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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
04 November 2021 (04.11.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/222158 A1

(51) International Patent Classification:
G06F 21/35 (2013.01) *G06F 21/62* (2013.01)
G06F 21/44 (2013.01) *H04L 9/32* (2006.01)
G06F 21/60 (2013.01)

(21) International Application Number:
PCT/US2021/029277

(22) International Filing Date:
27 April 2021 (27.04.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/863,750 30 April 2020 (30.04.2020) US

(71) Applicant: **CAPITAL ONE SERVICES, LLC** [US/US]; 1680 Capital One Dr., McLean, Virginia 22102 (US).

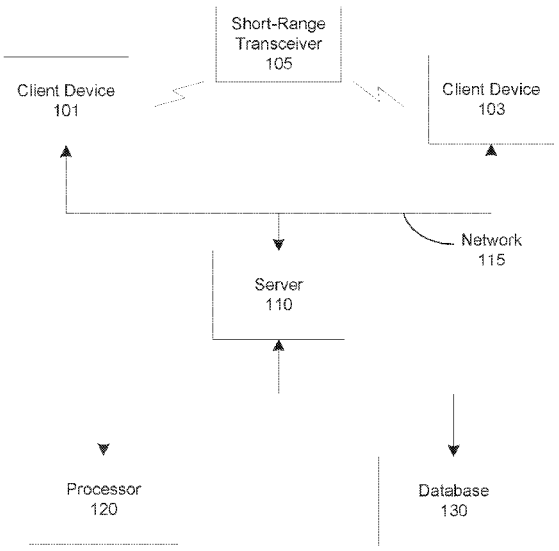
(72) Inventors: **ILINCIC, Rajko**; 1680 Capital One Drive, McLean, Virginia 22102 (US). **RULE, Jeffrey**; 1680 Capital One Dr., McLean, Virginia 22102 (US).

(74) Agent: **KASNEVICH, Andrew D.** et al.; Hunton Andrews Kurth LLP, Intellectual Property Department, 2200 Pennsylvania Ave., NW, Washington, District of Columbia 20037 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: SYSTEMS AND METHODS FOR DATA ACCESS CONTROL OF PERSONAL USER DATA USING A SHORT-RANGE TRANSCEIVER



System 100

FIG. 1A

(57) Abstract: Systems and methods for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device are presented. An exemplary system and method may include establishing a database storing identifiers and keys for users and service providers, receiving from a client device of the service provider, via a network, a service provider token and a request for a data access key, the request generated in response to a tap action between a contactless card associated with a user and the client device, verifying the service provider is authorized to receive access to personal user data encrypted and stored on the contactless card, generating a data access key based on a user key, and transmitting to the service provider client device, via the network, the data access key, such that the client device may decrypt the personal user data obtained from the contactless card.

WO 2021/222158 A1

[Continued on next page]

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

SYSTEMS AND METHODS FOR DATA ACCESS CONTROL OF PERSONAL USER DATA USING A SHORT-RANGE TRANSCEIVER

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application No. 16/863750 filed April 30, 2020, the disclosure of which is incorporated herein by reference in its entirety.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates generally to user data control and, more specifically, to exemplary systems and methods for active control of access to personal user data through the interaction of a short-range transceiver with a client device.

BACKGROUND

[0003] A typical user has personal user information or data that may be of a sensitive or confidential nature, including, for example, such information as personal health data, social security number, family contacts, etc. When a user creates an account, the user will generally provide a certain amount of personal, identifying information regarding the user, as well as information for account access such as a username and password. Entities other than the user may add to the personal user data. Different entities may have, for example, different user data retention policies, different use policies, and different user data sharing policies. The policies of using user-information may further change without any notification to the user. In addition, the possessor of the user information may also change through a merger or buy-out of one entity by another, many times without any notice to the user.

[0004] Account access will often rely on log-in credentials (e.g., username and password) to confirm a cardholder's identity. However, if the log-in credentials are compromised,

another person could have access to the user's account and, potentially, to the user's sensitive or confidential information or data. In addition, the more entities or individuals that a user shares their personal information with, the greater the risk of the user's information being stolen by a breach at one of the entities. Further, a user may only desire to share certain pieces of personal information with an entity or individual for limited purposes or limited in time.

[0005] Thus, it may be beneficial to provide exemplary systems and methods which allow users to control the use of user information to overcome at least some of the deficiencies described herein.

SUMMARY

[0006] Aspects of the disclosed technology include systems and methods for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device. Data access control may be provided in the context of personal user data, including handling requests to obtain access to personal user data via the interaction of a short-range transceiver, such as a contactless card, with a client device such that the personal user data is only provided to service providers who are authorized to review the data and disclosure of certain account identifier information, or account login information, need not be disclosed to service providers requesting access to personal user data.

