



(51) International Patent Classification:

*H04W 12/041* (2021.01)      *H04W 4/80* (2018.01)  
*H04W 12/047* (2021.01)      *G06Q 20/32* (2012.01)  
*H04W 12/47* (2021.01)      *G06Q 20/34* (2012.01)  
*H04L 9/08* (2006.01)

(21) International Application Number:

PCT/US2024/062387

(22) International Filing Date:

31 December 2024 (31.12.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

18/403,001      03 January 2024 (03.01.2024)      US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US];

1680 Capital One Drive, McLean, Virginia 22102 (US).

(72) Inventors: **OSBORN, Kevin**; c/o Capital One Services, LLC, 1680 Capital One Drive, McLean, Virginia 22102 (US). **CHIGURUPATI, Srinivasa**; c/o Capital One Services, LLC, 1680 Capital One Drive, McLean, Virginia 22102 (US). **JONES, John**; c/o Capital One Services, LLC, 1680 Capital One Drive, McLean, Virginia 22102 (US).

(74) Agent: **KASNEVICH, Andrew D.** et al.; KDW Firm PLLC, 2601 Weston Parkway Suite 103, Cary, North Carolina 27513 (US).

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

(54) Title: SYSTEMS AND METHODS FOR GENERATING SHARED SECRET KEY FOR TRANSACTION CARDS

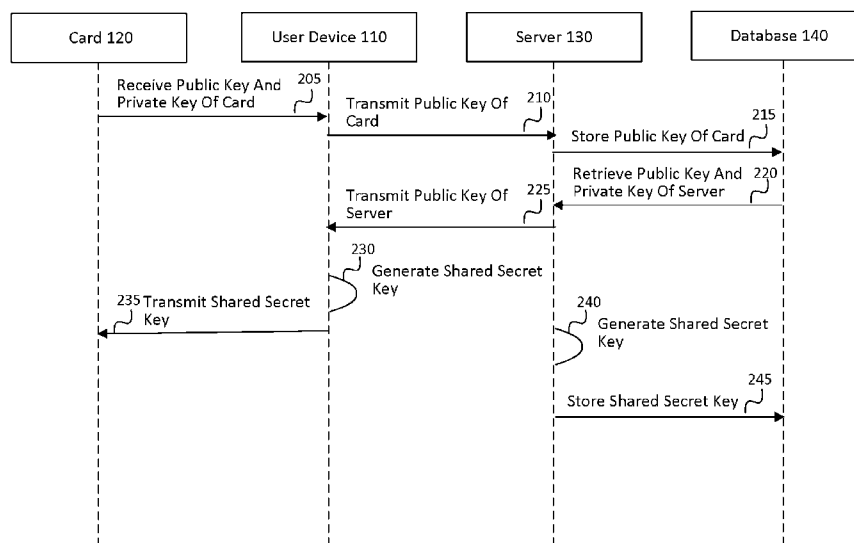


FIG. 2

200

(57) Abstract: Systems and methods for generating a shared secret key for a transaction card are provided. An exemplary system can include: a transaction card including a card private key and a card public key derived from the card private key; a server including a server private key and a server public key derived from the server private key; and a user device. The user device can be configured to: open a communication field, read the card public key, transmit the card public key to the server, wherein the server generates a shared secret key from the card public key and the server private key, receive the server public key from the server, and transmit the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

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

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

**Published:**

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

## **SYSTEMS AND METHODS FOR GENERATING SHARED SECRET KEY FOR TRANSACTION CARDS**

### **CROSS-REFERENCE TO RELATED APPLICATION**

**[0001]** This patent application claims the benefit of priority to U.S. Patent Application No. 18/403,001, filed January 3, 2024. The contents of the above-noted patent application are incorporated herein by reference in their entirety.

### **FIELD OF THE INVENTION**

**[0002]** The present disclosure relates generally to data security, and more particularly, to systems and methods for generating shared secret key for transaction cards.

### **BACKGROUND**

**[0003]** Transaction cards can be authenticated using symmetric keys between the card itself and a backend server. In a conventional system, when the card is issued, the card is provisioned with a shared secret key, and the server has the shared secret key as well. They each use the shared secret key to create the symmetric keys. Typically, these shared secret keys are generated and stored on the card itself before the card is issued to a user.

**[0004]** However, these conventional methods are inconvenient for some situations. For example, when a transaction card is being re-issued or a new transaction card is issued at a vending machine, a new shared secret key is typically needed for that re-issued card or the new card. This requires transmitting the new shared secret key between that re-issued card or the new card and the back end server, which poses security risks.

**[0005]** These and other deficiencies exist. Accordingly, there is a need to provide systems and methods that overcome these deficiencies to dynamically generate shared secret keys between a transaction card and a back end server.

## SUMMARY

[0006] In some aspects, the techniques described herein relate to a system for generating a shared secret key for a transaction card, the system including: a transaction card including a card private key and a card public key derived from the card private key; a server including a server private key and a server public key derived from the server private key; and a user device configured to: open a communication field, read the card public key, transmit the card public key to the server, wherein the server generates a shared secret key from the card public key and the server private key, receive the server public key from the server, and transmit the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

[0007] In some aspects, the techniques described herein relate to a method for generating a shared secret key for a transaction card, the system including: providing a transaction card including a card private key and a card public key derived from the card private key; providing a server including a server private key and a server public key derived from the server private key; and opening, by a user device, a communication field, reading, by the user device, the card public key, transmitting, by the user device, the card public key to the server, wherein the server generates a shared secret key from the card public key and the server private key, receiving, by the user device, the server public key from the server, and transmitting, by the user device, the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

[0008] In some aspects, the techniques described herein relate to a non-transitory computer readable medium containing computer executable instructions that, when executed by a computer hardware arrangement, cause the computer hardware arrangement to perform procedures including: opening a communication field; reading, from a card upon entering the

communication field, the card public key; transmitting, the card public key to a server, wherein the server generates a shared secret key from the card public key and the server private key, receiving, the server public key from the server, and transmitting, the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

[0009] Further features of the disclosed systems and methods, and the advantages offered thereby, are explained in greater detail hereinafter with reference to specific example embodiments illustrated in the accompanying drawings.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0010] Figure 1 is a diagram of a system for dynamically generating shared secret keys between a transaction card and a back end server according to an example embodiment.

[0011] Figure 2 is a diagram of a sequence of interactions between components of the system in Figure 1 according to an example embodiment.

[0012] Figure 3 is a contactless card that can be used for enhancing transaction messages for fraud prevention according to an example embodiment.

[0013] Figure 4 is a diagram of the processor of the contactless card in Figure 3 according to an example embodiment.

[0014] Figure 5 is a flow chart of a method for dynamically generating a shared secret key for a transaction card on the back end server side according to an example embodiment.

[0015] Figure 6 is a flow chart of a method for dynamically generating a shared secret key for a transaction card on the transaction card side according to an example embodiment.

[0016] Figure 7 is a diagram of tapping a transaction card to a mobile device according to an example embodiment.

[0017] Figure 8 is a flow chart of a method for generating a cryptogram using a shared secret key on the transaction card side according to an example embodiment.

[0018] Figure 9 is a flow chart of a method for validating a cryptogram using a shared secret key on the back end server side according to an example embodiment.

[0019] Figure 10 is a flow chart of a method for dynamically generating a shared secret key between a transaction card and a back end server according to an example embodiment.

### **DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS**

[0020] The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. The embodiments described should be recognized as capable of implementation separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the invention. The description of embodiments should facilitate understanding of the invention to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the invention.

[0021] The described features and teachings of the embodiments may be combined in any suitable manner. A person of ordinary skill in the art will recognize that the embodiments may be practiced without one or more of the specific features and teachings of an embodiment. In other instances, additional features and teachings may be recognized in certain embodiments that may not be present in all embodiments. A person of ordinary skill in the art will understand

that the described features and teachings of any embodiment can be interchangeably combined with the features and teachings of any other embodiment.

**[0022]** Secret keys can be diversified at card manufacturing time to create the symmetric keys that are associated with transaction cards and with an identity of users. There can have applications for this identity assertion and card authentication to work with mobile devices acting as the card authenticator. Mobile devices have secure elements that can store and handle the secret keys for the message authentication code (MAC) construction and encryption, however, provisioning of those keys to both the mobile device and the back end validation systems in a secure way is challenging.

**[0023]** The present disclosure provides shared secret key agreement protocol and subsequent key handling methods. In the present disclosure, any number of key agreement protocols such as Diffie-Hellman or elliptic-curve Diffie Hellman (ECDH) can be used to create a secret key in parallel on the mobile device side and the back end validation server side. These key agreement protocols can use split components where one component is shared with the other side, but the other component is held secret. Both parties end up computing the same shared secret to create a shared secret key. The shared secret keys can then be provisioned into the mobile device's secure element/keychain and/or the transaction card.

**[0024]** On the back end server validation side, the generated shared secret keys can be encrypted with a key encryption key and stored in a database associated with the identity of the user associated with the mobile device. The identity of the user may be established with multifactor authentication, or authority endorsement before accepting this association.

**[0025]** For validation by the back end server, a transaction card message can be parsed and the unique identification number (UID) of the transaction card is looked up. The encrypted keys included in the transaction card message are provisioned to the hardware security module

(HSM) of the back end server, and the appropriate decryption and MAC validation can be performed in the HSM based on the shared secret key that was already stored in the HSM or is dynamically generated at that moment.

**[0026]** In addition to the ECDH, example embodiments of the present disclosure can be implemented with any other number of secret key algorithm, such as triple data encryption algorithm (3DES), and advanced encryption standard (AES).

**[0027]** Figure 1 illustrates a system 100 for dynamically generating a shared secret key between a transaction card and a back end server according to an example embodiment. As further discussed below, the system 100 may comprise a user device 110, a card 120, a server 130, a database 140, and a network 150,. Although Figure 1 illustrates single instances of the components, the system 100 may include any number of components.

**[0028]** The user device 110 may be associated with a user who is issued the card 120. The user device 110 may be a network-enabled computer device. Exemplary network-enabled computer devices include, without limitation, a server, a network appliance, a personal computer, a workstation, a phone, a handheld personal computer, a personal digital assistant, a thin client, a fat client, an Internet browser, a mobile device, a kiosk, or other a computer device or communications device. For example, network-enabled computer devices may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

**[0029]** The user device 110 may include a processor 111, a memory 112, and an application 113. The processor 111 may be a processor, a microprocessor, or other processor, and the user device 110 may include one or more of these processors. The processor 111 may include

processing circuitry, which may contain additional components, including additional processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

**[0030]** The processor 111 may be coupled to the memory 112. The memory 112 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the user device 110 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-programmed many times after leaving the factory. It may also be read many times. The memory 112 may be configured to store one or more software applications, such as the application 113, and other data, such as user's shopping and financial account information.

