(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 May 2020 (22.05.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/101803 A1

(51) International Patent Classification:
G06Q 20/32 (2012.01) *H04L 9/08* (2006.01)
G06Q 20/38 (2012.01)

(21) International Application Number:
PCT/US2019/052130

(22) International Filing Date:
20 September 2019 (20.09.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
18206253.9 14 November 2018 (14.11.2018) EP

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Ourchase Street, Purchase, NY 10577 (US).

(72) Inventors: **NOE, James**; 50 Wickham Chase, West Wickham BR4 0BL (GB). **TIERNEY, John**; 7 Highfields Heswall, Wirral Merseyside CH60 7TF (GB).

(74) Agent: **DOBBYN, Colm, J.**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: CREDENTIAL MANAGEMENT FOR MOBILE DEVICES

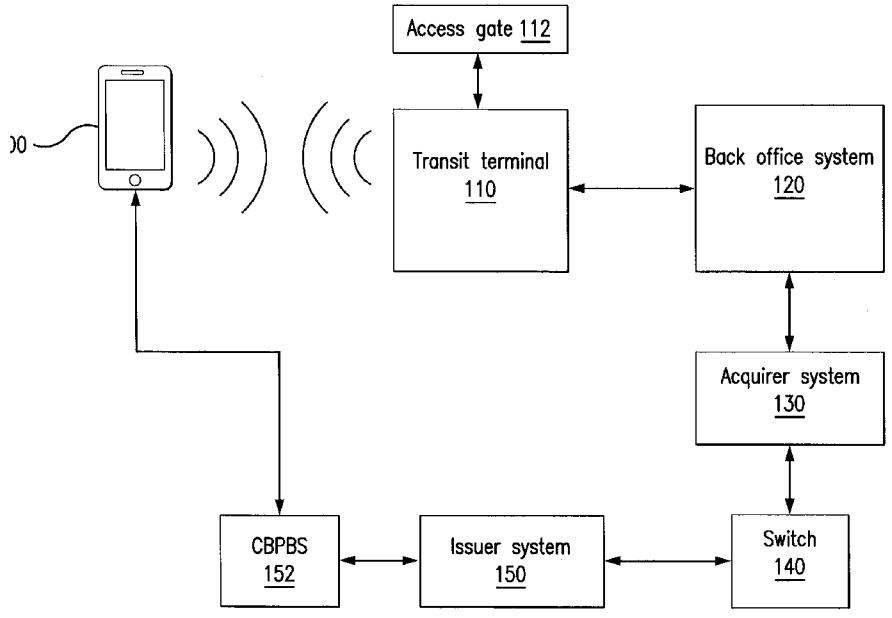


FIG. 1

(57) **Abstract:** The present disclosure relates to credential management for mobile devices that can be used for access to secured physical environments. One aspect comprises a computer implemented method comprising a mobile computing device: receiving, from a server system, and storing, on the mobile computing device: one or more application sequence counter values, one or more limited use credentials (LUCs), each LUC being bound to a corresponding one of the application sequence counter values; one or more emergency credentials, and an account token; subsequently receiving an authentication request from a terminal; in response to receiving the authentication request, determining that no LUC is available for fulfilling the request; and in response to determining that no LUC is available for fulfilling the request: transmitting, to the terminal, the account token and an application cryptogram generated from an emergency credential of said one or more emergency credentials; and updating a current application sequence counter.

WO 2020/101803 A1

[Continued on next page]

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

CREDENTIAL MANAGEMENT FOR MOBILE DEVICES

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of, and priority to, EP Patent Application No. 18206253.9 filed on November 14, 2018. The entire disclosure of the above application is incorporated herein by reference.

BACKGROUND

The present disclosure relates to credential management for mobile devices that can be used for access to secured physical environments, such as mass transit systems.

Mobile computing devices, such as smartphones and smart watches, are becoming ubiquitous in modern society. In addition to communications functionality, mobile devices have been used more recently in other applications such as payments. In particular, it is possible to store payment credentials on a mobile device which has a contactless interface, such as a near field communications (NFC) or magnetic secure transmission (MST) interface, such that the mobile device may be used at a payment terminal in the same way as a conventional payment card equipped with an integrated circuit or magnetic stripe.

Because payment credentials are highly sensitive, it is necessary for them to be handled in a secure manner by the mobile device. Some mobile devices are equipped with a secure element (SE) which is physically and logically protected against attack, and which stores the cryptographic software, keys and credentials needed for the device to be used as a payment device. Other devices employ a Trusted Execution Environment (TEE), which is a secure area of a main processor that is accessible only to trusted applications. In such devices the cryptographic software and keys, as well as payment and/or identification credentials may be stored in the TEE.

Another way to enable payment functionality on a mobile device is to employ a technique known as Host Card Emulation (HCE). An HCE-enabled device does not store sensitive payment information directly on the device. Instead, the sensitive information is stored by a remotely-located cloud-based payments backend system (CBPBS) and payment credentials are provisioned to the device over a secure

communications channel as needed. For this reason, HCE-implemented payments are sometimes called "cloud based payments".

Typically, a small number (10 to 20) of limited-use credentials (LUCs) may be transmitted to the mobile device for use by a transaction application on the device. Over time, the LUCs are consumed and their number may fall below a threshold level (e.g. less than 50%), at which point the device may send a request to the CBPBS for additional LUCs. Each LUC can be used for at least one transaction. Use of each LUC is limited to either a predetermined number of transactions or a predetermined time period. In one type of implementation each LUC can only be used for a single transaction and can never be re-used.

LUCs are used, for example, in Mastercard Cloud-Based Payments. In that system, an LUC always comprises a credential known as a Session Key (SK) to validate the device. In some implementations, the LUC may also comprise another SK credential, or another type of credential known as a Single Use Key (SUK), to authenticate the user. (SUKs are only used if the Consumer Device Cardholder Verification Method (CDCVM) mechanism uses a Mobile PIN, which is normally entered by the consumer but may be automatically provided by the payment application in some implementations.) Thus each LUC may comprise either a single SK, two SKs or an SK plus an SUK. Whatever the LUC's composition, each component of the LUC is associated with the same diversification value which is based on an application transaction counter (ATC), for example according to Appendix A1.3 of EMV Integrated Circuit Card Specifications for Payment Systems, version 4.3, Book 2 (Security and Key Management). The diversification value may be limited to use in a predetermined number of transactions (which could be one), or for a predetermined time period, thus limiting use of the LUC as described in the preceding paragraph.

In some HCE implementations, a master key is stored in volatile memory for the purpose of providing access to the LUCs. The LUC master key is generated by the CBPBS for example using device specific information and transmitted to the device when it is powered on, and is used to decrypt LUCs on request by, for example, a transaction application. When the device is powered off, the master key is deleted, such that a malicious actor cannot obtain and use any of the LUCs.

Payment devices, including conventional cards and payment-enabled mobile devices, can now be used for access to some mass transit systems. This is known as an "open loop" system because it allows devices other than those issued by the transit operator to be used for access and payment. For example, fare payments on some city public transport networks formerly required the use of paper tickets or a dedicated prepaid contactless card, whereas now credit, debit and prepaid cards and payment-enabled mobile devices with contactless functionality are often accepted for this purpose.

When a payment device is used at a transit terminal, authorisation of a transaction (whether carried out online or offline) proceeds in much the same way as for a normal payment transaction. That is, the transit terminal acts as a contactless payment terminal to enable fare payments, and may also include a gate control circuit or other means for controlling opening and closing of a gate depending on the outcome of the fare payment. In the case of a payment-enabled mobile device which employs LUCs as discussed above, an LUC is consumed once its usage limits are exceeded. This may occur following a predetermined number of uses (which could be a single use), or following expiry of a predetermined time period.

Some transit systems require users to "tap in" and "tap out" at contactless terminals for entry and exit, respectively. This may give rise to a problem in the context of HCE-based transaction applications, because the user may lose connectivity after entry. If the user's LUCs are depleted on entry, or otherwise become inaccessible during the journey (such as by being locked if the user happens to power off their device and thus loses the LUC master key), there is no way for the device to go online to replenish the LUC store. The user is thus unable to tap out and may be unable to exit the transit system, or may be overcharged due to not having tapped out at the actual exit point. Furthermore, any ticket/revenue inspection during the journey may also fail for the reasons listed above.

The present disclosure seeks to address the above problem.

SUMMARY

According to a first aspect, there is provided a computer implemented method comprising a mobile computing device: receiving, from a server system, and storing, on the mobile computing device: one or more application sequence counter values, one or more limited use credentials (LUCs), each LUC being bound to a

corresponding one of the application sequence counter values; one or more emergency credentials, and an account token; subsequently receiving an authentication request from a terminal; in response to receiving the authentication request, determining that no LUC is available for fulfilling the request; and in response to determining that no LUC is available for fulfilling the request: transmitting, to the terminal, the account token and an application cryptogram generated from an emergency credential of said one or more emergency credentials; and updating a current application sequence counter.

The method can further comprise: receiving an LUC master key with which the stored LUCs are encrypted; and storing the LUC master key only in a volatile memory device of the mobile computing device.

Each emergency credential can be bound to a corresponding one of the application sequence counter values and the application cryptogram can be generated from both the emergency credential and its corresponding application sequence counter value; or the application cryptogram can be generated from the emergency credential and the current application sequence counter value.

The method can further comprise the mobile computing device: subsequent to updating the current application sequence counter, determining that the current application sequence counter value matches the application sequence counter value of one of the LUCs; and in response to determining that the current application sequence counter value matches the application sequence counter value of one of the LUCs, deleting the matching LUC from the mobile computing device.

