Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 3239475 A1 2023/06/22

(21) 3 239 475

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) **Date de dépôt PCT/PCT Filing Date:** 2022/11/23
(87) **Date publication PCT/PCT Publication Date:** 2023/06/22
(85) **Entrée phase nationale/National Entry:** 2024/05/28
(86) **N° demande PCT/PCT Application No.:** US 2022/050885
(87) **N° publication PCT/PCT Publication No.:** 2023/113986
(30) **Priorité/Priority:** 2021/12/15 (US17/551,670)

(51) **Cl.Int./Int.Cl.** ***G06Q 20/38*** (2012.01), ***G06Q 20/32*** (2012.01), ***G06Q 20/34*** (2012.01), ***G06Q 20/36*** (2012.01)

(71) **Demandeur/Applicant:**
CAPITAL ONE SERVICES, LLC, US

(72) **Inventeurs/Inventors:**
OSBORN, KEVIN, US;
PRASAD, JAIKISHAN, US;
CATALA CASTELLAR, JOSE, US

(74) **Agent:** ROBIC AGENCE PI S.E.C./ROBIC IP AGENCY LP

(54) **Titre : RECUPERATION DE CLE BASEE SUR AUTHENTIFICATION DE CARTE SANS CONTACT**
(54) **Title: KEY RECOVERY BASED ON CONTACTLESS CARD AUTHENTICATION**

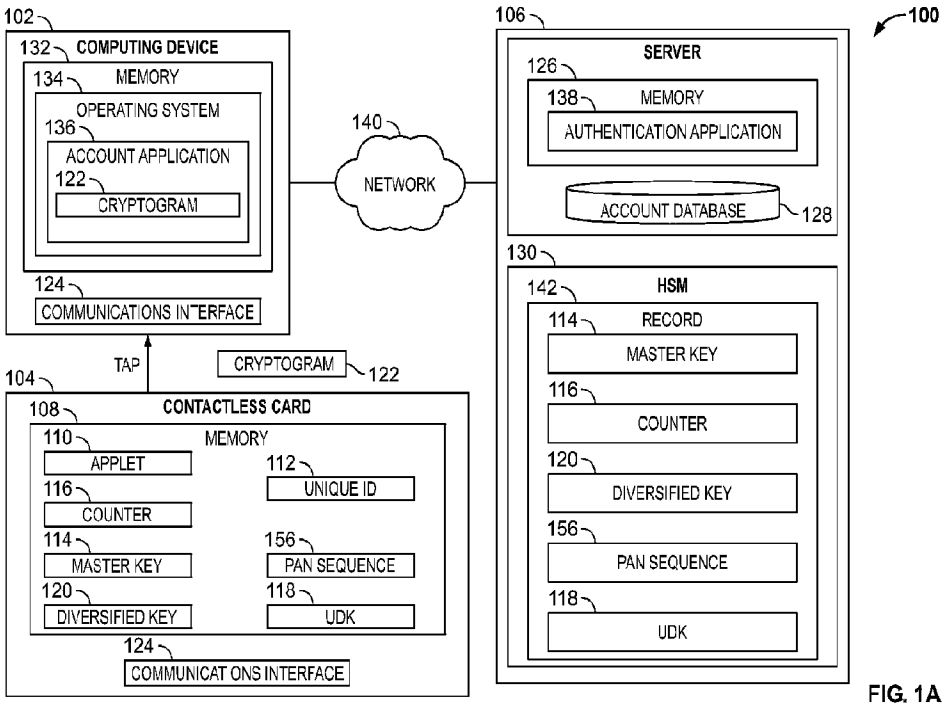


FIG. 1A

(57) **Abrégé/Abstract:**
Systems, methods, apparatuses, and computer-readable media for key recovery based on contactless card cryptograms. A server may receive, from an application, a request to recover a private key for a digital wallet, the request includes a first cryptogram generated by a contactless card. The server may decrypt the first cryptogram based on a key for the contactless card. The server may determine, based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet. The server may generate the private key based on the unique identifier and the diversification factor. The server may transmit the private key to the application via a network.

Date Submitted: 2024/05/28

CA App. No.: 3239475

Abstract:

Systems, methods, apparatuses, and computer-readable media for key recovery based on contactless card cryptograms. A server may receive, from an application, a request to recover a private key for a digital wallet, the request includes a first cryptogram generated by a contactless card. The server may decrypt the first cryptogram based on a key for the contactless card. The server may determine, based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet. The server may generate the private key based on the unique identifier and the diversification factor. The server may transmit the private key to the application via a network.

KEY RECOVERY BASED ON CONTACTLESS CARD AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application Serial No. 17/551,670, entitled "KEY RECOVERY BASED ON CONTACTLESS CARD AUTHENTICATION" filed on December 15, 2021. The contents of the aforementioned application are incorporated herein by reference in their entirety.

BACKGROUND

[0002] Digital wallets have numerous advantages but pose security and privacy challenges. The most common risks include theft and lost (or forgotten) access keys. Furthermore, custodial wallets are tied to a specific institution and do not permit portability. Proxy wallets have risks of security breaches and/or theft, leaving access keys being compromised. Hardware wallets may provide recovery seeds, but these seeds are prone to theft and/or other types of loss (e.g., when a user cannot recall the seeds or cannot locate their record of the seeds).

SUMMARY

[0003] Systems, methods, apparatuses, and computer-readable media for key recovery based on contactless card authentication. In one aspect, a method, includes receiving, by a server from an application, a request to recover a private key for a digital wallet, the request includes a first cryptogram generated by a contactless card, decrypting, by the server, the first cryptogram based on a key for the contactless card, determining, by the server based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet in a hardware security module, generating, by the server based on the unique identifier and the diversification factor, the private key, and transmitting, by the server to the application via a network, the private key.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0004] To easily identify the discussion of any particular element or act, the most significant digit or digits in a reference number refer to the figure number in which that element is first introduced.

[0005] FIG. 1A illustrates an aspect of the subject matter in accordance with one embodiment.

[0006] FIG. 1B illustrates an aspect of the subject matter in accordance with one embodiment.

[0007] FIG. 1C illustrates an aspect of the subject matter in accordance with one embodiment.

CA 03239475 2024-5-28

[0008] FIG. 2A illustrates an aspect of the subject matter in accordance with one embodiment.

[0009] FIG. 2B illustrates an aspect of the subject matter in accordance with one embodiment.

[0010] FIG. 2C illustrates an aspect of the subject matter in accordance with one embodiment.

[0011] FIG. 3A illustrates an aspect of the subject matter in accordance with one embodiment.

[0012] FIG. 3B illustrates an aspect of the subject matter in accordance with one embodiment.

[0013] FIG. 4 illustrates a routine 400 in accordance with one embodiment.

[0014] FIG. 5 illustrates a routine 500 in accordance with one embodiment.

[0015] FIG. 6 illustrates a routine 600 in accordance with one embodiment.

[0016] FIG. 7A illustrates a contactless card in accordance with one embodiment.

[0017] FIG. 7B illustrates a contactless card 104 in accordance with one embodiment.

[0018] FIG. 8 illustrates a data structure 800 in accordance with one embodiment.

[0019] FIG. 9 illustrates an example of a system 900 in accordance with embodiments.

[0020] FIG. 10 illustrates an example of a logical model 1000 in accordance with embodiments.

[0021] FIG. 11 illustrates an example of a logical model 1100 in accordance with embodiments.

[0022] FIG. 12 illustrates a computer architecture 1200 in accordance with one embodiment.

DETAILED DESCRIPTION

[0023] Embodiments disclosed herein provide techniques for secure recovery of cryptographic keys used to access digital wallets, such as cryptocurrency wallets, using a contactless card. To create a digital wallet, a computing device may instruct a contactless card to generate a cryptogram. An application executing on the computing device may receive the cryptogram via wireless communications with the contactless card and transmit the cryptogram to a server for verification. If the server verifies the cryptogram, the server may create a private key which is required to access or otherwise perform operations using the digital wallet. The server may then create a public key corresponding to the private key and generate a wallet address for the digital wallet based on the public key. The server may then store one or more inputs to a cryptographic algorithm used to create the private key in a

CA 03239475 2024-5-28

hardware security module (HSM). The inputs may include one or more of a key (or keys) associated with the contactless card, a unique identifier of the contactless card, and a diversification factor. In some embodiments, the keys may be stored in the HSM, while the unique identifier and diversification factor may be provided as inputs to the HSM for diversifying the private key (e.g., the unique identifier and diversification factor need not be stored in the HSM).

[0024] The server may securely transmit the private key, public key, and wallet address to the application, which may generate a digital wallet and store the private key, public key, and wallet address therein. In some embodiments, when the user attempts to access the digital wallet, cryptographic verification using the contactless card may be used to authenticate access to the digital wallet. If the cryptographic verification is not successful, the user may be restricted from accessing the wallet, thereby improving the security of the wallet.

[0025] Because the digital wallet stores obfuscated versions of the private key, the user may lose, forget, or otherwise not be able to provide the private key as a precondition to performing transactions with the digital wallet (e.g., to transfer cryptocurrency, etc.). Advantageously, embodiments disclosed herein provide a secure solution to recover the private key using the contactless card. Generally, to recover the private key, the contactless card may generate a cryptogram that is verified by the server. If the server is able to verify the cryptogram, the inputs used to generate the private key may be provided to the HSM. The server may then recreate the private key, and transmit the recreated private key to the requesting application and/or device in one or more portions.

[0026] Advantageously, embodiments disclosed herein provide secure techniques to recover private keys used to access digital wallets using cryptograms generated by contactless cards. By leveraging cryptograms, embodiments of the disclosure may securely verify the identity of the user with minimal risk of fraudulent activity. Furthermore, doing so ensures that the private key is are only restored when the user has access to a contactless card that facilitates the cryptogram verification with the server. Further still, the security of the digital wallet is enhanced by requiring the cryptographic verification as a precondition to accessing the digital wallet and/or recovering the private key.

[0027] With general reference to notations and nomenclature used herein, the detailed descriptions herein may be presented in terms of program procedures executed on a computer or network of computers. These procedural descriptions and representations are

CA 03239475 2024-5-28

used by those skilled in the art to effectively convey the substance of their work to others skilled in the art.

[0028] A procedure is here, and generally, conceived to be a self-consistent sequence of operations leading to a desired result. These operations are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be noted, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to those quantities.

[0029] Further, the manipulations performed are often referred to in terms, such as adding or comparing, which are commonly associated with mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable in most cases, in any of the operations described herein, which form part of one or more embodiments. Rather, the operations are machine operations. Useful machines for performing operations of various embodiments include digital computers or similar devices.

[0030] Some embodiments may be described using the expression "coupled" and "connected" along with their derivatives. These terms are not necessarily intended as synonyms for each other. For example, some embodiments may be described using the terms “connected” and/or “coupled” to indicate that two or more elements are in direct physical or electrical contact with each other. The term "coupled," however, may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other.

[0031] Various embodiments also relate to apparatus or systems for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a computer as selectively activated or reconfigured by a computer program stored in the computer. The procedures presented herein are not inherently related to a particular computer or other apparatus. Various machines may be used with programs written in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these machines will appear from the description given.

[0032] Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for purposes of

CA 03239475 2024-5-28

explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. However, the novel embodiments can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modifications, equivalents, and alternatives consistent with the claimed subject matter.

[0033] In the Figures and the accompanying description, the designations "a" and "b" and "c" (and similar designators) are intended to be variables representing any positive integer. Thus, for example, if an implementation sets a value for a = 5, then a complete set of components 123 illustrated as components 123-1 through 123-*a* (or 123a) may include components 123-1, 123-2, 123-3, 123-4, and 123-5. The embodiments are not limited in this context.

[0034] Figure 1A depicts an exemplary computing architecture 100, also referred to as a system, consistent with disclosed embodiments. Although the computing architecture 100 shown in Figures 1A-1C has a limited number of elements in a certain topology, it may be appreciated that the computing architecture 100 may include more or less elements in alternate topologies as desired for a given implementation.

[0035] The computing architecture 100 comprises one or more computing devices 102, one or more servers 106, and one or more contactless cards 104. The contactless card 104 is representative of any type of card, such as a credit card, debit card, ATM card, gift card, payment card, smart card, and the like. The contactless card 104 may comprise one or more communications interfaces 124, such as a radio frequency identification (RFID) chip, configured to communicate with a communications interface 124 (also referred to herein as a "card reader", a "wireless card reader", and/or a "wireless communications interface") of the computing devices 102 via NFC, the EMV standard, or other short-range protocols in wireless communication. Although NFC is used as an example communications protocol herein, the disclosure is equally applicable to other types of wireless communications, such as the EMV standard, Bluetooth, and/or Wi-Fi.

[0036] The computing device 102 is representative of any number and type of computing device, such as smartphones, tablet computers, wearable devices, laptops, portable gaming devices, virtualized computing system, merchant terminals, point-of-sale systems, servers, desktop computers, and the like. A mobile device may be used as an example of the computing device 102, but should not be considered limiting of the disclosure. The server 106 is representative of any type of computing device, such as a server, workstation, compute cluster, cloud computing platform, virtualized computing system, and the like.

CA 03239475 2024-5-28

Although not depicted for the sake of clarity, the computing device 102, contactless card 104, and server 106 each include one or more processor circuits, e.g., to execute programs, code, and/or instructions.

[0037] As shown, a memory 108 of the contactless card 104 includes an applet 110, a counter 116, one or more master keys 114, one or more diversified keys 120, a unique ID 112, a primary account number (PAN) sequence number 156, and one or more Unique Derived Keys (UDKs) 118. The unique ID 112 may be any identifier that uniquely identifies the contactless card 104 relative to other contactless cards 104. The PAN sequence 156 may include a counter value stored by the contactless card 104. The applet 110 is executable code configured to perform some or all of the operations described herein. The counter 116 is a value that is synchronized between the contactless card 104 and server 106. The counter 116 may comprise a number that changes each time data is exchanged between the contactless card 104 and the server 106 (and/or the contactless card 104 and the computing device 102). The counter 116, master keys 114, diversified keys 120, UDKs 118, PAN sequence 156, and/or unique ID 112 are used to provide security in the system 100 as described in greater detail below.

[0038] As shown, a memory 132 of the computing device 102 includes an instance of an operating system 134. Example operating systems include the Android® OS, iOS®, macOS®, Linux®, and Windows® operating systems. As shown, the operating system 134 includes an account application 136. The account application 136 allows users to perform various account-related operations, such as managing digital wallets, processing transactions using the wallet, processing blockchain and/or cryptocurrency transactions, activating payment cards, viewing account balances, purchasing items, processing payments, and the like. In some embodiments, a user may authenticate using authentication credentials to access certain features of the account application 136. For example, the authentication credentials may include a username (or login) and password, biometric credentials (e.g., fingerprints, Face ID, etc.), and the like.

[0039] As shown, a memory 126 of the server 106 includes an authentication application 138 and an account database 128. The account database 128 generally includes information related to an account holder (e.g., one or more users), one or more accounts of the account holder, and one or more contactless cards 104 of the account.

[0040] As stated, the account application 136 may be used to create, manage, access, or otherwise use digital wallets. A digital wallet allows one party to make electronic transactions with another party. In some embodiments, the digital wallet is a cryptocurrency

CA 03239475 2024-5-28

wallet that stores private keys and/or public keys for cryptocurrencies. The cryptocurrencies may be any type of cryptocurrency, such as Bitcoin, Ethereum, and the like. To create a digital wallet, the user may authenticate into the account using authentication credentials. The account application 136 may then instruct the user to tap the contactless card 104 to the computing device 102.

[0041] In the embodiment depicted in Figure 1A, the user may tap the contactless card 104 to the computing device 102 (or otherwise bring the contactless card 104 within communications range of the communications interface 124 of the device 102). The account application 136 may then instruct the applet 110 to generate a cryptogram 122. The cryptogram 122 may be generated based on any suitable cryptographic technique. In some embodiments, the cryptogram 122 may be based on the unique ID 112 of the contactless card 104. In some embodiments, the applet 110 may include the cryptogram 122 and an unencrypted identifier (e.g., the counter 116, the PAN sequence 156, the unique ID 112, and/or any other unique identifier) as part of a data package including the cryptogram 122. In at least one embodiment, the data package is an NDEF file.

[0042] As stated, the computing architecture 100 is configured to implement key diversification to secure data, which may be referred to as a key diversification technique herein. Generally, the server 106 (or another computing device) and the contactless card 104 may be provisioned with the same master key 114 (also referred to as a master symmetric key). More specifically, each contactless card 104 is programmed with a distinct master key 114 that has a corresponding pair in the hardware security module (HSM) 130 of the server 106. For example, when a contactless card 104 is manufactured, a unique master key 114 may be programmed into the memory 108 of the contactless card 104. Similarly, the unique master key 114 may be stored in a record 142 in the HSM 130.

[0043] Furthermore, when a given card 104 is manufactured, a UDK 118 may be diversified from the master key 114 via an HSM function that takes, as input, a diversification factor and a reference to the master key 114 index in the HSM 130 (e.g., an index to the record 142). In some embodiments, the diversification factor may be the unique ID 112 and PAN sequence 156 of the contactless card 104. The UDK 118 may be stored in the contactless card 104 and the record 142 of the HSM 130. The master key 114 and UDK 118 may be kept secret from all parties other than the contactless card 104 and server 106, thereby enhancing security of the system 100. Although depicted as being stored in the record 142, in some embodiments, the counter 116 and/or PAN sequence 156 are not stored

CA 03239475 2024-5-28

in the HSM 130. For example, the unique ID 112, counter 116, and PAN sequence 156 may be stored in the account database 128.

[0044] In some embodiments, to generate the cryptogram 122, the applet 110 may provide the UDK 118, unique ID 112, and a diversification factor as input to a cryptographic algorithm, thereby producing a diversified key 120. In some embodiments, the diversification factor is the counter 116. In other embodiments, the PAN sequence 156 is the diversification factor. The diversified key 120 may then be used to encrypt some data, such as the diversification factor (e.g., the counter 116 and/or the PAN sequence 156) or other sensitive data. The applet 110 and the server 106 may be configured to encrypt the same type of data to facilitate the decryption and/or verification processing of a cryptogram.