[0007] Embodiments of the present disclosure provide a data access control system, comprising: a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider; a server configured for data communication with a client device associated with the service provider; a contactless card associated with the user, the

contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet, a user token, and personal user data associated with the user, wherein the personal user data is encrypted using the user key; a client application comprising instructions for execution on the client device, the client application configured to: in response to a tap action between the contactless card and the client device: receive the user token from the contactless card, and transmit to the server a service provider token, the user token, and a request for a data access key, wherein the service provider token is associated with the service provider; receive from the server the data access key; receive from the contactless card the encrypted personal user data; and using the data access key, decrypt the encrypted personal user data; and, a processor in data communication with the server and the database, the processor configured to: receive from the client device the service provider token, the user token, and the request for the data access key; identify the service provider based on the service provider token; identify the user based on the user token; verify that the service provider is authorized to receive access to the personal user data; and transmit to the client device the data access key.

[0008] Embodiments of the present disclosure provide a method for controlling data access, comprising: establishing a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a first service provider key associated with a service provider; receiving from a first client device associated with the service provider, via a network, a service provider token and a request for a data access key to access personal user data stored on a contactless card associated with the user, the personal user data encrypted using the user key, the request generated in response to a tap action between the contactless card and the first client device, the request accompanied

by a user token stored on the contactless card; identifying the service provider based on the service provider token; identifying the user based on the user token; verifying that the service provider is authorized to receive access to personal user data stored on the contactless card; generating the data access key based on the user key; and transmitting to the first client device the data access key.

[0009] Embodiments of the present disclosure provide a method for controlling data access, comprising: establishing a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider; providing a contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a user token, wherein the communications interface is configured to support at least one of near field communication, Bluetooth, or Wi-Fi, and wherein the contactless card is associated with the user; providing a client application comprising instructions for execution on a client device associated with the service provider, the client application configured to: in response to a tap action between the contactless card and the client device: receive the user token from the contactless card, and transmit, to a server, a service provider token, the user token, and a request for a data access key, wherein the service provider token is associated with the service provider; receive from the server the data access key and a link to a data repository storing encrypted personal user data associated with the user, wherein the data access key is generated based on the user key; transmit to the data repository, via the link, a request for the encrypted personal user data; receive from the data repository the encrypted personal user data; and using the data access key, decrypt the encrypted personal user data; receiving from the client device, via a network, a service provider token and the request for the data access

key to access the personal user data associated with the user, the request accompanied by the user token; identifying the service provider based on the service provider token; identifying the user based on the user token; verifying that the service provider is authorized to receive access to the personal user data associated with the user; generating the link to the data repository storing the encrypted personal user data; generating the data access key based on the user key; and transmitting to the client device the data access key and the link to the data repository storing the encrypted personal user data.

[0010] Further features of the disclosed design, and the advantages offered thereby, are explained in greater detail hereinafter with reference to specific example embodiments described below and illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1A is a diagram of a data access control system according to one or more example embodiments.

[0012] FIG. 1B is a diagram illustrating a sequence for providing data access control according to one or more example embodiments.

[0013] FIG. 1C is a diagram illustrating a sequence for providing data access control according to one or more example embodiments.

[0014] FIG. 2 illustrates components of a client device used in a data access control system according to one or more example embodiments.

[0015] FIG. 3 illustrates components of a short-range transceiver used in a data access control system according to one or more example embodiments.

[0016] FIG. 4 is diagram illustrating interaction between a client device and a short-range transceiver used in a data access control system according to one or more example embodiments.

[0017] FIG. 5 is diagram illustrating interaction between a client device and a short-range transceiver used in a data access control system according to one or more example embodiments.

[0018] FIGs. 6A-6B provide a flowchart illustrating a method of data access control according to one or more example embodiments.

[0019] FIGs. 7A-7C provide a flowchart illustrating one or more methods of data access control according to one or more example embodiments.

[0020] FIG. 8 is a diagram of a data access control system according to one or more example embodiments.

DETAILED DESCRIPTION

[0021] 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.

[0022] Exemplary embodiments of the disclosed systems and methods provide for controlling data access through the interaction of a short-range transceiver, such as a contactless card, with a client device. Data access control may be provided in the context of controlling access to personal user data. Requests for access to personal user data may be handled via the interaction of a short-range transceiver, such as a contactless card, with a client device such that the personal user data is only provided to service providers who are authorized to review the data, and disclosure of certain account identifier information, or account login information, need not be disclosed to service providers requesting access to personal user data. Benefits of the disclosed technology may include improved data security for personal user data, improved access to personal user data when access is required without user response or intervention (such as, e.g., during an emergency), and improved user experience.

[0023] FIG. 1A shows a diagram illustrating a data access control system 100 according to one or more example embodiments. As discussed further below, system 100 may include client device 101, client device 103, short-range transceiver 105, server 110, processor 120 and database 130. Client device 101 and client device 103 may communicate with server 110 via network 115. Although FIG. 1 illustrates certain components connected in certain ways, system 100 may include additional or multiple components connected in various ways.