The method can further comprise the mobile computing device, in response to receiving the authentication request, determining that the authentication request relates to a zero-value transaction; wherein transmitting the account token and the application cryptogram is in response to determining that the authentication request relates to a zero-value transaction.

The method can further comprise the mobile computing device, subsequent to transmitting the application cryptogram to the terminal and updating the current application sequence counter: detecting that communication over the internet is possible; and in response to detecting that communication over the internet is possible, transmitting a request, to a server system, for one or more additional LUCs and one or more additional emergency credentials, wherein the request comprises the current application sequence counter value.

According to a second aspect, there is provided a mobile computing device comprising a memory and communication apparatus each communicatively coupled to a processor, the memory storing instructions which, when executed by the processor, cause the mobile computing device to perform the method of the first aspect.

According to a third aspect, there is provided a computer implemented method comprising a server system: receiving a provisioning request from a mobile computing device, the request comprising account credentials; authenticating that the provisioning request was received from a mobile computing device linked to the account the account credentials are for; storing the account credentials; generating an account token bound to the account credentials; generating one or more limited use credentials (LUCs) using an application sequence counter, each LUC being bound to a corresponding application sequence counter value; generating one or more emergency credentials; and transmitting the account token, the one or more LUCs, their respective application sequence counter values and the one or more emergency credentials to the mobile computing device.

The method can further comprise, subsequent to transmitting the one or more emergency credentials to the mobile computing device: receiving, from a payment network, a request to validate use of one of the one or more emergency credentials in a transaction; and transmitting a transaction validation to the payment network.

Each LUC can be generated based on a first issuer master key and each emergency credential can be generated based on a second, different, issuer master key.

The one or more LUCs and the one or more emergency credentials can all be generated based on the same issuer master key; the method can further comprise, subsequent to receiving the request to validate use of one of the one or more emergency credentials in a transaction, determining that the transaction is a zero-value transaction; wherein the transaction validation is transmitted to the payment network in response to determining that the transaction is a zero-value transaction.

The one or more LUCs can be transmitted to the mobile computing device together with an LUC master key with which they are either already encrypted, or with which they will be encrypted for storage when received by the mobile

computing device; the one or more emergency credentials can be generated using the application sequence counter, each emergency credential being bound to a corresponding application sequence counter value; and the one or more emergency credentials can be transmitted together with their respective application sequence counter values.

The method can further comprise, subsequent to transmitting the account token, the one or more LUCs, their respective application sequence counter values and the one or more emergency credentials to the mobile computing device: receiving a request from the mobile computing device for one or more additional LUCs and one or more additional emergency credentials, wherein the request comprises an application sequence counter value, being the application sequence counter value most recently used by the mobile computing device; generating one or more additional LUCs using the application sequence counter, each LUC being bound to a corresponding additional application sequence counter value, with the first additional application sequence counter value being the received application sequence counter value incremented by one; generating one or more additional emergency credentials; and transmitting the account token, the one or more additional LUCs, their respective additional application sequence counter values and the one or more additional emergency credentials to the mobile computing device.

According to a fourth aspect, there is provided a server system comprising a memory and communication apparatus each communicatively coupled to a processor, the memory storing instructions which, when executed by the processor, cause the server system to perform the method of the third aspect.

According to a fifth aspect, there is provided a computer readable medium comprising computer executable instructions which, when executed by a computer processor, cause the computer to perform the method of either of the first or third aspects.

BRIEF DESCRIPTION OF THE FIGURES

Aspects of the present disclosure will now be described by way of example with reference to the accompanying figures. In the figures:

Figure 1 schematically illustrates an exemplary interaction of a mobile device with a transit network and payment network;

Figure 2 schematically illustrates an exemplary architecture of a mobile device;

Figure 3 schematically illustrates an exemplary architecture of a CBPBS;

Figure 4 is a flowchart illustrating an exemplary method of provisioning credentials to a mobile device;

Figure 5 is a flowchart illustrating an exemplary transaction process;

Figure 6A is a flowchart illustrating example operation of a server system; and

Figure 6B is a flowchart illustrating example operation of a mobile computing device.

DETAILED DESCRIPTION OF THE FIGURES

Referring initially to Figure 1, the interaction of a payment-enabled mobile device 100 with a transit terminal 110, operative to control an entry or exit gate 112, is shown in schematic form. The mobile device 100 communicates with the transit terminal 110 using a short-range radio communication protocol such as NFC, for example by sending and receiving application protocol data units (APDUs) as defined by the ISO/IEC 7816-4 standard. When the mobile device 100 enters the polling field of the transit terminal 110, a transaction application on the mobile device 100 is activated and transmits a request, indicating payment and/or identification credentials, to the transit terminal 110 to cause it to open the gate 112, as will be described in more detail below.

The mobile device 100 is also able to communicate with a CBPBS 152 in order to request, and receive, credentials for use in payment and/or non-payment contexts, such as transit or other physical access applications such as hotel room access or car hire. The CBPBS 152 generates tokens, which are representations of payment card credentials that do not contain the real primary account number (PAN) of the payment card, and provisions the tokens to mobile device 100 for future use in payments and/or non-payment transactions.

In Figure 1, a transit terminal 110 is shown. The transit terminal 110 may alternatively be referred to as a "transit system transaction terminal" or "transit system contactless transaction terminal" in the sense that the terminal 110 may engage in "transactions" with devices such as contactless IC cards, payment-enabled mobile

devices, etc. The term "transaction" should be understood to refer to any exchange of data between the transit system terminal 110 and another device in which the other device identifies the holder of the device and/or indicates that the holder is entitled to enter the transit system and/or provides data required for arrangements to be made for payment for the holder's use of the transit system. An access gate 112 to the transit system is operatively coupled to the transit terminal 110 and is under control of the transit terminal 110. In some examples, the transit terminal 110 may be physically integrated with the access gate 112.

The transit terminal 110 may include a processor/CPU (central processing unit) which provides overall control of the functioning of the transit system terminal 110. The transit terminal 110 may also include one or more memory/storage devices. The memory may be in communication with the processor and may store program instructions that control the processor such that the transit system terminal 110 provides desired functionality. The transit terminal 110 may further include a gate control circuit operatively coupled to, and controlled by, the processor, the gate control circuit providing signals for controlling opening and closing of the access gate 112.

Turning now to Figure 2, an exemplary architecture of a mobile device 100 is shown. The mobile device 100 includes a mobile processor 202, and a storage/memory device or devices 204. The storage/memory devices 204 are in communication with the processor 202 and may contain program instructions to control the processor 202 to manage and perform various functions of the mobile device 100. Applications 206 executable by the mobile device 100 may be stored in block 204, together with a mobile operating system having HCE support built into its kernel (not shown), for execution by the processor 202.

A transaction application 208 is shown separately from the applications 206. The transaction application 208 may be stored in the memory 204 in similar fashion to the other applications 206 executable by the mobile device 100, or may be stored in other hardware components of the mobile device 100, such as a secure element, or in a trusted execution environment of the main processor 202.

Typically, the transaction application 208 is a general purpose payment app that provides access to a payment account system that is accepted by a mass transit system. The payment app in this case need not be specially adapted for obtaining entry to transit systems. In particular, the transaction application 208 may

contain code and data to enable the mobile device 100 to be used in EMV-type transactions. In some examples, code and/or data of the transaction application 208 may be protected, for example by obfuscation, white box cryptography and/or other techniques.

As is typical for mobile devices, the mobile device 100 may include mobile communications functions as represented by block 212. The mobile communications functions may comprise voice and data communications via a mobile communication network with which the mobile device 100 is registered.

In addition, to facilitate use as a payment-enabled device, the mobile device 100 may include short-range radio communications capabilities, including for example an NFC interface 214. Thus block 214 may represent a suitable antenna (not separately shown) that is appropriate for NFC communications as well as driving and receiving circuitry associated with the antenna.

Also represented by block 214, and associated with the short-range radio communications capabilities of the mobile device 100, is hardware known as the contactless frontend (CLF). The CLF may overlap with other aspects of block 214 that have already been mentioned.

It will be appreciated that the blocks depicted in Figure 2 as components of the mobile device 100 may in effect overlap with each other, and/or there may be functional connections among the blocks which are not explicitly shown in the drawing. It may also be assumed that, like a typical smartphone, the mobile device 100 may include a rechargeable battery (not shown) that is contained within a housing of the mobile device 100 and that provides electrical power to its active components.

The mobile device 100 may be embodied as a smartphone, but this assumption is not intended to be limiting, as the mobile device 100 may alternatively, in at least some cases, be constituted by a tablet computer, smartwatch or by other types of portable electronic devices.

Figure 3 shows an exemplary architecture of a CBPBS 152, which may comprise one or more servers configured to carry out various functions of the system. Each of the modules shown in Figure 3 may be executed by a separate server, for example. Different servers may be operated by different entities. For example, the authorisation module 306 may be operated by an issuer 150 while the tokenisation

module 308 and credential management module 312 may be operated by a trusted third party.

The CBPBS 152 comprises a tokenisation module 308 which receives requests from the transaction application 208 of the mobile device 100 to provision credentials such that they can be used by the transaction application 208 in transactions conducted with the mobile device 100 at a contactless terminal. For example, when a user of the mobile device 100 requests provisioning of a payment card (which may be a physical card or a virtual card), the tokenisation module 308 may generate a token which maps to the primary account number (PAN), expiry date and card verification code (CVC) of the card. The token may comprise an alphanumeric string, such as a 16-digit number, which has the same format as a PAN and is recognised as such by a payment network for the purposes of processing an authorisation request. The tokenisation module 308 stores the mapping between the token and the payment credentials, in a token vault 310 which is accessible only to the CBPBS 152. Further, the tokenisation module 308 may associate one or more rules with the token, such as restrictions on the number of transactions, its lifetime, a type of merchant at which it may be used, or a transaction environment in which it may be used.