**[0031]** The application 113 may comprise one or more software applications comprising instructions for execution on the user device 110. In some examples, the user device 110 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of the system 100, transmit and/or receive data, and perform the functions described herein. Upon execution by the processor 111, the application 113 may provide the functions described in this specification, specifically to execute and perform the steps and functions in the process flows described below. For example, the application 113 may be executed to perform authenticating the user. Such processes may be implemented in software, such as software modules, for execution by

computers or other machines. The application 113 may provide GUIs through which a user may view and interact with other components and devices within the system 100. The GUIs may be formatted, for example, as web pages in HyperText Markup Language (HTML), Extensible Markup Language (XML) or in any other suitable form for presentation on a display device depending upon applications used by users to interact with the system 100.

**[0032]** The user device 110 may further include a display 114 and input devices 115. The display 114 may be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices 115 may include any device for entering information into the user device 110 that is available and supported by the user device 110, such as a touch-screen, keyboard, mouse, cursor-control device, microphone, digital camera, video recorder or camcorder. These devices may be used to enter information and interact with the software and other devices described herein.

**[0033]** The system 100 may include a card 120 which is further explained below with reference to FIG. 3 and FIG. 4. The card 120 may be any type of card, such as a contactless card, a security card, a payment card, an identification card, and the like. The card 120 may be issued to the user by a financial institution.

**[0034]** The card 120 can be configured to transmit a unique card identifier and a cryptographic payload including a cryptogram to the user device 110 upon tapping to the user device 110. The user device 110 may be configured to read the unique card identifier and the cryptographic payload including the cryptogram from the card 120 after entry of the card 120 into a communication field of the user device 110. The user device 110 may then transmit the unique card identifier and the cryptographic payload including the cryptogram to the server 130.

**[0035]** The card 120 can perform authentication and numerous other functions that may

otherwise require a user to carry a separate physical token in addition to the card 120. By employing a contactless interface, the card 120 may be provided with a method to interact and communicate between a user's device (such as a mobile phone or the user device 110) and the card itself. For example, the Europay, Mastercard, and Visa (EMV) protocol, which underlies many credit card transactions, includes an authentication process which suffices for operating systems for Android® but presents challenges for iOS®, which is more restrictive regarding near field communication (NFC) usage, as it can be used only in a read-only manner. Exemplary embodiments of the card 120 described herein can utilize NFC technology. The card 120 may comprise a substrate 121 and a contact pad 122. Details of an example contactless card 120 will be described in Figures 3 and 4.

[0036] The server 130 may be a back end server associated with an institution, such as a financial institution that issues the card 120, and can be configured to communicate with the user device 110. The institution associated with the server 130 may issue the card 120 to the user and accordingly may authenticate the user based on the card 120.

[0037] The server 130 may be a network-enabled computer device. Exemplary network-enabled computer devices include, without limitation, a server, a network appliance, a personal computer, a workstation, a phone, a handheld personal computer, a personal digital assistant, a thin client, a fat client, an Internet browser, a mobile device, a kiosk, or other a computer device or communications device. For example, network-enabled computer devices may include an iPhone, iPod, iPad from Apple® or any other mobile device running Apple's iOS® operating system, any device running Microsoft's Windows® Mobile operating system, any device running Google's Android® operating system, and/or any other smartphone, tablet, or like wearable mobile device.

[0038] The server 130 may include a processor 131, a memory 132, and an application 133.

The processor 131 may be a processor, a microprocessor, or other processor, and the server 130 may include one or more of these processors. The processor 131 may include processing circuitry, which may contain additional components, including additional processors, memories, error and parity/CRC checkers, data encoders, anti-collision algorithms, controllers, command decoders, security primitives and tamper-proofing hardware, as necessary to perform the functions described herein.

**[0039]** The processor 131 may be coupled to the memory 132. The memory 132 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM, and the server 130 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-programmed many times after leaving the factory. It may also be read many times. The memory 132 may be configured to store one or more software applications, such as the application 133, and other data, such as user's financial account information and the contactless card information.

**[0040]** The application 133 may comprise one or more software applications, such as a card authentication module, comprising instructions for execution on the server 130. In some examples, the server 130 may execute one or more applications, such as software applications, that enable, for example, network communications with one or more components of the system 100, transmit and/or receive data, and perform the functions described herein. Upon execution by the processor 131, the application 133 may provide the functions described in this specification, specifically to execute and perform the steps and functions in the process flows

described below. For example, a card authentication module of the application 133 may be executed to perform authenticating the user based on the contactless card 120. Such processes may be implemented in software, such as software modules, for execution by computers or other machines. The application 133 may provide GUIs through which a user may view and interact with other components and devices within the system 100. The GUIs may be formatted, for example, as web pages in HyperText Markup Language (HTML), Extensible Markup Language (XML) or in any other suitable form for presentation on a display device depending upon applications used by users to interact with the system 100.

**[0041]** The server 130 may further include a display 134 and input devices 135. The display 134 may be any type of device for presenting visual information such as a computer monitor, a flat panel display, and a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays. The input devices 135 may include any device for entering information into the server 130 that is available and supported by the server 130, such as a touch-screen, keyboard, mouse, cursor-control device, microphone, digital camera, video recorder or camcorder. These devices may be used to enter information and interact with the software and other devices described herein.

**[0042]** The database 140 may be one or more databases configured to store data, including without limitation, private information of users, financial accounts of users, contactless card information, online merchant account information, transactions of users, and merchant records indicative of corresponding merchants. The database 140 may comprise a relational database, a non-relational database, or other database implementations, and any combination thereof, including a plurality of relational databases and non-relational databases. In some examples, the database 140 may comprise a desktop database, a mobile database, or an in-memory database. Further, the database 140 may be hosted internally by the server 130 or may be

hosted externally of the server 130, such as by a server, by a cloud-based platform, or in any storage device that is in data communication with the server 130.

**[0043]** The system 100 may include one or more networks 150. In some examples, the network 150 may be one or more of a wireless network, a wired network or any combination of wireless network and wired network, and may be configured to connect the user device 110, the card 120, the server 130, and the database 140. For example, the network 150 may include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless local area network (LAN), a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, Radio Frequency Identification (RFID), Wi-Fi, and/or the like.

**[0044]** In addition, the network 150 may include, without limitation, telephone lines, fiber optics, IEEE Ethernet 902.3, a wide area network, a wireless personal area network, a LAN, or a global network such as the Internet. In addition, the network 150 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. The network 150 may further include one network, or any number of the exemplary types of networks mentioned above, operating as a stand-alone network or in cooperation with each other. The network 150 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. The network 150 may translate to or from other protocols to one or more protocols of network devices. Although the network 150 is depicted as a single network, it should be appreciated that according to one or more examples, the network 150 may comprise a plurality of interconnected networks, such as, for

example, the Internet, a service provider's network, a cable television network, corporate networks, such as credit card association networks, and home networks. The network 150 may further comprise, or be configured to create, one or more front channels, which may be publicly accessible and through which communications may be observable, and one or more secured back channels, which may not be publicly accessible and through which communications may not be observable.

**[0045]** In some examples, communications between the user device 110, server 130, and card 120 using the network 150 can occur using one or more front channels and one or more secure back channels. A front channel may be a communication protocol that employs a publicly accessible and/or unsecured communication channel such that a communication sent to the user device 110, server 130, and/or card 120 may originate from any other device, whether known or unknown to the user device 110, server 130, and/or card 120, if that device possesses the address (e.g., network address, Internet Protocol (IP) address) of the user device 110, server 130, and/or card 120. Exemplary front channels include, without limitation, the Internet, an open network, and other publicly-accessible communication networks. In some examples, communications sent using a front channel may be subject to unauthorized observation by another device. In some examples, front channel communications may comprise Hypertext Transfer Protocol (HTTP) secure socket layer (SSL) communications, HTTP Secure (HTTPS) communications, and browser-based communications with a server or other device.

**[0046]** A secure back channel may be a communication protocol that employs a secured and/or publicly inaccessible communication channel. A secure back channel communication sent to the user device 110, server 130, and/or card 120 may not originate from any device, and instead may only originate from a selective number of parties. In some examples, the selective number of devices may comprise known, trusted, or otherwise previously authorized devices.

Exemplary secure back channels include, without limitation, a closed network, a private network, a virtual private network, an offline private network, and other private communication networks. In some examples, communications sent using a secure back channel may not be subject to unauthorized observation by another device. In some examples, secure back channel communications may comprise Hypertext Transfer Protocol (HTTP) secure socket layer (SSL) communications, HTTP Secure (HTTPS) communications, and browser-based communications with a server or other device.

**[0047]** Figure 2 illustrates an example diagram 200 of sequence of interactions between the components of the system 100 according to an example embodiment. Figure 2 may reference the same or similar components as those illustrated in Figure 1, including a user device, a server, a database, and a card.

**[0048]** When a user is issued a card such as the card 120, the card is provisioned with a master key, a card unique identification number, a card public key and a card private key pairing with the card public key. The user may tap the card 120 to the user device 110. Upon tapping the card 120, the user device 110 may transmit an NFC prompt and/or query to the card 120. The user device 110 may include an NFC interface configured for establishing an NFC communication with other NFC-equipped devices (the card 120 in this embodiment). In some of these embodiments, the NFC interface of the user device 110 may be or include an NFC receiver configured for selectively activating a magnetic field for use in establishing near field communication with an NFC transmitter. The NFC interface of the user device 110 is configured for establishing NFC communication when a passive NFC tag or other NFC-enabled device is brought into the magnetic field and within the NFC communication range of the user device 110. The NFC interface of the user device 110 is configured, in particular, for communication with the NFC-enabled card 120 when the card 120 is brought within a

communication range of the user device 110 (such as, the card 120 is tapped by the user to the user device 110). As used herein, a tap of the card 120 to the user device 110 may not indicate that the card 120 is in a physical contact with the user device 110. A tap of the card 120 to the user device 110 may refer to entry of the card 120 into the NFC communication field of the user device 110. In response, the card 120 can transmit the card public key and the card private key to the user device 110. Accordingly, the user device 110, at step 205, can receive the card public key and the card private key of the card 120.

**[0049]** At step 210, the user device 110 may transmit the card public key of the card 120 to the server 130. Because it is the card public key, there have no security concerns of transmitting the card public key through the network 150 to the server 130.

**[0050]** At step 215, the server 130 may store the card public key of the card 120 to the database 140. At step 220, the server 130 may retrieve from the database 140 a server public key and a server private key pairing with the server public key.

**[0051]** At step 225, the server 130 may transmit the server public key of the server to the user device 110. As used herein, the card public key and the card private key of the card 120 and the server public key and the server private key of the server 130 are key pairs suitable for key agreement protocols such as elliptic curve cryptography.

**[0052]** At step 230, the user device 110 can generate a shared secret key based on the server public key of the server 130 and the card private key of the card 120. At step 235, the user device 110 may transmit the shared secret key to the card 120. The card 120 can store the shared secret key on the card 120.

**[0053]** At step 240, the server 130 may generate the same shared secret key independently based on the server private key of the server 130 and the card public key of the card 120. At step 245, the server 130 may store the same shared secret key on the database 140.

[0054] As described, transaction cards can be provisioned with a card unique identification number and a master key when the transaction cards are manufactured. The transaction cards are based on a symmetric cryptography system that relies on diversified keys diversified from such as the master key, the card unique identification number and a shared secret key. However, transmitting a shared secret key between a transaction card and a back end validation server can be exposed to data security risk. In the present disclosure, a same shared secret key can be independently generated by a user device and a back end validation server through key agreement protocols, which can improve data security.