[0024] System 100 may include one or more client devices, such as client device 101 and/or client device 103, which may each be a network-enabled computer. As referred to herein, a network-enabled computer may include, but is not limited to a computer device, or communications device including, e.g., a server, a network appliance, a personal computer, a workstation, a phone, a handheld PC, a personal digital assistant, a thin client, a fat client, an

Internet browser, or other device. Each of client devices 101 and 103 also may be a mobile device; for example, a mobile device 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. Additional features that may be included in a client device, such as client device 101 and/or client device 103, are further described below with reference to FIG. 2.

[0025] System 100 may include one or more short-range transceivers, such as short-range transceiver 105. Short-range transceiver 105 may be in wireless communication with a client device, such as client device 101 and/or client device 103, within a short-range communications field such as, for example, near field communication (NFC). Short-range transceiver 105 may include, for example, a contactless card, a smart card, or may include a device with a varying form factor such as a fob, pendant or other device configured to communicate within a short-range communications field. In other embodiments, the short-range transceiver 105 may be the same or similar as the client devices 101, 103. Additional features that may be included in a short-range transceiver, such as such as short-range transceiver 105, are further described below with reference to FIG. 3.

[0026] System 100 may include one or more servers 110. In some example embodiments, server 110 may include one or more processors (such as, e.g., a microprocessor) which are coupled to memory. Server 110 may be configured as a central system, server or platform to control and call various data at different times to execute a plurality of workflow actions. Server 110 may be a dedicated server computer, such as bladed servers, or may be personal

computers, laptop computers, notebook computers, palm top computers, network computers, mobile devices, or any processor-controlled device capable of supporting the system 100.

[0027] Server 110 may be configured for data communication (such as, e.g., via a connection) with one or more processors, such as processor 120. In some example embodiments, server 110 may incorporate processor 120. In some example embodiments, server 110 may be physically separate and/or remote from processor 120. Processor 120 may be configured to serve as a back-end processor. Processor 120 may be configured for data communication (such as, e.g., via a connection) with database 130 and/or to server 110. Processor 120 may include one or more processing devices such as a microprocessor, RISC processor, ASIC, etc., along with associated processing circuitry. Processor 120 may include, or be connected to, memory storing executable instructions and/or data. Processor 120 may communicate, send or receive messages, requests, notifications, data, etc. to/from other devices, such as client devices 101 and/or 103, via server 110.

[0028] Server 110 may be configured for data communication (such as, e.g., via a connection) with one or more databases, such as database 130. Database 130 may be a relational or non-relational database, or a combination of more than one database. In some example embodiments, server 110 may incorporate database 130. In some example embodiments, database 130 may be physically separate and/or remote from server 110, located in another server, on a cloud-based platform, or in any storage device that is in data communication with server 110.

[0029] Connections between server 110, processor 120 and database 130 may be made via any communications line, link or network, or combination thereof, wired and/or wireless, suitable for communicating between these components. Such network may include network

115 and/or one or more networks of same or similar type as those described herein with reference to network 115. In some example embodiments, connections between server 110, processor 120 and database 130 may include a corporate LAN.

[0030] Server 110 and/or database 130 may include user login credentials used to control access to user accounts. The login credentials may include, without limitation, user names, passwords, access codes, security questions, swipe patterns, image recognition, identification scans (e.g., driver's license scan and passport scan), device registrations, telephone numbers, email addresses, social media account access information, and biometric identification (e.g., voice recognition, fingerprint scans, retina scans, and facial scans).

[0031] Database 130 may contain data relating to one or more users, one or more service providers, and one or more accounts. Data relating to a user may include a user identifier and a user key, and may be maintained or organized in one or more accounts. Data relating to a service provider may include a service provider identifier and a service provider key, and may be maintained or organized in one or more accounts. Accounts may be maintained by (or on behalf of) and/or relate to any one or more of a variety of entities, such as, for example (and without limitation) a bank, merchant, online retailer, service provider, merchandizer, manufacturer, social media provider, provider or promoter of sporting or entertainment events, or hotel chain. For example, database 130 may include, without limitation, account identification information (e.g., account number, account owner identification number, account owner name and contact information -- any one or more of which may comprise an account identifier), account characteristics (e.g., type of account, funding and trading limitations, and restrictions on access and other activity), and may include information and data pertinent to the account, including financial (such as balance information, payment

history, and transaction history), social and/or personal information. Data stored in database 130 may be stored in any suitable format, and may be encrypted and stored in a secure format to prevent unauthorized access. Any suitable algorithm/procedure may be used for data encryption and for authorized decryption.

[0032] Server 110 may be configured to communicate with one or more client devices, such as such as client device 101 and/or client device 103, via one or more networks, such as network 115. Network 115 may include 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 client devices 101 and/or 103 to server 110. For example, network 115 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.

[0033] In addition, network 115 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, network 115 may support an Internet network, a wireless communication network, a cellular network, or the like, or any combination thereof. Network 115 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. Network 115 may utilize one or more protocols of one or more network elements to which they are communicatively coupled. Network 115 may translate to or from other protocols to one or more protocols of network devices. Although network 115 is depicted as a single network, it should be appreciated that according to one or more example embodiments, network 115 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, a LAN, and/or home networks.