The credential management module 312 is responsible for generating LUCs, for example in association with tokens generated by the tokenisation module 308, for provisioning to the mobile device 100. In order to do so, the credential management module 312 may derive, for a payment card requested to be provisioned by mobile device 100, an integrated circuit card (ICC) master key. The ICC master key is derived by passing an issuer master key of an issuer 150 of the payment card, and the tokenised or actual PAN, to a key derivation algorithm. Exemplary key derivation algorithms are set out in Appendix A1.4 of the EMV Integrated Circuit Card Specifications for Payment Systems, version 4.3, Book 2 (Security and Key Management). Next, one or more LUCs can be derived from the ICC master key and a diversification value which is based on an ATC, for example according to Appendix A1.3 of the aforementioned EMV specification. Accordingly, each LUC is bound to a unique ATC. Typically, ICC master keys are stored in a hardware security module (HSM) of the credential management module 312.

In some examples, the credential management module 312 generates an LUC master key which is used to encrypt the LUCs while stored on the mobile

device 100. This LUC master key may be transmitted alongside the LUCs, and stored by the transaction application 208 in volatile memory, such that it is available for use by the transaction application 208 while the mobile device 100 is powered on, but is deleted as soon as the device is powered off, such that the LUCs are protected while the device is powered off.

According to the present disclosure, in addition to LUCs, the credential management module 312 generates one or more emergency credentials. This may be done in several different ways, as will explained in more detail below. In one example, if an LUC master key is used to protect the LUCs, the emergency credentials may be generated in much the same way as the LUCs, with each being bound to an ATC, but may be transmitted to the mobile device 100 and stored without being encrypted by the LUC master key. This means that the emergency credentials are available even if the LUC master key is lost and the mobile device 100 does not have connectivity. In another example, the emergency credentials may be derived from a different issuer master key than the one used to derive the LUCs, but are not bound to a specific ATC.

Turning now to Figure 4, a method 400 of provisioning credentials to a mobile device is shown from the perspective of a CBPBS 152. The method 400 is carried out the first time that a user provisions a card for use with the transaction application 208.

At step 402, the CBPBS 152 receives a provisioning request from the mobile device 100. The provisioning request identifies the account to be provisioned onto the mobile device via account credentials. For example, the request may comprise a PAN, expiry date, and CVC and optionally cardholder name and billing address. The CBPBS must then authenticate that the provisioning request originates from a mobile device held by an authorised user of the account. In order to do this, at step 404, the CBPBS 152 (for example, via tokenisation module 308) may transmit a request to the issuer 150 of the card to cause the generation of a confirmation code, which is sent to the mobile device 100 by the issuer 150 using contact details the issuer stores as registered to the account, for example by email or SMS. The code is also sent to the CBPBS 152. The user is requested to enter, at the mobile device 100, the confirmation code, and on the CBPBS 152 confirming that it matches the code it has received from the issuer 150, the CBPBS 152 generates a token, and stores a mapping of the token to the PAN in the token vault 310. Alternative authentication

methods could be used, for example making use of a mobile banking app running on the mobile device.

At step 406, the CBPBS 152 retrieves an issuer master key for the issuer 150. This may be stored by the CBPBS 152 (in an HSM, for example), or may be requested from the issuer 150 at runtime. Next, at step 408, the credential management module 312 of the CBPBS 152 derives an ICC master key for the card being provisioned, stores this securely (such as in an HSM), and at step 410, generates one or more LUCs using the ICC master key and an ATC. Successively generated LUCs have progressively greater ATCs, typically increasing in increments of 1.

At step 412, method 400 may choose to provision the LUCs in conjunction with an LUC master key, in which case the method 400 branches to step 414, where the generated LUCs are encrypted using the LUC master key. The LUC master key may itself be derived in a number of different ways, for example based on device-specific information. If proceeding along this branch, the credential management module 312 then generates one or more emergency credentials using the ICC master key and an ATC as inputs to a key derivation algorithm. Again, the ATC for each successive emergency credential is greater than the one before. For example, the credential management module 312 may generate two emergency credentials which are not protected by the LUC master key, such that a first one of the emergency credentials can be used for an inspection tap (i.e., for a transit official to confirm validity of the mobile device 100 for fare payment), and a second emergency credential can be used to exit at an access gate 112.

If an LUC master key is not to be used, then at step 412 the method 400 branches to step 418, where one or more emergency credentials are generated, each emergency credential not being associated with an ATC. The credential management module 312 of the CBPBS 152 may request a second, different, issuer master key for the purpose of deriving a second ICC master key as input to a key derivation algorithm to generate an emergency credential. Alternatively, the credential management module 312 may use the same issuer master key and thus ICC master key to generate an emergency credential, but restrict the generated emergency credential to be used for specific, non-retail transactions, such as transit-related transactions or other zero-value transactions.

At step 420, the LUCs, emergency credentials, and LUC master key (if any) are transmitted to the mobile device 100, together with the token, for storage on

memory 204 of the mobile device 100. If an LUC master key is transmitted, it is stored only in volatile memory of the memory 204.

The flowchart of Figure 4 depicts the end-to-end process of provisioning a card for the first time. As LUCs and/or emergency credentials are depleted during use of the mobile device 100, the mobile device 100 will eventually need to go back online and connect to CBPBS 152 to replenish one or both sets of credentials. The replenishment process may proceed in substantially the same manner as steps 410 to 420 of Figure 4, with the exception that the CBPBS 152 also receives, from the mobile device 100, a most recently used ATC value. This value is used as the starting point for incrementing the ATC values which are embedded in the LUCs (and, if appropriate, the emergency credentials).

Turning now to Figure 5, an exemplary transaction process 500 which makes use of emergency credentials is shown.

To initiate the process 500, the mobile device 100 enters the polling field of a terminal 110, and the transaction application 208 executing on the mobile device 100 and the terminal 110 exchange data in order to initiate a contactless transaction via the NFC interface 214 (and its counterpart in the terminal 110). The nature of the data that are exchanged, and the processing steps undertaken by the respective devices during initiation (such as application selection), will be understood with reference to the EMV specifications. Once initiation is complete, at step 502 the terminal 110 sends an offline authentication request which is received by the transaction application 208.

In response to the authentication request, at step 504, the transaction application 208 determines whether any LUC is available. The LUCs may have become unavailable in a transit context if, for example, a last one of the LUCs on the mobile device 110 has been used to tap in to a transit system, and the mobile device 110 is unable to go online to replenish the LUCs, for example due to being out of network coverage, e.g. underground. In another example, the LUCs may be unavailable if they are encrypted by an LUC master key which has been deleted from memory during a device power-off or reset event. In either case, the transaction application 208 may cause a warning to be displayed via the user interface 210, such as "You are able to complete this journey, but are unable to make any purchases or start any new journeys until you connect your device to the internet to refresh your payment data".

If at least one LUC is available, then the process branches to step 506, where the transaction application 208 determines whether an LUC master key is present and is required to decrypt the LUC. If so, then the LUC is decrypted, and a generator key of the decrypted LUC is used to generate an EMV application cryptogram, in particular an ARQC (authorisation request cryptogram), at step 508.

If no LUC is available at step 504, the process branches to step 510, where an emergency credential is retrieved and used to generate the ARQC. If the emergency credential is bound to an ATC, that ATC is used in generation of the ARQC. Otherwise, a current value of an ATC stored on the memory 204 of the mobile device 110 is used in generation of the ARQC. This current value corresponds to the ATC of the most recent transaction, i.e. the previous "tap". In this case, the transaction application 208 checks whether the current ATC value matches the ATC of any LUC. If it does, the matching LUC is deleted, to prevent ATC reuse.

In some examples, the transaction application 208 may restrict use of the emergency credentials to non-payment transactions. For example, the transaction application 208 may require that transaction data received from a terminal, such as the terminal 110, indicate that the terminal is a transit (or other non-payment) terminal, and/or has a transaction value of zero. In some examples, the terminal may transmit a merchant category code (MCC) which is indicative of a non-payment transaction, such as an MCC of 4111, 4131 or 4784, each of which relate to transit. Furthermore, the terminal may transmit the specific merchant name, which could also be used to limit the extent to which the emergency credentials may be used.

At step 512, the current value of the ATC is updated on the memory 204 of mobile device 100, and at step 514, the generated ARQC is transmitted to the terminal 110 for online processing of the transaction.

Further steps of the transaction will now be described with reference to Figure 1. The access gate 112 will allow the user to enter or exit as long as offline data authentication is successfully performed and the device generates an application cryptogram, which is typically an ARQC indicating that an online authorisation is required. Alternatively, a transaction certificate (TC) application cryptogram may be generated indicating offline approval. The access gate will not allow the consumer to enter/exit if an application authentication cryptogram (AAC, offline decline) is generated by the device.

Following receipt of the ARQC or TC application cryptogram, the terminal 110 may initiate an authorisation request via a back office system 120, such as a public transport operator system, with which it is in communication. The authorisation request may take the form of an ISO8583 0100 authorisation request message. The back office system 120 may store the tokenised PAN and the ATC embedded in the ARQC. In a transit system, this information, and the terminal ID, may be used for fare calculation purposes. The ATC may be compared to the previous ATC for the same tokenised PAN to confirm that the mobile device 100 is valid for travel.