[0055] The present disclosure allows dynamically generating shared secret keys and diversifying other keys after transactions cards are issued to users. For example, a card can be newly issued to a user or re-issued to a user on a vending machine. Exemplary embodiments of the present disclosure can securely unlock the card and allow for storing a new shared secret key and other new diversified keys in the card. The card can be unlocked by the user device or a reader of the vending machine.

[0056] A protocol such as ECDH can be used to generate a shared secret key for the card and for validation that can then be stored on the card. By applying the ECDH, a user device/a card can provide a public key associated with the card to a back end server while keeping a private key associated with the card, likewise, the back end server can provide a public key associated with the back end server to the user device/the card while keeping a private key associated with the back end server. A same shared secret key can be dynamically and separately generated by the user device/the card and the back end server. For example, as shown in Figure 2, the user device/the card can use the public key associated with the back end server and the private key associated with the card to generate the same shared secret key, and likewise, the back end server can use the public key associated with the card and the private key associated

with the back end server to generate the same shared secret key independently. In this way, the shared secret key is not needed to be transmitted between the back end server and the user device/the card, which can improve data security.

**[0057]** The shared secret key can be stored in the card. The shared secret key can also be stored in the back end server for validation of the card. Preferably, the back end server can store the components that will be needed to regenerate the shared secret key for validation of the card, such as storing the public key associated with the card and the private key associated with the back end server in the HSM of the back end server. Firmware may be needed for the HSM of the back end server to recreate the shared secret key and other diversified keys on the back end server. For example, the HSM may need to implement specific key diversification algorithms for generating a shared secret key and other diversified keys on the back end server. The specific key diversification algorithms can include static ECDH to maintain a consistent shared secret key for the card. The specific key diversification algorithms can also include seed keys to derive the keys.

**[0058]** In some embodiments, multifactor authentication of a user may be performed on a user device in order to generate a shared secret key for a card. For example, the multifactor authentication may include login credentials (user name and password) of the user, a one-time passcode, and so forth.

**[0059]** Figure 3 describes a contactless card 300 that can be used in the system 100 of Figure 1. For example, the card 120 in Figure 1 can be the contactless card 300 described herein. The contactless card 300 is configured to communicate with the user device 110 of system 100. The contactless card 300 may comprise a payment card, such as a credit card, debit card, or gift card, issued by a service provider 305 (such as a bank associated with the server 130) displayed on the front or back of the contactless card 300. In some examples, the contactless

card 300 is not related to a payment card, and may comprise, without limitation, an identification card, a membership card, and a transportation card. In some examples, the contactless card 300 may comprise a dual interface contactless payment card.

**[0060]** The contactless card 300 may comprise a substrate 310, 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 300 may have physical characteristics compliant with the ID-1 format of the ISO/IEC 7810 standard, and the contactless card 300 may otherwise be compliant with the ISO/IEC 14443 standard. However, it is understood that the contactless card 300 according to the present disclosure may have different characteristics, and the present disclosure does not require the contactless card 300 to be implemented in a payment card.

**[0061]** The contactless card 300 may also include identification information 315 displayed on the front and/or back of the contactless card 300, and a contact pad 320. The contact pad 320 may be configured to establish contact with another communication device, such as a user device, smart phone, laptop, desktop, point of sale (PoS), a vending machine, or tablet computer. The contactless card 300 may also include processing circuitry, antenna and other components. These components may be located behind the contact pad 320 or elsewhere on the substrate. The contactless card 300 may also include a magnetic strip or tape, or an EMV integrated circuitry chip, which may be located on the back of the contactless card 300.

**[0062]** Figure 4 illustrates an example contact pad 405 of the contactless card 300. The contact pad 405 of the contactless card 300 may include processing circuitry 410 for storing and processing information, including a processor 420 and a memory 425. It is understood that the

processing circuitry 410 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.

**[0063]** The memory 425 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 300 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-programmed many times after leaving the factory. It may also be read many times.

**[0064]** In some embodiments, the memory 425 may also have stored public and private card encryption keys. In some embodiments, the private and public encryption keys may be permanently hard-wired into the memory 425. In various embodiments, the memory 425 may have stored therein instructions for generating encrypted information and transmitting it to a receiving device (e.g., the user device 110). Such encrypted information may be or include an encrypted verification block or signature that may be used to authenticate and verify the presence of the card 300 during transaction processing. In some embodiments, encrypted information may be unique to a particular communication (e.g., a particular NFC transmission by the card 300).

**[0065]** The memory 425 may be configured to store one or more applets 430, one or more counters 435, and a unique customer identifier 440 (also referred to a card unique identification

number as above). The one or more applets 430 may comprise one or more software applications configured to execute on one or more contactless cards, such as Java Card applet. However, it is understood that the one or more applets 430 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 applets 430 may comprise an EMV applet. The one or more counters 435 may comprise a numeric counter sufficient to store an integer. The unique customer identifier 440 may comprise a unique alphanumeric identifier assigned to a user of the contactless card 300, and the identifier may distinguish the user of the contactless card 300 from other contactless card users. In some examples, the customer identifier 440 may identify both a customer and an account assigned to that customer and may further identify the contactless card 300 associated with the customer's account.

**[0066]** The processor 420 and memory 425 elements of the foregoing exemplary embodiments are described with reference to the contact pad 405, but the present disclosure is not limited thereto. It is understood that these elements may be implemented outside of the contact pad 405 or entirely separate from it, or as further elements in addition to the processor 420 and the memory 425 elements located within the contact pad 405.

**[0067]** In some examples, the contactless card 300 may comprise one or more antennas 415. The one or more antennas 415 may be placed within the contactless card 300 and around the processing circuitry 410 of the contact pad 405. For example, the one or more antennas 415 may be integral with the processing circuitry 410 and the one or more antennas 415 may be used with an external booster coil. As another example, the one or more antennas 415 may be external to the contact pad 405 and the processing circuitry 410.

**[0068]** In an embodiment, the coil of contactless card 300 may act as the secondary of an air core transformer. A terminal (such as the user device 110) may communicate with the

contactless card 300 by cutting power or amplitude modulation. The contactless card 300 may infer the data transmitted from the terminal using the gaps in the contactless card's power connection, which may be functionally maintained through one or more capacitors. The contactless card 300 may communicate back by switching a load on the contactless card's coil or load modulation. Load modulation may be detected in the terminal's coil through interference.

**[0069]** As explained above, the contactless card 300 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 (applet 430) may be securely executed. Applets may be added to contactless cards to provide a one-time password (OTP) for multifactor authentication (MFA) in various mobile application-based use cases. Applets 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 (the user device 110), and produce an NDEF message that comprises a cryptographically secure OTP encoded as an NDEF text tag.

**[0070]** The contactless card 300 may be configured for communication with the user device 110 via a communication interface configured for establishing communication with the user device 110. The communication interface may be configured for contact-based communication, in which case the interface may have electrical circuitry and contact pads on the surface of the card 300 for establishing direct electrical communication between the card 300 and the user device 110. Alternatively or in addition, the communication interface may be configured for contactless communication with the user device 110. In such embodiments, the communication interface may be or include an NFC communication interface configured for communication with other NFC communication devices when the card 300 is within a predetermined NFC range. In some embodiments, the card 300 may include a second

communication interface configured for establishing short range communication with the user device 110 via Bluetooth, or other short range communication methodology. In such embodiments, the card 300 may have a short range communication antenna that is included in or connected to the short range communication interface. The card 300 may also include a power management system for use in managing the distribution of power during an NFC transaction.

**[0071]** Figure 5 illustrates a flow chart of a method for dynamically generating a shared secret key for a transaction card on the back end server side according to an example embodiment. Figure 5 may reference the same or similar components as those illustrated in Figures 1-4, including a user device, a server, a database, and a contactless card. The method 500 can be implemented in the system 100 and may include, but is not limited to, the following steps.

**[0072]** At step 505, the server 130 may generate a public key and a private key of the server 130. The public key and the private key of the server 130 can be a key pair suitable for key agreement protocols such as elliptic curve cryptography.

**[0073]** At step 510, the server 130 may receive a public key of the card 120, from the user device 110. The public key of the card 120 is provisioned on the card 120 when the card 120 is manufactured. Upon tapping the card 120 to the user device 110, the card 120 can transmit the public key of the card 120 to the user device 110. The user device 110 can then transmit the public key of the card 120 to the server 130.

**[0074]** At step 515, the server 130 may generate a shared secret key based on the private key of the server 130 and the public key of the card 120 by using a key agreement protocol such as ECDH.

[0075] At step 520, the server 130 may store the public key of the card 120 on the database 140, such that the same shared secret key can be regenerated by the server 130 based on the public key of the card 120 when the card 120 is validated for future transactions.

[0076] At step 525, the server 130 may further store the shared secret key on the database 140. Although the shared secret key can be stored on the database 140 for later validation of the card 120, the same shared secret key may be preferably regenerated when validating the card 120 in the future.

[0077] Figure 6 illustrates a flow chart of an example method 600 for dynamically generating a shared secret key for a transaction card on the transaction card side according to an example embodiment. Figure 6 may reference the same or similar components as those illustrated in Figures 1-5, including a user device, a server, a database, and a contactless card. The method 600 can be implemented in the system 100 and may include, but is not limited to the following steps.

[0078] At step 605, a public key and a private key of the card 120 is generated. When a user is issued the card 120, the card 120 can be provisioned with a master key, a card unique identification number, the public key and the private key of the card 120. The user may tap the card 120 to the user device 110. Upon tapping the card 120, the card 120 may transmit to the user device 110 the public key and the private key of the card 120.

[0079] At step 610, the user device 110 may receive a public key of the server 130. The private key of the server 130 is kept by the server 130, such as on the database 140.

[0080] At step 615, the user device 110 can generate a shared secret key based on the public key of the server 130 and the private key of the card 120. The shared secret key can be generated using a key agreement protocol such as ECDH based on the public key of the server 130 and the private key of the card 120.

[0081] At step 620, the user device 110 may transmit the shared secret key to the card 120. The card 120 can store the shared secret key on the card 120.

[0082] Figure 7 illustrates a diagram 700 of tapping a transaction card to a mobile device according to an example embodiment. Figure 7 may reference the same or similar components as those illustrated in Figures 1-6, including a user device, a server, a database, and a contactless card.

[0083] Figure 7 illustrates near field communication (NFC) according to an exemplary embodiment. Generally, NFC is the transmission of data through electromagnetic radio fields which enable two or more devices to communicate with each other without touching. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. When two NFC-enabled devices are placed within a very small distances (e.g. a few centimeters), they can perform a transaction of information. NFC is beneficial to consumer transactions because it allows for near instantaneous reading of information. The receiving device reads the transmitted data the instant that it is sent. Therefore, human error is greatly reduced. Additionally, NFC reduces the time need to read a card. Rather than swipe a card through a reader, a consumer can simply touch the card or user device to an NFC enabled reader. Additionally, NFC reduces the risk of interference from fraudulent parties. Because NFC devices may communicate only over a very short distance, it is extremely difficult to intercept the information being sent between the devices.