[0034] In some example embodiments, server 110 may access records, including records in database 130, to determine a method or methods for communicating with client device 101 and/or client device 103. The communication method may include an actionable push notification with an application stored on client device 101 and/or client device 103. Other communication methods may include a text message or an e-mail, or other messaging techniques appropriate in a network-based client/server configuration. Messages or requests by client devices 101 and/or 103 may be communicated to server 110 via an application on the client device, or may be sent by a text message or an e-mail, or other messaging techniques appropriate in a network-based client/server configuration. Communications originating with client device 101 or client device 103 may be sent to server 110 using the same communications method as communications originating with server 110, or via a different communications method.

[0035] FIG. 1B shows a diagram illustrating a sequence for providing data access control according to one or more example embodiments, which may include a request by a service provider for a data access key to access or decrypt personal user data stored on a short-range transceiver. FIG. 1B references similar components of example embodiment system 100 as

illustrated in FIG. 1A. Client device 101 may be associated with a service provider. The service provider may have an associated service provider token. Client device 101 may include application 102, which may include instructions for execution by client device 101. Client device 101 may include features further described below with reference to FIG. 2. Application 102 may be configured to provide a user interface for the service provider when using client device 101. Application 102 may be configured to communicate, via client device 101, with other client devices, with short-range transceiver 105, and with server 110. Application 102 may be configured to receive requests and send messages as described herein with reference to client device 101. Service provider information and user information, including identifiers and/or keys, may be stored in database 130.

[0036] Short-range transceiver 105 may be associated with a user. Short-range transceiver 105 may include, for example, a contactless card, and may include features further described below with reference to FIG. 3. Short-range transceiver 105 may have memory storing an applet 106 and/or a token 107, and storing personal user data 108. Token 107 and personal user data 108 may be associated with the user.

[0037] A token may be used to increase security through token authorization. Server 110 may send a validation request to a client device, such as client device 101, receive responsive information from the client device, and if validated, send a validation token back to the client device. The validation token may be based on a pre-determined token, or may be a dynamic token based on an algorithm that can be secret and known only to server 110 and the client device; the algorithm may include live parameters independently verifiable by the participants, such as the temperature at a particular location or the time. The token may be

used to verify the identity of the service provider or the user. The validation request and/or validation token may be based on token 107 stored on short-range transceiver 105.

[0038] Personal user data 108 may include personal user information or data that may be of a sensitive or confidential nature, such as, for example, personal health data, social security number, family contacts, etc. (including types of data identified herein with reference to Fig. 3). Personal user data 108 may be encrypted and stored in a secure format to prevent unauthorized access.

[0039] In some example embodiments, personal user data may include personal health data such as, e.g., height, weight, blood type, prescription medications, allergies, emergency contacts, treatment or DNR instructions, etc. Personal user data may also include personal identifying data such as name, gender, date of birth, etc. A service provider using client device 101 may be, e.g., a first responder, an emergency team member, or an emergency health care provider or technician, and may be associated with a service entity, such as a fire or ambulance department, a police department, a hospital, etc.

[0040] In some example embodiments, application 102 may display an instruction on client device 101 prompting the service provider to initiate a tap action between short-range transceiver 105 and client device 101. As used herein, a tap action may include tapping short-range transceiver 105 against client device 101 (or vice-versa). For example, if short-range transceiver 105 is a contactless card and client device 101 is a mobile device, the tap action may include tapping the contactless card on a screen or other portion of client device 101. However, a tap action is not limited to a physical tap by short-range transceiver 105 against client device 101, and may include other gestures, such as, e.g., a wave or other movement of short-range transceiver 105 in the vicinity of client device 101 (or vice-versa).

[0041] At label 150, there may be a tap action between short-range transceiver 105 and client device 101. The tap action may be in response to a prompt displayed on client device 101.

[0042] At label 152, application 102 may communicate (via client device 101) with short-range transceiver 105 (e.g., after short-range transceiver 105 is brought near client device 101). Communication between application 102 and short-range transceiver 105 may involve short-range transceiver 105 (such as, e.g., a contactless card) being sufficiently close to a card reader (not shown) of the client device 101 to enable NFC data transfer between application 102 and short-range transceiver 105, and may occur in conjunction with (or response to) a tap action between short-range transceiver 105 and client device 101 (such as, e.g., the tap action at label 150). The communication may include exchange of data or commands to establish a communication session between application 102 and short-range transceiver 105. The exchange of data may include transfer or exchange of one or more keys, which may be preexisting keys or generated as session keys. In some example embodiments, the communication may occur upon entry of short-range transceiver 105 into a short-range communication field of client device 101 prior to a tap action between short-range transceiver 105 and client device 101.