[0045] As stated, the UDKs 118 of the contactless card 104 and server 106 may be used in conjunction with the counters 116 to enhance security using key diversification. As stated, the counters 116 comprise values that are synchronized between the contactless card 104 and server 106. The counter 116 may comprise a number that changes each time data is exchanged between the contactless card 104 and the server 106 (and/or the contactless card 104 and the computing device 102). When preparing to send data (e.g., to the server 106 and/or the device 102), the applet 110 of the contactless card 104 may increment the counter 116. The applet 110 of the contactless card 104 may then provide the UDK 118, unique ID 112, and counter 116 as input to a cryptographic algorithm, which produces a diversified key 120 as output. The cryptographic algorithm may include encryption algorithms, hash-based message authentication code (HMAC) algorithms, cipher-based message authentication code (CMAC) algorithms, and the like. Non-limiting examples of the cryptographic algorithm may include a symmetric encryption algorithm such as 3DES or AES107; a symmetric HMAC algorithm, such as HMAC-SHA-256; and a symmetric CMAC algorithm such as AES-CMAC. Examples of key diversification techniques are described in greater detail in United States Patent Application 16/205,119, filed November 29, 2018. The aforementioned patent application is incorporated by reference herein in its entirety. In some embodiments, the PAN sequence 156 is used as input to the cryptographic algorithm instead of the counter 116 to generate the diversified key 120, e.g., by encrypting the UDK 118, unique ID 112 and PAN sequence 156.

[0046] The applet 110 may then encrypt some data (e.g., the unique ID 112, the counter 116, the PAN sequence 156, a command, and/or any other data) using the diversified key 120 and the data as input to the cryptographic algorithm. For example, encrypting the unique ID 112 with the diversified key 120 may result in an encrypted unique ID 112 (e.g.,

CA 03239475 2024-5-28

a cryptogram 122). As stated, the applet 110 and the server 106 may be configured to encrypt the same data.

[0047] In some embodiments, two diversified keys 120 may be generated, e.g., based on one or more portions of the input to the cryptographic function. In some embodiments, the two diversified keys 120 are generated based on two distinct master keys 114, two distinct UDKs 118, the unique ID 112, and the counter 116 (or the PAN sequence 156). In such embodiments, a message authentication code (MAC) is generated using one of the diversified keys 120, and the MAC may be encrypted using the other one of the diversified keys 120. The MAC may be generated based on any suitable data input to a MAC algorithm, such as sensitive data, the unique ID 112, the counter 116, and/or the PAN sequence 156. More generally, the applet 110 and the server 106 may be configured to generate the MAC based on the same data. In some embodiments, the cryptogram 122 is included in a data package such as an NDEF file. The account application 136 may then read the data package including cryptogram 122 via the communications interface 124 of the computing device 102.

[0048] Figure 1B depicts an embodiment where the account application 136 transmits the cryptogram 122 to the server 106. The server 106 may provide the cryptogram 122 to the authentication application 138 and/or the HSM 130 for verification based at least in part on the instance of the master key 114 and/or UDK 118 stored by the server 106. In some embodiments, the authentication application 138 and/or the HSM 130 may identify the UDK 118 (or master key 114) and counter 116 using the unencrypted unique ID 112 provided to the server 106. In examples where the PAN sequence 156 is used to generate the cryptogram 122, the server 106 may identify the PAN sequence 156 in the account database 128 and/or HSM 130 using the unencrypted unique ID 112. In some examples, the authentication application 138 may provide the UDK 118, unique ID 112, and counter 116 as input to the cryptographic function of the HSM 130, which produces one or more diversified keys 120 as output. In other embodiments, the server encrypts the UDK 118, unique ID 112, and PAN sequence 156 to generate the diversified keys 120. The resulting diversified keys 120 may correspond to the diversified keys 120 of the contactless card 104, which may be used to decrypt the cryptogram 122 and/or verify the MAC once decrypted. For example, the server 106 may generate a MAC based on the same data as the applet 110, e.g., the sensitive data, the unique ID 112, the counter 116, and/or the PAN sequence 156. If the MAC generated by the server 106 matches the decrypted MAC in the cryptogram 122, the server 106 may verify or otherwise authenticate the cryptogram 122.

CA 03239475 2024-5-28

[0049] Regardless of the decryption technique used, the authentication application 138 and/or the HSM 130 may successfully decrypt the cryptogram 122 and verify the MAC, thereby verifying or authenticating the cryptogram 122. If the decryption and/or MAC verification is successful, the authentication application 138 and/or the HSM 130 may generate a digital wallet 144 for the user. Generally, to create the digital wallet 144, a private key 146 may be generated. In some embodiments, a random number is provided as input into an encryption (0r hash) algorithm, such as the SHA-2 algorithm or any other suitable algorithm, to generate a private key 146 of any length. In other embodiments, the unique ID 112 of the contactless card 104 and the PAN sequence 156 are concatenated and provided as input to the hash algorithm to generate the private key 146. In other embodiments, the unique ID 112 of the contactless card 104 and the counter 116 are concatenated and provided as input to the hash algorithm to generate the private key 146.

[0050] In other embodiments, the master key 114, the unique ID 112, and the counter 116 of the contactless card 104 are concatenated and provided as input to the hash algorithm to generate the private key 146. In embodiments where the master key 114 is used to generate the private key 146, a first master key 114 of the contactless card 104 may be used to generate the cryptogram 122, and a second master key 114 of the contactless card 104 may be used to generate the private key 146, where the first and second master keys 114 are distinct keys. In other embodiments, one of the diversified keys 120, the unique ID 112, and the counter 116 of the contactless card 104 are concatenated and provided as input to the hash algorithm to generate the private key 146. In other embodiments, one of the UDKs 118, the unique ID 112, and the counter 116 of the contactless card 104 are concatenated and provided as input to the hash algorithm to generate the private key 146. Regardless of the input used to generate the private key 146, in some embodiments, salt (e.g., random data) is included in the input to the hash algorithm to generate the private key 146.

[0051] The private key 146 may then be used to generate a corresponding public key 148. In some embodiments, the public key 148 may be generated based on the private key 146 using the Elliptic Curve Digital Signature Algorithm (ECDSA). In some embodiments, the public key 148 may be concatenated (or compressed), e.g., using a hash algorithm. In some embodiments, salt is used to generate the public key 148. A wallet address 150 may be generated for the digital wallet 144 based on the public key 148, e.g., by hashing the public key 148. Although depicted as being stored in the HSM 130, in some embodiments, the digital wallet 144 is not permanently stored in the HSM 130. Instead, as described in greater detail herein, elements used to recreate the private key 146 may be stored in the HSM 130

CA 03239475 2024-5-28

and/or the account database 128. For example, the unique ID 112 and the counter 116 may be stored in the HSM 130 and/or the account database 128. In another example, the unique ID 112 and the PAN sequence 156 may be stored in the HSM 130 and/or the account database 128.

[0052] In some embodiments, the private key 146 and/or public key 148 may be further diversified, e.g., to create hierarchical deterministic keys. For example, the private key 146 may be diversified with the counter 116, the unique ID 112, a salt value 154, or any other predetermined seed value. Doing so may diversify the private key 146. Similarly, the public key 148 may be diversified with the counter 116, the unique ID 112, a salt value 154, or any other predetermined seed value to create a diversified public key 148. In such embodiments, any seed value that is used to diversify the private key 146 and/or public key 148 may be stored in a recovery record 152 of the account database 128 and/or HSM 130. More generally, the private key 146 and/or public key 148 may be diversified using the seed value a plurality of times, thereby generating a tree (or hierarchy) of diversified private keys 146 and/or diversified public keys 148. In such embodiments, one or more paths of the tree (or hierarchy) may be used to specify different diversified keys. More generally, each node of the tree may correspond to a diversified public key and/or a diversified child key. Given the private and public key of a node of the tree, the diversified private and public keys of all descendant nodes in the tree may be derived. Furthermore, each leaf node in the tree may correspond to a diversified public key and/or a diversified child key. In some embodiments, the path is further used to specify attributes for a transaction, such as a currency, an amount of the currency, a first wallet address for the transaction (e.g., a sending wallet address), a second wallet address for the transaction (e.g., a recipient wallet address), and any other attribute. These attributes may be stored in a given node of the tree.

[0053] Returning to the decryption, if the authentication application 138 is unable to decrypt the cryptogram 122 (and/or is unable to verify the MAC) the authentication application 138 does not validate the cryptogram 122. In such an example, the authentication application 138 determines to refrain from generating a digital wallet. The authentication application 138 may transmit an indication of the failed decryption and/or verification to the computing device 102.

[0054] Figure 1C depicts an embodiment where the authentication application 138 transmits the digital wallet 144 to the computing device 102. As shown, the account application 136 may store the digital wallet 144 (in the memory 132 and/or a non-volatile storage, not pictured for the sake of clarity), which includes the private key 146, the public

CA 03239475 2024-5-28

key 148, and the wallet address 150. The account application 136 may hash, encrypt, or otherwise obfuscate the private key 146, public key 148, and/or wallet address 150. The account application 136 may protect the digital wallet 144 with authentication controls, such as a username and/or password, biometric credentials, etc. In addition and/or alternatively, the account application 136 may require cryptogram decryption and/or verification using the contactless card 104 to access the digital wallet 144 (e.g., the contactless card 104 generates a cryptogram which is verified by the server 106 as described herein). In addition, in some embodiments, the account application 136 may require the user to provide the private key 146 to access the digital wallet 144 and/or perform operations using the digital wallet 144. More generally, the account application 136 may provide a variety of interfaces to access, use, or otherwise manage the digital wallet 144.

[0055] In some embodiments, the digital wallet 144 may be stored in a cloud-based wallet, e.g., in the server 106 or another computing system that provides cloud-based wallet services to clients. Embodiments are not limited in this context. The cloud-based wallet may provide an interface to access or otherwise use the digital wallet 144, e.g., via the account application 136.

[0056] As shown, the server 106 has created a recovery record 152 in the account database 128 based on the creation of the digital wallet 144. The recovery record 152 includes the unique ID 112, the diversification factor 158 (e.g., the counter 116 and/or the PAN sequence 156), and any salt 154 (if used) to generate the private key 146. In some embodiments, the recovery record 152 may be indexed based on the wallet address 150 of the wallet 144. In other embodiments, the recovery record 152 may be indexed based on the record 142 of the HSM 130 that stores the keys of the contactless card 104. In other embodiments, the recovery record 152 is indexed based on the unique ID 112 of the contactless card 104. The recovery record 152 may then be used to recreate the private key 146, e.g., based on the unique ID 112, diversification factor 158, and/or the salt 154 and the appropriate algorithm. In embodiments where a diversified key 120, a UDK 118, or a master key 114 are used to generate the private key 146, advantageously, the diversified key 120, UDK 118, or master key 114 are not stored in the recovery record 152 to improve security. In such embodiments, the HSM 130 may store the master key 114, UDK 118, and/or diversified key 120 used to recreate the private key 146, while the unique ID 112, diversification factor 158, and/or the salt 154 may be stored in the account database 128.

[0057] Figure 2A is a schematic 200 illustrating an embodiment where a user requests to recover the private key 146. As shown, to recover the private key 146, the account

CA 03239475 2024-5-28

application 136 may instruct the user to tap the contactless card 104 to the computing device 102, which causes the contactless card 104 to generate a cryptogram 208. The cryptogram 208 may be generated as described above with reference to the cryptogram 122. For example, the applet 110 may increment the counter 116 and encrypt one or more UDKs 118, the unique ID 112, and the counter 116 to generate one or more diversified keys 120. The one or more diversified keys 120 may be used to generate a MAC based on some data and encrypt the MAC and/or the data. In some embodiments, the MAC is generated based on the wallet address 150 and one of the diversified keys 120. In such an embodiment, the wallet address 150 and the MAC are encrypted using the other one of the diversified keys 120 to generate the cryptogram 208. As another example, the public key 148 may be used to generate the MAC, and the public key 148 may be encrypted with the MAC.

[0058] Figure 2B depicts an embodiment where the account application 136 transmits the cryptogram 208 to the server 106 for verification. Generally, the server 106 may increment the counter 116 and encrypt the UDK 118, the unique ID 112, and the counter 116 of the contactless card 104 to generate one or more diversified keys 120 corresponding to the keys generated by the contactless card 104. The one or more diversified keys 120 may be used to decrypt the cryptogram 208 and/or verify the MAC.

[0059] If the server 106 is able to decrypt the cryptogram 208 and/or verify the MAC, the server 106 may recreate the private key 146 based on the recovery record 152. In embodiments where the wallet address 150 is encrypted in the cryptogram 208, the recovery record 152 may be indexed (e.g., searched) based on the wallet address 150, and the server 106 may access the recovery record 152 using the decrypted wallet address 150. In embodiments where the public key 148 is encrypted in the cryptogram 208, the server 106 may regenerate the wallet address 150 using the public key 148, and index the account database 128 using the regenerated wallet address 150. In other embodiments, the account database 128 is indexed using the unique ID 112 to identify the recovery record 152. In such embodiments, the unique ID 112 is determined based on an unencrypted version of the unique ID 112 included with the cryptogram 208.

[0060] Once the server 106 identifies the recovery record 152, the recovery record 152 may be used to recreate the private key 146. For example, the unique ID 112, diversification factor 158, and salt 154 (if used) of the recovery record 152 may be provided as input to the function of the HSM 130 used to initially create the private key 146. Doing so recreates the private key 146.

CA 03239475 2024-5-28

[0061] In some embodiments, the server 106 further recreates the private key 146 based on the master key 114 or the UDK 118. For example, the server 106 may provide the master key 114 of the contactless card 104 and the data in the recovery record 152 (e.g., the unique ID 112, diversification factor 158, and any salt 154) as input to the function of the HSM 130 used to create the private key 146. Doing so recreates the private key 146. As another example, the server 106 may provide the UDK 118 of the contactless card 104 and the data in the recovery record 152 (e.g., the unique ID 112, diversification factor 158, and any salt 154) as input to the function of the HSM 130 used to create the private key 146. Doing so also recreates the private key 146.

[0062] In some embodiments, the UDK 118, unique ID 112, diversification factor 158, and any salt 154 are input to the function of the HSM 130 to generate the diversified key 120 used to generate the private key 146. The diversified key 120, diversification factor 158, and any salt 154 may be provided as input to the function of the HSM 130 to recreate the private key 146.

[0063] If, on the other hand, the HSM 130 is unable to decrypt the cryptogram 122 and/or verify the MAC, the HSM 130 does not validate the cryptogram 122. In such an example, the authentication application 138 determines to refrain from recovering the private key 146. The authentication application 138 may transmit an indication of the failed decryption and/or MAC verification to the computing device 102. In such embodiments, the user is restricted from recovering the private key 146 using the recovery record 152.

[0064] Figure 2C depicts an embodiment where the HSM 130 has recreated the private key 146 based on the recovery record 152 and transmits the private key 146 to the account application 136. In some embodiments, the server 106 may transmit the private key 146 in one or more data portions. More generally, the server 106 may transmit the private key 146 using a secured connection with the computing device 102. The computing device 102 may then display the private key 146, allowing the user to recover the private key 146. The user may then use the private key 146 to perform one or more operations using the digital wallet 144 and/or any cryptocurrencies associated with the digital wallet 144. For example, the private key 146 may be used to generate a transaction in a blockchain 906.

[0065] In some embodiments, the private key 146 is not transmitted to the computing device 102. For example, in a cloud-based wallet embodiment, the private key 146 may be used to sign transactions or other types of data. In such an example, the user may authenticate their account in the account application 136 using account authentication credentials and provide details of an intended transaction (e.g., a purchase, a cryptocurrency

CA 03239475 2024-5-28

transfer, etc.). The account application 136 may provide the transaction details to the server 106. In some embodiments, the account application 136 provides the transaction details in a cryptogram and/or a data package including the cryptogram. The cryptogram may be similar to the cryptogram 122 and/or cryptogram 208. The server 106 may then retrieve the data used to diversify they keys from the recovery record 152 (e.g., the unique ID 112, the counter 116, the PAN sequence 156, and/or the salt 154). The data from the recovery record 152 may be provided to the HSM 130, which generates a digital signature for the transaction using the data from the recovery record and the master key 114 and/or the UDK 118. Doing so generates the signature required for the transaction. For example, by generating a valid signature, the transaction may be verified using the public key 148. In such examples, a transaction may be added to a blockchain to reflect the verified transaction.

[0066] Figure 3A is a schematic 300a illustrating an embodiment where a contactless card 104 is tapped to a computing device 102, e.g., to recover the private key 146. As stated, when the contactless card 104 is tapped to the computing device 102, the applet 110 may generate a cryptogram (e.g., the cryptogram 122 and/or the cryptogram 208). The cryptogram and any other data (e.g., unencrypted unique ID 112) may be included in a data package, such as an NDEF file, that is read by the computing device 102. The computing device 102 may then transmit the cryptogram to the server 106 for verification (e.g., decryption and/or MAC verification) as described herein.

[0067] Figure 3B is a schematic 300b illustrating an embodiment where the server 106 verified the cryptogram generated in Figure 3A. Based on the verification, the server 106 may recreate the private key 146 based on the recovery record 152. The server 106 may then transmit the private key 146 to the account application 136. As shown, the account application 136 may then display the private key 146 on the display as a string of characters. In some embodiments, a matrixed code 302 may be generated to represent the private key 146. Doing so allows the matrixed code 302 to be scanned to determine the private key 146.

[0068] Operations for the disclosed embodiments may be further described with reference to the following figures. Some of the figures may include a logic flow. Although such figures presented herein may include a particular logic flow, it can be appreciated that the logic flow merely provides an example of how the general functionality as described herein can be implemented. Further, a given logic flow does not necessarily have to be executed in the order presented unless otherwise indicated. Moreover, not all acts illustrated in a logic flow may be required in some embodiments. In addition, the given logic flow may be

CA 03239475 2024-5-28

implemented by a hardware element, a software element executed by a processor, or any combination thereof. The embodiments are not limited in this context.

[0069] Figure 4 illustrates an embodiment of a logic flow, or routine, 400. The logic flow 400 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 400 may include some or all of the operations to create a digital wallet. Embodiments are not limited in this context.

[0070] In block 402, a server 106 may receive, from the account application 136 executing on a computing device 102, a request to generate a digital wallet. The request may include a cryptogram generated by the contactless card 104 and transmitted to the computing device 102. In block 404, the server may decrypt the cryptogram by generating one or more diversified keys 120 based on the master key 114, UDK 118, and a counter 116. The server 106 may further verify the cryptogram, e.g., determine that a MAC generated by the server 106 matches a MAC in the decrypted cryptogram.

[0071] In block 406, the server 106 generates a private key 146 based on the successful decryption and/or verification of the cryptogram at block 404. The private key 146 may be based on input to a cryptographic function of the HSM 130. The input may include the unique ID 112 and the diversification factor 158 (e.g., the counter 116 and/or a PAN sequence 156 of the contactless card 104). In some embodiments, the input may further include a master key 114, a UDK 118, and/or a diversified key 120. In block 408, the server 106 may generate a public key 148 based on the private key 146. The server may further create a wallet address 150 for the digital wallet 144 based on the public key 148. In block 410, the server may transmit, to the application, the private key 146, the public key 148, and the wallet address 150. In block 412, the server 106 stores one or more inputs used to generate the private key in the account database 128 (e.g., the unique ID 112 and diversification factor 158).