[0084] Some examples of NFC communication include NFC card emulation where smartphones act like smart cards allowing users to perform transactions such as payment. As another example, NFC reader/writer communication allows devices to read information stored on NFC tags embedded into labels or smart posters. As another example, NFC peer-to-peer

communication allows two NFC-enabled devices to communicate with each other to exchange information.

**[0085]** NFC standards cover communications protocols and data exchange formats, and are based on existing RFID standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum.

**[0086]** In Figure 7, a user device 705 (such as the user device 110) and a contactless card 710 (such as the card 120) are interacting within an NFC field 715. The user device 705 is further explained with reference to Figure 1. The contactless card 710 is further explained with reference to Figures 3 and 4. Both the user device 705 and contactless card 710 may be enabled with NFC technology. The user device 705 and the card 710 are in close contact with each other so that they can exchange information within the communication field 715, for example by tapping the contactless card 710 to the user device 705 as described above.

**[0087]** Figure 8 is a flow chart of a method 800 for generating a cryptogram using a shared secret key on the transaction card side according to an example embodiment. Figure 8 may reference the same or similar components as those illustrated in Figures 1-7, including a user device, a server, a database, and a contactless card. The method 800 can be implemented in the system 100 and may include, but is not limited to the following steps.

**[0088]** When a transaction is conducted using the card 120, the card 120 can be tapped to the user device 110, as shown in Figure 7. At step 810, the card 120 may update the counter to increment the counter. The counter can be updated with every conversation between the card 120/the user device 110 and the server 130. The counter may comprise a numeric counter sufficient to store an integer. The card 120 may increment the counter one or more times.

**[0089]** As described above, the card 120 may be provisioned with a master symmetric key. At step 815, the card 120 may use the master symmetric key to generate an encryption session

key (ENC session key) and a message authentication code (MAC) session key through an appropriate symmetric cryptographic algorithm, which may include at least one of a symmetric encryption algorithm, HMAC algorithm, and a CMAC algorithm. The ENC session key and the MAC session key may be referred to as diversified keys. In some examples, the symmetric algorithm used to process the diversification value may comprise any symmetric cryptographic algorithm used as needed to generate the desired length diversified symmetric key. Non-limiting examples of the symmetric algorithm may include a symmetric encryption algorithm such as 3DES or AES128, a symmetric HMAC algorithm, such as HMAC-SHA-256, and a symmetric CMAC algorithm, such as AES-CMAC.

**[0090]** The card 120 may use the master symmetric key to process the counter to generate the two session keys: the ENC (encryption) session key and the MAC session key. The card 120 may encrypt the counter with the selected symmetric encryption algorithm using the master symmetric key to create the two session keys.

**[0091]** At step 820, the card 120 may generate the MAC over the counter, the unique customer identifier, and the shared secret key using the MAC session key. The shared secret key is generated using the private key of the card 120 and the public key of the server 130 and then stored on the card 120. The customer identifier may comprise a unique alphanumeric identifier assigned to a user of the contactless card, and the identifier may distinguish the user of the contactless card from other contactless card users. In some examples, the customer identifier may identify both a customer and an account assigned to that customer and may further identify the contactless card associated with the customer's account.

**[0092]** At step 825, the card 120 encrypts the MAC with the ENC session key. As encrypted, the MAC can become a cryptogram. In some examples, a cryptographic operation other than encryption may be performed, and a plurality of cryptographic operations may be performed

using the diversified symmetric keys prior to transmittal of the protected data.

**[0093]** In some examples, the MAC cryptogram can be a digital signature used to verify user information. Other digital signature algorithms, such as public key asymmetric algorithms, e.g., the Digital Signature Algorithm and the RSA algorithm, or zero knowledge protocols, may be used to perform this verification.

**[0094]** In step 830, the card 120 transmits the cryptogram to the user device 110. The user device 110 may further transmit the cryptogram to the server 130 for validation. The cryptogram can include the applet information of the card 120, the unique customer identifier, the counter, and the encrypted MAC.

**[0095]** Figure 9 is a flow chart of a method 900 for validating a cryptogram using a shared secret key on the back end server side according to an example embodiment. Figure 9 may reference the same or similar components as those illustrated in Figures 1-8, including a user device, a server, a database, and a contactless card. The method 900 can be implemented in the system 100 and may include, but is not limited to the following steps.

**[0096]** The user device 110 may transmit to the server 130 a first cryptogram of the card 120 for validation. In step 905, the server receives from the user device 110 the first cryptogram generated by the card 120.

**[0097]** In step 910, the server 130 may increase the counter value associated with the card 120. This counter value may be stored in the database and associated with the card 120 and the user of the card 120.

**[0098]** In step 915, the server 130 may retrieve from the database 140 the public key of the card 120 and the private key of the server 130. The public key of the card 120 was received by server 130 earlier from the user device 110.

[0099] In step 920, the server 130 generates the same shared secret key based on the public key of the card 120 and the private key of the server 130. The same shared secret key is generated by a key agreement protocol such as the ECDH encryption method, which is also used by the user device 110 to generate the same shared secret key.

[0100] In step 925, the server 130 can use the unique customer identifier of the card 120, the counter value, and/or the master key to generate two session keys: one ENC (encryption) session key and one MAC (message authentication code) session key.

[0101] In step 930, the server 130 generates a MAC over the counter, the unique customer identifier, and the shared secret key using the MAC session key.

[0102] In step 935, the server encrypts the MAC with the ENC session key. As encrypted, the MAC can become a second cryptogram.

[0103] In step 940, the server 130 may compare the first cryptogram with the second cryptogram to determine whether the first cryptogram matches with the second cryptogram.

[0104] In step 945, the server 130 may validate the first cryptogram. If the first cryptogram is determined to match with the second cryptogram, the first cryptogram can be validated. The card 120 can be validated accordingly.

[0105] Figure 10 is a flow chart of a method 1000 for dynamically generating a shared secret key between a transaction card and a back end server according to an example embodiment. Figure 10 may reference the same or similar components as those illustrated in Figures 1-9, including a user device, a server, a database, and a contactless card. The method 1000 can be implemented in the system 100 and may include, but is not limited to the following steps.

[0106] In step 1005, a transaction card such as the card 120 is provided. The transaction card is provisioned with a card private key and a card public key derived from the card private key. The transaction card may also be provisioned with a master key for deriving other keys.

[0107] In step 1010, a server such as the server 130 is provided. The server is provisioned with a server private key and a server public key derived from the server private key. The server may also be provisioned with a same master key for deriving other key.

[0108] In step 1015, a user device such as the user device 110 opens a communication field. The user device 110 can be in data communication with the transaction card and/or the server through the communication field.

[0109] In step 1020, the user device receives from the card the card public key. For example, the user device may read the card public key by tapping the card to the user device.

[0110] In step 1025, the user device transmits the card public key to the server. The server generates a shared secret key from the card public key and the server private key in accordance with a key agreement protocol. The server may store the shared secret key on a database such as the database 140.

[0111] In step 1030, the user device receives from the server the server public key.

[0112] In step 1035, the user device transmits the server public key to the transaction card. The transaction card generates the same shared secret key from the server public key and the card private key in accordance with the same key agreement protocol.

[0113] In some embodiments, the user device may generate the same shared secret key from the server public key and the card private key in accordance with the same key agreement protocol. The user device may then transmit the same shared secret key to the transaction card.

[0114] In some aspects, the techniques described herein relate to a system for generating a shared secret key for a transaction card, the system including: a transaction card including a card private key and a card public key derived from the card private key; a server including a server private key and a server public key derived from the server private key; and a user device configured to: open a communication field, read the card public key, transmit the card public

key to the server, wherein the server generates a shared secret key from the card public key and the server private key, receive the server public key from the server, and transmit the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

**[0115]** In some aspects, the techniques described herein relate to a system, wherein the card stores the shared secret key in a card memory.

**[0116]** In some aspects, the techniques described herein relate to a system, wherein the communication field includes at least one selected from the group of a near field communication (NFC) field, a radio-frequency identification (RFID) field, or Bluetooth.

**[0117]** In some aspects, the techniques described herein relate to a system, wherein the card is newly or recently issued.

**[0118]** In some aspects, the techniques described herein relate to a system, wherein both the card public key and server public key are further derived from a shared common value.

**[0119]** In some aspects, the techniques described herein relate to a system, wherein the shared common value is a unique identifier associated with the card.

**[0120]** In some aspects, the techniques described herein relate to a system, wherein the user device opens a second communication field and receives from the transaction card the shared secret key.

**[0121]** In some aspects, the techniques described herein relate to a system, wherein the server encrypts the shared secret key with a key encryption key, then stores the encrypted shared secret key in a data storage unit.

**[0122]** In some aspects, the techniques described herein relate to a system, wherein prior to storing the key, the server transmits an authentication request to the user device, then receives an authentication credential from the user device.

[0123] In some aspects, the techniques described herein relate to a method for generating a shared secret key for a transaction card, the system including: providing a transaction card including a card private key and a card public key derived from the card private key; providing a server including a server private key and a server public key derived from the server private key; opening, by a user device, a communication field; reading, by the user device, the card public key; transmitting, by the user device, the card public key to the server, wherein the server generates a shared secret key from the card public key and the server private key; receiving, by the user device, the server public key from the server; and transmitting, by the user device, the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

[0124] In some aspects, the techniques described herein relate to a method, wherein the communication field includes at least one selected from the group of a near field communication (NFC) field, a radio-frequency identification (RFID) field, or Bluetooth.

[0125] In some aspects, the techniques described herein relate to a method, further including authenticating the user device based on the shared secret key.

[0126] In some aspects, the techniques described herein relate to a method, further including automatically initiating the key exchange process upon detecting proximity to the transaction card.

[0127] In some aspects, the techniques described herein relate to a method, wherein the user device and the transaction card are associated the same user.

[0128] In some aspects, the techniques described herein relate to a method, further including requesting an authentication credential from the user associated with the user device before initiating the key exchange process.

[0129] In some aspects, the techniques described herein relate to a method, further including

generating a unique transaction-specific shared secret key for each transaction.

**[0130]** In some aspects, the techniques described herein relate to a method, wherein the method further includes: receiving, by the user device from the server, a request for the shared secret key; transmitting, by the user device to the server, the shared secret key; and receiving, by the user device from the server, a validation response indicating that the shared secret key from the card matches the shared secret key on the server.

**[0131]** In some aspects, the techniques described herein relate to a method, wherein the method further includes generating a unique session specific shared secret key for each transaction.

**[0132]** In some aspects, the techniques described herein relate to a method, wherein the encryption data includes at least one selected from the group of a unique user identification datum, a unique card datum, or time datum.

**[0133]** In some aspects, the techniques described herein relate to a non-transitory computer readable medium containing computer executable instructions that, when executed by a computer hardware arrangement, cause the computer hardware arrangement to perform procedures including: opening a communication field; reading, from a card upon entering the communication field, the card public key; transmitting, the card public key to a server, wherein the server generates a shared secret key from the card public key and the server private key; receiving, the server public key from the server; and transmitting, the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

**[0134]** Throughout the disclosure, the terms “bank” or “issuer bank” are used, and it is understood that the present disclosure is not limited to a particular bank or type of bank. Rather, the present disclosure includes any type of bank, account and/or card issuer, or other entity involved in the creation, issuance, or provisioning of accounts or cards associated with

accounts.