The back office system 120 may forward the request to an acquirer processing system 130 (operated by the public transport operator's financial institution), which in turn forwards it to a switch 140 that is capable of routing the request to the correct issuer (i.e., the issuer 150 of the card that has been provisioned onto the mobile device 100 and used in the transaction). The switch 140 may be that of a payment network operator such as Mastercard. Prior to issuer processing, a third party token vault, such as the Mastercard Digital Enablement Service (MDES), may detokenise the transaction and validate the application cryptogram data.

Once received by the issuer processing system 150, the authorisation request message is examined to determine the account for which authorisation is required and any relevant cryptographic validation is performed (if this has not already been performed by a third party token vault). If the issuer is performing detokenisation and/or cryptogram validation, the issuer processing system 150 may forward the token and the application cryptogram to its own CBPBS 152, such that the CBPBS 152 can detokenise the PAN (i.e., map the token back to the actual PAN).

If a non-payment emergency credential has been used to generate the ARQC, the CBPBS 152 may determine this and check that the transaction is a transit transaction and that the tap was for a zero amount. This could be done in a number of ways. If the same master key is used to generate the emergency credential and the LUCs then it could be done based on the ATC. Otherwise the backend could infer from previous LUC usage and confirm that the information about the transaction (e.g. merchant category code and transaction amount in the EMV data) imply a zero-value deferred authorisation transit transaction. Implementations could for example use bits in the chip data which are currently un-used to signal this to the CBPBS.

If authorisation of the transaction by the issuer processing system 150 is successful, an authorisation approval message is transmitted to the acquirer processing system 130 via the switch 140, and then forwarded to the back office system 120. The back office system 120 uses the approval as input to its fare calculation system.

Figures 6A and 6B are flowcharts illustrating example operation of, respectively, a server system (such as the CBPBS 152 described above) and a mobile computing device (such as the mobile device 100 described above).

Figure 6A begins at step 601, where the server system receives a provisioning request from the mobile computing device, the request comprising account credentials. At step 602, the server system authenticates that the provisioning request was received from a mobile computing device linked to the account the account credentials are for. In response to this authentication, the account credentials are then stored at step 603.

At step 604, the server system generates an account token bound to the account credentials. One or more LUCs are generated using an application sequence counter at step 605, each LUC being bound to a corresponding application sequence counter value. (Each LUC may optionally be generated based on a first issuer master key.) At step 606, the server system generates one or more emergency credentials. (If the first issue master key is used to generate the one or more LUCs, each emergency credential may optionally be generated based on a second issuer master key, different from the first issuer master key.)

The server system transmits the account token, the one or more LUCs, their respective application sequence counter values and the one or more emergency credentials to the mobile computing device at step 607. All of these may be transmitted together in one message, or split between multiple messages. For example, the emergency credentials may be transmitted in a later message than the account token, the one or more LUCs and their respective application sequence counter values.

The one or more LUCs may optionally be transmitted to the mobile computing device together with an LUC master key with which they are either already encrypted, or with which they will be encrypted for storage when received by the mobile computing device. (Alternatively an LUC master key may be transmitted separately from the LUCs.) The one or more emergency credentials may be generated

using the application sequence counter, each emergency credential being bound to a corresponding application sequence counter value; and the one or more emergency credentials may be transmitted together with their respective application sequence counter values.

Turning now to Figure 6B, at step 608 the mobile computing device receives and stores the one or more application sequence counter values, one or more LUCs, one or more emergency credentials, and the account token from the server system. The mobile computing device may optionally also receive an LUC master key with which the stored LUCs are encrypted, and store the LUC master key only in a volatile memory device of the mobile computing device.

Later, at step 609, the mobile computing device receives an authentication request from a terminal, such as the transit terminal 110 described above. At step 610 it is determined that no LUC is available for fulfilling the request. The mobile computing device may optionally also check at step 611 that the authentication request relates to a zero-value transaction, and only proceed to step 612 if so. In response to determining that no LUC is available for fulfilling the request at step 610, and optionally that the authentication request relates to a zero-value transaction at step 611, at step 612 the mobile computing device transmits, to the terminal, the account token and an application cryptogram generated from an emergency credential of said one or more emergency credentials. Each emergency credential may optionally be bound to a corresponding one of the application sequence counter values and, in that case, the application cryptogram may be generated from both the emergency credential and its corresponding application sequence counter value. Alternatively, the application cryptogram may be generated from the emergency credential and the current application sequence counter value. Once the application cryptogram has been generated, the mobile computing device updates a current application sequence counter.

Receipt of the account token and application cryptogram by the terminal may trigger communication from the terminal through a payment network to the server system. For example, the payment network may comprise back office system 120, acquirer system 130, switch 140 and issuer system 150 as described above. Returning to Figure 6A, this may result in the server system, at step 613, receiving a request to validate use of one of the one or more emergency credentials it

provided to the mobile device at step 607 in a transaction. The server system transmits a validation of the transaction to the payment network at step 615.

If the one or more LUCs and the one or more emergency credentials are all generated based on the same issuer master key then at step 614 the server system may check that the transaction is a zero-value transaction, and only proceed to transmit a transaction validation to the payment network at step 615 if so.

Returning to Figure 6B, once the application sequence counter has been updated at step 612, the mobile computing device may optionally check, at step 616, whether the current application sequence counter value matches the application sequence counter value of any of the LUCs. Any matching LUCs are then deleted from the mobile computing device at step 617.

At a time subsequent to transmitting the application cryptogram to the terminal and updating the current application sequence counter at step 612, the mobile computing device may detect that communication over the internet is possible at step 618. In response, it may optionally transmit a request, at step 619, to the server system, for one or more additional LUCs and one or more additional emergency credentials, wherein the request comprises the current application sequence counter value.

Returning to Figure 6A, the request for one or more additional LUCs and one or more additional emergency credentials is received by the server system at step 620. At step 621 the server system then increments the received application sequence counter value by one and uses this to return to step 605 to generate one or more additional LUCs, then step 606 to generate and one or more additional emergency credentials, and step 607 to transmit the account token, the one or more additional LUCs, their respective additional application sequence counter values and the one or more additional emergency credentials to the mobile computing device.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the embodiments disclosed herein. It is intended that the specification and examples be considered as exemplary only.

In addition, where this application has listed the steps of a method or procedure in a specific order, it could be possible, or even expedient in certain circumstances, to change the order in which some steps are performed, and it is intended that the particular steps of the method or procedure claims set forth herein not be construed as being order-specific unless such order specificity is expressly

stated in the claim. That is, the operations/steps may be performed in any order, unless otherwise specified, and embodiments may include additional or fewer operations/steps than those disclosed herein. It is further contemplated that executing or performing a particular operation/step before, contemporaneously with, or after another operation is in accordance with the described embodiments.

The methods described herein may be encoded as executable instructions embodied in a computer readable medium, including, without limitation, non-transitory computer-readable storage, a storage device, and/or a memory device. Such instructions, when executed by a processor (or one or more computers, processors, and/or other devices) cause the processor (the one or more computers, processors, and/or other devices) to perform at least a portion of the methods described herein. A non-transitory computer-readable storage medium includes, but is not limited to, volatile memory, non-volatile memory, magnetic and optical storage devices such as disk drives, magnetic tape, compact discs (CDs), digital versatile discs (DVDs), or other media that are capable of storing code and/or data.

Where a processor is referred to herein, this is to be understood to refer to a single processor or multiple processors operably connected to one another. Similarly, where a memory is referred to herein, this is to be understood to refer to a single memory or multiple memories operably connected to one another.

The methods and processes can also be partially or fully embodied in hardware modules or apparatuses or firmware, so that when the hardware modules or apparatuses are activated, they perform the associated methods and processes. The methods and processes can be embodied using a combination of code, data, and hardware modules or apparatuses.

Examples of processing systems, environments, and/or configurations that may be suitable for use with the embodiments described herein include, but are not limited to, embedded computer devices, personal computers, server computers (specific or cloud (virtual) servers), hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, mobile telephones, network personal computers (PCs), minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like. Hardware modules or apparatuses described in this disclosure include, but are not limited to, application-specific integrated

circuits (ASICs), field-programmable gate arrays (FPGAs), dedicated or shared processors, and/or other hardware modules or apparatuses.

User devices can include, without limitation, static user devices such as PCs and mobile user devices such as smartphones, tablets, laptops and smartwatches.

Receivers and transmitters as described herein may be standalone or may be comprised in transceivers. A communication link as described herein comprises at least one transmitter capable of transmitting data to at least one receiver over one or more wired or wireless communication channels. Such a communication link can optionally further comprise one or more relaying transceivers.

User input devices can include, without limitation, microphones, buttons, keypads, touchscreens, touchpads, trackballs, joysticks and mice. User output devices can include, without limitation, speakers, graphical user interfaces, indicator lights and refreshable braille displays. User interface devices can comprise one or more user input devices, one or more user output devices, or both.

CLAIMS

1. A computer implemented method comprising a mobile computing device:

receiving, from a server system, and storing, on the mobile computing device:

one or more application sequence counter values,

one or more limited use credentials (LUCs), each LUC being bound to a corresponding one of the application sequence counter values;

one or more emergency credentials, and

an account token;

subsequently receiving an authentication request from a terminal;

in response to receiving the authentication request, determining that no LUC is available for fulfilling the request; and

in response to determining that no LUC is available for fulfilling the request:

transmitting, to the terminal, the account token and an application cryptogram generated from an emergency credential of said one or more emergency credentials; and

updating a current application sequence counter.