[0043] At label 154, short-range transceiver 105 may send user token 107 associated with the user to application 102. Token 107 may include a user identifier. In some example embodiments, user token 107 may include a key associated with the user. In some example embodiments, the sending of token 107 to application 102 may be in conjunction with (or response to) a tap action between short-range transceiver 105 and client device 101 (such as, e.g., the tap action at label 150). In some example embodiments, the sending of token 107 to

application 102 may occur upon entry of short-range transceiver 105 into a short-range communication field of client device 101 prior to a tap action between short-range transceiver 105 and client device 101.

[0044] At label 156, application 102 may send user token 107 to server 110, along with a service provider token associated with the service provider and a request for a data access key. This may be carried out in response to a tap action between short-range transceiver 105 and client device 101 (such as, e.g., the tap action at label 150). The data access key would enable the service provider to decrypt the encrypted personal user data 108.

[0045] At label 158, processor 120 may receive (e.g. via server 110) the user token, the service provider token, and the data access key request. Processor 120 may use the user token to identify the user. Processor 120 may use the service provider token to identify the service provider as the sender of the data access key request. In some example embodiments, identifying the service provider may be carried out by using a service provider identifier in the token to look up information in database 130. In some example embodiments, at label 159, if the service provider token includes a key associated with the service provider, processor 120 may use the service provider key to authenticate the service provider; likewise, if the user token includes a key associated with the user, processor 120 may use the user key to authenticate the user. Based on the identity of the service provider (and as such identity may be authenticated), processor 120 may verify whether the service provider is authorized to receive the data access key to decrypt -- and thereby obtain access to -- personal user data 108. In an example embodiment, the service provider key may be available to a service provider and valid for a limited period of time, such as, e.g., a daily, weekly, monthly or other basis. Client device 101 may transmit to server 110 a request for the service provider

key at intervals when a new key becomes available (e.g., daily, weekly, monthly or other basis). Receiving the service provider key by client device 101 does not require the service provider to be in the vicinity of short-range transceiver 105, and the service provider key may be requested or received by client device 101 independently of any tap action with short-range transceiver 105.

[0046] At label 160, processor 120 may send the data access key to client device 101. As mentioned above, processor 120 may verify that the service provider is authorized to receive the data access key. The data access key may be stored in database 130, or may be generated based on the user key, on the service provider key, or on a combination of both the user key and the service provider key. The user key may be stored in database 130 or included in user token 107. The service provider key may be stored in database 130 or included in the service provider token received from client device 101.

[0047] In an example embodiment, processor 120 may instead send a denial notification (not shown) to client device 101, indicating that the service provider is not authorized to receive the data access key.

[0048] At label 162, short-range transceiver 105 may send encrypted personal user data 108 to application 102 via client device 101. Of note, the timing of transmission of encrypted personal user data 108 by short-range transceiver 105 to client device 101, in relation to the other events described with respect to FIG. 1B, is not critical. The encrypted personal user data 108 may be sent upon the first tap action, or at any time including after receipt of the data access key by client device 101.

[0049] Application 102 may be configured to receive, decrypt, and access encrypted personal user data 108 using the received data access key. In some embodiments, application

102 may cause the display of the personal user data on client device 101. In some embodiments, application 102 may be permitted to store the personal user data on client device 101 for retrieval on a time-limited, or limited number of uses, basis.

[0050] In one or more example embodiments, access by the service provider to personal user data may be limited in accordance with data control parameters. In an example embodiment, data control parameters may be stored in database 130. In an example embodiment, data control parameters may be stored in memory of short-range transceiver 105. Data control parameters stored in memory of short-range transceiver 105 may be sent to application 102 and used by application 102 to limit access by the service provider to personal user data. Applet 106 may be configured to receive the data control parameters and store the data control parameters in in memory of short-range transceiver 105.

[0051] In one or more example embodiments, data control parameters may be used to limit access by the service provider to personal user data in one or more ways. For example, the data control parameters may permit access only for a specific or limited period of time. As another example, the data control parameters may permit access to a single use by the service provider. As another example, the data control parameters may permit access only when short-range transceiver 105 is detected within range of a short-range communication field of client device 101. In one or more embodiments, the user may be prompted to confirm that the service provider may access the personal user data. In one or more embodiments, the user may pre-approve access to personal data by service providers, such that the user would not need to give permission at the time a service provider attempts to gain data access. The user may confirm or pre-approve access to personal user data by various

means, including by tapping the user's short-range transceiver to a client device in response to a prompt.

[0052] In an example embodiment, the personal user data may be stored in database 130 and may be updated. The updated personal user data may be stored in database 130 and transmitted to client device 101 upon request for the personal user data.

[0053] In an example embodiment, application 102 may be launched in response to a tap action between short-range transceiver 105 and client device 101.

[0054] FIG. 1C shows a diagram illustrating a sequence for providing data access control according to one or more example embodiments, which may include a request by a service provider for a data access key to access or decrypt personal user data stored on a short-range transceiver. FIG. 1C references similar components of example embodiment system 100 as illustrated in FIG. 1A and similar features of example embodiment system 100 as illustrated in FIG. 1B, including features described above with respect to labels 150-159 (which are not repeated here). The service provider referenced in the description above relating to FIG. 1B will be referred to as the first service provider in describing FIG. 1C. Referring to FIG. 1C, upon identifying the first service provider as the sender of a data access key request for access to personal user data of the user, according to procedures described above with reference to labels 150-159, it may be determined that two person approval is required.