**[0135]** As used herein, the term “account” is not limited to a particular type of account. Rather, it is understood that the term “account” can refer to a variety of accounts, including without limitation, a financial account (e.g., a credit account, a debit account), a membership account, a loyalty account, a subscription account, a services account, a utilities account, a transportation account, and a physical access account. It is further understood that the present disclosure is not limited to accounts issued by a particular entity.

**[0136]** In some examples, exemplary procedures in accordance with the present disclosure described herein can be performed by a processing arrangement and/or a computing arrangement (e.g., a computer hardware arrangement). Such processing and/or computing arrangement can be, for example entirely or a part of, or include, but not limited to, a computer/processor that can include, for example one or more microprocessors, and use instructions stored on a computer-accessible medium (e.g., RAM, ROM, hard drive, or other storage device). For example, a computer-accessible medium can be part of the memory of a first device, a user device, a server, or other computer hardware arrangement.

**[0137]** In some examples, a computer-accessible medium (e.g., as described herein above, a storage device such as a hard disk, floppy disk, memory stick, CD-ROM, RAM, ROM, etc., or a collection thereof) can be provided (e.g., in communication with the processing arrangement). The computer-accessible medium can contain executable instructions thereon. In addition or alternatively, a storage arrangement can be provided separately from the computer-accessible medium, which can provide the instructions to the processing arrangement so as to configure the processing arrangement to execute certain exemplary procedures, processes, and methods, as described herein above, for example.

[0138] It is further noted that the systems and methods described herein may be tangibly embodied in one or more physical media, such as, but not limited to, a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a hard drive, read only memory (ROM), random access memory (RAM), as well as other physical media capable of data storage. For example, data storage may include random access memory (RAM) and read only memory (ROM), which may be configured to access and store data and information and computer program instructions. Data storage may also include storage media or other suitable type of memory (e.g., such as, for example, RAM, ROM, programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), magnetic disks, optical disks, floppy disks, hard disks, removable cartridges, flash drives, and any type of tangible and non-transitory storage medium), where the files that comprise an operating system, application programs including, for example, web browser application, email application and/or other applications, and data files may be stored. The data storage of the network-enabled computer systems may include electronic information, files, and documents stored in various ways, including, for example, a flat file, indexed file, hierarchical database, relational database, such as a database created and maintained with software from, for example, Oracle® Corporation, Microsoft® Excel file, Microsoft® Access file, a solid state storage device, which may include a flash array, a hybrid array, or a server-side product, enterprise storage, which may include online or cloud storage, or any other storage mechanism. Moreover, the figures illustrate various components (e.g., servers, computers, processors, etc.) separately. The functions described as being performed at various components may be performed at other components, and the various components may be combined or separated. Other modifications also may be made.

[0139] Computer readable program instructions described herein can be downloaded to respective computing and/or processing devices from a computer readable storage medium or to an external computer or external storage device via a network, for example, the Internet, a local area network, a wide area network and/or a wireless network. The network may comprise copper transmission cables, optical transmission fibers, wireless transmission, routers, firewalls, switches, gateway computers and/or edge servers. A network adapter card or network interface in each computing and/or processing device receives computer readable program instructions from the network and forwards the computer readable program instructions for storage in a computer readable storage medium within the respective computing and/or processing device.

[0140] Computer readable program instructions for carrying out operations of the present invention may be assembler instructions, instruction-set-architecture (ISA) instructions, machine instructions, machine dependent instructions, microcode, firmware instructions, state-setting data, or either source code or object code written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like, and conventional procedural programming languages, such as the “C” programming language or similar programming languages. The computer readable program instructions may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider). In some embodiments, electronic circuitry including, for example, programmable logic circuitry,

field-programmable gate arrays (FPGA), or programmable logic arrays (PLA) may execute the computer readable program instructions by utilizing state information of the computer readable program instructions to personalize the electronic circuitry, to perform aspects of the present invention.

**[0141]** These computer readable program instructions may be provided to a processor of a general-purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions specified herein. These computer-readable program instructions may also be stored in a computer-readable storage medium that can direct a computer, a programmable data processing apparatus, and/or other devices to function in a manner, such that the computer readable storage medium having instructions stored therein comprises an article of manufacture including instructions which implement aspects of the functions specified herein.

**[0142]** The computer readable program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other device to cause a series of operational steps to be performed on the computer, other programmable apparatus or other device to produce a computer implemented process, such that the instructions which execute on the computer, other programmable apparatus, or other device implement the functions specified herein.

**[0143]** Implementations of the various techniques described herein may be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Implementations may be implemented as a computer program product, e.g., a computer program tangibly embodied in an information carrier, e.g., in a machine readable storage device or in a propagated signal, for execution by, or to control the operation of, data processing apparatus, e.g., a programmable processor, a computer, or multiple computers. A

computer program, such as the computer program(s) described above, can be written in any form of programming language, including compiled or interpreted languages, and can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one site or distributed across multiple sites and interconnected by a communication network.

**[0144]** Method steps may be performed by one or more programmable processors executing a computer program to perform functions by operating on input data and generating output. Method steps also may be performed by, and an apparatus may be implemented as, special purpose logic circuitry, e.g., an FPGA (field programmable gate array) or an ASIC (application specific integrated circuit).

**[0145]** Throughout the disclosure, the following terms take at least the meanings explicitly associated herein, unless the context clearly dictates otherwise. The term “or” is intended to mean an inclusive “or.” Further, the terms “a,” “an,” and “the” are intended to mean one or more unless specified otherwise or clear from the context to be directed to a singular form.

**[0146]** In this description, numerous specific details have been set forth. It is to be understood, however, that implementations of the disclosed technology may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description. References to “some examples,” “other examples,” “one example,” “an example,” “various examples,” “one embodiment,” “an embodiment,” “some embodiments,” “example embodiment,” “various embodiments,” “one implementation,” “an implementation,” “example implementation,” “various implementations,” “some implementations,” etc., indicate that the implementation(s) of the disclosed technology so described may include a particular feature,

structure, or characteristic, but not every implementation necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrases “in one example,” “in one embodiment,” or “in one implementation” does not necessarily refer to the same example, embodiment, or implementation, although it may.

[0147] As used herein, unless otherwise specified the use of the ordinal adjectives “first,” “second,” “third,” etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0148] While certain implementations of the disclosed technology have been described in connection with what is presently considered to be the most practical and various implementations, it is to be understood that the disclosed technology is not to be limited to the disclosed implementations, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

[0149] This written description uses examples to disclose certain implementations of the disclosed technology, including the best mode, and also to enable any person skilled in the art to practice certain implementations of the disclosed technology, including making and using any devices or systems and performing any incorporated methods. The patentable scope of certain implementations of the disclosed technology is defined in the claims, and may include other examples that occur to those skilled in the art. Such other examples are intended to be within the scope of the claims if they have structural elements that do not differ from the literal language of the claims, or if they include equivalent structural elements with insubstantial differences from the literal language of the claims.

## CLAIMS

What is claimed is:

1. A system for generating a shared secret key for a transaction card, the system comprising:
  - a transaction card comprising a card private key and a card public key derived from the card private key;
  - a server comprising a server private key and a server public key derived from the server private key; and
  - a user device configured to:
    - open a communication field,
    - read the card public key,
    - transmit the card public key to the server, wherein the server generates a shared secret key from the card public key and the server private key,
    - receive the server public key from the server, and
    - transmit the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.
2. The system of claim 1, wherein the card stores the shared secret key in a card memory.
3. The system of claim 1, wherein the communication field comprises at least one selected from the group of a near field communication (NFC) field, a radio-frequency identification (RFID) field, or Bluetooth.
4. The system of claim 1, wherein the card is newly or recently issued.

5. The system of claim 1, wherein both the card public key and server public key are further derived from a shared common value.

6. The system of claim 5, wherein the shared common value is a unique identifier associated with the card.

7. The system of claim 1, wherein the user device opens a second communication field and receives from the transaction card the shared secret key.

8. The system of claim 1, wherein the server encrypts the shared secret key with a key encryption key, then stores the encrypted shared secret key in a data storage unit.

9. The system of claim 8, wherein prior to storing the key, the server transmits an authentication request to the user device, then receives an authentication credential from the user device.

10. A method for generating a shared secret key for a transaction card, comprising:

providing a transaction card comprising a card private key and a card public key

derived from the card private key;

providing a server comprising a server private key and a server public key derived

from the server private key;

opening, by a user device, a communication field;

reading, by the user device, the card public key;

transmitting, by the user device, the card public key to the server, wherein the server

generates a shared secret key from the card public key and the server private key;

receiving, by the user device, the server public key from the server; and

transmitting, by the user device, the server public key to the transaction card, wherein the card generates the same shared secret key from the server public key and the card private key.

11. The method of claim 10, wherein the communication field comprises at least one selected from the group of a near field communication (NFC) field, a radio-frequency identification (RFID) field, or Bluetooth.

12. The method of claim 10, further comprising authenticating the user device based on the shared secret key.

13. The method of claim 10, further comprising automatically initiating a key exchange process upon detecting proximity to the transaction card.

14. The method of claim 10, wherein the user device and the transaction card are associated the same user.

15. The method of claim 10, further comprising requesting an authentication credential from the user associated with the user device before initiating a key exchange process.

16. The method of claim 10, further comprising generating a unique transaction-specific

shared secret key for each transaction.

17. The method of claim 10, further comprising:

- receiving, by the user device from the server, a request for the shared secret key;
- transmitting, by the user device to the server, the shared secret key; and
- receiving, by the user device from the server, a validation response indicating that the shared secret key from the card matches the shared secret key on the server.

18. The method of claim 10, wherein the method further comprises generating a unique session specific shared secret key for each transaction.

19. The method of claim 18, wherein encryption data includes at least one selected from the group of a unique user identification datum, a unique card datum, or time datum.

20. A non-transitory computer readable medium containing computer executable instructions that, when executed by a computer hardware arrangement, cause the computer hardware arrangement to perform procedures comprising:

- opening a communication field;
- reading, from a transaction card upon entering the communication field, a card public key;
- transmitting the card public key to a server, wherein the server generates a shared secret key from the card public key and a server private key;
- receiving a server public key from the server; and
- transmitting the server public key to the transaction card, wherein the transaction card

generates the same shared secret key from the server public key and a card private key.