2. The method of claim 1, further comprising:

receiving an LUC master key with which the stored LUCs are encrypted; and

storing the LUC master key only in a volatile memory device of the mobile computing device.

3. The method of either of claims 1 or 2, wherein:

each emergency credential is bound to a corresponding one of the application sequence counter values and the application cryptogram is generated from both the emergency credential and its corresponding application sequence counter value; or

the application cryptogram is generated from the emergency credential and the current application sequence counter value.

4. The method of any of claims 1 to 3, further comprising the mobile computing device:

subsequent to updating the current application sequence counter, determining that the current application sequence counter value matches the application sequence counter value of one of the LUCs; and

in response to determining that the current application sequence counter value matches the application sequence counter value of one of the LUCs, deleting the matching LUC from the mobile computing device.

5. The method of any preceding claim, further comprising the mobile computing device, in response to receiving the authentication request, determining that the authentication request relates to a zero-value transaction;

wherein transmitting the account token and the application cryptogram is in response to determining that the authentication request relates to a zero-value transaction.

6. The method of any preceding claim, further comprising the mobile computing device, subsequent to transmitting the application cryptogram to the terminal and updating the current application sequence counter:

detecting that communication over the internet is possible; and

in response to detecting that communication over the internet is possible, transmitting a request, to a server system, for one or more additional LUCs and one or more additional emergency credentials, wherein the request comprises the current application sequence counter value.

7. A mobile computing device comprising a memory and communication apparatus each communicatively coupled to a processor, the memory storing instructions which, when executed by the processor, cause the mobile computing device to perform the method of any preceding claim.

8. A computer implemented method comprising a server system:

receiving a provisioning request from a mobile computing device, the request comprising account credentials;

authenticating that the provisioning request was received from a mobile computing device linked to the account the account credentials are for;

storing the account credentials;

generating an account token bound to the account credentials;

generating one or more limited use credentials (LUCs) using an application sequence counter, each LUC being bound to a corresponding application sequence counter value;

generating one or more emergency credentials; and

transmitting the account token, the one or more LUCs, their respective application sequence counter values and the one or more emergency credentials to the mobile computing device.

9. The method of claim 8, further comprising, subsequent to transmitting the one or more emergency credentials to the mobile computing device:

receiving, from a payment network, a request to validate use of one of the one or more emergency credentials in a transaction; and

transmitting a transaction validation to the payment network.

10. The method of either of claims 8 or 9, wherein each LUC is generated based on a first issuer master key and each emergency credential is generated based on a second, different, issuer master key.

11. The method of claim 9,

wherein the one or more LUCs and the one or more emergency credentials are all generated based on the same issuer master key;

the method further comprising, subsequent to receiving the request to validate use of one of the one or more emergency credentials in a transaction, determining that the transaction is a zero-value transaction;

wherein the transaction validation is transmitted to the payment network in response to determining that the transaction is a zero-value transaction.

12. The method of either of claims 8 or 9, wherein:

the one or more LUCs are transmitted to the mobile computing device together with an LUC master key with which they are either already encrypted, or with which they will be encrypted for storage when received by the mobile computing device;

the one or more emergency credentials are generated using the application sequence counter, each emergency credential being bound to a corresponding application sequence counter value; and

the one or more emergency credentials are transmitted together with their respective application sequence counter values.

13. The method of any of claims 8 to 12, further comprising, subsequent to transmitting the account token, the one or more LUCs, their respective application sequence counter values and the one or more emergency credentials to the mobile computing device:

receiving a request from the mobile computing device for one or more additional LUCs and one or more additional emergency credentials, wherein the request comprises an application sequence counter value, being the application sequence counter value most recently used by the mobile computing device;

generating one or more additional LUCs using the application sequence counter, each LUC being bound to a corresponding additional application sequence counter value, with the first additional application sequence counter value being the received application sequence counter value incremented by one;

generating one or more additional emergency credentials; and

transmitting the account token, the one or more additional LUCs, their respective additional application sequence counter values and the one or more additional emergency credentials to the mobile computing device.

14. A server system comprising a memory and communication apparatus each communicatively coupled to a processor, the memory storing instructions which, when executed by the processor, cause the server system to perform the method of any of claims 8 to 13.

15. A computer readable medium comprising computer executable instructions which, when executed by a computer processor, cause the computer to perform the method of any of claims 1 to 6 or 8 to 13.

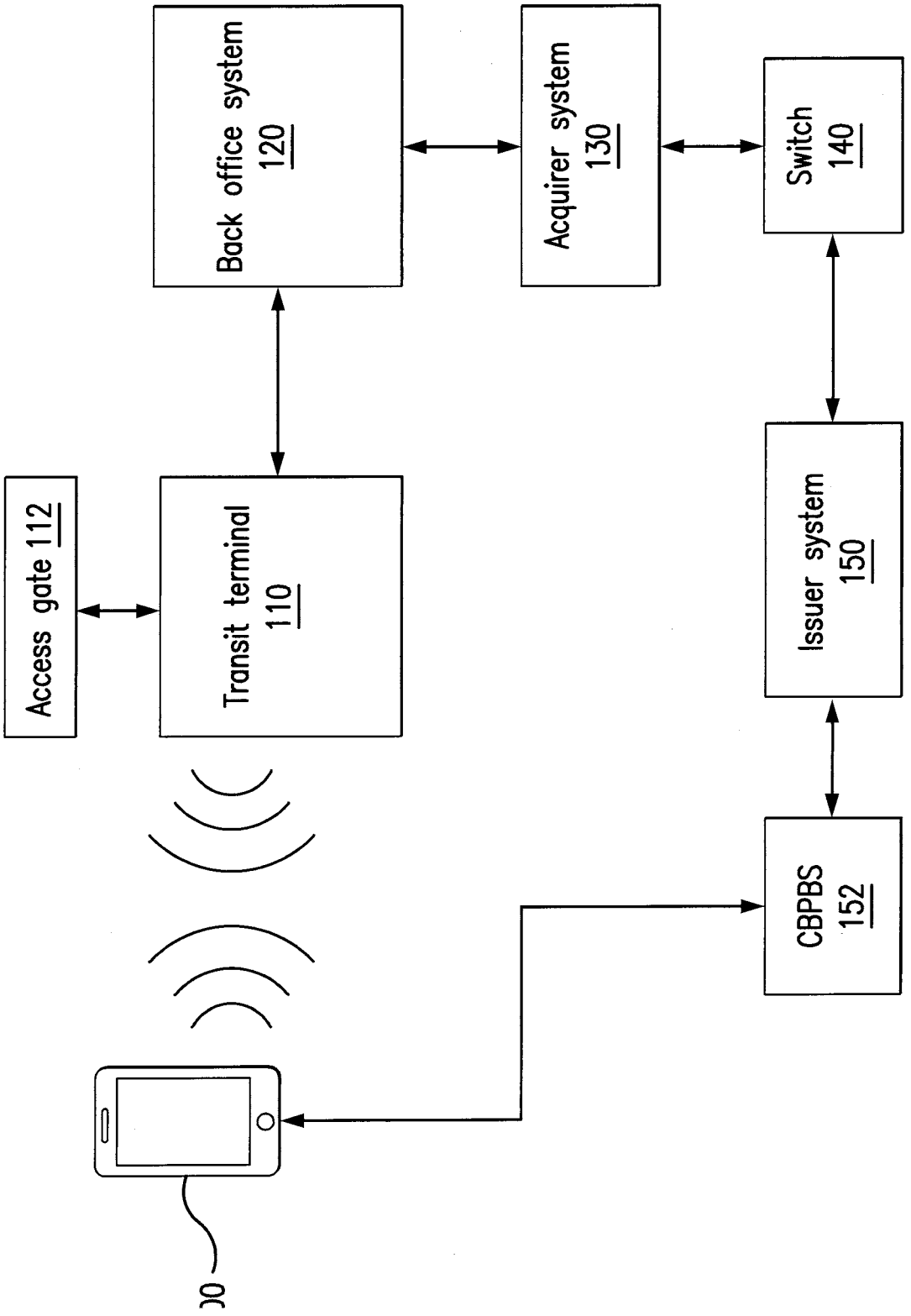

Back office system
120
Acquirer system
130
Switch
140
Access gate 112
Transit terminal
110
Issuer system
150
CBPBS
152
00