[0055] Responding to the two person approval requirement may involve client device 103 associated with a second service provider. The second service provider may be associated with the same service entity as the first service provider (referenced above), or may be associated with an entity related to that service entity, or associated with a different entity. Client device 103 may include application 104, which may include instructions for

execution by client device 103. Client device 103 may include features further described below with reference to FIG. 2. Application 104 may be configured to provide a user interface for the second service provider when using client device 103. Application 104 may be configured to communicate, via client device 103, with other client devices, with short-range transceiver 105, and with server 110. Application 104 may be configured to receive requests and send messages as described herein with reference to client device 103.

[0056] At label 164, processor 120 may send (e.g. via server 110) a two person approval notice to client device 101, notifying the first service provider that a second service provider is needed to approve the data access key request. Application 102 may cause a message to be displayed on client device 101 indicating that the system is awaiting approval of the request by a second service provider. In some example embodiments, the notification may be sent to client device 103, or to both client device 101 and client device 103. Processor 120 may open a data access session with application 102 to provide tracking of the data access key request (relating to the user, via the user token) while awaiting approval.

[0057] At label 166, there may be a tap action between short-range transceiver 105 and client device 103. The tap action may be responsive to the two person approval notice. Application 104 may receive the user token 107 from short-range transceiver 105.

[0058] At label 168, application 104 may send the user token to server 110, along with a second service provider token associated with the second service provider and a data access key request; this may be in response to the tap action described above with reference to label 166. The second service provider token may include a second service provider key. Processor 120 may open a data access session with application 104 to provide separate tracking of the data access key request (relating to the user, via the user token) from the

second service provider. Processor 120 may use the second service provider token to identify the second service provider as the sender of the data access key request. Based on the user token, processor 120 may determine that the data access key request made by the second service provider corresponds to the open data access key request made by the first service provider, and thus may be seeking to approve access to the personal user data by the first service provider.

[0059] At label 170, processor 120 may send an approval notice to application 104 requesting approval by the second service provider of the data access key request submitted by the first service provider.

[0060] Application 104 may display an instruction on client device 103 for the second service provider to approve the data access key request made by the first service provider. In some example embodiments, the display may instruct the second service provider to tap short-range transceiver 105 with/against client device 103 to indicate approval (e.g., as shown in FIG. 5). In some example embodiments, the display may instruct the second service provider to press a button (not shown in FIG. 5) to indicate approval. In one or more example embodiments, the display on client device 103 of an instruction to approve the data access key request may be in response to the approval notice of label 170. In one or more example embodiments, the display on client device 103 of an instruction to approve the data access key request may be in response to the two person approval notice of label 164.

[0061] At label 172, once the second service provider has acted (e.g., by a tap action or pressing a button) to indicate approval, application 104 may send an approval message to server 110. Based on the approval message, processor 120 may determine that the second service provider has approved the data access key request by the first service provider.

[0062] In an example embodiment, in response to a two person approval notice, application 102 may display on client device 101 a code (such as a QR code or a numeric code), to be scanned by or otherwise entered into client device 103. Application 104 may transmit the code (as scanned or entered into client device 103) to server 110 to indicate approval of the data access key request. Based on the transmitted code, processor 120 may determine that the second service provider has approved the data access key request by the first service provider.

[0063] At label 174, processor 120 may send the data access key to client device 101. The data access key may be stored in database 130, or may be generated based on the user key, on the first service provider key, or on a combination of the user key and the first service provider key, or on a combination of the user key, the first service provider key and the second service provider key. The user key may be stored in database 130 or included in user token 107. The first service provider key may be stored in database 130 or included in the first service provider token received from client device 101. The second service provider key may be stored in database 130 or included in the second service provider token received from client device 103.

[0064] At label 176, short-range transceiver 105 may send encrypted personal user data 108 to application 102 via client device 101. Of note, the timing of transmission of encrypted personal user data 108 by short-range transceiver 105 to client device 101, in relation to the other events described with respect to FIG. 1B or 1C, is not critical. The encrypted personal user data 108 may be sent upon the first tap action, or at any time including after receipt of the data access key by client device 101.

[0065] As discussed above with reference to FIG. 1B, application 102 may be configured to receive, decrypt, and access encrypted personal user data 108 using the received data access key, including, for example, causing the display of the personal user data on client device 101, and/or storing the personal user data on client device 101 for retrieval on a time-limited, or limited number of uses, basis. In an example embodiment, the received data access key may be stored on client device 101, and application 102 may display the personal user data on the client device only if the data access key remains stored on the client device.

[0066] In an example embodiment, application 104 may be launched in response to a tap action between short-range transceiver 105 and client device 103.