System 100

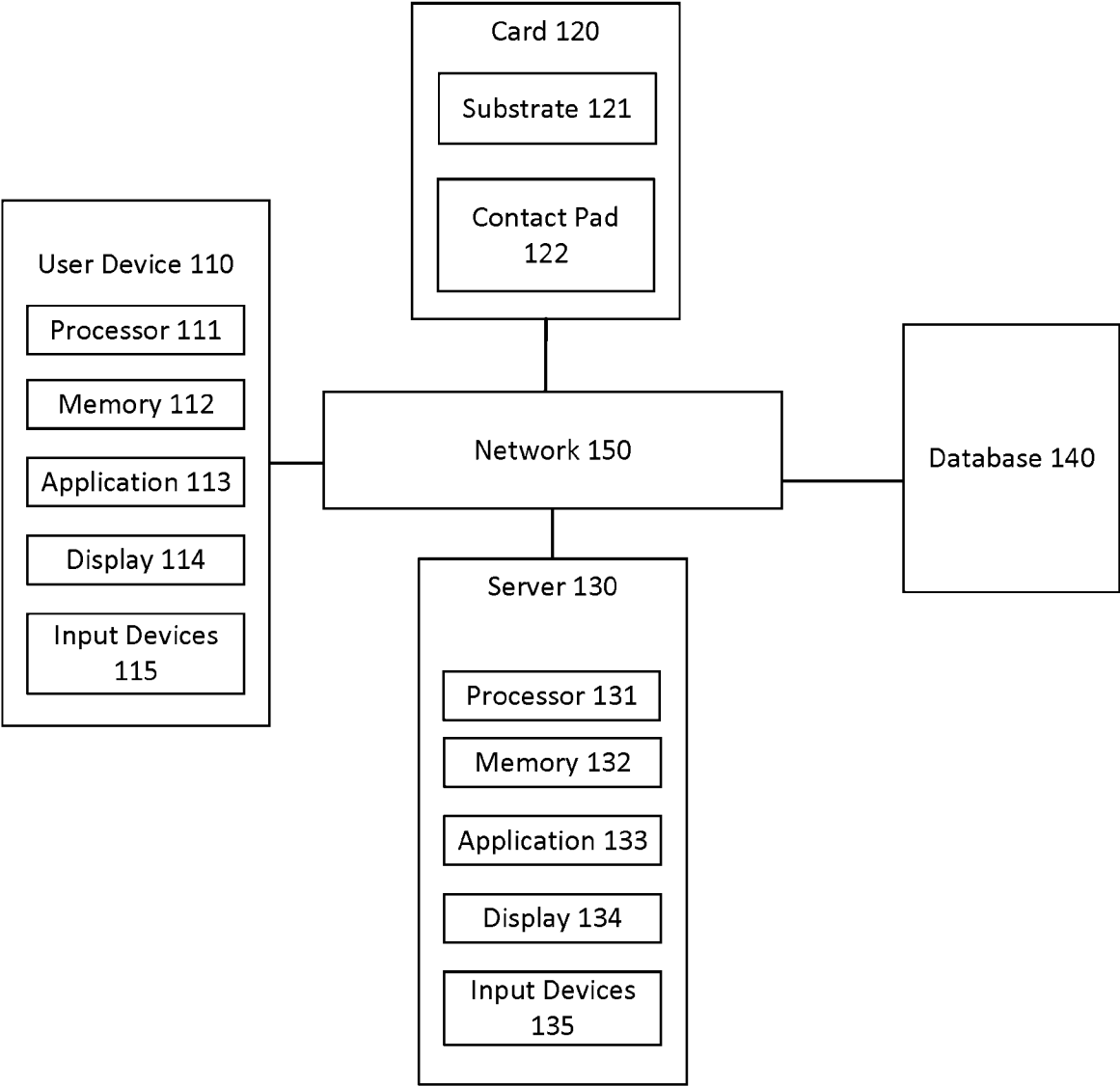
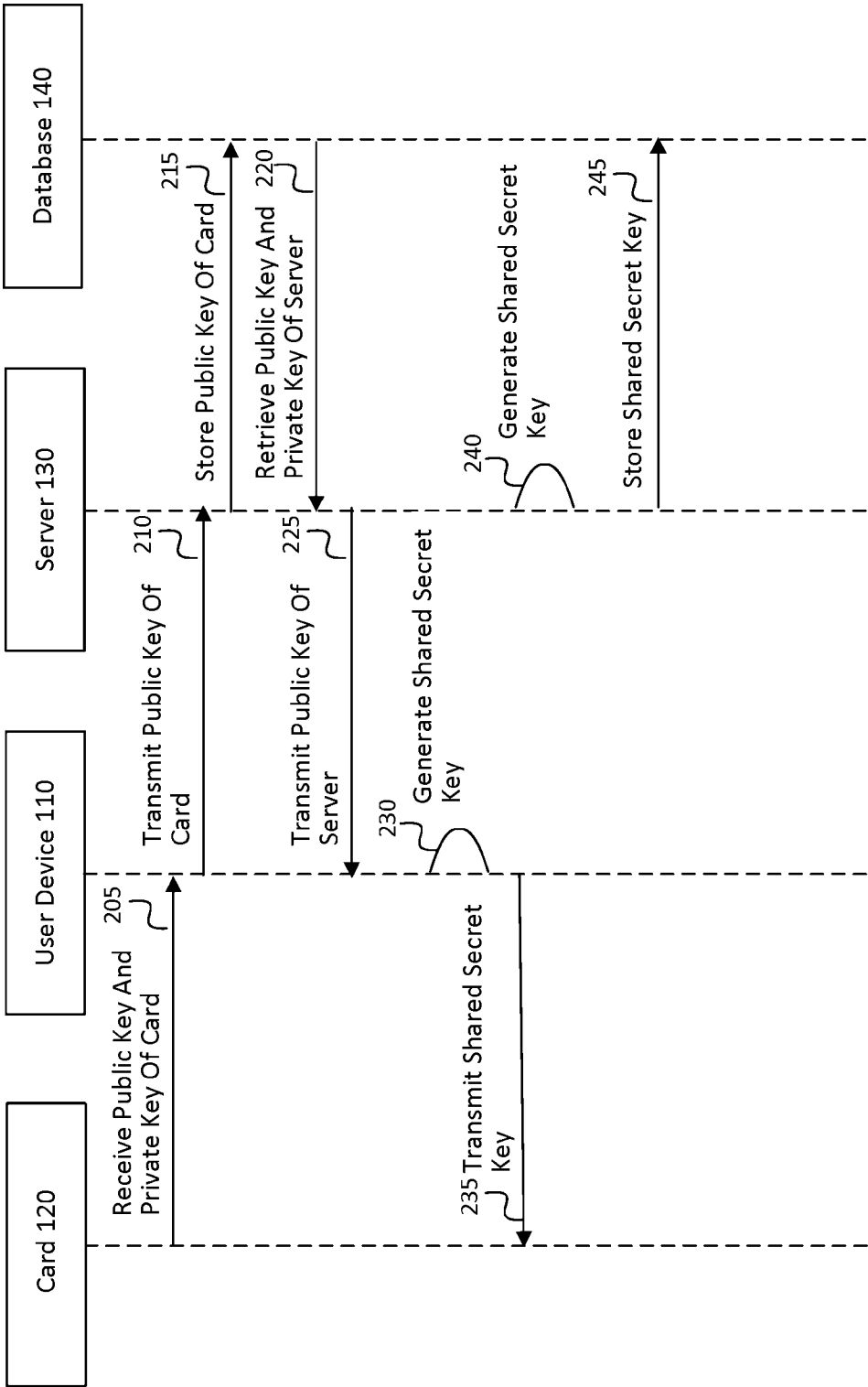


