send lifecycle management events such as suspend, resume, delete.

[0294] On shutdown, mobile application 1212 may ensure that the state of each payment account is in a suitable state. This may apply when mobile application 1212 is going through an expected shutdown sequence as well as when mobile application 1212 is unexpectedly terminated. The previous account verification applied during manual launch may be reversed, and payment account CDCVM verification indicators may be set to the negative. Mobile application 1212 may ensure that the consumer's chosen settings are reflected and that the payment accounts are in their regular idle states.

[0295] MOBILE APPLICATION SHUTDOWN/CLEAN UP

[0296] Mobile application 1212 may perform cleanup when it is closed unexpectedly (e.g., the portable communication device shuts off due to low battery power) or on purpose. In any payment mode, mobile application 1212 may save the payment mode, account parameters, associated thresholds, and default card settings so that they are available when mobile application 1212 is launched again. Mobile application 1212 may terminate any ongoing transaction, close any open session with the MAP, save transaction logs if shutdown was immediately preceded by a successful transaction, and free up any system and memory resources being used by mobile application 1212. In some embodiments, mobile application 1212 may choose to set or reset the "CDCVM successfully performed" flag, depending on how the CDCVM verification logic is implemented.

[0297] The implementation logic related to PPSE configuration may differ during shutdown/cleanup depending on the payment mode selected when mobile application 1212 is shut down. In Always-On Mode, mobile application 1212 may save the PPSE configuration so that the PPSE picks up the default card as the only active card for payment when mobile application 1212 is launched again. In Manual Mode, the PPSE configuration may not be saved upon shutdown. Instead, the PPSE may be re-populated when the consumer selects a card to pay the next time mobile application 1212 is launched. On mobile application 1212 shutdown, mobile application 1212 may ensure that the consumer's chosen settings are reflected and that the payment accounts are in their regular idle states.

[0298] NAVIGATING FROM THE MOBILE APPLICATION

[0299] When the consumer presses the portable communication device's home button or back button to move out of mobile application 1212 and then come back to it, mobile application 1212 may continue running in the background and continue the operation being performed. Mobile application 1212 may apply restrictions for additional security, such as timeouts, to limit the time that it can continue running in the background. If a consumer puts mobile application 1212 in the background while a transaction is in progress, mobile application 1212 may continue the transaction processing.

[0300] MOBILE APPLICATION UNINSTALL

[0301] As part of an uninstallation process, mobile application 1212 may clear any sensitive data such as keys, certificates, and account parameters. Mobile application 1212 may inform MAP so that CBPP and the issuer/host system can execute the necessary lifecycle management processes for accounts provisioned in mobile application 1212 at the time of uninstallation. Mobile application 1212 may close any open session with MAP, terminate the ongoing transaction if present, and release any system and memory resources being used by mobile application 1212.

[0302] ACCOUNT ENROLLMENT

Mobile application 1212 may include enrollment logic 1232 to enroll/add a payment account into the cloud-based payment program, unless the issuer has provided another channel to accomplish this. The issuer may be directly involved in the enrollment process (e.g., the issuer directly may make the accept/decline enrollment decision or delegates the decision to a third party under pre-defined conditions). In both cases, the issuer may be in full control of the acceptance criteria and specifically defines card account verification methods and consumer authentication methods.

[0303] Enrollment logic 1232 may allow a consumer to input card details to initiate a payment account enrollment. The details to capture may be determined by the issuer/host system and/or CBPP, but should be sufficient to uniquely identify and verify the payment account. The issuer/host system and/or CBPP can determine the method and information required to authenticate the consumer who owns that

account. Mobile application 1212 may send payment account enrollment data to MAP, which will then send and manage the account enrollment and account verification process with the issuer/host system and/or CBPP.