[0072] Figure 5 illustrates an embodiment of a logic flow, or routine, 500. The logic flow 500 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 500 may include some or all of the operations to access a digital wallet. Embodiments are not limited in this context.

[0073] In block 502, routine 500 receives, by a server 106 from an account application 136 executing on a computing device 102, a request to access a digital wallet 144, the request comprising a cryptogram. In block 504, the server 106 may decrypt the cryptogram by generating one or more diversified keys 120 based on the master key 114, the UDK 118, and a counter 116. The server 106 may further verify the cryptogram, e.g., determine that a

CA 03239475 2024-5-28

MAC generated by the server 106 matches a MAC in the decrypted cryptogram. In block 506, the server may generate an authorization based on the successful decryption and verification. The authorization may generally indicate that the requested access to the digital wallet 144 is to be permitted. In block 508, the server transmits the authorization to the account application 136. The authorization may cause the account application 136 to permit the requested access to the digital wallet 144. In some embodiments, however, the private key 146 is further required to access the digital wallet 144.

[0074] Figure 6 illustrates an embodiment of a logic flow, or routine, 600. The logic flow 600 may be representative of some or all of the operations executed by one or more embodiments described herein. For example, the logic flow 600 may include some or all of the operations to recover the private key for a digital wallet. Embodiments are not limited in this context.

[0075] In block 602, routine 600 receives, by a server 106 from an account application 136, a request to recover a private key 146 for a digital wallet 144. The request may comprise a cryptogram generated by a contactless card 104 based on key diversification (e.g., based on the master key 114, UDK 118, and one or more diversified keys 120). In block 604, the server 106 may decrypt the cryptogram by generating one or more diversified keys 120 based on the master key 114, the UDK 118, and a counter 116. The server 106 may further verify the cryptogram, e.g., determine that a MAC generated by the server 106 matches a MAC in the decrypted cryptogram.

[0076] In block 606, the server 106 may determine, based on the decryption and verification, a unique ID 112 of the contactless card 104 and a diversification factor 158 (e.g., a counter 116 and/or a PAN sequence 156) in the account database 128. In block 608, the server 106 recreates the private key 146 based on the unique ID 112, the diversification factor 158, and any salt 154. In some embodiments, the server 106 recreates the private key 146 based on the master key 114, the unique ID 112, the diversification factor 158, and any salt 154. In some embodiments, the server 106 recreates the private key 146 based on the UDK 118, the unique ID 112, the diversification factor 158, and any salt 154. In some embodiments, the server 106 recreates the private key 146 based on the diversified key 120, the unique ID 112, the diversification factor 158, and any salt 154. In block 610, the server 106 transmits the recreated private key 146 to the account application 136 via a network.

[0077] FIG. 7A is a schematic 700 illustrating an example configuration of a contactless card 104, which may include a payment card, such as a credit card, debit card, or gift card, issued by a service provider as displayed as service provider indicia 702 on the front or back

CA 03239475 2024-5-28

of the contactless card 104. In some examples, the contactless card 104 is not related to a payment card, and may include, without limitation, an identification card. In some examples, the transaction card may include a dual interface contactless payment card, a rewards card, and so forth. The contactless card 104 may include a substrate 704, which may include a single layer or one or more laminated layers composed of plastics, metals, and other materials. Exemplary substrate materials include polyvinyl chloride, polyvinyl chloride acetate, acrylonitrile butadiene styrene, polycarbonate, polyesters, anodized titanium, palladium, gold, carbon, paper, and biodegradable materials. In some examples, the contactless card 104 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7816 standard, and the transaction card may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 104 according to the present disclosure may have different characteristics, and the present disclosure does not require a transaction card to be implemented in a payment card.

[0078] The contactless card 104 may also include identification information 706 displayed on the front and/or back of the card, and a contact pad 708. The contact pad 708 may include one or more pads and be configured to establish contact with another client device, such as an ATM, a user device, smartphone, laptop, desktop, or tablet computer via transaction cards. The contact pad may be designed in accordance with one or more standards, such as ISO/IEC 7816 standard, and enable communication in accordance with the EMV protocol. The contactless card 104 may also include processing circuitry, antenna and other components as will be further discussed in FIG. 7B. These components may be located behind the contact pad 708 or elsewhere on the substrate 704, e.g. within a different layer of the substrate 704, and may electrically and physically coupled with the contact pad 708. The contactless card 104 may also include a magnetic strip or tape, which may be located on the back of the card (not shown in FIG. 7A). The contactless card 104 may also include a Near-Field Communication (NFC) device coupled with an antenna capable of communicating via the NFC protocol. Embodiments are not limited in this manner.

[0079] As illustrated in FIG. 7B, the contact pad 708 of contactless card 104 may include processing circuitry 710 for storing, processing, and communicating information, including a processor 712, a memory 108, and one or more communications interface 124. It is understood that the processing circuitry 710 may contain additional components, including processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware, as necessary to perform the functions described herein.

CA 03239475 2024-5-28

[0080] The memory 108 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the contactless card 104 may include one or more of these memories. A read-only memory may be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write once/read-multiple memory may be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it may not be rewritten, but it may be read many times. A read/write memory may be programmed and re-programed many times after leaving the factory. A read/write memory may also be read many times after leaving the factory. In some instances, the memory 108 may be encrypted memory utilizing an encryption algorithm executed by the processor 712 to encrypted data.

[0081] The memory 108 may be configured to store one or more applet 110, one or more counters 116, a unique ID 112, the master key 114, the UDK 118, diversified key 120, and the PAN sequence 156. The one or more applets 110 may comprise one or more software applications configured to execute on one or more contactless cards 104, such as a Java® Card applet. However, it is understood that applets 110 are not limited to Java Card applets, and instead may be any software application operable on contactless cards or other devices having limited memory. The one or more counters 116 may comprise a numeric counter sufficient to store an integer. The unique ID 112 may comprise a unique alphanumeric identifier assigned to the contactless card 104, and the identifier may distinguish the contactless card 104 from other contactless cards 104. In some examples, the unique ID 112 may identify both a customer and an account assigned to that customer.

[0082] The processor 712 and memory elements of the foregoing exemplary embodiments are described with reference to the contact pad 708, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad 708 or entirely separate from it, or as further elements in addition to processor 712 and memory 108 elements located within the contact pad 708.

[0083] In some examples, the contactless card 104 may comprise one or more antenna(s) 714. The one or more antenna(s) 714 may be placed within the contactless card 104 and around the processing circuitry 710 of the contact pad 708. For example, the one or more antenna(s) 714 may be integral with the processing circuitry 710 and the one or more antenna(s) 714 may be used with an external booster coil. As another example, the one or more antenna(s) 714 may be external to the contact pad 708 and the processing circuitry 710.

CA 03239475 2024-5-28

[0084] In an embodiment, the coil of contactless card 104 may act as the secondary of an air core transformer. The terminal may communicate with the contactless card 104 by cutting power or amplitude modulation. The contactless card 104 may infer the data transmitted from the terminal using the gaps in the power connection of the contactless card 104, which may be functionally maintained through one or more capacitors. The contactless card 104 may communicate back by switching a load on the coil of the contactless card 104 or load modulation. Load modulation may be detected in the terminal's coil through interference. More generally, using the antenna(s) 714, processor 712, and/or the memory 108, the contactless card 104 provides a communications interface to communicate via NFC, Bluetooth, and/or Wi-Fi communications.

[0085] As explained above, contactless card 104 may be built on a software platform operable on smart cards or other devices having limited memory, such as JavaCard, and one or more or more applications or applets may be securely executed. Applet 110 may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applet 110 may be configured to respond to one or more requests, such as near field data exchange requests, from a reader, such as a mobile NFC reader (e.g., of a mobile computing device 102 or point-of-sale terminal), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag. The NDEF message may include a cryptogram such as the cryptogram 122 or cryptogram 208, and any other data.

[0086] One example of an NDEF OTP is an NDEF short-record layout (SR=1). In such an example, one or more applet 110 may be configured to encode the OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may comprise one or more records. The applet 110 may be configured to add one or more static tag records in addition to the OTP record.

[0087] In some examples, the one or more applet 110 may be configured to emulate an RFID tag. The RFID tag may include one or more polymorphic tags. In some examples, each time the tag is read, different cryptographic data is presented that may indicate the authenticity of the contactless card. Based on the one or more applet 110, an NFC read of the tag may be processed, the data may be transmitted to a server, such as a server of a banking system, and the data may be validated at the server.

[0088] In some examples, the contactless card 104 and server may include certain data such that the card may be properly identified. The contactless card 104 may include one or more unique identifiers (not pictured). Each time a read operation takes place, the counter

CA 03239475 2024-5-28

116 may be configured to increment. In some examples, each time data from the contactless card 104 is read (e.g., by a mobile device), the counter 116 is transmitted to the server for validation and determines whether the counter 116 are equal (as part of the validation) to a counter of the server.

[0089] The one or more counter 116 may be configured to prevent a replay attack. For example, if a cryptogram has been obtained and replayed, that cryptogram is immediately rejected if the counter 116 has been read or used or otherwise passed over. If the counter 116 has not been used, it may be replayed. In some examples, the counter that is incremented on the contactless card 104 is different from the counter that is incremented for transactions. The contactless card 104 is unable to determine the application transaction counter 116 since there is no communication between applets 110 on the contactless card 104. In some examples, the contactless card 104 may comprise a first applet 440-1, which may be a transaction applet, and a second applet 440-2. Each applet 440-1 and 440-2 may comprise a respective counter 116.

[0090] In some examples, the counter 116 may get out of sync. In some examples, to account for accidental reads that initiate transactions, such as reading at an angle, the counter 116 may increment but the application does not process the counter 116. In some examples, when the device 102 is woken up, NFC may be enabled and the computing device 102 may be configured to read available tags, but no action is taken responsive to the reads.

[0091] To keep the counter 116 in sync, an application, such as a background application, may be executed that would be configured to detect when the computing device 102 wakes up and synchronize with the server of a banking system indicating that a read that occurred due to detection to then move the counter 116 forward. In other examples, Hashed One Time Password may be utilized such that a window of mis-synchronization may be accepted. For example, if within a threshold of 10, the counter 116 may be configured to move forward. But if within a different threshold number, for example within 10 or 600, a request for performing re-synchronization may be processed which requests via one or more applications that the user tap, gesture, or otherwise indicate one or more times via the user's device. If the counter 116 increases in the appropriate sequence, then it possible to know that the user has done so.

[0092] The key diversification technique described herein with reference to the counter 116, master key 114, UDK 118, and diversified key 120, is one example of encryption and/or decryption a key diversification technique. This example key diversification

CA 03239475 2024-5-28

technique should not be considered limiting of the disclosure, as the disclosure is equally applicable to other types of key diversification techniques.

[0093] During the creation process of the contactless card 104, two cryptographic keys may be assigned uniquely per card. The cryptographic keys may comprise symmetric keys which may be used in both encryption and decryption of data. Triple DES (3DES) algorithm may be used by EMV and it is implemented by hardware in the contactless card 104. By using the key diversification process, one or more keys may be derived from a master key based upon uniquely identifiable information for each entity that requires a key.

[0094] In some examples, to overcome deficiencies of 3DES algorithms, which may be susceptible to vulnerabilities, a session key may be derived (such as a unique key per session) but rather than using the master key, the unique card-derived keys (e.g., the UDKs 118) and the counter may be used as diversification data. For example, each time the contactless card 104 is used in operation, a different key may be used for creating the message authentication code (MAC) and for performing the encryption. This results in a triple layer of cryptography. The session keys may be generated by the one or more applets and derived by using the application transaction counter with one or more algorithms (as defined in EMV 4.3 Book 2 A1.3.1 Common Session Key Derivation).

[0095] Further, the increment for each card may be unique, and assigned either by personalization, or algorithmically assigned by some identifying information. For example, odd numbered cards may increment by 2 and even numbered cards may increment by 5. In some examples, the increment may also vary in sequential reads, such that one card may increment in sequence by 1, 3, 5, 2, 2, ... repeating. The specific sequence or algorithmic sequence may be defined at personalization time, or from one or more processes derived from unique identifiers. This can make it harder for a replay attacker to generalize from a small number of card instances.

[0096] The authentication message may be delivered as the content of a text NDEF record in hexadecimal ASCII format. In another example, the NDEF record may be encoded in hexadecimal format.

[0097] FIG. 8 illustrates an NDEF short-record layout (SR=1) data structure 800 according to an example embodiment. One or more applets 110 may be configured to encode an OTP as an NDEF type 4 well known type text tag. In some examples, NDEF messages may comprise one or more records. The applets may be configured to add one or more static tag records in addition to the OTP record. Exemplary tags include, without limitation, Tag type: well known type, text, encoding English (en); Applet ID: D2760000850101; Capabilities:

CA 03239475 2024-5-28

read-only access; Encoding: the authentication message may be encoded as ASCII hex; type-length-value (TLV) data may be provided as a personalization parameter that may be used to generate the NDEF message. In an embodiment, the authentication template may comprise the first record, with a well-known index for providing the actual dynamic authentication data. The data structure 800 may include a cryptogram such as cryptogram 122 or cryptogram 208, and any other data provided by the applet 110.

[0098] FIG. 9 depicts a schematic of an exemplary system 900, consistent with disclosed embodiments. The system 900 may comprise systems with access to blockchain 906 over network 902.

[0099] The system 900 can generate a non-reputable record of interactions using the blockchain 906. Furthermore, the blockchain 906 can be distributed across a plurality of computing systems, encouraging trust in the validity of the records stored in the blockchain 906. In this manner, the disclosed systems provide an innovative technical solution to at least the above-mentioned technical problems with conventional systems.

[0100] User system(s) 904 may include the computing device 102. User system(s) 904 may be configured to process transactions using the digital wallet 144, consistent with disclosed embodiments. User system 904 may comprise a computing device, such as a server, workstation, desktop, or mobile device (e.g., laptop, tablet, phablet, smartphone, smartwatch, or similar mobile computing device). As described below with respect to Figure 12, user system 904 may be configured with a display and input/output interfaces. User system 904 may be configured to interact with a user (not shown) using the display and input/output interfaces.

[0101] Member system 908 may be configured to process transactions, consistent with disclosed embodiments. Member system 908 may include one or more computing devices, such as servers, workstations, desktop computers, or special-purpose computing devices. Member system 908 may be standalone, or it may be part of a subsystem, which may be part of a larger system. For example, member system 908 may be associated with a commercial institution. Member system 908 may include distributed servers that are remotely located and communicate with other systems of the financial institution over a public network, or over a dedicated private network.

[0102] Member system 908 may be configured to receive a request to process a transaction using cryptocurrency of a digital wallet 144. In some embodiments, member system 908 may be configured to receive the request from another element of the system 900, such as

CA 03239475 2024-5-28

another member system 908 and/or a user system 904. Member system 908 may be configured to interact with blockchain 906 to process the transaction request.

[0103] Member system 908 may be configured to store messages in blockchain 906, consistent with disclosed embodiments. In some aspects, member system 908 may be configured to add blocks containing the messages to blockchain 906. In various aspects, member system 908 may be configured to provide the messages to an authorized system. The authorized system may be configured to add blocks containing the messages to blockchain 906. As described below with regards to FIG. 10, the messages may comprise transaction records.

[0104] Blockchain 906 may comprise a distributed data structure, consistent with disclosed embodiments. Blockchain 906 may be a private blockchain. For example, authorized systems may store copies of blockchain 906. These authorized systems may be configured to add blocks to blockchain 906 and publish the blocks to other authorized systems. Authorized systems may be configured to receive messages from other systems for publication in blockchain 906. These other systems may have read-only access to blockchain 906. In some embodiments, one or more member systems 908 are authorized systems. In some embodiments, one or more user systems 904 are authorized systems. As described in detail with respect to Figure 9, blockchain 906 may be configured to store messages from member systems, the messages including transactions.

[0105] Network 902 may be configured to provide communications between components of FIG. 9. For example, network 902 may be any type of network (including infrastructure) that provides communications, exchanges information, and/or facilitates the exchange of information, such as the Internet, a Local Area Network, or other suitable connection(s) that enables authentication system 900 to send and receive information between the components of authentication system 900.

[0106] FIG. 10 depicts a logical model 1000 of an exemplary blockchain 906, consistent with disclosed embodiments. Blockchain 906 may comprise many such blockchains maintained by many different systems (e.g., member systems 908, or other systems). Such exemplary blockchains may comprise blocks, such as block 1006a through block 1006d. Blocks may include messages, such as message 1008a through message 1008d. Generally, blocks may include a header, such as headers 1002a through 1002d, which uniquely identifies each block. The headers 1002a through 1002d may include a hash value generated by a hash function. A hash function is any function that can be used to map input data of arbitrary size to a hash value of a fixed size. For example, a header may include at

CA 03239475 2024-5-28

least one of the previous block's hash value, a hash value generated based on any messages in the block (e.g., a Merkle root), and a timestamp. Consistent with disclosed embodiments, system 900 may require that blocks added to blockchain 906 satisfy at least one of a proof-of-work condition and a digital signature condition. For example, the headers 1002a through 1002d may include a nonce chosen to ensure the header satisfies the proof-of-work condition 1004a through 1004d. As a non-limiting example, the proof-of-work condition 1004a through 1004d may require the hash of the header fall within a predetermined range of values. As an additional example, the header may be digitally signed with a cryptographic key (e.g., a private key 146) of an authorized system, and the digital signature may be included in the header. This digital signature may be verified using a key available to the members of system 900.

[0107] FIG. 11 depicts a logical model 1100 of a message 1008b stored in a blockchain (e.g., an element of blockchain 906), consistent with disclosed embodiments. In some embodiments, message 1008b may comprise index information 1102. In certain aspects, index information 1102 may comprise information identifying a user. For example, index information 1102 may be at least one of a full name, email address, phone number, or other non-sensitive personal information of the user. In various aspects, index information 1102 may include one or more references to earlier blocks in the private blockchain. For example, index information 1102 may include one or more references to one or more earlier blocks associated with the same user. A reference may include, as a non-limiting example, a hash of a preceding block in the blockchain associated with the same user. In some aspects, index information 1102 may be obfuscated or encrypted according to methods known to one of skill in the art. For example, index information 1102 may be encrypted with a cryptographic key, such as the private key 146. As an additional example, index information 1102 may comprise a hash of the at least one of a full name, email address, phone number, or other non-sensitive personal information of the user.

[0108] Message 1008b may comprise additional information 1104, consistent with disclosed embodiments. The additional information 1104 may include transaction details, e.g., an amount of cryptocurrency being transferred from one digital wallet 144 to another digital wallet 144. In various aspects, additional information 1104 may be obfuscated or encrypted according to methods known to one of skill in the art. For example, root system information 1104 may be encrypted with a cryptographic key such as the private key 146.