FIG. 1



200

FIG. 2

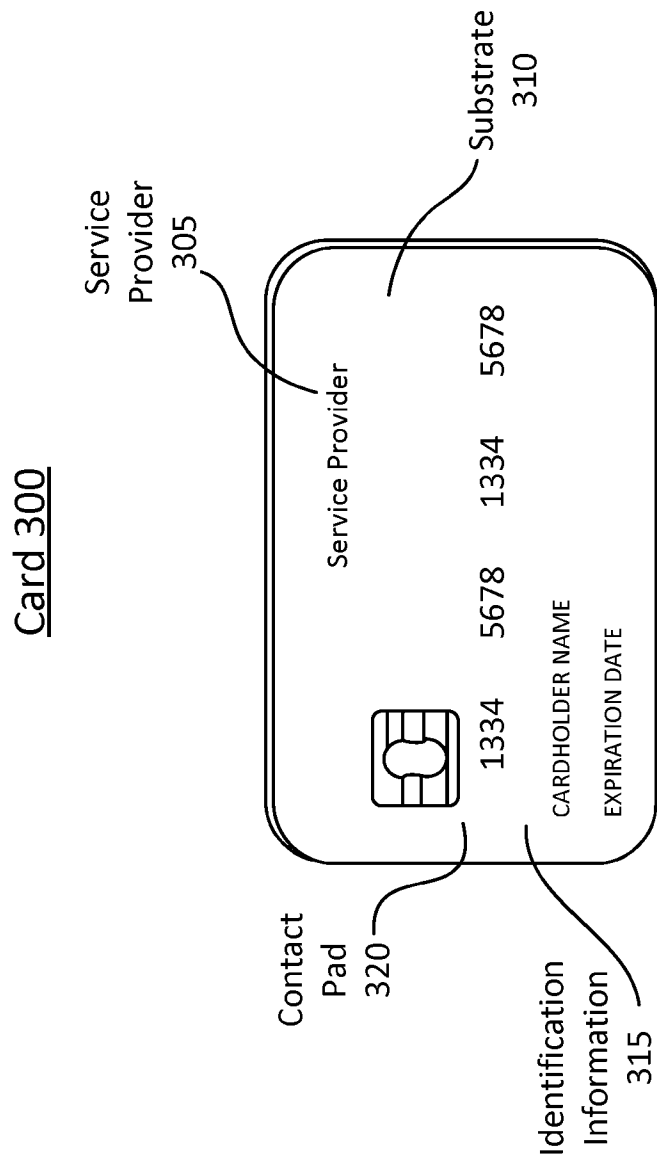


**FIG. 3**

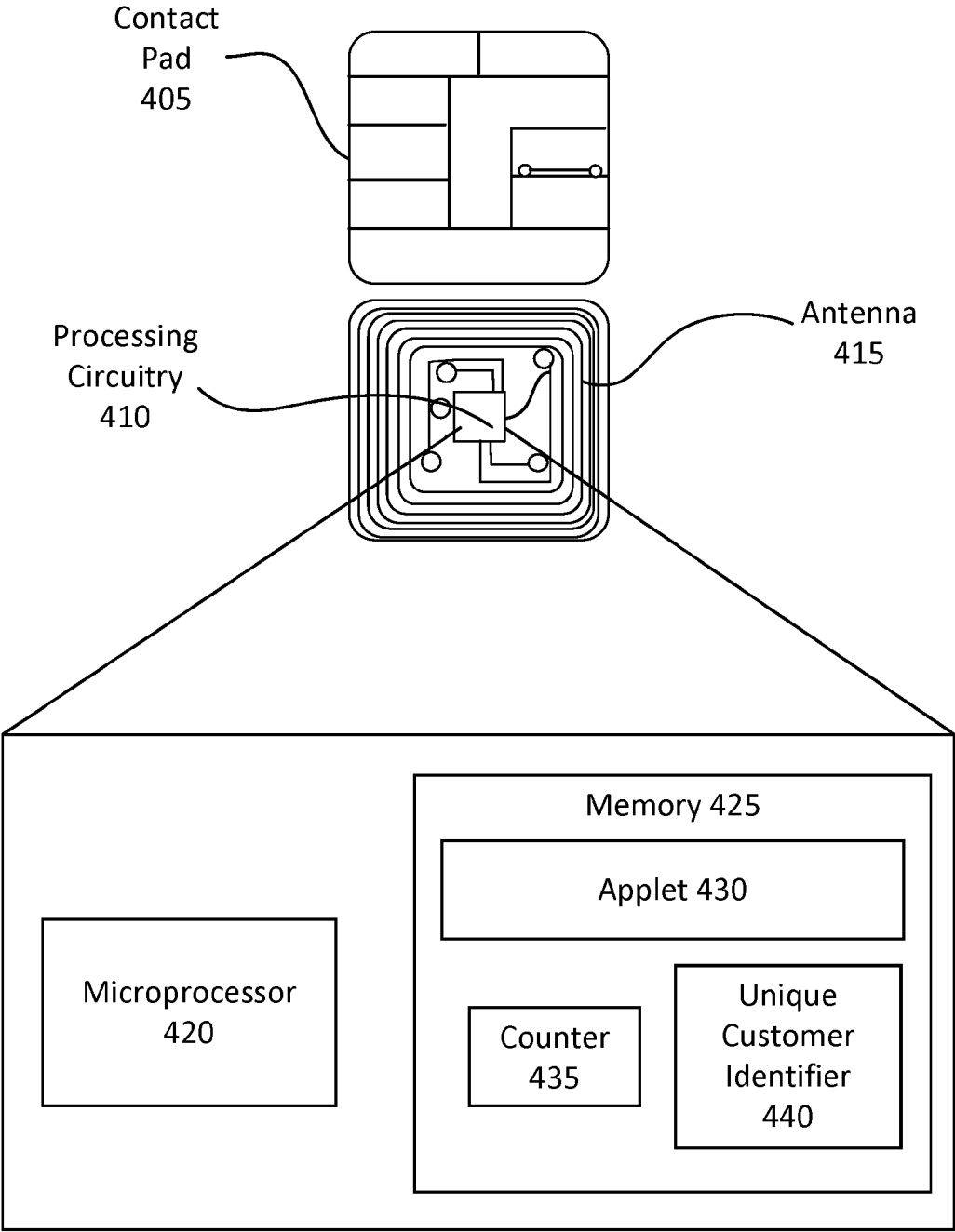
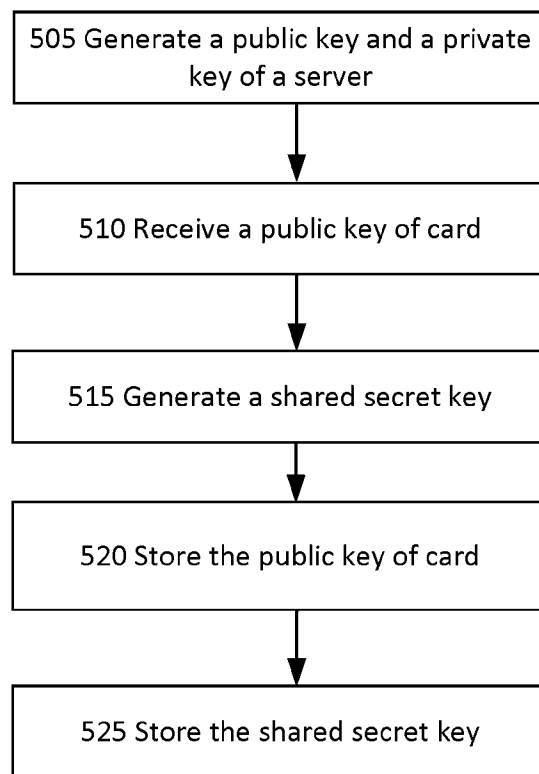


FIG. 4

Method 500**FIG. 5**

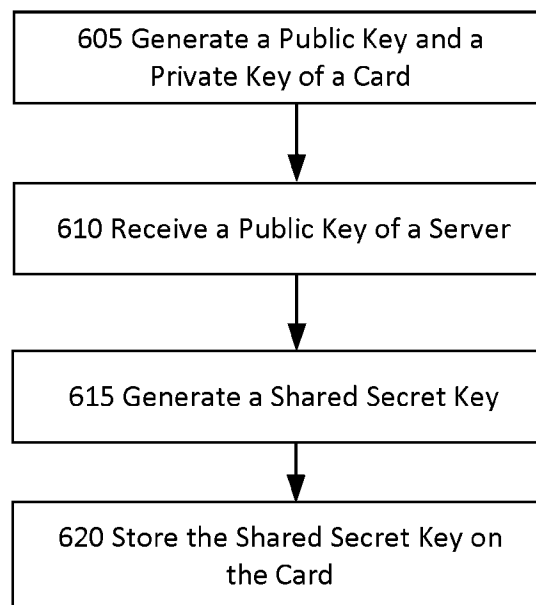
Method 600**FIG. 6**

Diagram 700

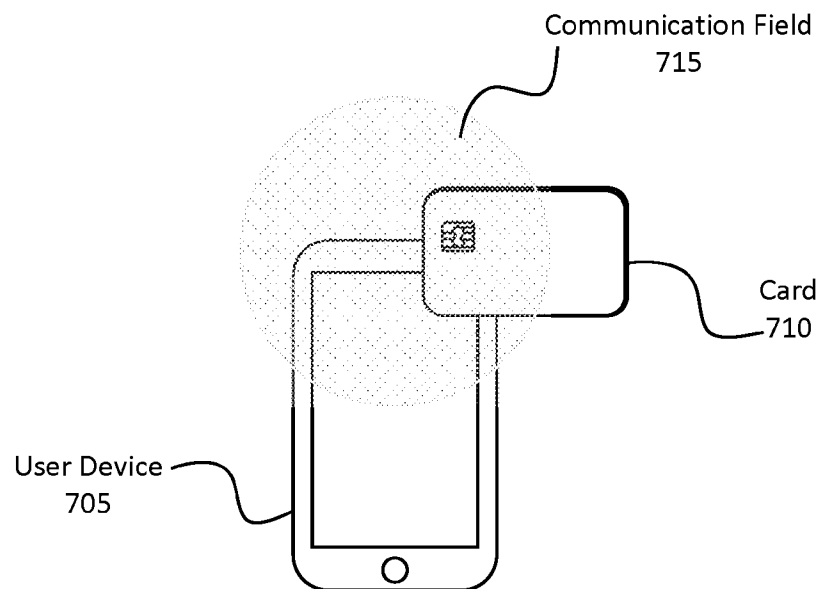
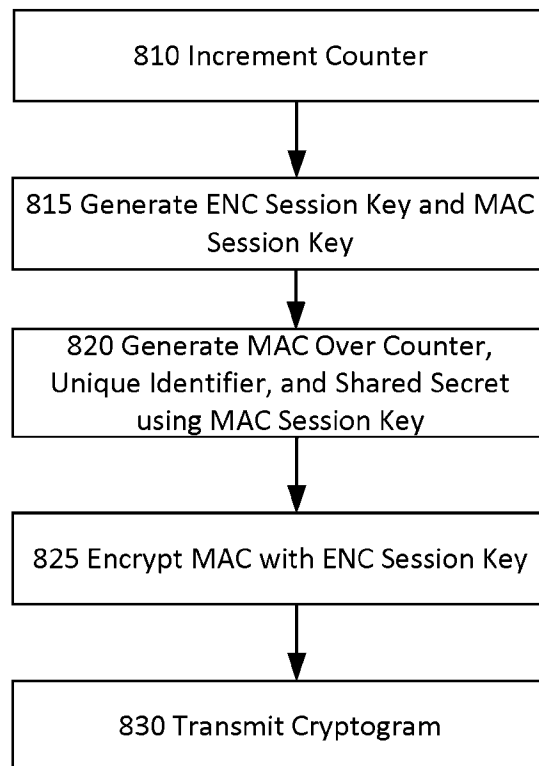
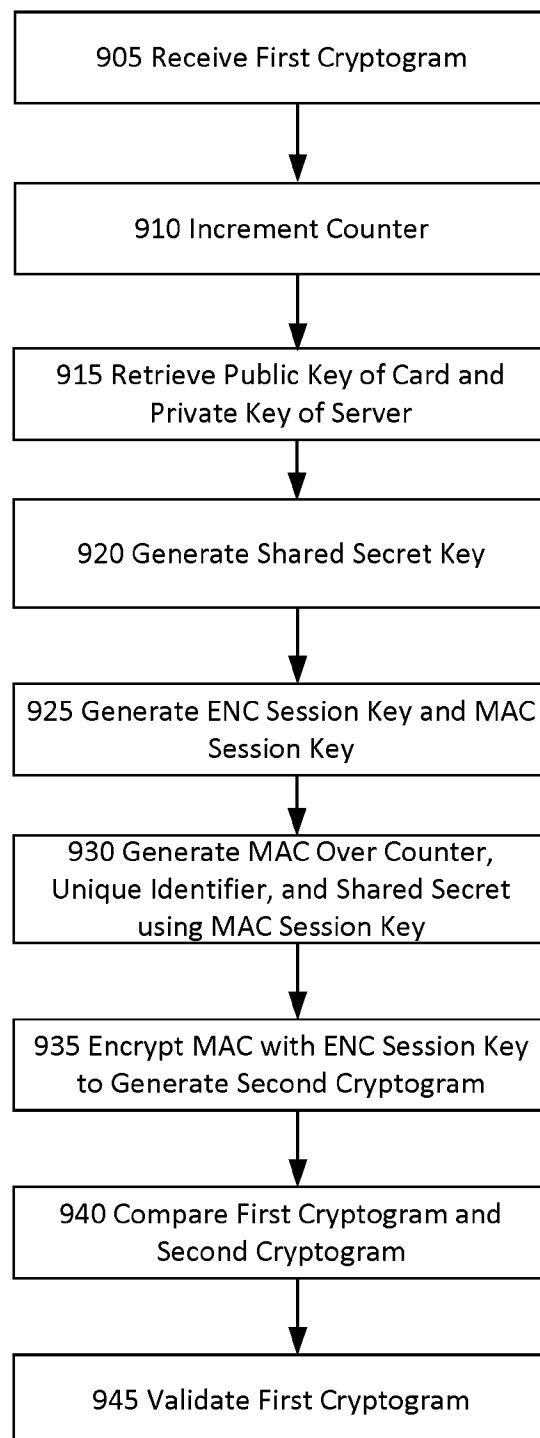
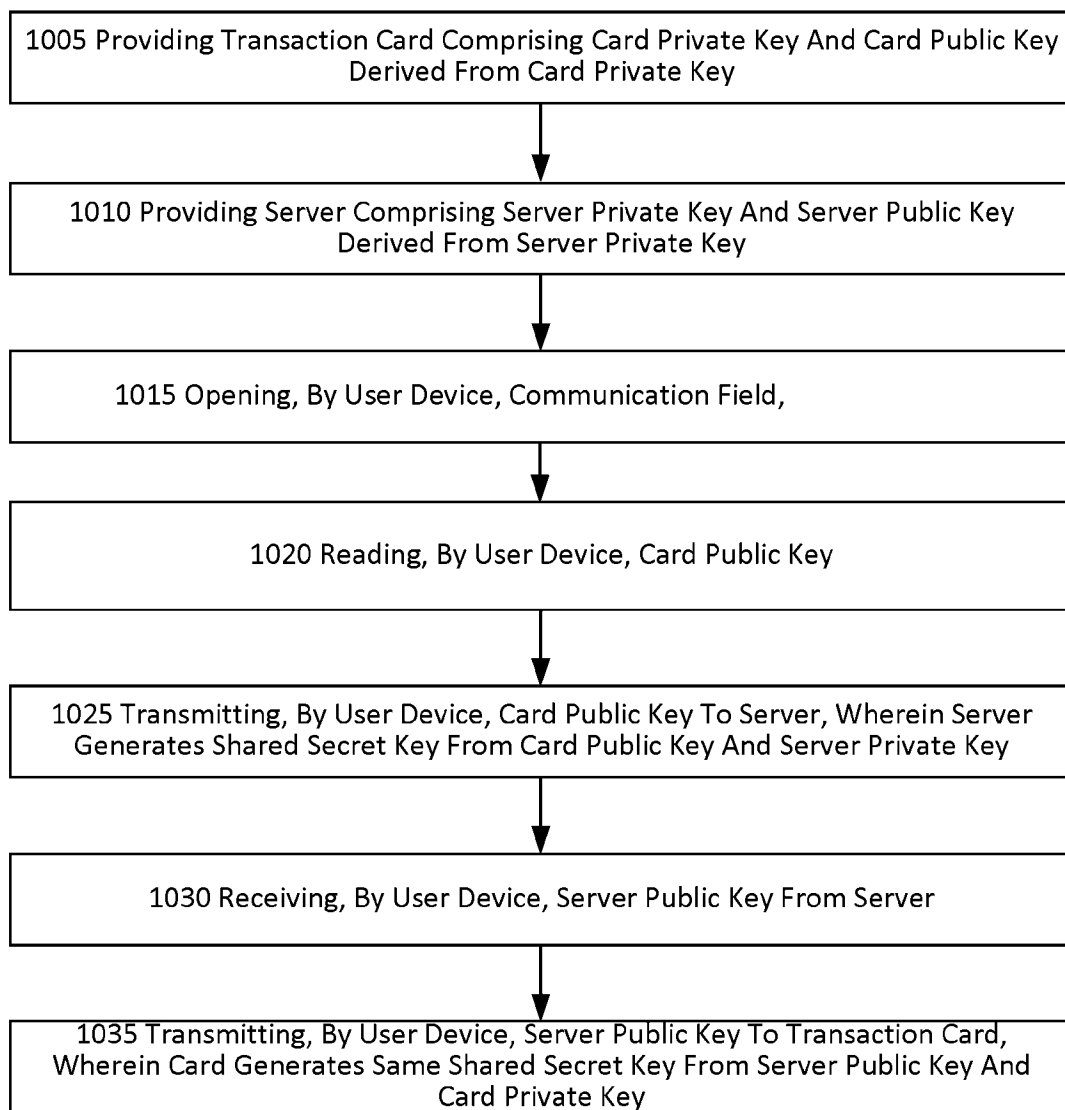