[0067] FIG. 2 illustrates components of a client device 200 used in a data access control system according to one or more example embodiments. In one or more example embodiments, client device 200 may be one or more of client devices 101 and/or 103, described above with reference to FIG. 1A and FIGs. 1B-1C. Client device 200 may include one or more applications 201, one or more processors 202, a short-range communications interface 203, and a network interface 204. Application 201 may include a software application or executable program code to be executed on processor 202 and configured to carry out features described herein for any of the client devices, such as client devices 101 and/or 103, and/or any of the features described herein with reference to application 102. Application 201 may be configured, for example, to transmit and/or receive data with other devices via client device 101, such as, e.g., via short-range communications interface 203 and/or network interface 204. For example, application 201 may be configured to initiate one or more requests, such as near field data exchange requests to a short-range transceiver (such as a contactless card). Application 201 may also be configured to provide a user

interface via a display (not shown) for a user of the client device. Application 201 may be stored in memory in client device 200; the memory may include a read-only memory, write-once read-multiple memory and/or read/write memory, e.g., RAM, ROM, and EEPROM.

[0068] Processor 202 may include one or more processing devices such as a microprocessor, RISC processor, ASIC, etc., and may include associated processing circuitry. Processor 202 may include, or be connected to, memory storing executable instructions and/or data, as may be necessary or appropriate to control, operate or interface with the other features of client device 200, including application 201. Processor 202 (including any associated processing circuitry) 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.

[0069] Short-range communications interface 203 may support communication via a short-range wireless communication field, such as NFC, RFID, or Bluetooth. Short-range communications interface 203 may include a reader, such as a mobile device NFC reader. Short-range communications interface 203 may be incorporated into network interface 204, or may be provided as a separate interface.

[0070] Network interface 204 may include wired or wireless data communication capability. These capabilities may support data communication with a wired or wireless communication network, including the Internet, a cellular network, a wide area network, a local area network, a wireless personal area network, a wide body area network, any other wired or wireless network for transmitting and receiving a data signal, or any combination thereof. Such network may include, without limitation, telephone lines, fiber optics, IEEE

Ethernet 902.3, a wide area network, a local area network, a wireless personal area network, a wide body area network or a global network such as the Internet.

[0071] Client device 200 may also include a display (not shown). Such display may be any type of device for presenting visual information such as a computer monitor, a flat panel display, or a mobile device screen, including liquid crystal displays, light-emitting diode displays, plasma panels, and cathode ray tube displays.

[0072] Client device 200 may also include one or more device inputs (not shown). Such inputs may include any device for entering information into the client device that is available and supported by the client device 300, such as a touch-screen, keyboard, mouse, cursor-control device, touch-screen, microphone, digital camera, video recorder, or camcorder. The device inputs may be used to enter information and interact with the client device 200 and, by extension, with the systems described herein.

[0073] FIG. 3 illustrates components of a short-range transceiver 300 used in a data access control system according to one or more example embodiments. In one or more example embodiments, short-range transceiver 300 may be one or more of short-range transceiver 105, described above with reference to FIG. 1A and FIGs. 1B-1C. Short-range transceiver 300 may include, for example, a contactless card, or may include a device with a varying form factor such as a fob, pendant or other device configured to communicate within a short-range communications field. Short-range transceiver 300 may include a processor 301, memory 302, and short-range communications interface 306.

[0074] Processor 301 may include one or more processing devices such as a microprocessor, RISC processor, ASIC, etc., and may include associated processing circuitry. Processor 301 may include, or be connected to, memory storing executable

instructions and/or data, as may be necessary or appropriate to control, operate or interface with the other features of short-range transceiver 300, including applet 303. Processor 301 (including any associated processing circuitry) 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.

[0075] Memory 302 may be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM, and EEPROM. Memory 302 may be configured to store one or more applets 303, one or more tokens 304, and personal user data 305. Applet 303 may comprise one or more software applications configured to execute on processor 301, such as a Java Card applet that may be executable on a contact less card. However, it is understood that applet 303 is not limited to Java Card applets, and instead may be any software application operable on contactless cards or other devices having limited memory. Applet 303 may be configured to respond to one or more requests, such as near field data exchange requests from a client device, including requests from a device having a reader such as a mobile device NFC reader. Applet 303 may be configured to read (or write) data, including token 304 and/or personal user data 305 from (or to) memory 302 and provide such data in response to a request.

[0076] Token 304 may include a unique alphanumeric identifier assigned to a user of the short-range transceiver 300, and the identifier may distinguish the user of the short-range transceiver 300 from other users of other short-range transceivers (such as other contactless card users). In some example embodiments, token 304 may identify both a customer and an account assigned to that customer and may further identify the short-range transceiver (such

as a contactless card) associated with the customer's account. In some example embodiments, token 304 may include a key unique to the user or customer with which the short-range transceiver is associated.