[0109] Message 1008b may comprise authentication record 1106, consistent with disclosed embodiments. In some aspects, authentication record 1106 may comprise information

CA 03239475 2024-5-28

enabling subsequent auditing of transactions. For example, authentication record 1106 may identify at least one of member system 908, a commercial institution associated with member system 908, a purpose of the authentication record 1106 (e.g., transaction details). In some aspects, authentication record 1106 may be obfuscated or encrypted according to methods known to one of skill in the art. For example, authentication record 1106 may be encrypted with a cryptographic key, such as the private key 146.

[0110] Cryptographic keys such as the private keys 146 may be used to encrypt elements of messages in blocks, consistent with disclosed embodiments. In some aspects, such cryptographic keys may be associated with members of authentication system 900 (e.g., member system 908). In various aspects, at least some of the cryptographic keys may be associated with authorized systems. Corresponding cryptographic keys such as the public keys 148 may be available to decrypt the encrypted message elements, consistent with disclosed embodiments. For example, when an element of a message in a block is encrypted with a symmetric key, the same symmetric key may be available for decrypting the encrypted element. As another example, when an element of a message in a block is encrypted with a private key 146, a corresponding public key 148 may be available for decrypting the encrypted element. In some aspects, the corresponding cryptographic keys may be available to members of authentication system (e.g., member systems 908).

[0111] FIG. 12 illustrates an embodiment of an exemplary computer architecture 1200 suitable for implementing various embodiments as previously described. In one embodiment, the computer architecture 1200 may include or be implemented as part of computing architecture 100.

[0112] As used in this application, the terms "system" and "component" are intended to refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution, examples of which are provided by the exemplary computing computer architecture 1200. For example, a component can be, but is not limited to being, a process running on a processor, a processor, a hard disk drive, multiple storage drives (of optical and/or magnetic storage medium), an object, an executable, a thread of execution, a program, and/or a computer. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers. Further, components may be communicatively coupled to each other by various types of communications media to coordinate operations. The coordination may involve the uni-directional or bi-directional

CA 03239475 2024-5-28

exchange of information. For instance, the components may communicate information in the form of signals communicated over the communications media. The information can be implemented as signals allocated to various signal lines. In such allocations, each message is a signal. Further embodiments, however, may alternatively employ data messages. Such data messages may be sent across various connections. Exemplary connections include parallel interfaces, serial interfaces, and bus interfaces.

[0113] The computer architecture 1200 includes various common computing elements, such as one or more processors, multi-core processors, co-processors, memory units, chipsets, controllers, peripherals, interfaces, oscillators, timing devices, video cards, audio cards, multimedia input/output (I/O) components, power supplies, and so forth. The embodiments, however, are not limited to implementation by the computing computer architecture 1200.

[0114] As shown in FIG. 12, the computer architecture 1200 includes a computer 1212 comprising a processor 1202, a system memory 1204 and a system bus 1206. The processor 1202 can be any of various commercially available processors. The computer 1212 may be representative of the computing device 102 and/or the server 106.

[0115] The system bus 1206 provides an interface for system components including, but not limited to, the system memory 1204 to the processor 1202. The system bus 1206 can be any of several types of bus structure that may further interconnect to a memory bus (with or without a memory controller), a peripheral bus, and a local bus using any of a variety of commercially available bus architectures. Interface adapters may connect to the system bus 1206 via slot architecture. Example slot architectures may include without limitation Accelerated Graphics Port (AGP), Card Bus, (Extended) Industry Standard Architecture ((E)ISA), Micro Channel Architecture (MCA), NuBus, Peripheral Component Interconnect (Extended) (PCI(X)), PCI Express, Personal Computer Memory Card International Association (PCMCIA), and the like.

[0116] The computer architecture 1200 may include or implement various articles of manufacture. An article of manufacture may include a computer-readable storage medium to store logic. Examples of a computer-readable storage medium may include any tangible media capable of storing electronic data, including volatile memory or non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and so forth. Examples of logic may include executable computer program instructions implemented using any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, object-

CA 03239475 2024-5-28

oriented code, visual code, and the like. Embodiments may also be at least partly implemented as instructions contained in or on a non-transitory computer-readable medium, which may be read and executed by one or more processors to enable performance of the operations described herein.

[0117] The system memory 1204 may include various types of computer-readable storage media in the form of one or more higher speed memory units, such as read-only memory (ROM), random-access memory (RAM), dynamic RAM (DRAM), Double-Data-Rate DRAM (DDRAM), synchronous DRAM (SDRAM), static RAM (SRAM), programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), flash memory, polymer memory such as ferroelectric polymer memory, ovonic memory, phase change or ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, magnetic or optical cards, an array of devices such as Redundant Array of Independent Disks (RAID) drives, solid state memory devices (e.g., USB memory, solid state drives (SSD) and any other type of storage media suitable for storing information. In the illustrated embodiment shown in FIG. 12, the system memory 1204 can include non-volatile 1208 and/or volatile 1210. A basic input/output system (BIOS) can be stored in the non-volatile 1208.

[0118] The computer 1212 may include various types of computer-readable storage media in the form of one or more lower speed memory units, including an internal (or external) hard disk drive 1214, a magnetic disk drive 1216 to read from or write to a removable magnetic disk 1218, and an optical disk drive 1220 to read from or write to a removable optical disk 1222 (e.g., a CD-ROM or DVD). The hard disk drive 1214, magnetic disk drive 1216 and optical disk drive 1220 can be connected to the system bus 1206 by an HDD interface 1224, and FDD interface 1226 and an optical disk drive interface 1228, respectively. The HDD interface 1224 for external drive implementations can include at least one or both of Universal Serial Bus (USB) and IEEE 1394 interface technologies.

[0119] The drives and associated computer-readable media provide volatile and/or nonvolatile storage of data, data structures, computer-executable instructions, and so forth. For example, a number of program modules can be stored in the drives and non-volatile 1208, and volatile 1210, including an operating system 1230, one or more applications 1232, other program modules 1234, and program data 1236. In one embodiment, the one or more applications 1232, other program modules 1234, and program data 1236 can include, for example, the various applications and/or components of the system 100.

CA 03239475 2024-5-28

[0120] A user can enter commands and information into the computer 1212 through one or more wire/wireless input devices, for example, a keyboard 1238 and a pointing device, such as a mouse 1240. Other input devices may include microphones, infra-red (IR) remote controls, radio-frequency (RF) remote controls, game pads, stylus pens, card readers, dongles, finger print readers, gloves, graphics tablets, joysticks, keyboards, retina readers, touch screens (e.g., capacitive, resistive, etc.), trackballs, track pads, sensors, styluses, and the like. These and other input devices are often connected to the processor 1202 through an input device interface 1242 that is coupled to the system bus 1206 but can be connected by other interfaces such as a parallel port, IEEE 1394 serial port, a game port, a USB port, an IR interface, and so forth.

[0121] A monitor 1244 or other type of display device is also connected to the system bus 1206 via an interface, such as a video adapter 1246. The monitor 1244 may be internal or external to the computer 1212. In addition to the monitor 1244, a computer typically includes other peripheral output devices, such as speakers, printers, and so forth.

[0122] The computer 1212 may operate in a networked environment using logical connections via wire and/or wireless communications to one or more remote computers, such as a remote computer(s) 1248. The remote computer(s) 1248 can be a workstation, a server computer, a router, a personal computer, portable computer, microprocessor-based entertainment appliance, a peer device or other common network node, and typically includes many or all the elements described relative to the computer 1212, although, for purposes of brevity, only a memory and/or storage device 1250 is illustrated. The logical connections depicted include wire/wireless connectivity to a local area network 1252 and/or larger networks, for example, a wide area network 1254. Such LAN and WAN networking environments are commonplace in offices and companies, and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network, for example, the Internet.

[0123] When used in a local area network 1252 networking environment, the computer 1212 is connected to the local area network 1252 through a wire and/or wireless communication network interface or network adapter 1256. The network adapter 1256 can facilitate wire and/or wireless communications to the local area network 1252, which may also include a wireless access point disposed thereon for communicating with the wireless functionality of the network adapter 1256.

[0124] When used in a wide area network 1254 networking environment, the computer 1212 can include a modem 1258, or is connected to a communications server on the wide

CA 03239475 2024-5-28

area network 1254 or has other means for establishing communications over the wide area network 1254, such as by way of the Internet. The modem 1258, which can be internal or external and a wire and/or wireless device, connects to the system bus 1206 via the input device interface 1242. In a networked environment, program modules depicted relative to the computer 1212, or portions thereof, can be stored in the remote memory and/or storage device 1250. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

[0125] The computer 1212 is operable to communicate with wire and wireless devices or entities using the IEEE 802 family of standards, such as wireless devices operatively disposed in wireless communication (e.g., IEEE 802.11 over-the-air modulation techniques). This includes at least Wi-Fi (or Wireless Fidelity), WiMax, and Bluetooth™ wireless technologies, among others. Thus, the communication can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices. Wi-Fi networks use radio technologies called IEEE 802.11 (a, b, g, n, ac, ax, etc.) to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wire networks (which use IEEE 802.3-related media and functions).

[0126] The various elements of the devices as previously described with reference to FIGS. 1A-12 may include various hardware elements, software elements, or a combination of both. Examples of hardware elements may include devices, logic devices, components, processors, microprocessors, circuits, processors, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), memory units, logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software elements may include software components, programs, applications, computer programs, application programs, system programs, software development programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. However, determining whether an embodiment is implemented using hardware elements and/or software elements may vary in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates,

CA 03239475 2024-5-28

memory resources, data bus speeds and other design or performance constraints, as desired for a given implementation.

[0127] One or more aspects of at least one embodiment may be implemented by representative instructions stored on a machine-readable medium which represents various logic within the processor, which when read by a machine causes the machine to fabricate logic to perform the techniques described herein. Such representations, known as "IP cores" may be stored on a tangible, machine readable medium and supplied to various customers or manufacturing facilities to load into the fabrication machines that make the logic or processor. Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with the embodiments. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and/or software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), optical disk, magnetic media, magneto-optical media, removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, encrypted code, and the like, implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

[0128] The components and features of the devices described above may be implemented using any combination of discrete circuitry, application specific integrated circuits (ASICs), logic gates and/or single chip architectures. Further, the features of the devices may be implemented using microcontrollers, programmable logic arrays and/or microprocessors or any combination of the foregoing where suitably appropriate. It is noted that hardware, firmware and/or software elements may be collectively or individually referred to herein as "logic" or "circuit."

CA 03239475 2024-5-28

[0129] It will be appreciated that the exemplary devices shown in the block diagrams described above may represent one functionally descriptive example of many potential implementations. Accordingly, division, omission or inclusion of block functions depicted in the accompanying figures does not infer that the hardware components, circuits, software and/or elements for implementing these functions would be necessarily be divided, omitted, or included in embodiments.

[0130] At least one computer-readable storage medium may include instructions that, when executed, cause a system to perform any of the computer-implemented methods described herein.

[0131] Some embodiments may be described using the expression "one embodiment" or "an embodiment" along with their derivatives. These terms mean that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment. Moreover, unless otherwise noted the features described above are recognized to be usable together in any combination. Thus, any features discussed separately may be employed in combination with each other unless it is noted that the features are incompatible with each other.

[0132] It is emphasized that the Abstract of the Disclosure is provided to allow a reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in a single embodiment for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein," respectively. Moreover, the terms "first," "second," "third," and so forth, are used merely as labels, and are not intended to impose numerical requirements on their objects.

[0133] What has been described above includes examples of the disclosed architecture. It is, of course, not possible to describe every conceivable combination of components and/or

CA 03239475 2024-5-28

methodologies, but one of ordinary skill in the art may recognize that many further combinations and permutations are possible. Accordingly, the novel architecture is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims.

[0134] The foregoing description of example embodiments has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. It is intended that the scope of the present disclosure be limited not by this detailed description, but rather by the claims appended hereto. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner, and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.

CA 03239475 2024-5-28

CLAIMS

What is claimed is:

1. A method, comprising:

receiving, by a server from an application, a request to recover a private key for a digital wallet, the request comprising a first cryptogram generated by a contactless card;

decrypting, by the server, the first cryptogram based on a key for the contactless card;

determining, by the server based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet;

generating, by the server based on the unique identifier and the diversification factor, the private key; and

transmitting, by the server to the application via a network, the private key.

2. The method of claim 1, wherein the diversification factor comprises an application primary account number (PAN) sequence number of the contactless card.

3. The method of claim 1, wherein the diversification factor comprises an application transaction counter (ATC) of the contactless card.

4. The method of claim 1, further comprising prior to receiving the request:

receiving, by the server from the application, a second cryptogram generated by the contactless card;

decrypting, by the server, the second cryptogram;

generating the private key by the server based on the decryption of the second cryptogram;

generating, by the server, a public key based on the private key and a wallet address for the digital wallet based on the public key; and

transmitting, by the server to the application, the private key, the public key, and the wallet address.

5. The method of claim 4, wherein the unique identifier of the contactless card and the diversification factor are determined based on the wallet address of the digital wallet.

6. The method of claim 5, further comprising generating the wallet address of the digital wallet based on the decryption of the first cryptogram.

7. The method of claim 1, wherein the server further determines a salt value associated with the digital wallet, wherein the server further generates the private key based on the salt value, the method further comprising:

accessing, by the application based on the private key, the digital wallet.

CA 03239475 2024-5-28

8. A non-transitory computer-readable storage medium, the computer-readable storage medium including instructions that when executed by a processor, cause the processor to:

receive, from an application, a request to recover a private key for a digital wallet, the request comprising a first cryptogram generated by a contactless card;

decrypt the first cryptogram based on a key for the contactless card;

determine, based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet;

generate, based on the unique identifier and the diversification factor, the private key; and

transmit the private key to the application via a network.

9. The computer-readable storage medium of claim 8, wherein the diversification factor comprises an application primary account number (PAN) sequence number of the contactless card.

10. The computer-readable storage medium of claim 8, wherein the diversification factor comprises an application transaction counter (ATC) of the contactless card.

11. The computer-readable storage medium of claim 8, wherein the instructions further cause the processor to, prior to receiving the request:

receive, from the application, a second cryptogram generated by the contactless card;

decrypt the second cryptogram;

generate the private key based on the decryption of the second cryptogram;

generate a public key based on the private key and a wallet address for the digital wallet based on the public key; and

transmit, to the application, the private key, the public key, and the wallet address.

12. The computer-readable storage medium of claim 11, wherein the unique identifier of the contactless card and the diversification factor are determined based on the wallet address of the digital wallet.

13. The computer-readable storage medium of claim 12, wherein the instructions further configure the computer to generate the wallet address of the digital wallet based on the decryption of the first cryptogram.

14. The computer-readable storage medium of claim 8, wherein the processor further determines a salt value associated with the digital wallet, wherein the processor further generates the private key based on the salt value.

15. A computing apparatus comprising:

a processor; and

CA 03239475 2024-5-28

a memory storing instructions that, when executed by the processor, cause the processor to:

receive, from an application, a request to recover a private key for a digital wallet, the request comprising a first cryptogram generated by a contactless card;

decrypt the first cryptogram based on a key for the contactless card;

determine, based on the decryption, a unique identifier of the contactless card and a diversification factor associated with the digital wallet;

generate, based on the unique identifier and the diversification factor, the private key; and

transmit the private key to the application via a network.

16. The computing apparatus of claim 15, wherein the diversification factor comprises an application primary account number (PAN) sequence number of the contactless card.

17. The computing apparatus of claim 15, wherein the diversification factor comprises an application transaction counter (ATC) of the contactless card.

18. The computing apparatus of claim 15, wherein the instructions further configure the apparatus to prior to receiving the request:

receive, from the application, a second cryptogram generated by the contactless card;

decrypt the second cryptogram;

generate the private key based on the decryption of the second cryptogram;

generate a public key based on the private key and a wallet address for the digital wallet based on the public key; and

transmit, to the application, the private key, the public key, and the wallet address.

19. The computing apparatus of claim 18, wherein the unique identifier of the contactless card and the diversification factor are determined based on the wallet address of the digital wallet, wherein the instructions further configure the processor to generate the wallet address of the digital wallet based on the decryption of the first cryptogram.

20. The computing apparatus of claim 15, wherein the processor further determines a salt value associated with the digital wallet, wherein the processor further generates the private key based on the salt value.