[0304] If enrollment is successful, mobile application 1212 may receive from MAP the data for provisioning the new payment account for payment, including a payment account application ID (AID), PPSE AID, payment account issuer settings, payment account card art, account parameters, account parameter settings and thresholds, etc. If enrollment is successful, enrollment logic 1232 may provision the payment account based on the information received from MAP. Mobile application 1212 may also, as part of the configuration process, request the consumer to set an account verification method (e.g., a passcode), if it is not already set. Upon completing the account configuration, mobile application 1212 may display a message to the consumer that the enrollment was successful. Mobile application 1212 may support and configure the account parameter thresholds as defined by the issuer/host system and/or CBPP. The account parameter thresholds may include a number of transactions (i.e. cumulative number of transactions that would trigger a replenish request for a specific payment account), time to live (i.e. amount of time to elapse before mobile application 1212 would trigger a replenish request for a specific payment account), and/or cumulative transaction amount (i.e. total monetary amount across one or more transactions conducted on a specific account before mobile application 1212 would trigger a replenish request for that account). If enrollment is not successful, mobile application 1212 may receive and process a the failure notification and reason code, and display a message to the consumer that the enrollment was not successful and request the consumer take any appropriate action.

[0305] PAYMENT USING MOBILE APPLICATION

[0306] Mobile application 1212 enables the user to perform contactless transactions at a contactless access device via portable communication device 1201. Mobile application 1212 facilitates this by using the account parameters provided by CBPP to generate the data format to conduct payment transactions. To avoid consumer confusion as to where the payment will be allocated to, if there are multiple payment mobile applications installed on portable communication device

1212, the consumer may be required to choose which mobile application to use for the payment. There are a number of options how this can be achieved. The consumer may, at the consumer's discretion, be able to set a default payment mobile application in the mobile OS settings. The consumer may be able to set a default payment product in a specific mobile application's settings. The consumer may be able to manually select a payment product within that mobile application. To ensure the consumer choice is used, mobile application 1212 may present the selected payment account to the access device. Mobile application 1212 may support either integrated chip based transaction path or magnetic stripe based transaction path, depending on which type of transaction the access device supports. Integrated chip based transaction is the default path used with a chip card capable access device, and magnetic stripe based transaction is the default path used with a magnetic stripe only capable access device.

[0307] In some embodiments, mobile application 1212 may support multiple application identifiers (AIDs) for a single account. A single account may have multiple AIDs associated with it, for example, if a transaction conducted on that account can be processed by different payment processing networks and/or if the account has different services, features, product-types, and payment capabilities associated with the account. The multiple AIDs can be communicated to the access device to allow an access device to select a preferred AID to choose how the transaction is processed (e.g., which payment processing network) and/or what services or features can be associated with the transaction. The multiple AIDs can be populated in the directory entry for the PPSE, and communicated to an access device for this purpose.

[0308] For example, a single account may have a common debit AID and a payment processing network specific AID (e.g., a Visa AID) associated with the single account. These AIDs can be populated in the directory entry for the PPSE, and the PPSE File Control Information (FCI) for each directory entry may include an Issuer Identification Number (IIN) and an Issuer Country Code (ICC). In some embodiments, the CVM for the debit AID can be an online CVM (e.g., an online PIN), while the CVM for the payment processing network specific AID can be a signature.

[0309] A contactless payment can be initiated by the consumer tapping portable communication device 1201 to a contactless reader (e.g., a NFC reader), or otherwise communicating with the contactless reader (e.g., displaying a QR code or bar code) of the access device. The access device may request a cardholder verification method (CVM) for transactions above a threshold amount (e.g., transactions above $20). Mobile application 1212 can support a number of different CVMs, including the mobile specific consumer device cardholder verification method (CDCVM). Not all access devices may support CDCVM, and in those cases, an alternative CVM can be requested such as signature or online PIN.

[0310] An indication of successful CDCVM entry is sent during the payment transaction to the contactless reader. Mobile application 1212 may configure the appropriate data in the account parameters at the time of payment when the CDCVM has been successfully confirmed. Whenever the CDCVM is successfully entered, mobile application 1212 may store this information so the CDCVM verified indicator and CDCVM type indicator can be set and passed to the contactless reader during the payment transaction. This may prevent the access device from prompting the consumer for CDCVM entry at the access device. Mobile application 1212 may have the capability to provide indication of a successful CDCVM when requested by a access device during a two-tap payment transaction.