FIG. 1

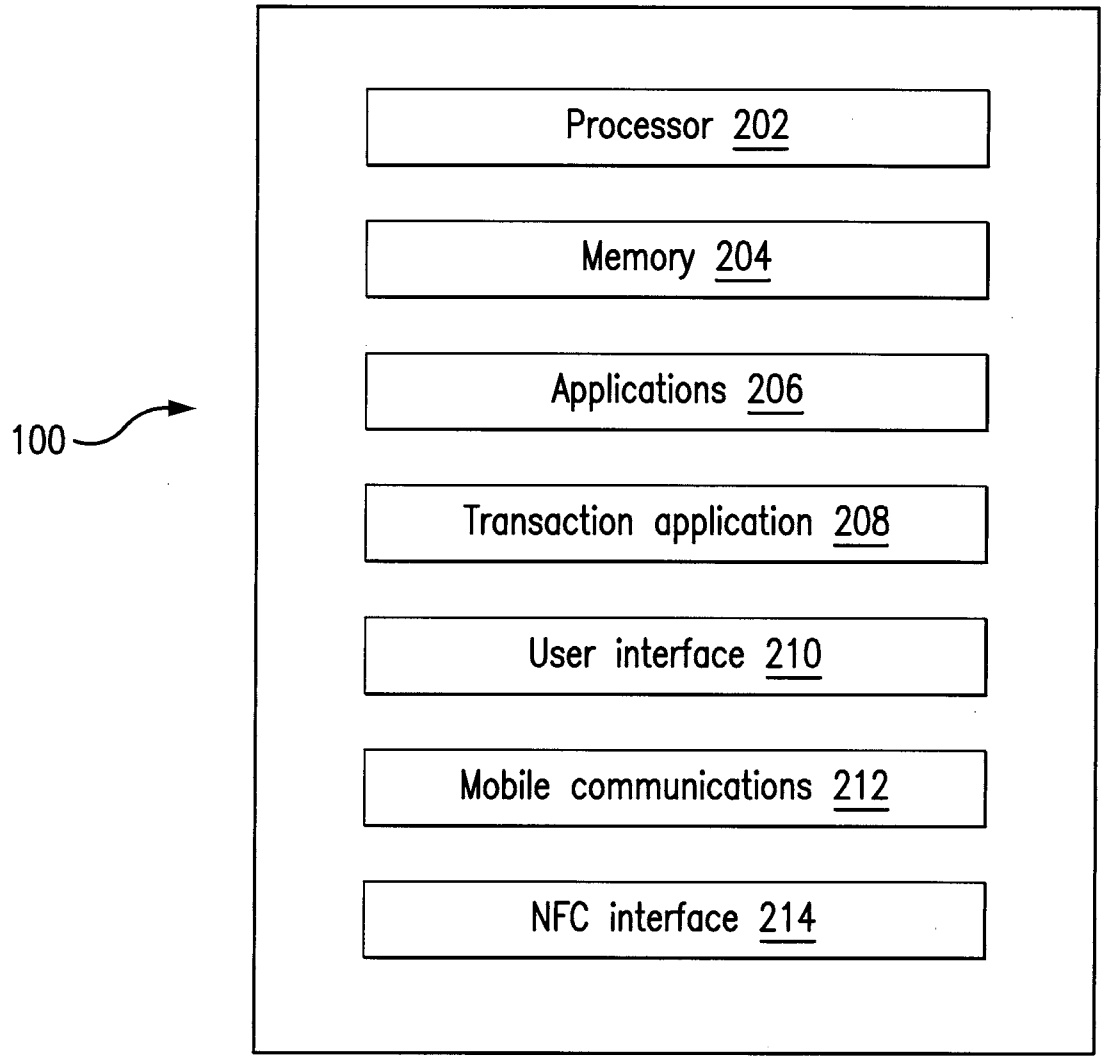

100
Processor 202
Memory 204
Applications 206
Transaction application 208
User interface 210
Mobile communications 212
NFC interface 214

FIG. 2

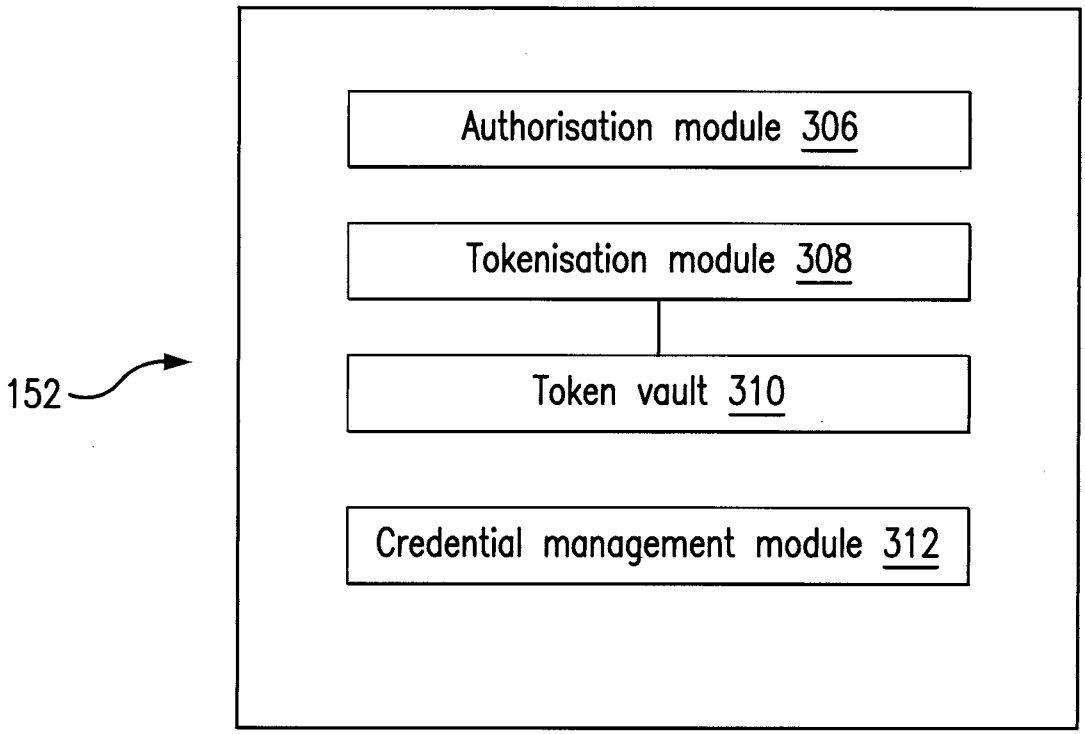

Authorisation module 306
Tokenisation module 308
Token vault 310
Credential management module 312
152

FIG. 3

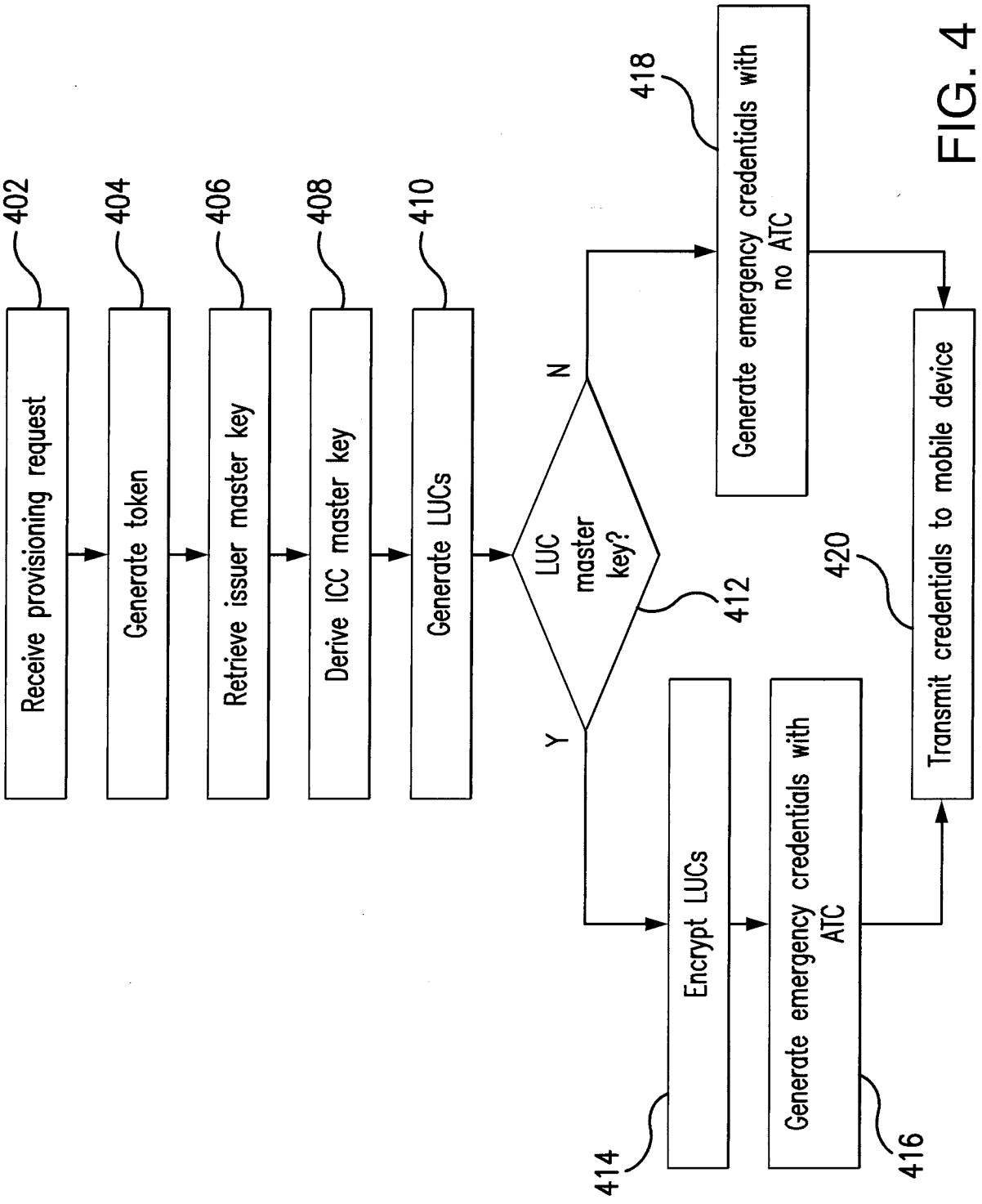

Receive provisioning request
402
Generate token
404
Retrieve issuer master key
406
Derive ICC master key
408
Generate LUCs
410
LUC master key?
412
N
Y
Generate emergency credentials with no ATC
418
Encrypt LUCs
414
Generate emergency credentials with ATC
416
Transmit credentials to mobile device
420