CA 03239475 2024-5-28

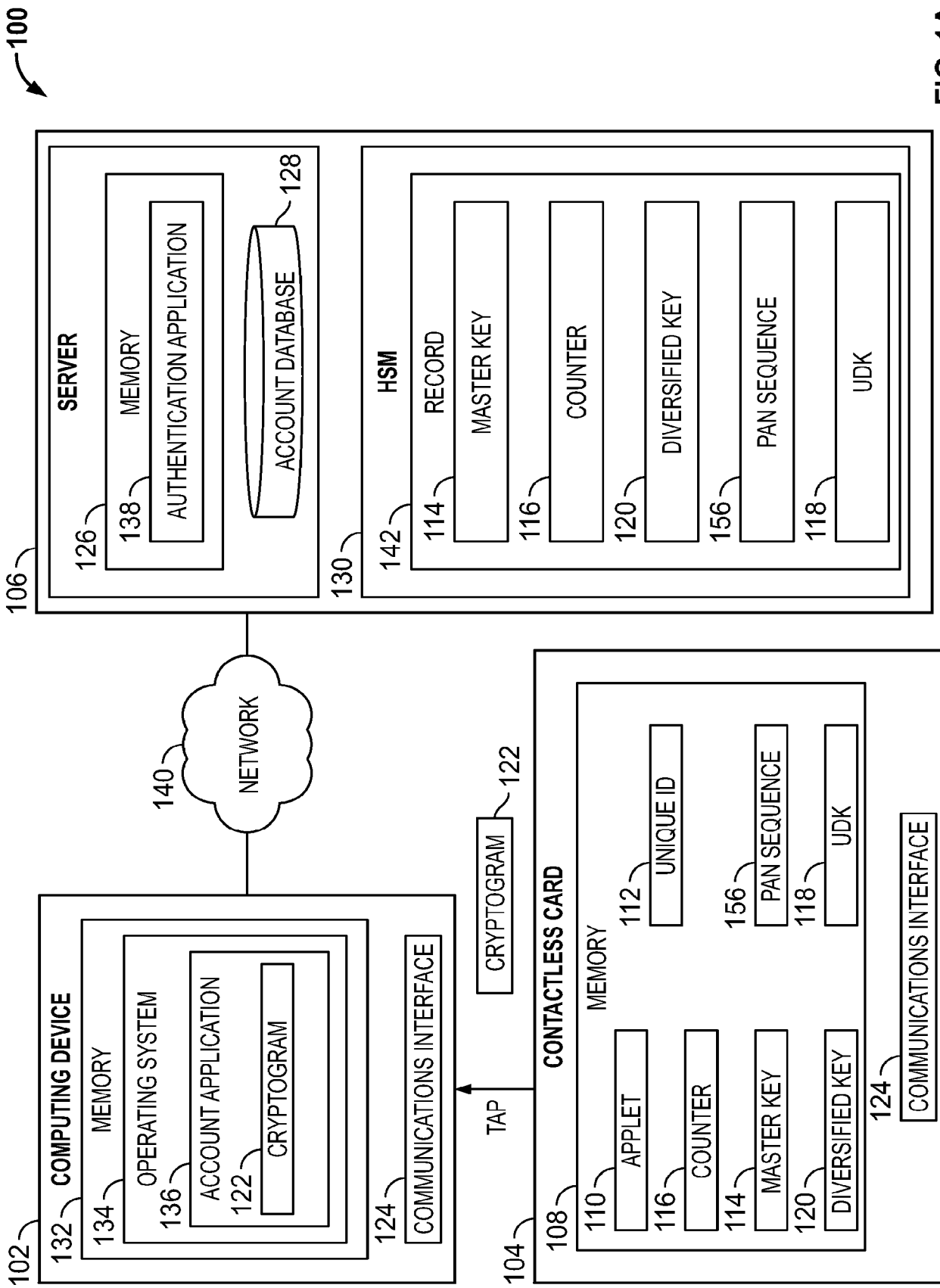

100
SERVER
106
126
MEMORY
138
AUTHENTICATION APPLICATION
128
ACCOUNT DATABASE
HSM
130
142
RECORD
114
MASTER KEY
116
COUNTER
120
DIVERSIFIED KEY
156
PAN SEQUENCE
118
UDK
140
NETWORK
122
CRYPTOGRAM
102
COMPUTING DEVICE
132
MEMORY
134
OPERATING SYSTEM
136
ACCOUNT APPLICATION
122
CRYPTOGRAM
124
COMMUNICATIONS INTERFACE
TAP
104
CONTACTLESS CARD
108
MEMORY
110
APPLET
116
COUNTER
114
MASTER KEY
120
DIVERSIFIED KEY
112
UNIQUE ID
156
PAN SEQUENCE
118
UDK
124
COMMUNICATIONS INTERFACE

FIG. 1A

FIG. 1B

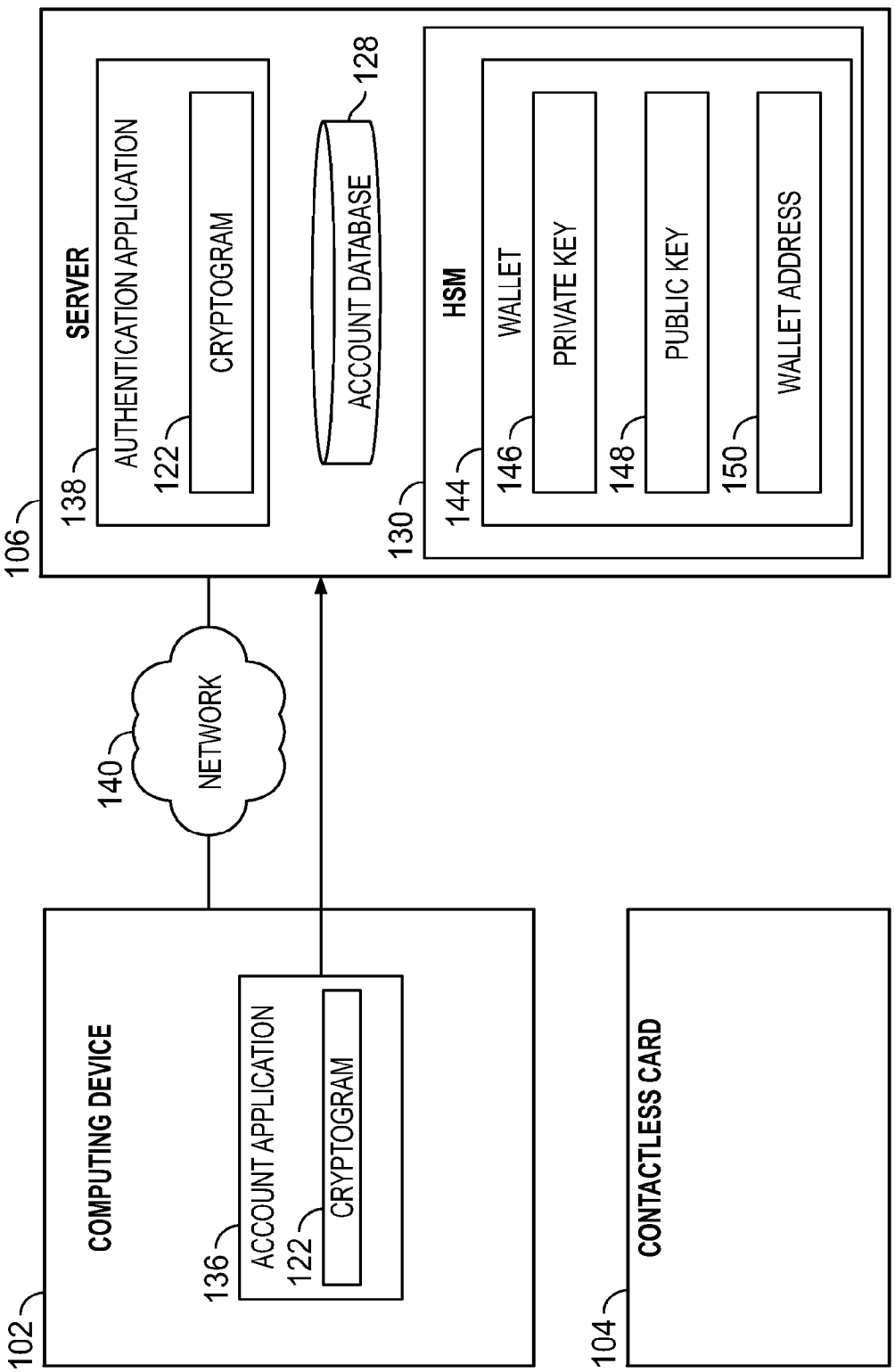
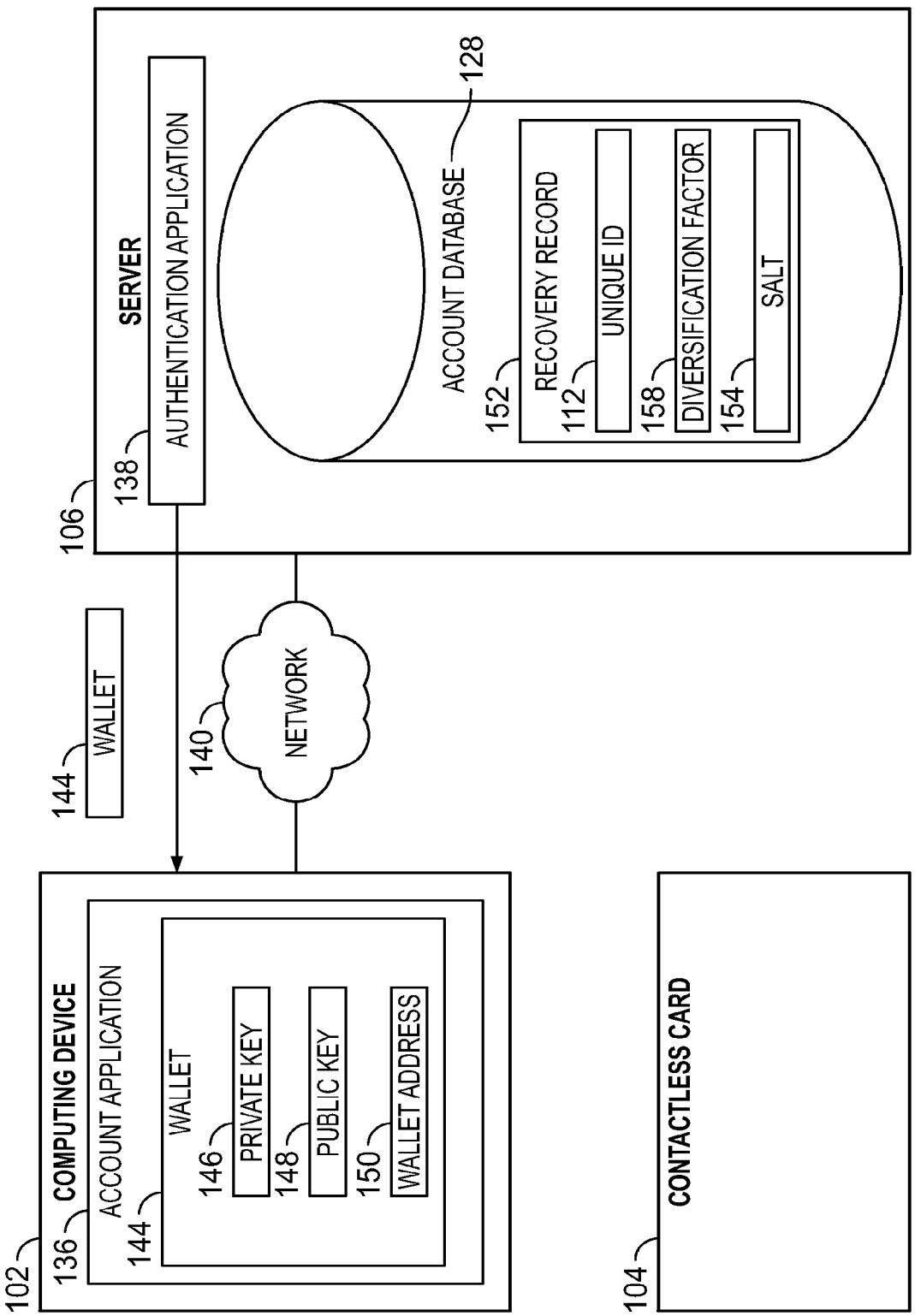

106
SERVER
138
AUTHENTICATION APPLICATION
122
CRYPTOGRAM
128
ACCOUNT DATABASE
130
HSM
144
WALLET
146
PRIVATE KEY
148
PUBLIC KEY
150
WALLET ADDRESS
140
NETWORK
102
COMPUTING DEVICE
136
ACCOUNT APPLICATION
122
CRYPTOGRAM
104
CONTACTLESS CARD

FIG. 1C


106
SERVER
138
AUTHENTICATION APPLICATION
128
ACCOUNT DATABASE
152
RECOVERY RECORD
112
UNIQUE ID
158
DIVERSIFICATION FACTOR
154
SALT
144
WALLET
140
NETWORK
102
136
COMPUTING DEVICE
ACCOUNT APPLICATION
144
WALLET
146
PRIVATE KEY
148
PUBLIC KEY
150
WALLET ADDRESS
104
CONTACTLESS CARD

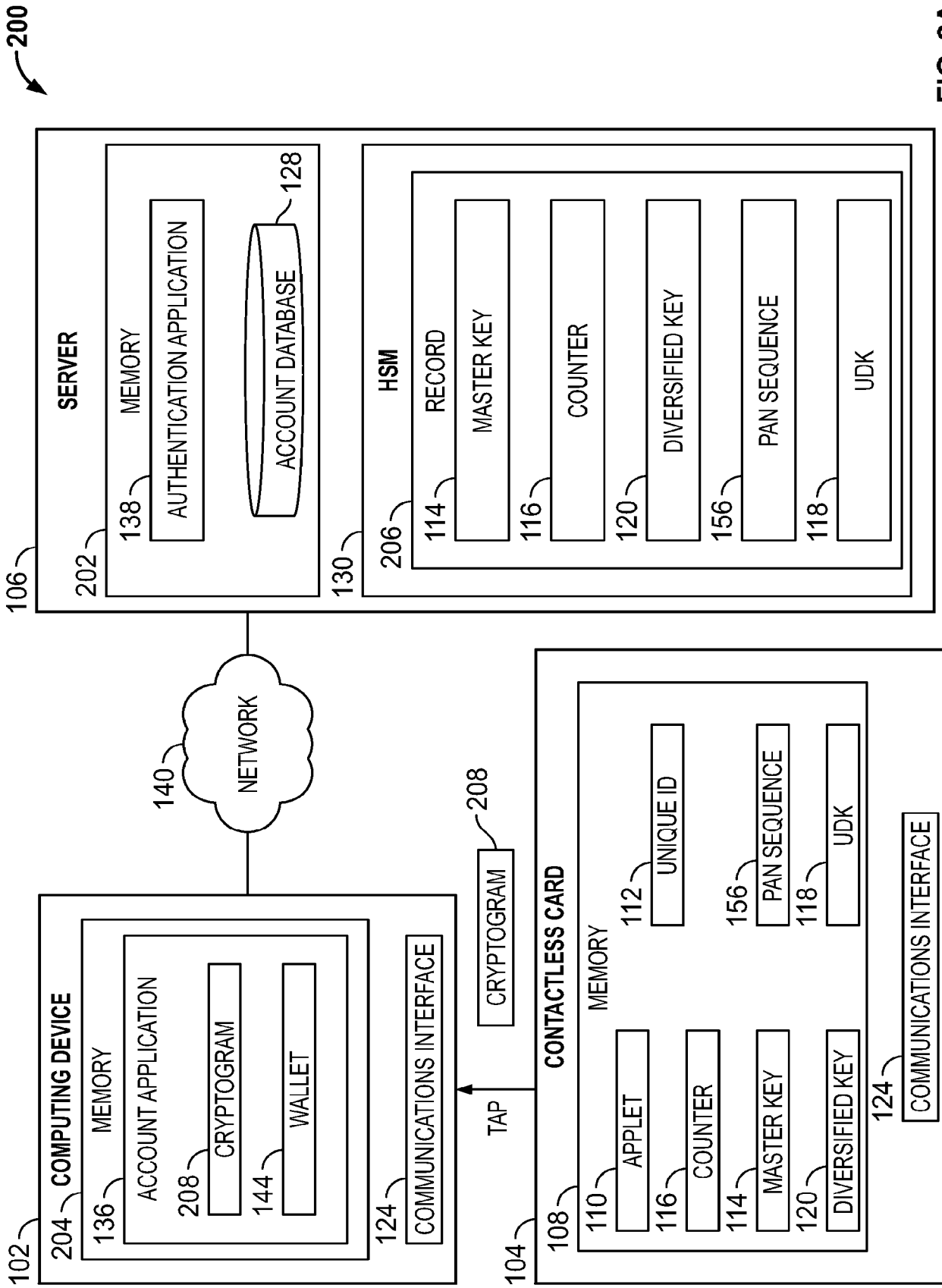

200
SERVER
106
MEMORY
202
AUTHENTICATION APPLICATION
138
ACCOUNT DATABASE
128
HSM
130
RECORD
206
MASTER KEY
114
COUNTER
116
DIVERSIFIED KEY
120
PAN SEQUENCE
156
UDK
118
NETWORK
140
COMPUTING DEVICE
102
MEMORY
204
ACCOUNT APPLICATION
136
CRYPTOGRAM
208
WALLET
144
COMMUNICATIONS INTERFACE
124
CRYPTOGRAM
208
TAP
CONTACTLESS CARD
104
MEMORY
108
APPLET
110
COUNTER
116
MASTER KEY
114
DIVERSIFIED KEY
120
UNIQUE ID
112
PAN SEQUENCE
156
UDK
118
COMMUNICATIONS INTERFACE
124