[0311] When mobile application 1212 is locked due to inactivity, mobile application 1212 may store this information so the CDCVM verified indicator can be set to negative. If a contactless payment is initiated in this state, the access device may prompt the consumer for CDCVM entry. Mobile application 1212 may provide the capability for CDCVM reset if it provides the consumer verification entry method for CDCVM. Mobile application 1212 may set a limit for number of consumer verification attempts, and locks mobile application 1212 if this limit is exceeded. For security purposes, issuers may request additional consumer verification before unlocking mobile application 1212. In some embodiments, mobile application 1212 may have a CDCVM that is not synchronized with the online PIN of a companion card.

[0312] In Manual Mode, the consumer may open or launch mobile application 1212 to enable payment functionality. When mobile application 1212 is opened,

functionality can be enabled so the consumer can initiate a payment by tapping portable communication device 1201 to a contactless reader. Portable communication device 1201 may prevent the consumer from performing a transaction based on any accounts stored in mobile application 1212 if mobile application 1212 is not open and active as the foreground application.

[0313] If the CDCVM indicator is not positive (i.e. a valid CDCVM entry has not yet been entered), mobile application 1212 can request CDCVM entry on opening. If this implementation path is selected, this may ensure the consumer is not requested again for CDCVM entry during a payment transaction (i.e., avoid the two-tap scenario for high value payments). Conversely, if this implementation path is not selected, usability for the consumer may be improved by omitting the request for CDCVM entry for transactions below a high value limit, with the trade-off being the consumer will be asked for the CDCVM entry if a high value payment is being conducted.

[0314] If there is more than one payment card or account available in mobile application 1212, the card or account selected as the default will be the one used for a payment transaction, unless the consumer selects an alternative card or account as active for payment. Once mobile application 1212 is open, PPSE 1256 may be populated and portable communication device 201 can initiate a payment transaction. Mobile application 1212 may display a message to the consumer indicating portable communication device 1201 is "Ready to Pay." Mobile application 1212 may define a time limit for inactivity, which when exceeded, may lock mobile application 1212. This ensures the consumer remains in control of the payment functionality, and the Manual Mode does not morph into Always-On Mode through inactivity. Mobile application 1212 can also enable the consumer to select a preferred time limit in settings. Depending on whether CDCVM is required or not, mobile application 1212 can require CDCVM entry to unlock mobile application 1212 after being locked due to inactivity.

[0315] In Always-On Mode, contactless payment capability is available whenever the phone screen is active. The contactless capability (e.g., NFC) may be available even if the phone screen is still in a locked state. To ensure consumers are aware of this capability and can opt-in to its usage, mobile application 1212 may preclude

setting Always-On Mode as the default mode. Whenever the phone screen is active, PPSE 1256 can be activated and populated, and portable communication device 1201 is able to initiate a payment transaction. When the consumer initiates a contactless transaction with the screen in a locked state, the contactless reader may request CDCVM entry. Where a device-level CDCVM is used, an icon indicator may be displayed on the notification bar, and the phone screen needs to be unlocked. Mobile application 1212 may then instruct the consumer to tap portable communication device 1201 to a contactless reader. Where a mobile application-level CDCVM is used, an icon indicator can be displayed on the notification bar. Mobile application 1212 may present the CDCVM entry screen to the consumer, and then instruct the consumer to tap portable communication device 1201 to a contactless reader once a successful CDCVM has been entered.