**FIG. 7**

Method 800**FIG. 8**

Method 900**FIG. 9**

Method 1000**FIG. 10**

## INTERNATIONAL SEARCH REPORT

International application No

PCT/US2024/062387

|                                                                                                                                                                         |                                                                                                                                                                                                                                                  |                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>A. CLASSIFICATION OF SUBJECT MATTER</b>                                                                                                                              |                                                                                                                                                                                                                                                  |                       |
| INV.                                                                                                                                                                    | H04W12/041                                                                                                                                                                                                                                       | H04W12/047            |
|                                                                                                                                                                         | G06Q20/32                                                                                                                                                                                                                                        | G06Q20/34             |
| ADD.                                                                                                                                                                    |                                                                                                                                                                                                                                                  |                       |
| According to International Patent Classification (IPC) or to both national classification and IPC                                                                       |                                                                                                                                                                                                                                                  |                       |
| <b>B. FIELDS SEARCHED</b>                                                                                                                                               |                                                                                                                                                                                                                                                  |                       |
| Minimum documentation searched (classification system followed by classification symbols)                                                                               |                                                                                                                                                                                                                                                  |                       |
| H04W H04L G06Q                                                                                                                                                          |                                                                                                                                                                                                                                                  |                       |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched                                           |                                                                                                                                                                                                                                                  |                       |
| Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)                                            |                                                                                                                                                                                                                                                  |                       |
| EPO-Internal                                                                                                                                                            |                                                                                                                                                                                                                                                  |                       |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>                                                                                                                           |                                                                                                                                                                                                                                                  |                       |
| Category*                                                                                                                                                               | Citation of document, with indication, where appropriate, of the relevant passages                                                                                                                                                               | Relevant to claim No. |
| X                                                                                                                                                                       | EP 3 534 565 A1 (ALIBABA GROUP HOLDING LTD [KY]) 4 September 2019 (2019-09-04)<br>figure 1A<br>paragraphs [0002], [0046], [0073], [0075], [0125], [0126], [0139], [0144], [0149] - [0150], [0170]<br>-----                                       | 1 - 20                |
| A                                                                                                                                                                       | US 2022/366410 A1 (RULE JEFFREY [US] ET AL) 17 November 2022 (2022-11-17)<br>paragraphs [0076] - [0077], [0086] - [0088], [0117] - [0119]<br>-----                                                                                               | 1 - 20                |
| A                                                                                                                                                                       | WO 2020/181161 A1 (MASTERCARD INTERNATIONAL INC [US])<br>10 September 2020 (2020-09-10)<br>pages 13-23<br>-----                                                                                                                                  | 1 - 20                |
| <input type="checkbox"/> Further documents are listed in the continuation of Box C.                                                                                     |                                                                                                                                                                                                                                                  |                       |
| <input checked="" type="checkbox"/> See patent family annex.                                                                                                            |                                                                                                                                                                                                                                                  |                       |
| <b>* Special categories of cited documents :</b>                                                                                                                        |                                                                                                                                                                                                                                                  |                       |
| "A" document defining the general state of the art which is not considered to be of particular relevance                                                                | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention                                              |                       |
| "E" earlier application or patent but published on or after the international filing date                                                                               | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone                                                                     |                       |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |                       |
| "O" document referring to an oral disclosure, use, exhibition or other means                                                                                            | "&" document member of the same patent family                                                                                                                                                                                                    |                       |
| "P" document published prior to the international filing date but later than the priority date claimed                                                                  |                                                                                                                                                                                                                                                  |                       |
| Date of the actual completion of the international search                                                                                                               | Date of mailing of the international search report                                                                                                                                                                                               |                       |
| 19 February 2025                                                                                                                                                        | 03/03/2025                                                                                                                                                                                                                                       |                       |
| Name and mailing address of the ISA/<br>European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016    | Authorized officer<br><br>Kufer, Léna                                                                                                                                                                                                            |                       |

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2024/062387

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s) | Publication<br>date |            |            |                  |            |
|-------------------------------------------|---------------------|----------------------------|---------------------|------------|------------|------------------|------------|
| EP 3534565                                | A1                  | 04-09-2019                 | AU 2017352361 A1    | 23-05-2019 |            |                  |            |
|                                           |                     |                            | AU 2019101594 A4    | 23-01-2020 |            |                  |            |
|                                           |                     |                            | BR 112019008371 A2  | 09-07-2019 |            |                  |            |
|                                           |                     |                            | CA 3041664 A1       | 03-05-2018 |            |                  |            |
|                                           |                     |                            | CN 107040369 A      | 11-08-2017 |            |                  |            |
|                                           |                     |                            | CN 111585749 A      | 25-08-2020 |            |                  |            |
|                                           |                     |                            | EP 3534565 A1       | 04-09-2019 |            |                  |            |
|                                           |                     |                            | ES 2837039 T3       | 29-06-2021 |            |                  |            |
|                                           |                     |                            | JP 7119040 B2       | 16-08-2022 |            |                  |            |
|                                           |                     |                            | JP 2019533384 A     | 14-11-2019 |            |                  |            |
|                                           |                     |                            | JP 2021083076 A     | 27-05-2021 |            |                  |            |
|                                           |                     |                            | KR 20190073472 A    | 26-06-2019 |            |                  |            |
|                                           |                     |                            | KR 20200127264 A    | 10-11-2020 |            |                  |            |
|                                           |                     |                            | PH 12019500938 A1   | 11-12-2019 |            |                  |            |
|                                           |                     |                            | RU 2715163 C1       | 25-02-2020 |            |                  |            |
|                                           |                     |                            | SG 11201903671W A   | 30-05-2019 |            |                  |            |
|                                           |                     |                            | TW 201817193 A      | 01-05-2018 |            |                  |            |
|                                           |                     |                            | US 2019253249 A1    | 15-08-2019 |            |                  |            |
|                                           |                     |                            | WO 2018077086 A1    | 03-05-2018 |            |                  |            |
|                                           |                     |                            | ZA 201902947 B      | 26-08-2020 |            |                  |            |
|                                           |                     |                            | -----               |            |            |                  |            |
|                                           |                     |                            | US 2022366410       | A1         | 17-11-2022 | AU 2022272897 A1 | 09-11-2023 |
|                                           |                     |                            |                     |            |            | CA 3216450 A1    | 17-11-2022 |
| CN 117321620 A                            | 29-12-2023          |                            |                     |            |            |                  |            |
| EP 4338112 A1                             | 20-03-2024          |                            |                     |            |            |                  |            |
| JP 2024520925 A                           | 27-05-2024          |                            |                     |            |            |                  |            |
| KR 20240007169 A                          | 16-01-2024          |                            |                     |            |            |                  |            |
| US 2022366410 A1                          | 17-11-2022          |                            |                     |            |            |                  |            |
| WO 2022240484 A1                          | 17-11-2022          |                            |                     |            |            |                  |            |
| -----                                     |                     |                            |                     |            |            |                  |            |
| WO 2020181161                             | A1                  | 10-09-2020                 | EP 3935594 A1       | 12-01-2022 |            |                  |            |
|                                           |                     |                            | EP 3935595 A1       | 12-01-2022 |            |                  |            |
|                                           |                     |                            | SG 11202108393Q A   | 30-08-2021 |            |                  |            |
|                                           |                     |                            | SG 11202108394T A   | 30-08-2021 |            |                  |            |
|                                           |                     |                            | US 2020286085 A1    | 10-09-2020 |            |                  |            |
|                                           |                     |                            | US 2020286098 A1    | 10-09-2020 |            |                  |            |
|                                           |                     |                            | US 2022335436 A1    | 20-10-2022 |            |                  |            |
|                                           |                     |                            | WO 2020181161 A1    | 10-09-2020 |            |                  |            |
| WO 2020181162 A1                          | 10-09-2020          |                            |                     |            |            |                  |            |
| -----                                     |                     |                            |                     |            |            |                  |            |