FIG. 2A

FIG. 2B

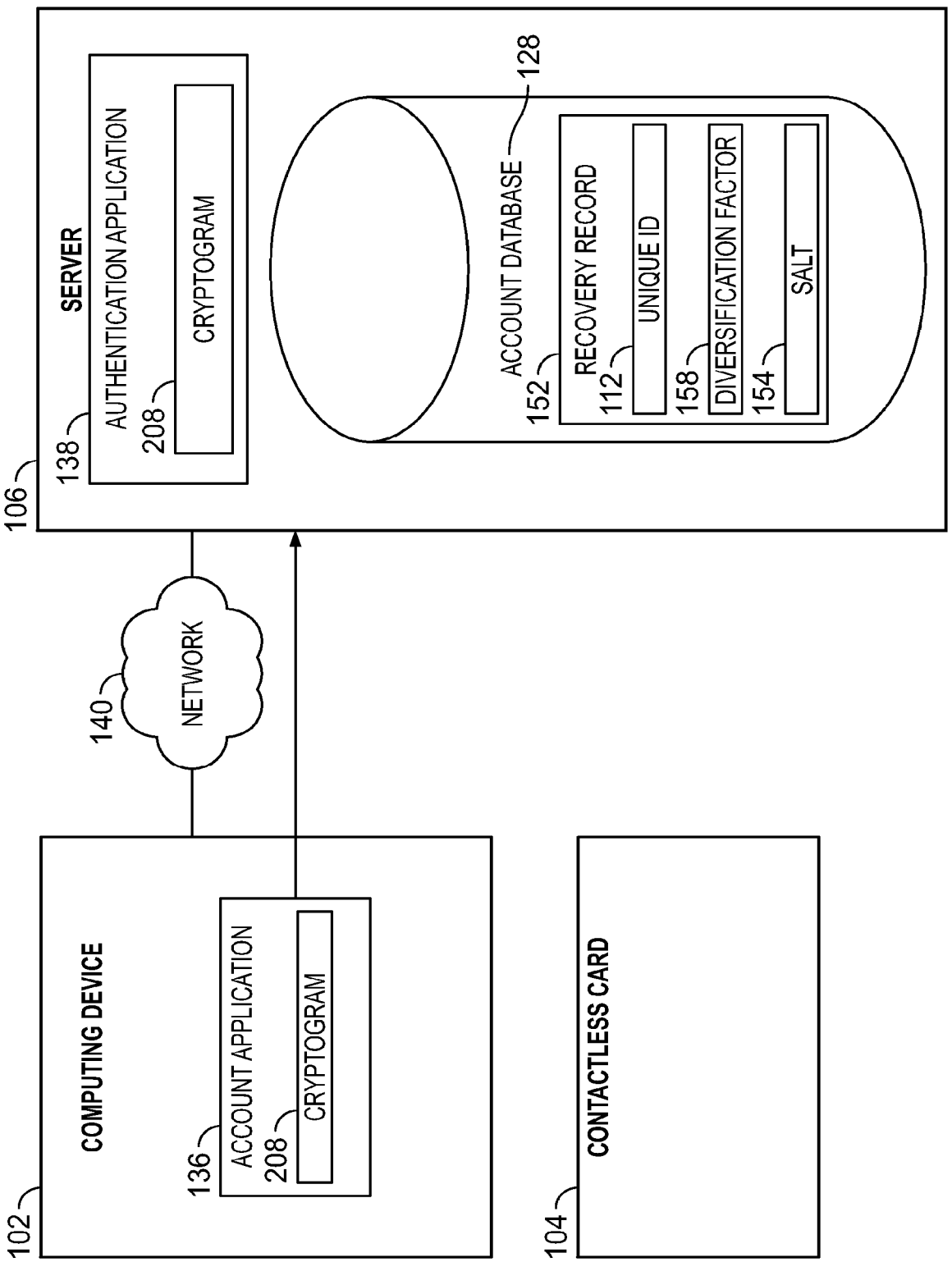
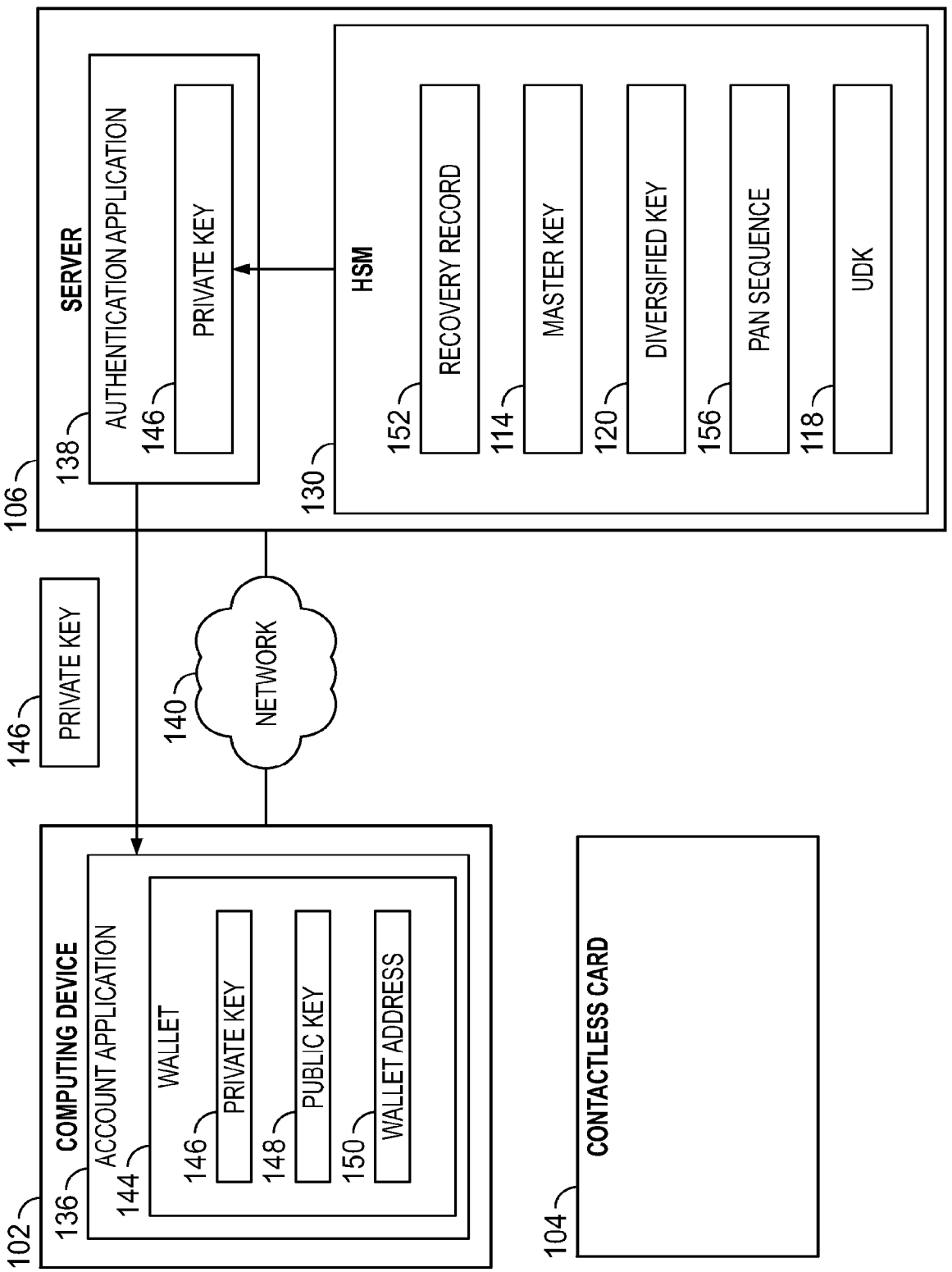

106
SERVER
138
AUTHENTICATION APPLICATION
208
CRYPTOGRAM
128
ACCOUNT DATABASE
152
RECOVERY RECORD
112
UNIQUE ID
158
DIVERSIFICATION FACTOR
154
SALT
140
NETWORK
102
COMPUTING DEVICE
136
ACCOUNT APPLICATION
208
CRYPTOGRAM
104
CONTACTLESS CARD

FIG. 2C


106
SERVER
138
AUTHENTICATION APPLICATION
146
PRIVATE KEY
130
HSM
152
RECOVERY RECORD
114
MASTER KEY
120
DIVERSIFIED KEY
156
PAN SEQUENCE
118
UDK
146
PRIVATE KEY
140
NETWORK
102
COMPUTING DEVICE
136
ACCOUNT APPLICATION
144
WALLET
146
PRIVATE KEY
148
PUBLIC KEY
150
WALLET ADDRESS
104
CONTACTLESS CARD

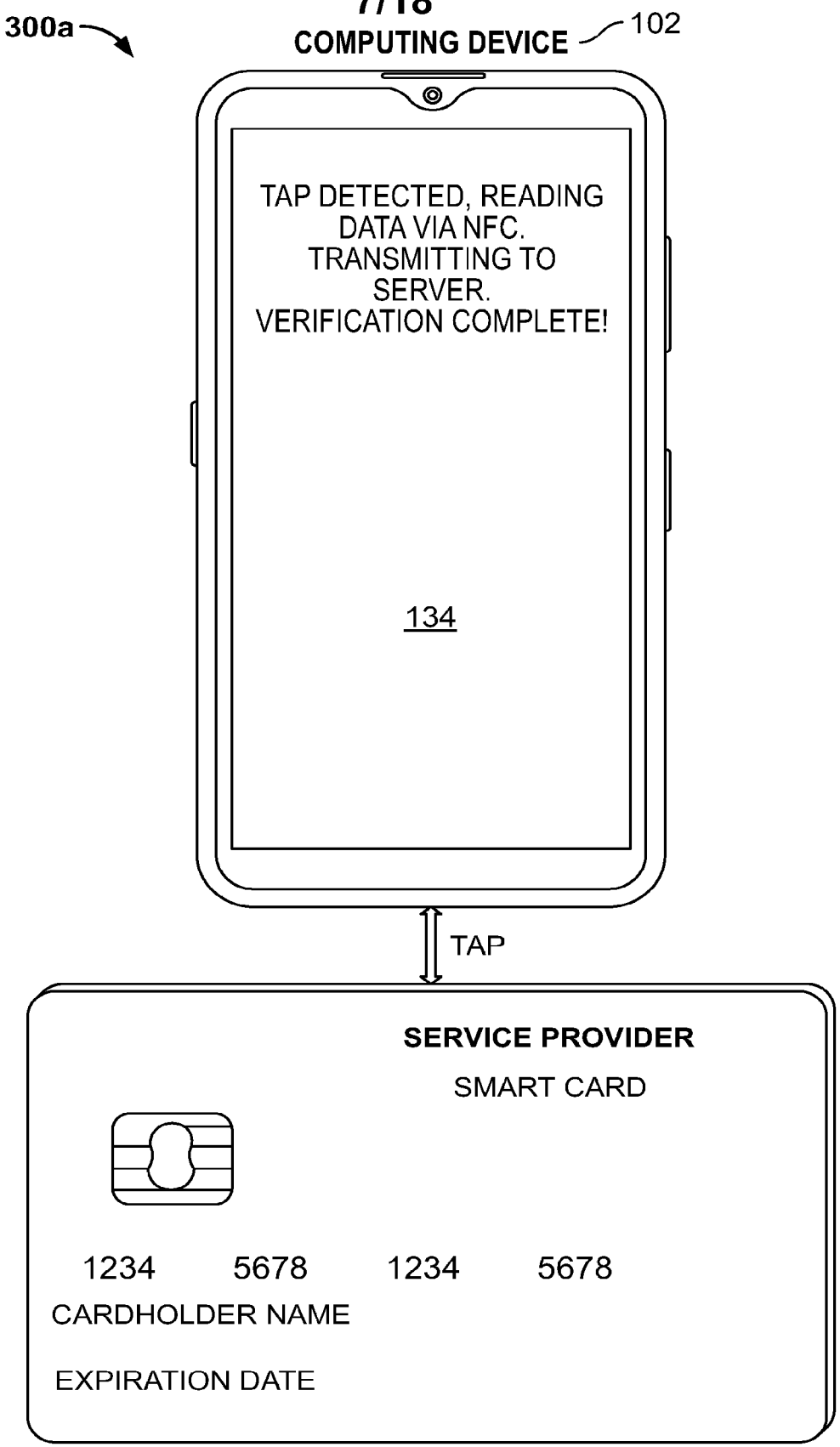

300a
COMPUTING DEVICE
102
TAP DETECTED, READING DATA VIA NFC. TRANSMITTING TO SERVER. VERIFICATION COMPLETE!
134
TAP
SERVICE PROVIDER
SMART CARD
1234 5678 1234 5678
CARDHOLDER NAME
EXPIRATION DATE
CONTACTLESS CARD
104

FIG. 3A

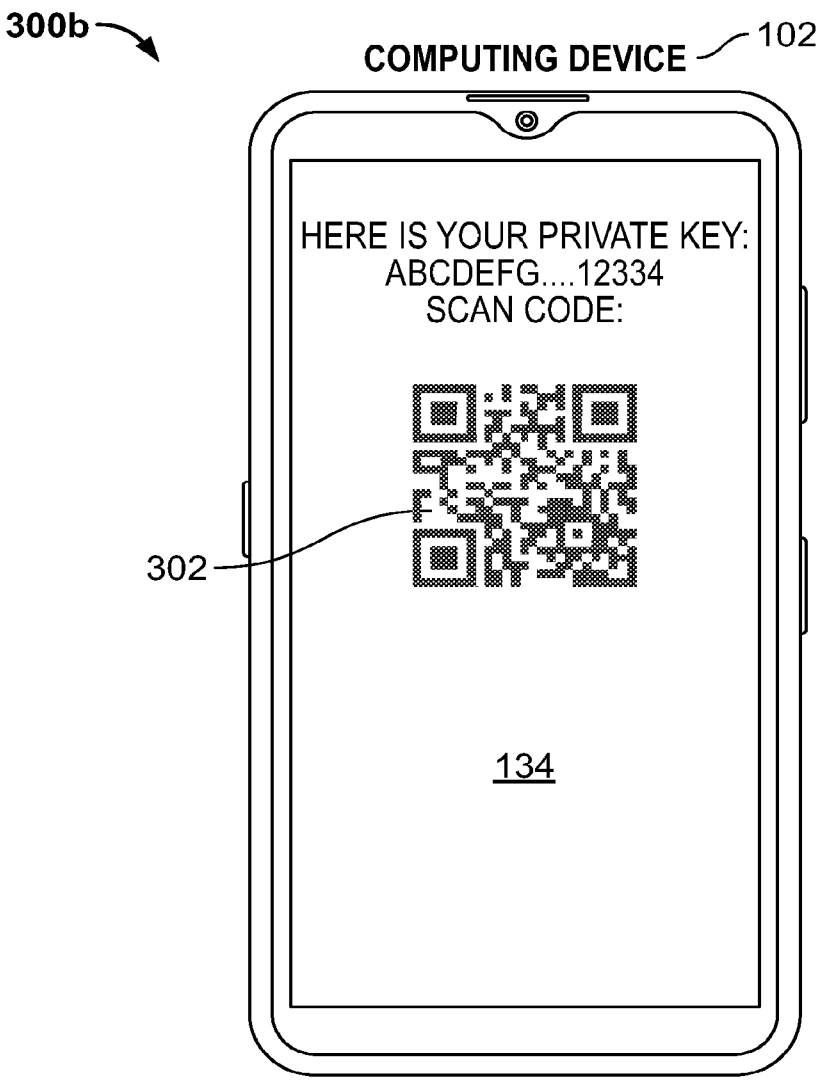

300b
COMPUTING DEVICE
102
HERE IS YOUR PRIVATE KEY:
ABCDEFG....12334
SCAN CODE:
302
134

FIG. 3B

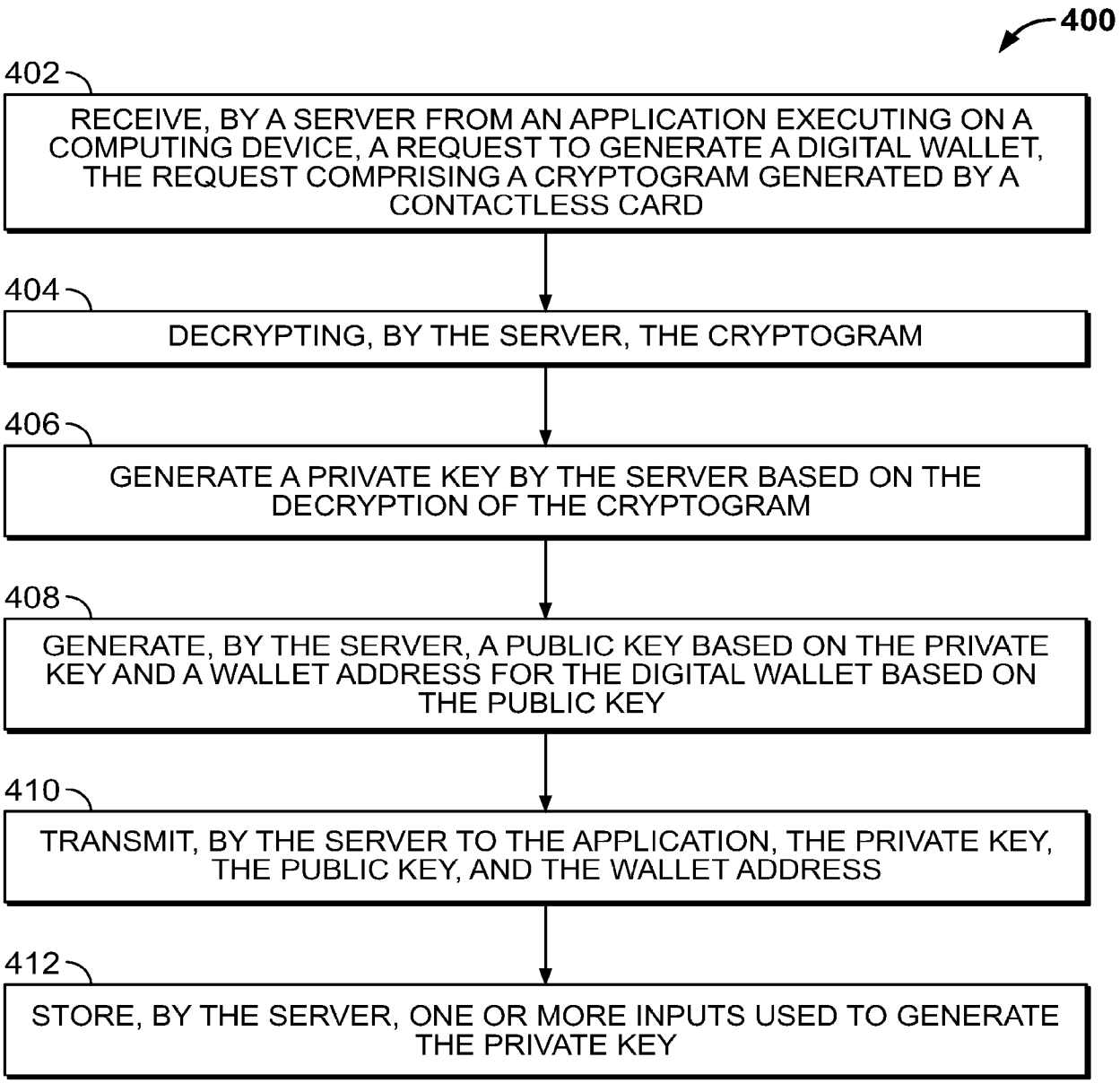

400
402
RECEIVE, BY A SERVER FROM AN APPLICATION EXECUTING ON A COMPUTING DEVICE, A REQUEST TO GENERATE A DIGITAL WALLET, THE REQUEST COMPRISING A CRYPTOGRAM GENERATED BY A CONTACTLESS CARD
404
DECRYPTING, BY THE SERVER, THE CRYPTOGRAM
406
GENERATE A PRIVATE KEY BY THE SERVER BASED ON THE DECRYPTION OF THE CRYPTOGRAM
408
GENERATE, BY THE SERVER, A PUBLIC KEY BASED ON THE PRIVATE KEY AND A WALLET ADDRESS FOR THE DIGITAL WALLET BASED ON THE PUBLIC KEY
410
TRANSMIT, BY THE SERVER TO THE APPLICATION, THE PRIVATE KEY, THE PUBLIC KEY, AND THE WALLET ADDRESS
412
STORE, BY THE SERVER, ONE OR MORE INPUTS USED TO GENERATE THE PRIVATE KEY