[0316] In Always-On with Device Verification Mode, contactless payment capability is available whenever the phone screen is active and unlocked. The contactless capability is not available when the phone screen is still in a locked state. Whenever the phone screen is unlocked, PPSE 1256 may be activated and populated, and portable communication device 1201 is able to initiate a payment transaction. If the consumer attempts to initiate a contactless payment with the screen in a locked state, the contactless reader will not be able to communicate with portable communication device 1201, and so nothing will happen on either the access device or on portable communication device 1201. When the consumer initiates a contactless payment with the screen in an unlocked state, the contactless reader may request CDCVM entry. Where a device-level CDCVM is used, mobile application 1212 may instruct the consumer to tap portable communication device 1201 to the contactless reader. Where a mobile application level CDCVM is used, mobile application 1212 may present the CDCVM entry screen to the consumer, and then instruct the consumer to tap portable communication device 1201 to the contactless reader once a successful CDCVM has been entered.

[0317] When mobile application 1212 and the access device have completed the communications to provide the data to complete the transaction, mobile application 1212 may display a message indicating that the payment has been sent. A contactless payment conducted using the integrated chip based transaction path may provide mobile application 1212 with some transaction data, such as transaction

amount and merchant information. Mobile application 1212 can populate the payment sent message with this information. A contactless payment conducted using the magnetic stripe based transaction path does not provide mobile application 1212 with any transaction data. Following a payment, mobile application 1212 may check the account parameter thresholds, and determine if mobile application 1212 needs to send a request for replenishment of the account parameters.

[0318] ACTIVE ACCOUNT MANAGEMENT

[0319] Active account management logic 1236 of mobile application 1212 initiates and manages the request to replenish account parameters when the account parameter thresholds have been exceeded. In order to mitigate the risk of the account parameters stored in account parameters storage 1240 from being compromised, account parameters can be periodically generated by CBPP and replenished in mobile application 1212 as well as refreshed in the issuer/host system in order to maintain the account in the active state. For the active account management process to be initiated, CBPP may receive a replenishment request for new account parameters from mobile application 1212 through MAP. CBPP 180 can also act upon a request received from the issuer/host system.

[0320] In some embodiments, active account management logic 1236 of mobile application 1212 can trigger the update or replenishment of the account parameters through an account parameters replenishment pull process. Active account management logic 1236 may attempt to initiate the account parameters replenishment flow at the time the consumer launches mobile application 1212, or after a transaction has been completed, and the account parameter thresholds 1252 have been exceeded. Upon receiving an updated set of account parameters, mobile application 1212 may process the account parameters payload and make the new account parameters available for payment. Upon successfully processing the new set of account parameters, mobile application 1212 may generate a notification to MAP. MAP may notify CBPP that the account parameters were successfully delivered to mobile application 1212. Note that updated account parameters can be accompanied with a new set of device threshold management parameters (e.g., different limited-use thresholds than the previous set of account parameters) that an issuer may want to use when the customer is in different environments (e.g. outside

of the domestic market). Before initiating the exchange of sensitive information, MAP may perform user, device, and application level authentication.

[0321] The update or replenishment of the account parameters can also be performed with an account parameter replenishment push process. In this flow, CBPP initiates the process to update the account parameters. CBPP sends a push message to MAP to initiate the replenishment push. MAP may then sends a push message to mobile application 1212. Mobile application 1212 then generates the account parameter update request per the replenishment pull flow described above. Before initiating the exchange of sensitive information, MAP may perform user, device, and application level authentication. If a user level authentication is used because previous authentication has expired, then mobile application 1212 may cache the request until the consumer opens mobile application 1212 and performs a user level authentication. After the successful authentication, mobile application 1212 follows the same procedure as in the replenishment pull flow. If user level authentication is not needed because the previous authentication has not expired, mobile application 1212 can immediately follow the same procedure as in the replenishment pull flow.

[0322] Upon receiving an updated set of account parameters, active account management logic 1236 may check the validity of the new account parameters, make the new account parameters available for payment, reset the account parameters thresholds, reset the account parameters threshold configurations, and delete the old set of account parameters. In some embodiments, mobile application 1212 may allow a transaction to be initiated even if the account parameters have not been updated due to lack of network connectivity. The issuer/host system or payment processing network acting on behalf of the issuer may make the decision to approve or decline the transaction based on knowledge of the stale account parameters in combination with other issuer defined risk metrics.