FIG. 4

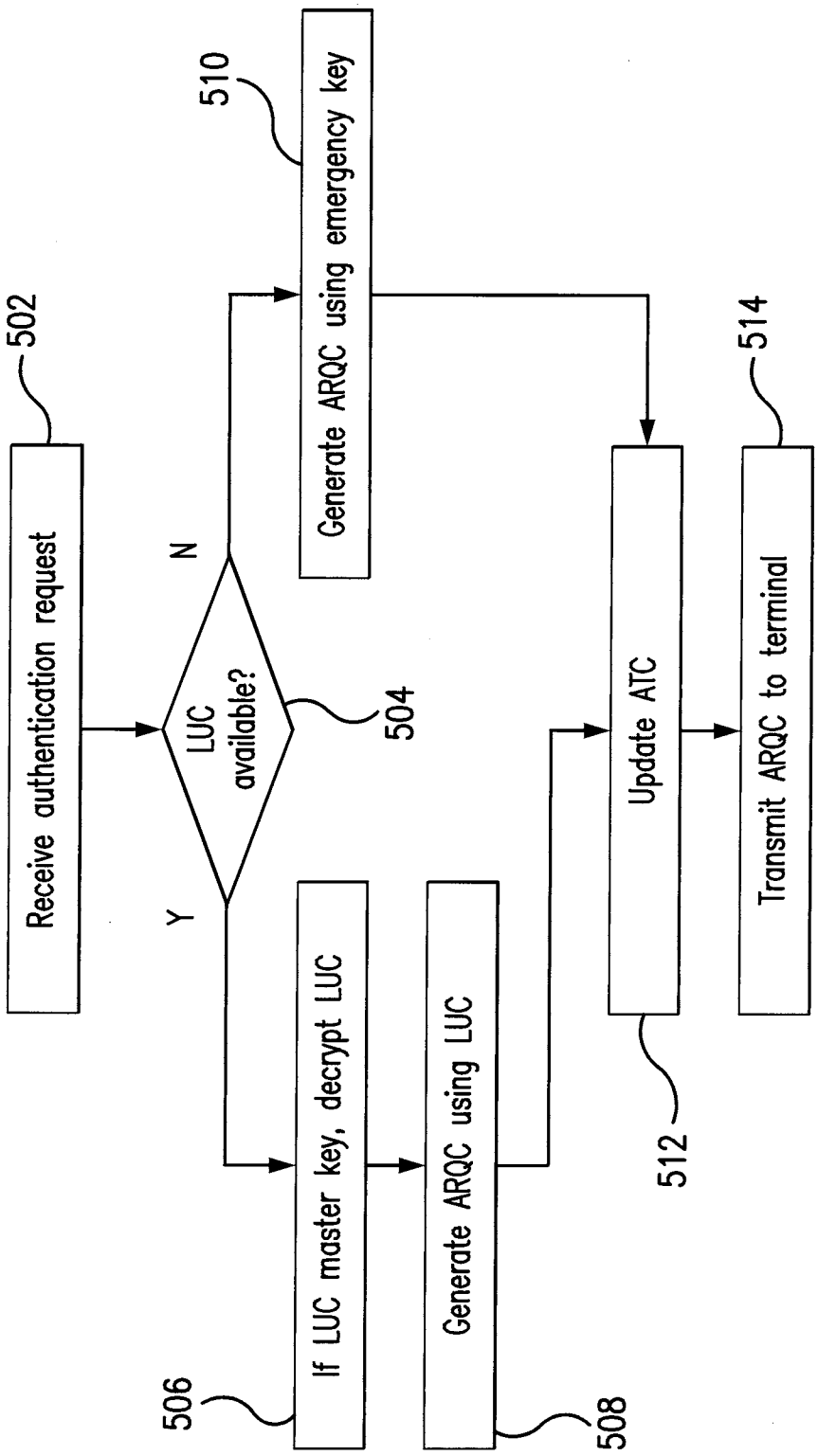

Receive authentication request
502
LUC available?
504
N
Y
Generate ARQC using emergency key
510
If LUC master key, decrypt LUC
506
Generate ARQC using LUC
508
Update ATC
512
Transmit ARQC to terminal
514

FIG. 5

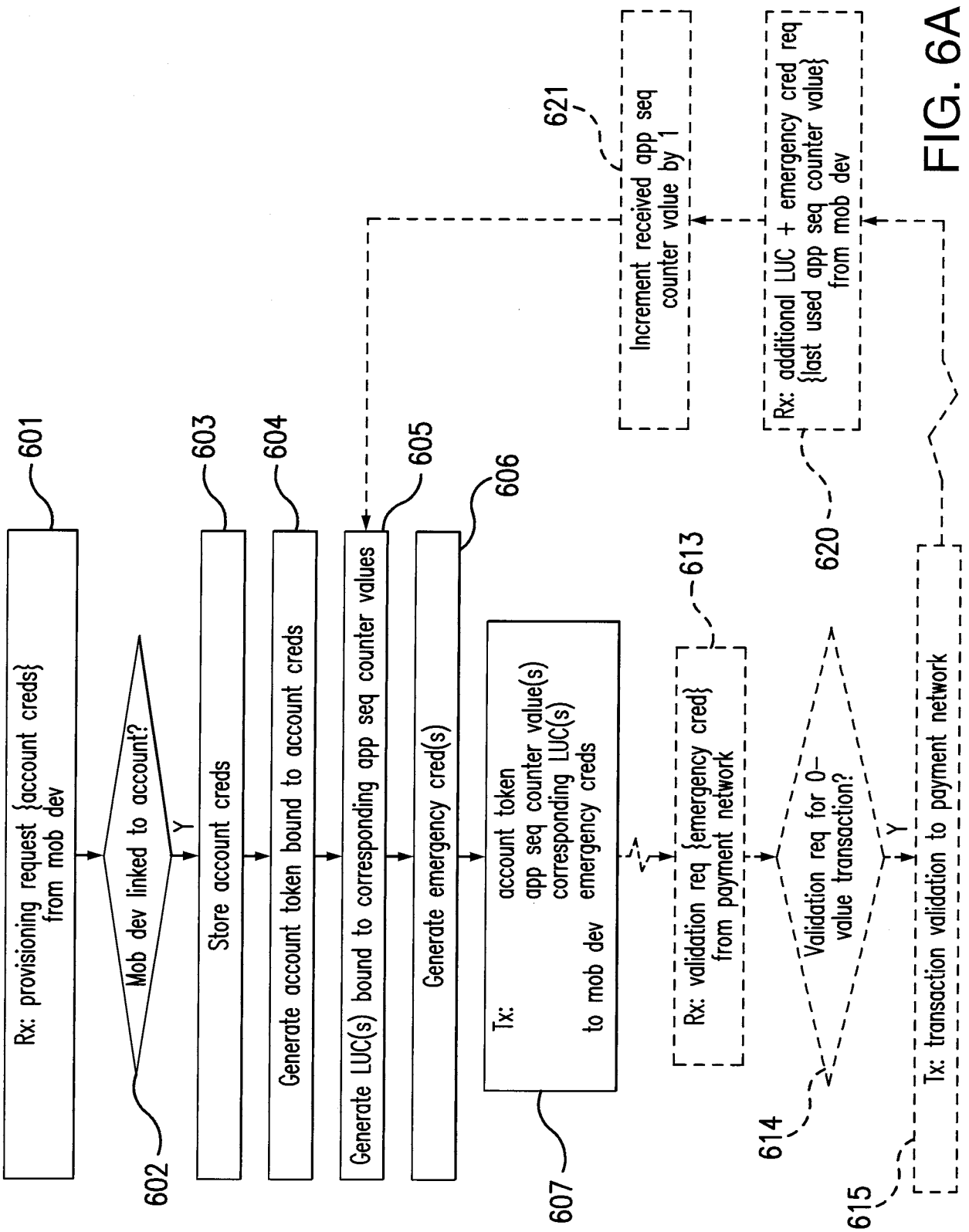

601
Rx: provisioning request {account creds} from mob dev
602
Mob dev linked to account?
Y
603
Store account creds
604
Generate account token bound to account creds
605
Generate LUC(s) bound to corresponding app seq counter values
606
Generate emergency cred(s)
607
Tx: account token app seq counter value(s) corresponding LUC(s) to mob dev emergency creds
613
Rx: validation req {emergency cred} from payment network
614
Validation req for 0-value transaction?
Y
615
Tx: transaction validation to payment network
620
Rx: additional LUC + emergency cred req {last used app seq counter value} from mob dev
621
Increment received app seq counter value by 1