FIG. 4

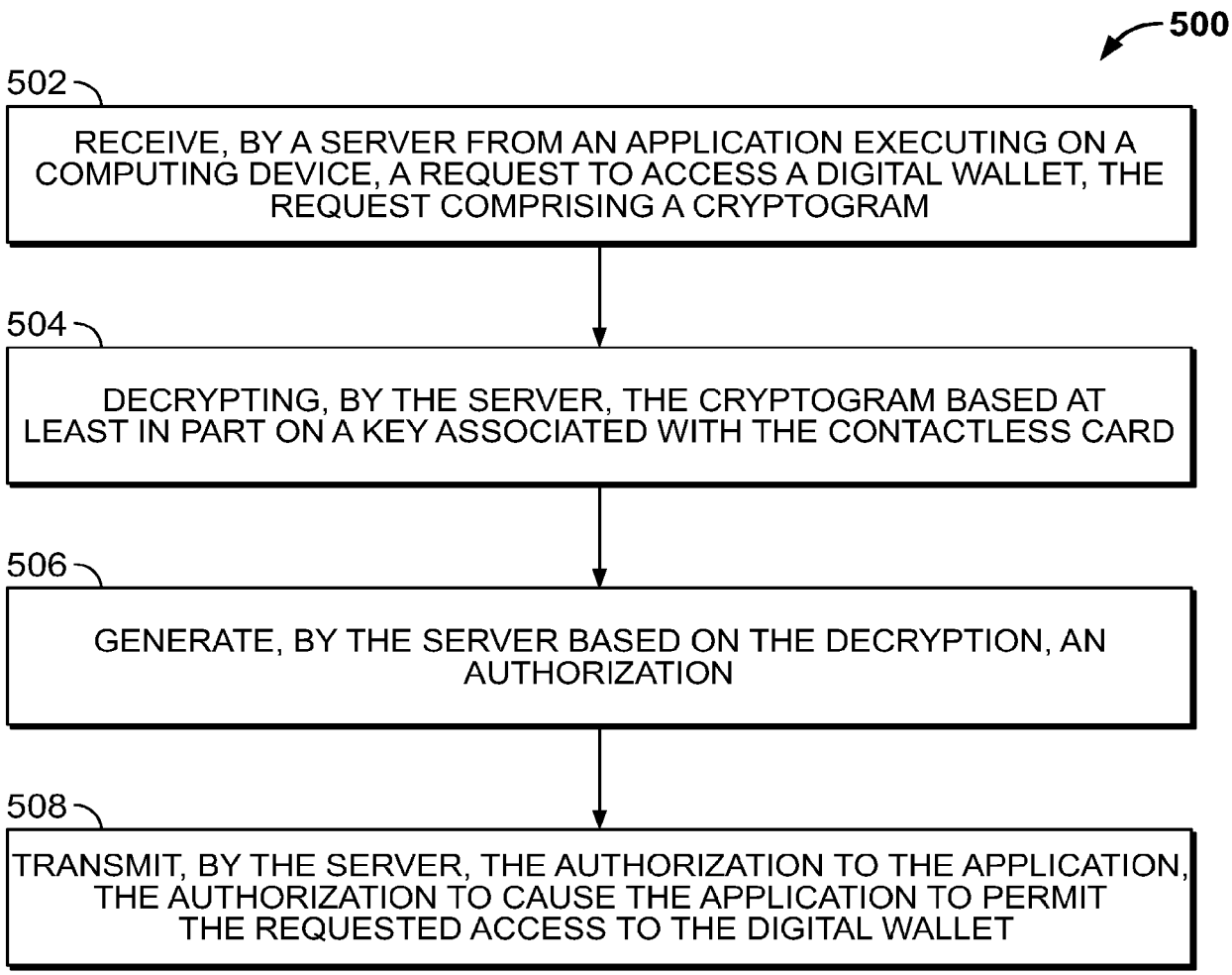

500
502
RECEIVE, BY A SERVER FROM AN APPLICATION EXECUTING ON A COMPUTING DEVICE, A REQUEST TO ACCESS A DIGITAL WALLET, THE REQUEST COMPRISING A CRYPTOGRAM
504
DECRYPTING, BY THE SERVER, THE CRYPTOGRAM BASED AT LEAST IN PART ON A KEY ASSOCIATED WITH THE CONTACTLESS CARD
506
GENERATE, BY THE SERVER BASED ON THE DECRYPTION, AN AUTHORIZATION
508
TRANSMIT, BY THE SERVER, THE AUTHORIZATION TO THE APPLICATION, THE AUTHORIZATION TO CAUSE THE APPLICATION TO PERMIT THE REQUESTED ACCESS TO THE DIGITAL WALLET

FIG. 5

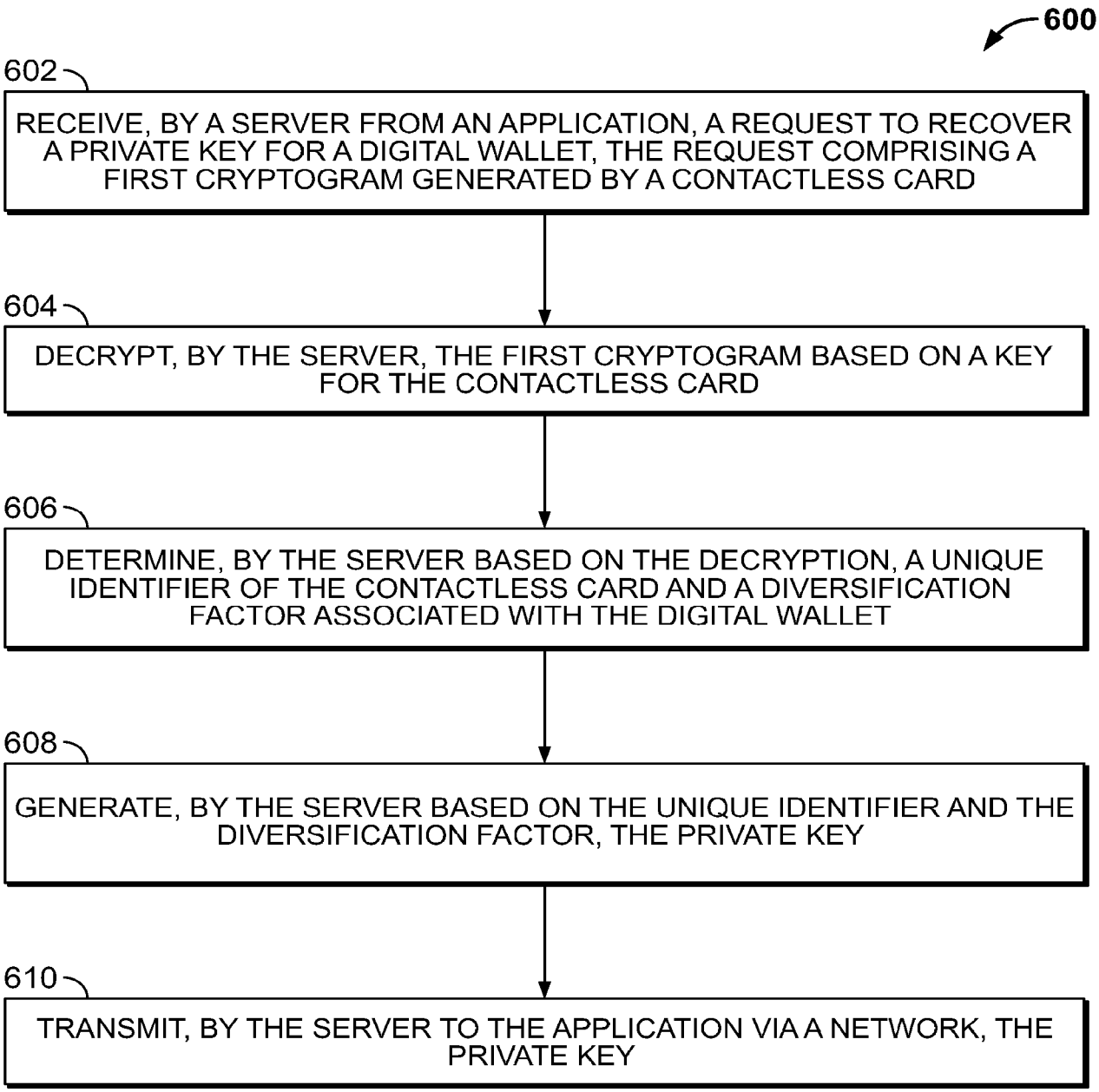

600
602
RECEIVE, BY A SERVER FROM AN APPLICATION, A REQUEST TO RECOVER A PRIVATE KEY FOR A DIGITAL WALLET, THE REQUEST COMPRISING A FIRST CRYPTOGRAM GENERATED BY A CONTACTLESS CARD
604
DECRYPT, BY THE SERVER, THE FIRST CRYPTOGRAM BASED ON A KEY FOR THE CONTACTLESS CARD
606
DETERMINE, BY THE SERVER BASED ON THE DECRYPTION, A UNIQUE IDENTIFIER OF THE CONTACTLESS CARD AND A DIVERSIFICATION FACTOR ASSOCIATED WITH THE DIGITAL WALLET
608
GENERATE, BY THE SERVER BASED ON THE UNIQUE IDENTIFIER AND THE DIVERSIFICATION FACTOR, THE PRIVATE KEY
610
TRANSMIT, BY THE SERVER TO THE APPLICATION VIA A NETWORK, THE PRIVATE KEY

FIG. 6

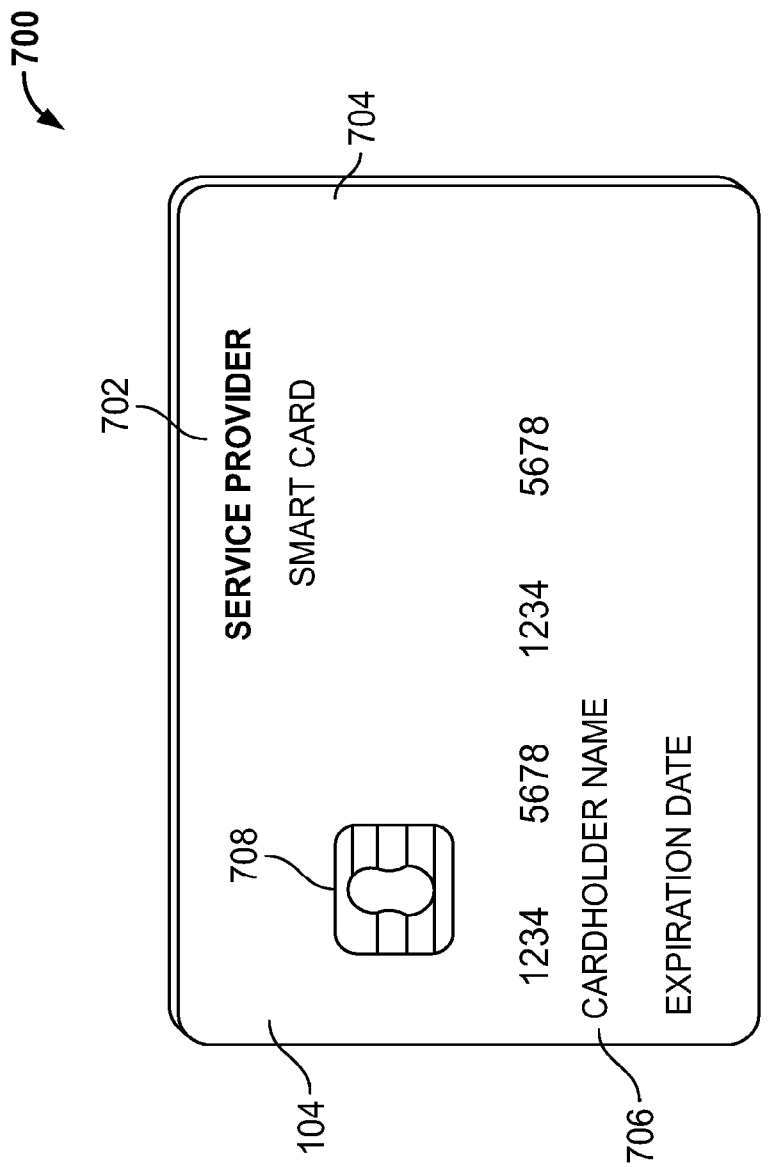

700
704
702
SERVICE PROVIDER
SMART CARD
5678
1234
5678
1234
CARDHOLDER NAME
EXPIRATION DATE
708
104
706

FIG. 7A

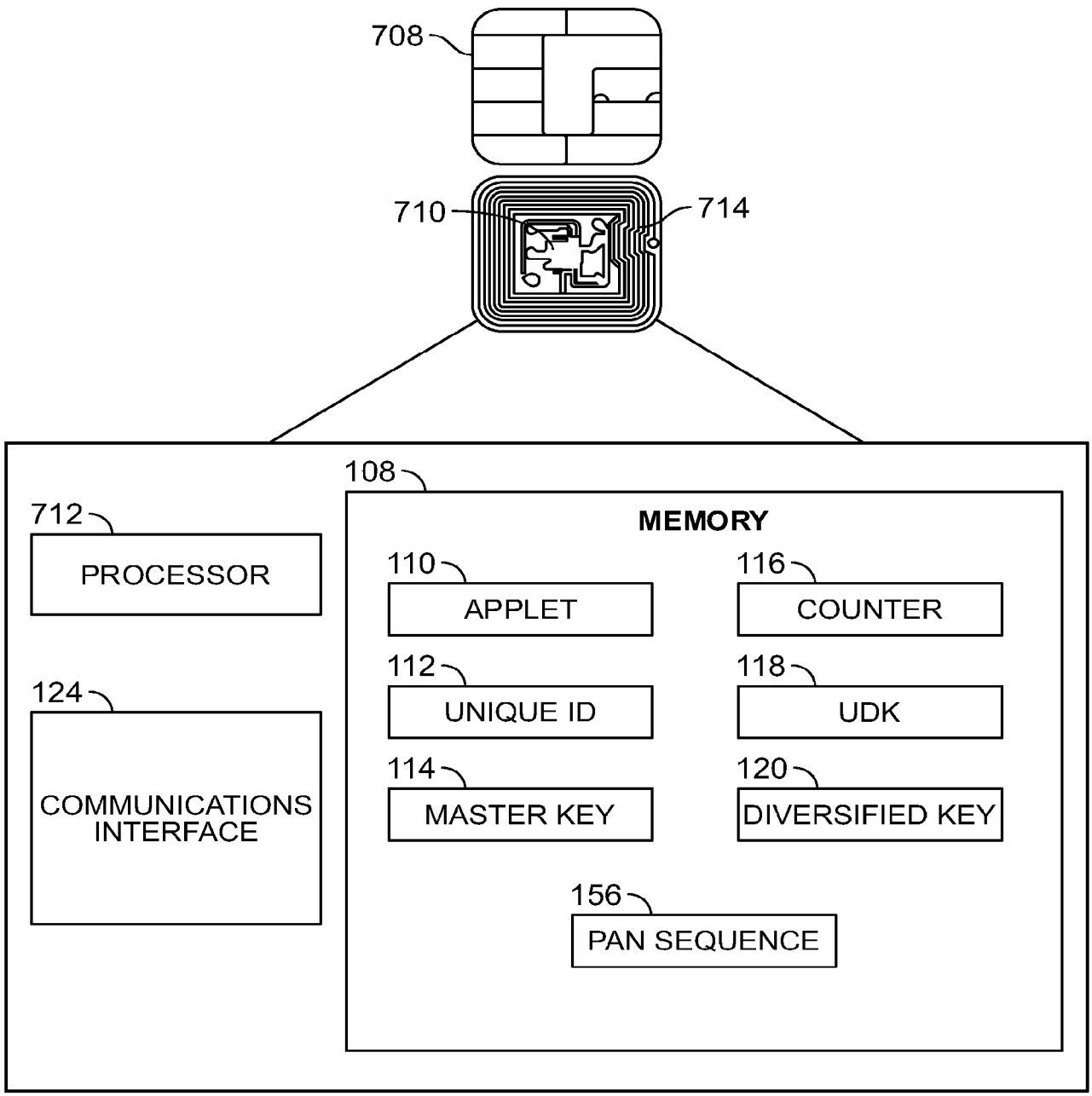

708
710
714
108
MEMORY
712
PROCESSOR
110
APPLET
116
COUNTER
112
UNIQUE ID
118
UDK
124
COMMUNICATIONS INTERFACE
114
MASTER KEY
120
DIVERSIFIED KEY
156
PAN SEQUENCE