[0323] Mobile application 1212 may include a number of cloud-based payments device account parameters thresholds 1252 or risk limits that trigger the update of the current set of account parameters. This may include a number of transactions, a time to live, and/or cumulative transaction amount, etc. If the account parameters are valid for a number of transactions in CBPP, then account parameter thresholds

1252 in mobile application 1212 can be configured with a lower threshold number of transactions (e.g., one less than the number of transactions in CBPP) to trigger replenishment. If account parameters have an expiration time in CBPP, account parameter thresholds 1252 in mobile application 1212 can be configured with a threshold amount of time sooner than the expiration time to trigger replenishment. Where available from the contactless reader, the transaction amount can be used by active account management logic 1236 to make a decision as to whether the account parameters should be updated. Smaller transaction amounts would not necessarily require an immediate update of the account parameters. This mechanism, however, may not be reliable in environments where mobile application 1212 does not consistently receive the transaction amount from the access terminal. Where available, a cumulative transaction amount can be used as the trigger for account parameters update. This limit is based on the sum of individual transaction amounts. This data may not be necessarily reliable from mobile application 1212 point of view unless the data gets synchronized with the issuer/host system to ensure that a given transaction has been approved. A domestic versus international risk setting can also be used to trigger updates for international transactions more often in case they are considered more risky.

[0324] ACCOUNT LIFECYCLE MANAGEMENT

[0325] Mobile application 1212 may include lifecycle management logic 1234 to provide a user-initiated delete option for the user to delete a card or account from mobile application 1212 via lifecycle management logic 1234. Account lifecycle logic 1234 may delete account parameters stored in account parameters storage 1240 associated with that account, along with all other account configuration data or artifacts. Lifecycle management logic 1234 may initiate the process of account deletion in CBPP by initiating a delete request to CBPP through MAP.

[0326] Lifecycle management logic 1234 may enable an issuer-initiated delete mechanism for an issuer to delete an account. The issuer/hos system may send a delete request to CBPP, and in turn, CBPP may route the request to mobile application 1212. Lifecycle management logic 1234 may delete locally stored account parameters associated with the account, along with all other account configuration data or artifacts. Mobile application 1212 may send an

acknowledgement to MAP indicating that the deletion was completed. Mobile application 1212 may also display a message to user informing that the account is deleted.

[0327] Lifecycle management logic 1234 may enable an issuer-initiated suspend mechanism for an issuer to suspend an account. The issuer/host system can send a suspend request to CBPP, and in turn, CBPP may route the request to mobile application 1212. Lifecycle management logic 1234 may suspend the card or account in mobile application 1212. In the suspended state, the account cannot be selectable in the mobile application settings to make a payment. Lifecycle management logic 1234 may send an acknowledgement to MAP after suspending the account. Mobile application 1212 may display a message to user informing that the account is suspended, and may also inform the consumer to contact the issuing bank.

[0328] Lifecycle management logic 1234 may enable an issuer-initiated resume mechanism for an issuer to resume an account when it has been suspended in mobile application 1212. The issuer/host system may send a resume request to CBPP, and in turn, CBPP may route the request to mobile application 1212. Lifecycle management logic 1234 may resume the card or account in mobile application 1212. After resuming, the card or account may be selectable in the mobile application settings for payment. Mobile application 1212 may send an acknowledgement to MAP after resuming the account, and display a message to user informing that the account has been resumed.

[0329] POST PAYMENT INTERACTIONS

[0330] Post payment interactions or processing can help issuers mitigate the risk of account parameters being compromised and hence can help limit the exposure of the account parameters stored on portable communication device 1201. Information contained in a transaction verification log may be used to provide a reference point for CBPP to assist in assurance that account parameter replenishment requests are originating from the expected portable communication device. Mobile application 1212 may include post payment logic 1238 to extract information from transaction verification log 1254 in order to construct account parameter replenishment requests.