FIG. 6A

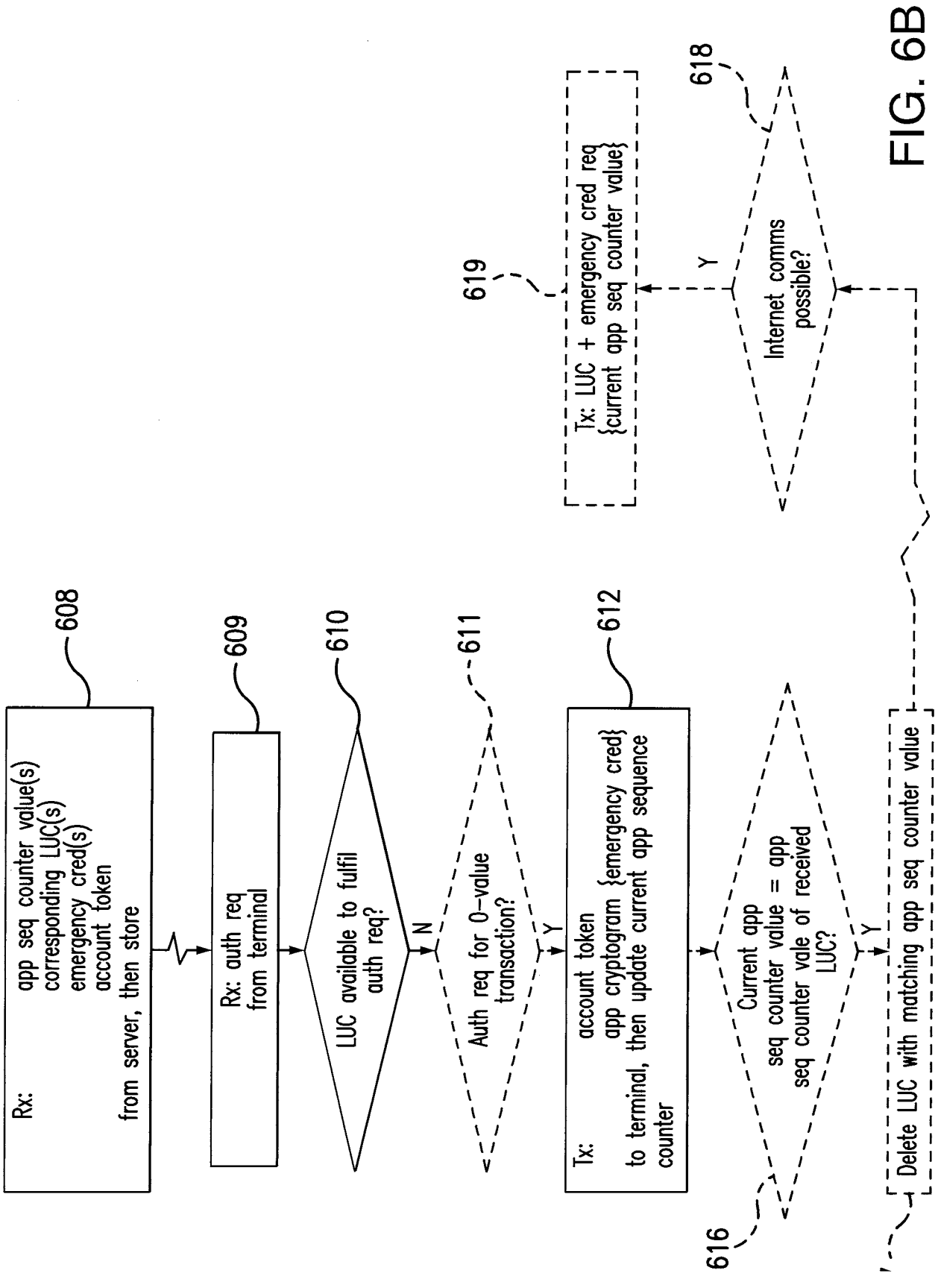

Rx: app seq counter value(s) corresponding LUC(s) emergency cred(s) account token from server, then store
608
Rx: auth req from terminal
609
LUC available to fulfil auth req?
610
N
Auth req for 0-value transaction?
611
Y
Tx: account token app cryptogram {emergency cred} to terminal, then update current app sequence counter
612
Current app seq counter value = app seq counter vale of received LUC?
616
Y
Delete LUC with matching app seq counter value
Internet comms possible?
618
Y
Tx: LUC + emergency cred req {current app seq counter value}
619

FIG. 6B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/052130

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 4-7,13-15
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required addtional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of any additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/052130

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/32(2012.01)i, G06Q 20/38(2012.01)i, H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q 20/32; G06Q 20/28; G06Q 20/34; G06Q 20/40; H04L 29/06; H04L 9/08; G06Q 20/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: limited use credential (LUC), emergency, credential, update, counter

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015-0180836 A1 (ERICK WONG et al.) 25 June 2015 See paragraphs [0010],[0062],[0095]-[0096],[0117],[0193]-[0194], claims 1-13 and figure 2.	1-3,8-12
Y	KR 10-1843660 B1 (VP INC.) 29 March 2018 See paragraphs [0044]-[0052], claims 1-5 and figures 1-2.	1-3,8-12
A	WO 2017-160877 A1 (MOZIDO, INC.) 21 September 2017 See paragraph [0079], claim 1 and figure 1.	1-3,8-12
A	US 2016-0140550 A1 (BANK OF AMERICA CORPORATION) 19 May 2016 See claims 1,10,18-19 and figure 1.	1-3,8-12
A	US 2016-0253651 A1 (SAMSUNG ELECTRONICS CO., LTD.) 01 September 2016 See paragraphs [0166],[0232],[0259],[0685]-[0686], claims 1,11 and figure 1.	1-3,8-12

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 January 2020 (03.01.2020)	**03 January 2020 (03.01.2020)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KANG, Min Jeong
Telephone No. +82-42-481-8131

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/052130

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015-0180836 A1	25/06/2015	AU 2014-368949 A1	09/06/2016
		CA 2931093 A1	25/06/2015
		CN 105830107 A	03/08/2016
		EP 3084701 A1	26/10/2016
		EP 3084701 A4	09/08/2017
		JP 06551850 B2	31/07/2019
		JP 2017-507518 A	16/03/2017
		JP 2019-180097 A	17/10/2019
		KR 10-2016-0101117 A	24/08/2016
		RU 2016129192 A	24/01/2018
		RU 2019111186 A	07/05/2019
		RU 2686014 C1	23/04/2019
		SG 10201900964 A	28/03/2019
		SG 11201604906 A	28/07/2016
		US 10402814 B2	03/09/2019
		US 2015-0178724 A1	25/06/2015
		US 2016-0140545 A1	19/05/2016
		US 2016-0217452 A1	28/07/2016
		US 2018-0189783 A1	05/07/2018
		US 2018-0232722 A1	16/08/2018
		US 2019-0295063 A1	26/09/2019
		US 9922322 B2	20/03/2018
		US 9972005 B2	15/05/2018
		WO 2015-095771 A1	25/06/2015
KR 10-1843660 B1	29/03/2018	CN 108269079 A	10/07/2018
WO 2017-160877 A1	21/09/2017	None	
US 2016-0140550 A1	19/05/2016	US 9692752 B2	27/06/2017
US 2016-0253651 A1	01/09/2016	AU 2016-216833 A1	10/08/2017
		AU 2016-216833 B2	15/08/2019
		AU 2016-224183 A1	13/04/2017
		AU 2016-224183 B2	19/07/2018
		CN 105894268 A	24/08/2016
		CN 105930040 A	07/09/2016
		CN 105933891 A	07/09/2016
		CN 107278313 A	20/10/2017
		CN 107408249 A	28/11/2017
		CN 107408251 A	28/11/2017
		CN 107408254 A	28/11/2017
		CN 107430657 A	01/12/2017
		CN 107430726 A	01/12/2017
		CN 108352007 A	31/07/2018
		EP 3057047 A1	17/08/2016
		EP 3057047 B1	03/04/2019
		EP 3062270 A1	31/08/2016
		EP 3062271 A1	31/08/2016

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/052130

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		EP 3262582 A1	03/01/2018
		EP 3262583 A1	03/01/2018
		EP 3262584 A1	03/01/2018
		EP 3262585 A1	03/01/2018
		EP 3262586 A1	03/01/2018
		EP 3262814 A1	03/01/2018
		EP 3264355 A1	03/01/2018
		EP 3332372 A1	13/06/2018
		EP 3335174 A1	20/06/2018
		EP 3370195 A1	05/09/2018
		KR 10-2016-0099464 A	22/08/2016
		KR 10-2016-0105261 A	06/09/2016
		KR 10-2016-0105278 A	06/09/2016
		KR 10-2016-0105279 A	06/09/2016
		KR 10-2016-0105292 A	06/09/2016
		KR 10-2016-0105296 A	06/09/2016
		KR 10-2016-0105297 A	06/09/2016
		KR 10-2016-0105300 A	06/09/2016
		KR 10-2016-0105346 A	06/09/2016
		KR 10-2016-0105352 A	06/09/2016
		US 10193700 B2	29/01/2019
		US 2016-0247144 A1	25/08/2016
		US 2016-0253652 A1	01/09/2016
		US 2016-0253657 A1	01/09/2016
		US 2016-0253664 A1	01/09/2016
		US 2016-0253666 A1	01/09/2016
		US 2016-0253669 A1	01/09/2016
		US 2016-0253670 A1	01/09/2016
		US 2016-0254918 A1	01/09/2016
		US 2017-0061436 A1	02/03/2017
		US 2017-0061437 A1	02/03/2017
		US 2017-0337542 A1	23/11/2017
		US 2018-0268398 A1	20/09/2018
		US 2018-0322484 A1	08/11/2018
		WO 2016-129863 A1	18/08/2016
		WO 2016-137271 A1	01/09/2016
		WO 2016-137277 A1	01/09/2016
		WO 2016-137297 A1	01/09/2016
		WO 2016-137298 A1	01/09/2016
		WO 2016-137300 A1	01/09/2016
		WO 2016-137302 A1	01/09/2016
		WO 2016-137304 A1	01/09/2016
		WO 2016-137307 A1	01/09/2016
		WO 2017-034281 A1	02/03/2017
		WO 2017-034312 A1	02/03/2017
		WO 2017-078365 A1	11/05/2017