FIG. 7B

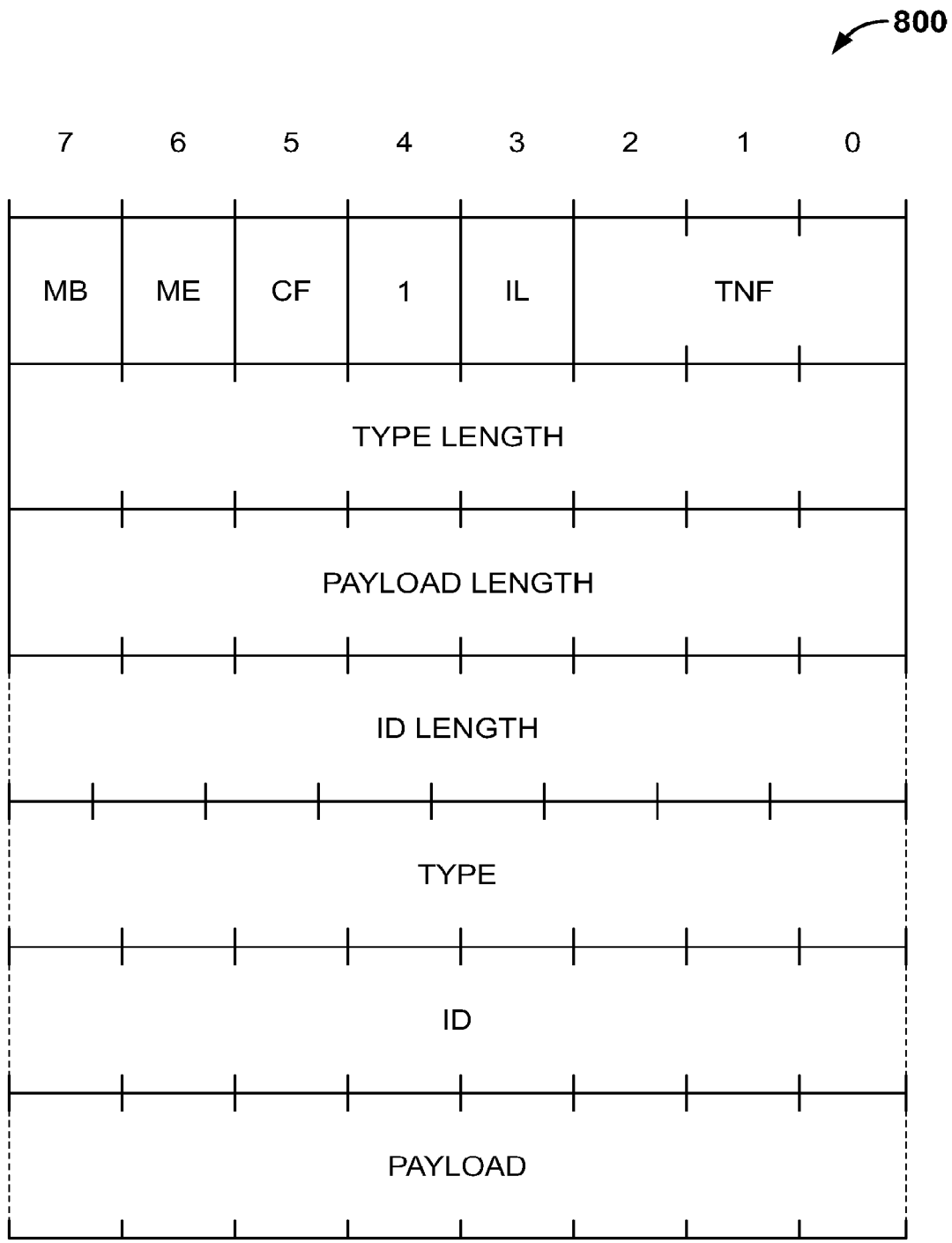

800
7
6
5
4
3
2
1
0
MB
ME
CF
1
IL
TNF
TYPE LENGTH
PAYLOAD LENGTH
ID LENGTH
TYPE
ID
PAYLOAD

FIG. 8

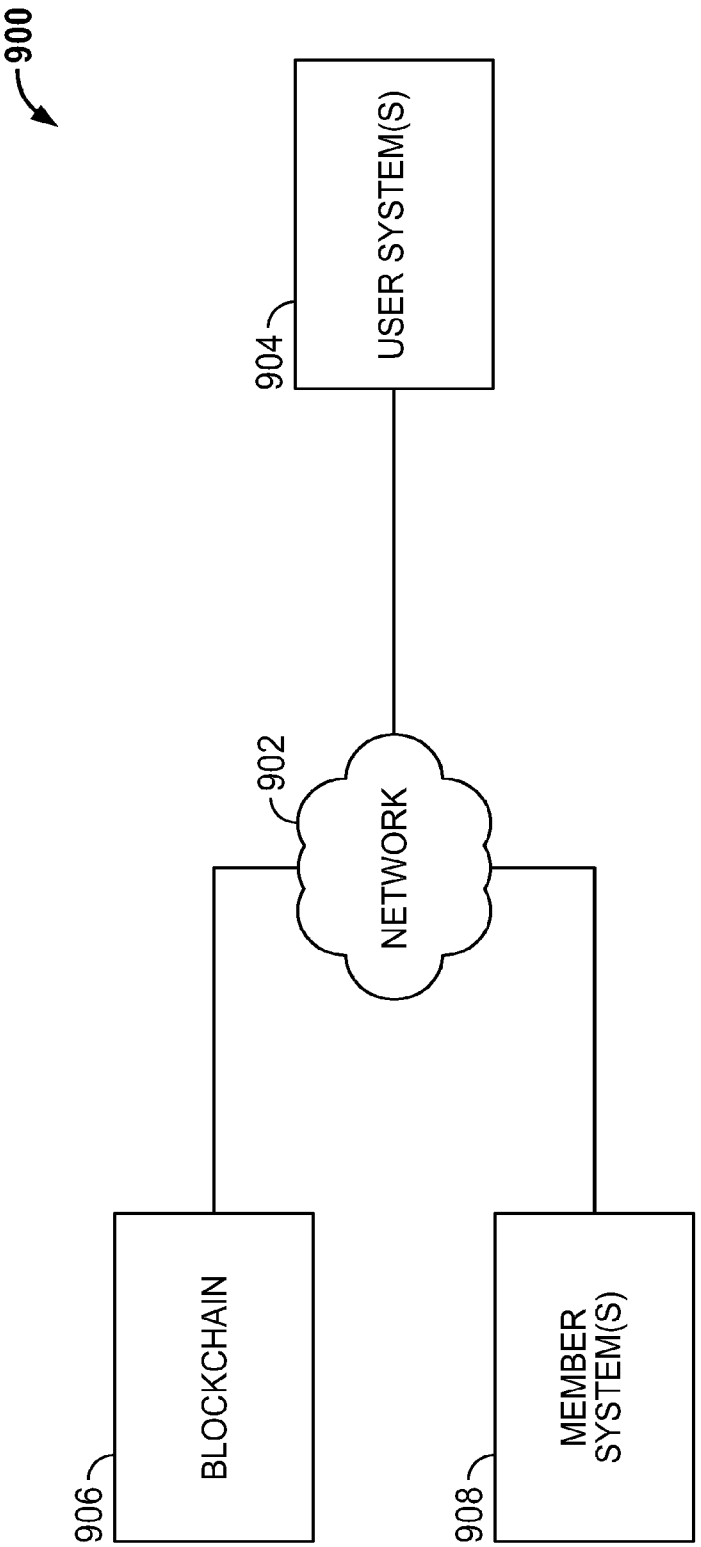

900
USER SYSTEM(S)
904
NETWORK
902
BLOCKCHAIN
906
MEMBER SYSTEM(S)
908

FIG. 9

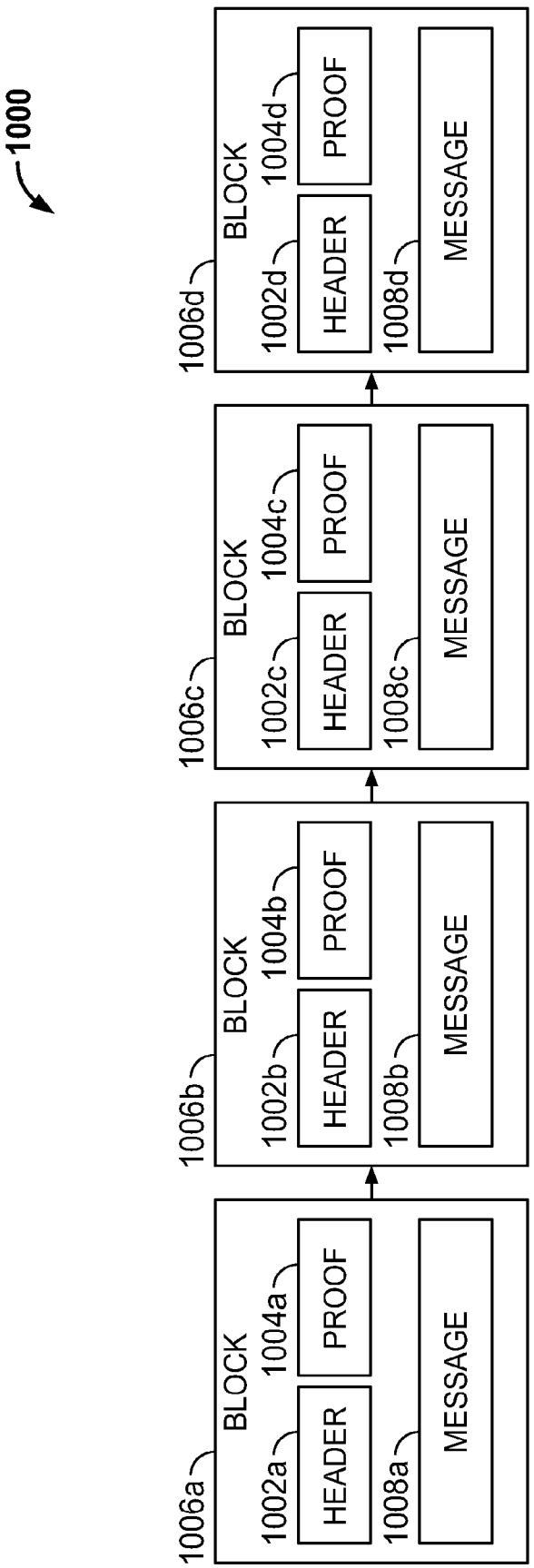

1000
1006a
BLOCK
1002a
HEADER
1004a
PROOF
1008a
MESSAGE
1006b
BLOCK
1002b
HEADER
1004b
PROOF
1008b
MESSAGE
1006c
BLOCK
1002c
HEADER
1004c
PROOF
1008c
MESSAGE
1006d
BLOCK
1002d
HEADER
1004d
PROOF
1008d
MESSAGE

FIG. 10

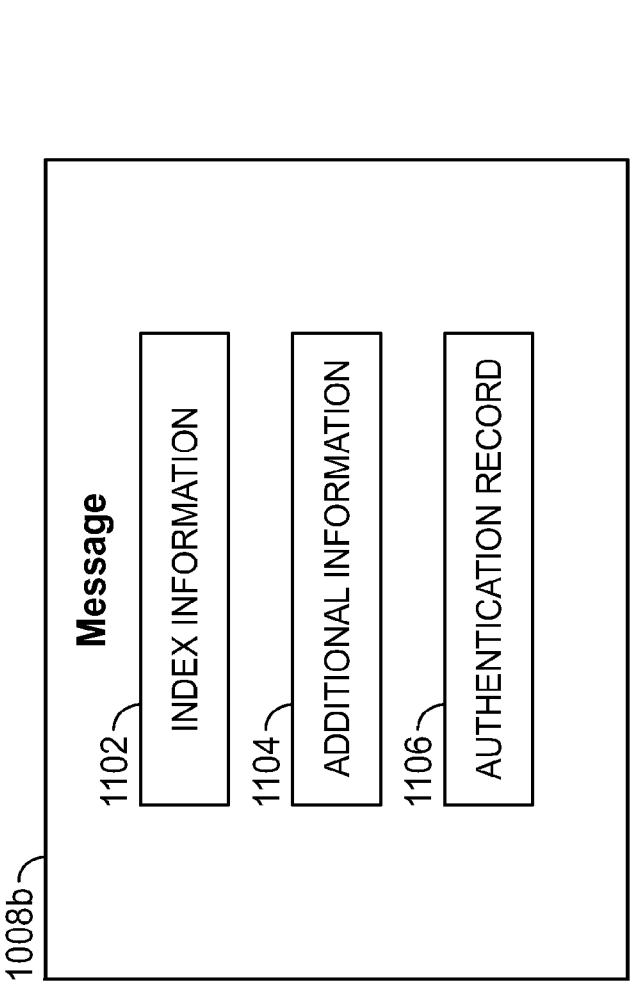

1100
Message
1102
INDEX INFORMATION
1104
ADDITIONAL INFORMATION
1106
AUTHENTICATION RECORD
1008b

FIG. 11

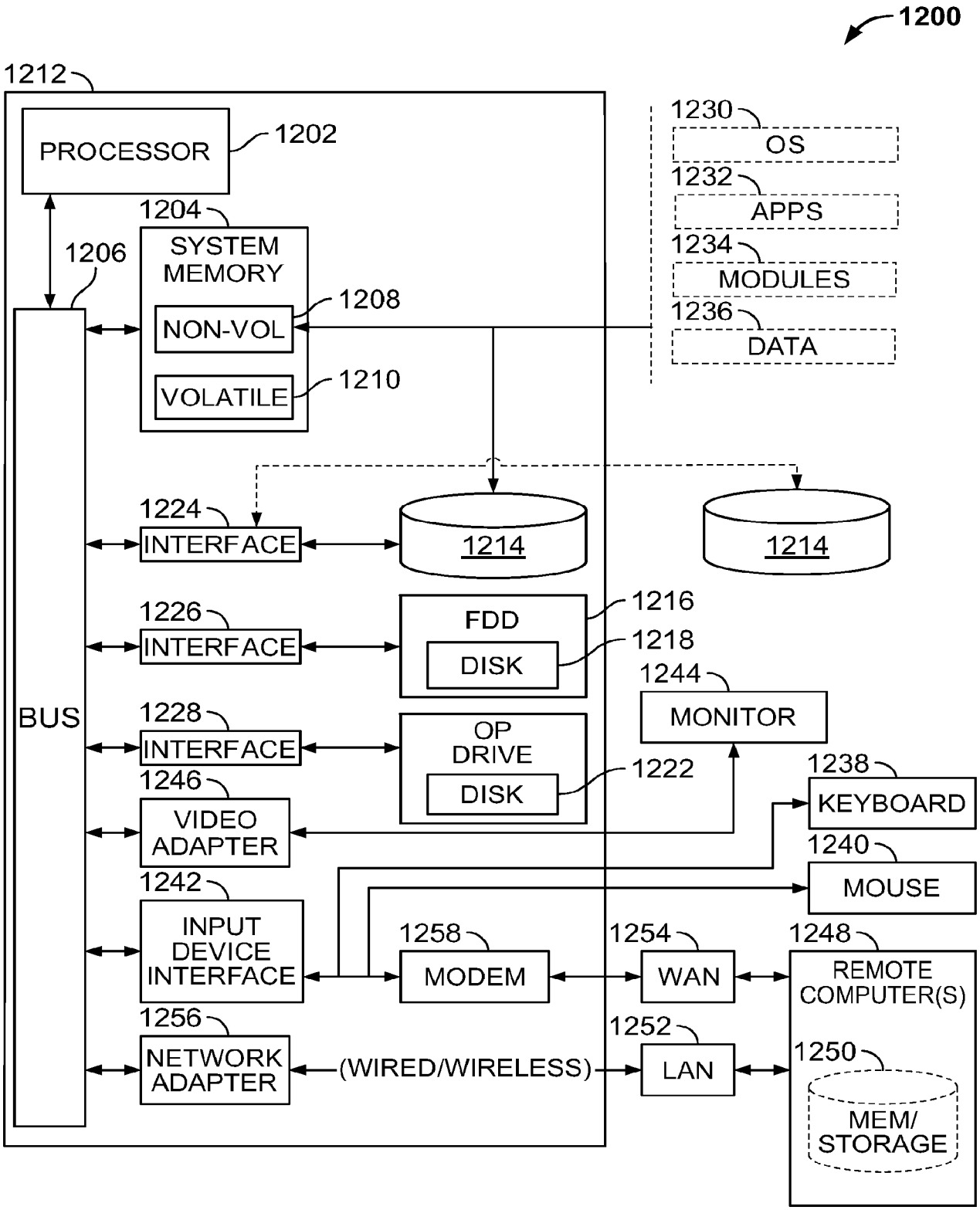

1200
1212
PROCESSOR
1202
1204
SYSTEM MEMORY
1206
NON-VOL
1208
VOLATILE
1210
1230
OS
1232
APPS
1234
MODULES
1236
DATA
BUS
1224
INTERFACE
1214
1214
1226
INTERFACE
FDD
1216
DISK
1218
1228
INTERFACE
OP DRIVE
DISK
1222
1244
MONITOR
1246
VIDEO ADAPTER
1238
KEYBOARD
1240
MOUSE
1242
INPUT DEVICE INTERFACE
1258
MODEM
1254
WAN
1248
REMOTE COMPUTER(S)
1256
NETWORK ADAPTER
(WIRED/WIRELESS)
1252
LAN
1250
MEM/ STORAGE

FIG. 12

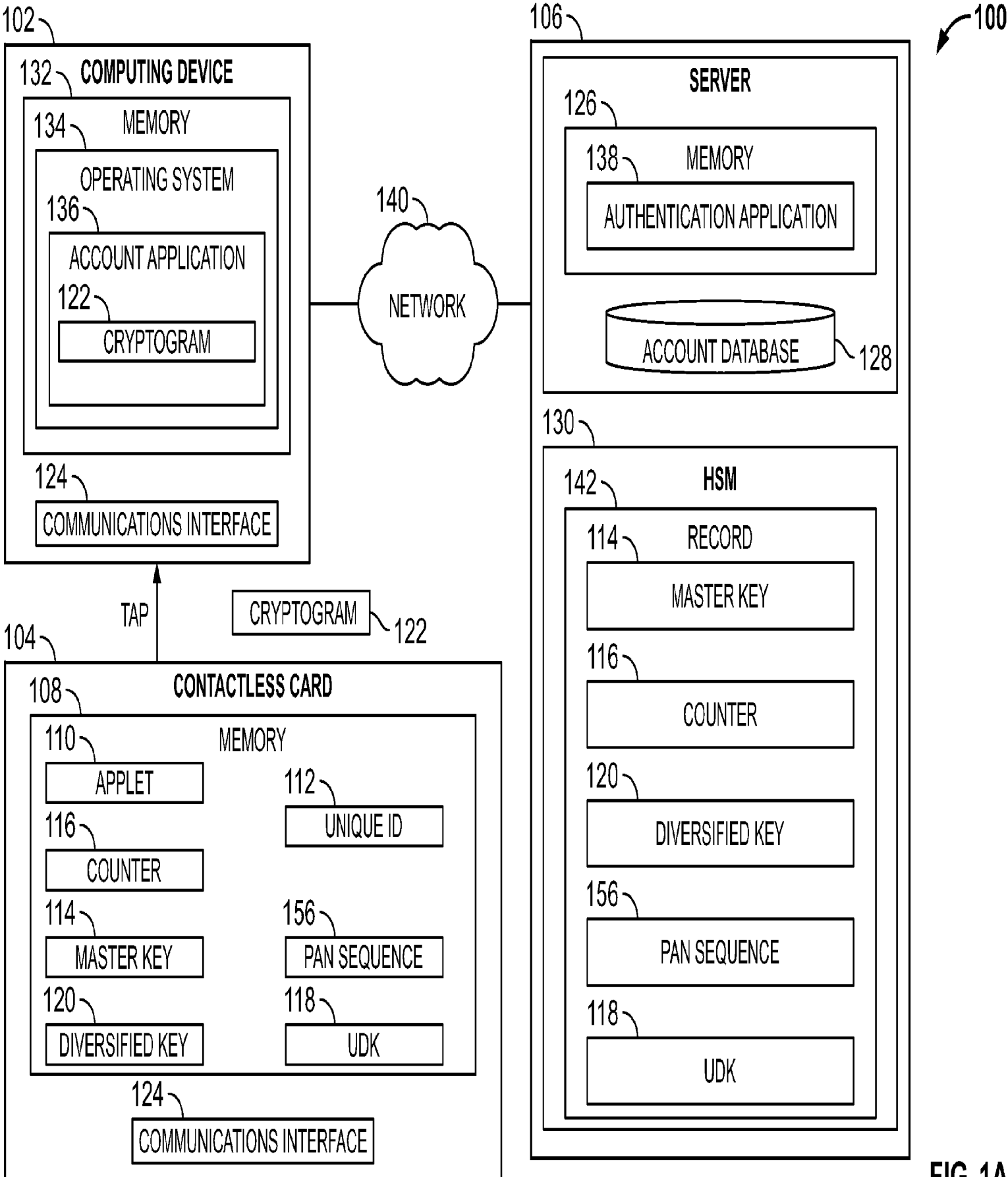

100
102
COMPUTING DEVICE
132
MEMORY
134
OPERATING SYSTEM
136
ACCOUNT APPLICATION
122
CRYPTOGRAM
124
COMMUNICATIONS INTERFACE
140
NETWORK
106
SERVER
126
MEMORY
138
AUTHENTICATION APPLICATION
ACCOUNT DATABASE
128
130
HSM
142
RECORD
114
MASTER KEY
116
COUNTER
120
DIVERSIFIED KEY
156
PAN SEQUENCE
118
UDK
TAP
CRYPTOGRAM
122
104
CONTACTLESS CARD
108
MEMORY
110
APPLET
112
UNIQUE ID
116
COUNTER
114
MASTER KEY
156
PAN SEQUENCE
120
DIVERSIFIED KEY
118
UDK
124
COMMUNICATIONS INTERFACE

FIG. 1A