[0331] Furthermore, the issuer/host system working in conjunction with CBPP may have the option of initiating a request, through MAP, for transaction verification log data captured and stored by mobile application 1212 to verify transactions. Mobile application 1212 may respond, through MAP, to the request with the requested transaction verification log data. This data can then be verified by the issuer/host system in order to confirm if a particular transaction had originated from the queried portable communication device. Examples of the data elements that may be included in the transaction verification log may include, for each transaction, transaction time (e.g., contactless interaction time, transaction amount, and unpredictable number received from the access device during the transaction) as well as account parameters information such as the key index associated with the LUK that was used to conduct the transactions. For payment transaction verification, mobile application 1212 may receive and process request from MAP for transaction verification log data captured and stored by mobile application 1212. Mobile application 1212 may respond to the MAP request with the requested transaction verification log data. Mobile application 1212 may use the current account parameter's LUK or equivalent in the dynamic data portion of the account parameters to sign the requested transaction verification log data.

[0332] TRANSACTION VERIFICATION LOG

[0333] Mobile application 1212 can maintain transaction verification log 1254 to log all contactless interactions (e.g., NFC) where payment account parameters where shared with an access device, irrespective if the transaction was accepted or declined, or irrespective of whether mobile application 1212 has visibility to the outcome of the transaction (e.g., accepted or declined). Mobile application 1212 may store the transaction verification log data for the current and the previous set of account parameters per payment account. In some embodiments, the transaction verification log data for old set of account parameters can be deleted once mobile application 1212 receives a new set of account parameters. Transaction verification log 1254 may or may not be accessible or visible to the user.

[0334] XII. EXEMPLARY COMPUTER SYSTEM

[0335] The various entities or components described herein with reference to FIG. 1 may be associated with or operate one or more computer apparatuses to facilitate

the functions described herein. Any of the entities or components in FIG. 1, including any server or database, may use any suitable number of subsystems to facilitate the functions.

[0336] Examples of such subsystems or components are shown in FIG. 16. The subsystems shown in FIG. 16 are interconnected via a system bus 1602. Additional subsystems such as a printer 1604, keyboard 1606, fixed disk 1608 (or other memory comprising computer readable media), monitor 1610, which is coupled to display adapter 1612, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 1614 (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 1616. For example, serial port 1616 or external interface 1618 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 1620 to communicate with each subsystem and to control the execution of instructions from system memory 1622 or the fixed disk 1608, as well as the exchange of information between subsystems. The system memory 1622 and/or the fixed disk 1608 may embody a computer readable medium.

[0337] Embodiments of the invention are not limited to the above-described embodiments. For example, although separate functional blocks are shown for an issuer, payment processing network, and acquirer, some entities perform all of these functions and may be included in embodiments of invention.

[0338] Specific details regarding some of the above-described aspects are provided above. The specific details of the specific aspects may be combined in any suitable manner without departing from the spirit and scope of embodiments of the invention. For example, back end processing, data analysis, data collection, and other transactions may all be combined in some embodiments of the invention. However, other embodiments of the invention may be directed to specific embodiments relating to each individual aspect, or specific combinations of these individual aspects.

[0339] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software (stored in a

tangible physical medium) in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0340] 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.

[0341] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0342] 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.

[0343] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0344] 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 for enhancing security of a communication device when conducting a transaction using the communication device, the method comprising:

receiving, from a remote computer, a limited-use key (LUK) that is associated with a set of one or more limited-use thresholds that limit usage of the LUK, wherein the LUK is usable for more than one transaction;

generating, by the communication device, a transaction cryptogram using the LUK;

sending, to an access device, a token instead of a real account identifier and the transaction cryptogram to conduct the transaction, wherein the transaction is authorized based on at least whether usage of the LUK has exceeded the set of one or more limited-use thresholds,

sending, to the remote computer, a replenishment request for a second LUK, the replenishment request including transaction log information derived from a transaction log stored on the communication device, the transaction log storing transaction data for a plurality of transactions conducted using the first LUK; and

receiving, from the remote computer, the second LUK when the transaction log information in the replenishment request matches transaction log information at the remote computer.

2. The method of claim 1, wherein the communication device does not store the LUK or the token in a secure element.

3. The method of claim 1, wherein receiving the LUK further includes receiving a key index that includes information pertaining to generation of the LUK.

4. The method of claim 3, wherein the key index is sent with the transaction cryptogram to the access device to conduct the transaction.

5. The method of claim 3, wherein the key index includes time information indicating when the LUK is generated.

6. The method of claim 3, wherein the key index includes a replenishment counter value indicating a number of times the LUK has been replenished.

7. The method of claim 3, wherein the key index includes a pseudo-random number that is used as a seed to generate the LUK.

8. The method of claim 3, wherein the key index includes a transaction counter value indicating a number of transactions that has been previously conducted by a mobile application of the communication device at the time the LUK is generated.

9. The method of claim 1, wherein the set of one or more limited-use thresholds includes at least one of:

a time-to-live indicating a time duration that the LUK is valid for;

a predetermined number of transactions that the LUK is valid for; and

a cumulative transaction amount indicating a total transaction amount that the LUK is valid for.

10. The method of claim 1, wherein the set of one or more limited-use thresholds includes an international usage threshold and a domestic usage threshold.

11. The method of claim 1, wherein the replenishment request further includes a first key index that includes information pertaining to generation of the LUK, and receiving the second LUK includes receiving a second key index associated with the second LUK.

12. The method of claim 1, wherein the transaction log stored on the communication device includes:

for each transaction conducted using the LUK:

a transaction timestamp indicating the time of the corresponding transaction;

an application transaction counter value associated with the corresponding transaction; and

a transaction type indicator indicating whether the corresponding transaction is a magnetic stripe based transaction or an integrated chip based transaction.

13. The method of claim 1, wherein the transaction log information sent to the remote computer includes an authentication code computed over at least the transaction log using the LUK.

14. The method of claim 1, wherein the replenishment request is sent in response to determining that a next transaction conducted with the LUK will exhaust the set of one or more limited-use thresholds.

15. The method of claim 1, wherein the replenishment request is sent in response to determining that the set of one or more limited-use thresholds associated with the LUK has been exhausted.

16. The method of claim 1, wherein the replenishment request is sent in response to receiving a push message requesting the communication device to replenish the LUK.

17. The method of claim 3, wherein the LUK is generated by:

encrypting account information using a first encryption key to generate a second encryption key;

encrypting the key index using the second encryption key to generate the LUK.

18. The method of claim 17, wherein encrypting the account information with the first encryption key to generate the second encryption key includes:

encrypting the account information using the first encryption key to generate a first portion of the second encryption key;

inverting the account information; and

encrypting the inverted account information using the first encryption key to generate a second portion of the second encryption key.

19. The method of claim 17, wherein encrypting the key index using the second encryption key to generate the LUK includes:

padding the key index with a first value to generate a first padded key index information;

encrypting the first padded key index information to generate a first portion of the LUK;

padding the key index with a second value to generate a second padded key index information; and

encrypting the second padded key index information to generate a second portion of the LUK.

20. The method of claim 1, wherein the transaction cryptogram is generated by:

enciphering transaction information using a first portion of the LUK;

deciphering the enciphered transaction information using a second portion of the LUK; and

re-enciphering the deciphered transaction information using the first portion of the LUK.

21. The method of claim 1, wherein the transaction cryptogram is generated by:

encrypting a predetermined numeric string using the LUK; and

decimalizing the encrypted predetermined numeric string.

22. The method of claim 21, wherein decimalizing the encrypted predetermined numeric string includes:

extracting numeric digits from the encrypted predetermined numeric string to form a first data block;

extracting hexadecimal digits from the encrypted predetermined numeric string and converting each extracted hexadecimal digit into a numeric digit to form a second data block; and

concatenating the first data block and the second data block.

23. A communication device comprising:

a processor; and

a memory coupled to the processor and storing a mobile application that performs operations for enhancing security of the communication device when conducting transactions using the communication device, the operations implementing the method of any of claims 1 to 22.