[0077] Personal user data 305 may be stored in memory 302, and may, e.g., be located in specific memory location or in a data file identified by file name. Personal user data 305 may include personal user information or data that may be of a sensitive or confidential nature, such as, for example, personal health data, social security number, family contacts, etc. Personal user data 305 may be encrypted and stored in a secure format to prevent unauthorized access. Any suitable algorithm/procedure (including, e.g., public/private key encryption) may be used for data encryption and for authorized decryption.

[0078] Personal user data 305 (and personal user data 108 described above with reference to Figs. 1B-1C) may include any one or more of the following categories of data: full name, date of birth, Email address, home address, ethnicity / race, gender, place of birth, mother's maiden name, Social Security number, national ID number(s), passport number, visa permit number, driver's license number, vehicle registration plate number, genetic information, medical information, disability information, insurance details, location information, what you are doing when, status, events attended, sexual orientation, education history, grades, employment history, salary, job position / title, account information for financial, social, utility, services, or other accounts, photos, political and religious leanings and affiliation, views on controversial issues, history / background, credit score / record, sites registered on, criminal record, and/or commercially sensitive information.

[0079] Short-range communications interface 306 may support communication via a short-range wireless communication field, such as NFC, RFID, or Bluetooth. Short-range

transceiver 300 may also include one or more antennas (not shown) connected to short-range communications interface 306 to provide connectivity with a short-range wireless communications field.

[0080] FIG. 4 is diagram illustrating the interaction 400 between a client device 401 and a short-range transceiver 420 used in a data access control system according to one or more example embodiments, including embodiments described above with reference to FIGs. 1A-1C. Client device 401 may be client device 101 described above with reference to FIG. 1A and FIGs. 1B-1C. Client device 401 may be associated with the (first) service provider as described above with reference to FIGs. 1B-1C. User interface 402 may be generated by application 102 described above with reference to FIGs. 1B-1C. Short-range transceiver 420 may be short-range transceiver 105 described above with reference to FIG. 1A and FIGs. 1B-1C. Upon entry of short-range transceiver 420 into a short-range communication field of client device 401 (such as, e.g., via a tap action), client device 401 may communicate with short-range transceiver 420. Client device 401 may send data or commands to short-range transceiver 420 via transmit signal 431, and may receive data from short-range transceiver 420, including token 422, via receive signal 432. Short-range transceiver 420 may also send to client device 401 encrypted personal user data (not shown). Communication between client device 401 and short-range transceiver 420 may proceed as described above with reference to Figs. 1B-1C (e.g., client device 101 or 103 and short-range transceiver 105).

[0081] User interface 402 may present on client device 401 a screen display for a user data access request 410, which may include field 411 and field 412. If necessary, the first service provider may enter a username in field 411 and password in field 412. The screen display may include an instruction 414 prompting the first service provider to tap short-range

transceiver 420 (in the example shown, short-range transceiver 420 may be a contactless card) to initiate a data access key request to obtain a data access key required to decrypt the encrypted personal user data. Instruction 414 may be a push notification from server 110 (shown in FIG. 1A and FIGs. 1B-1C). Client device 401 may transmit a data access key request to server 110 (shown in FIG. 1A and FIGs. 1B-1C) along with a user token 422 (from short-range transceiver 420) and a first service provider token in response to a tap action.

[0082] FIG. 5 is diagram illustrating the interaction 500 between a client device 501 and a short-range transceiver 520 used in a data access control system according to one or more example embodiments, including embodiments described above with reference to FIGs. 1A-1C. Client device 501 may be client device 103 described above with reference to FIG. 1A and FIG 1C. Client device 501 may be associated with the second service provider as described above with reference to FIG. 1C. User interface 502 may be generated by application 104 described above with reference to FIG 1C. Short-range transceiver 520 may be short-range transceiver 105 described above with reference to FIG. 1A and FIGs. 1B-1C. Upon entry of short-range transceiver 520 into a short-range communication field of client device 501 (such as, e.g., via a tap action), client device 501 may communicate with short-range transceiver 520. Client device 501 may send data or commands to short-range transceiver 520 via transmit signal 531, and may receive data from short-range transceiver 520, including token 522, via receive signal 532. Communication between client device 501 and short-range transceiver 520 may proceed as described above with reference to Figs. 1B-1C (e.g., client device 101 or 103 and short-range transceiver 105).

[0083] User interface 502 may present on client device 501 a screen display for a user data access request 510, which may include field 511 and field 512. If necessary, the second

service provider may enter a username in field 511 and password in field 512. The screen display may include an instruction 514 notifying the second service provider that two service providers are needed to approve the user data access request, and prompting the second service provider to tap short-range transceiver 520 (in the example shown, short-range transceiver 520 may be a contactless card) to complete the approval process. Instruction 514 may be a push notification from server 110 (shown in FIG. 1A and FIGs. 1B-1C). Client device 501 may transmit a user token 522 (from short-range transceiver 520) and a second service provider token to server 110 in response to a tap action.

[0084] FIG. 6A is a flowchart illustrating a method of data access control 600 according to one or more example embodiments, with reference to components and features described above, including but not limited to the figures and associated description. Data access control method 600 may be carried out by application 102 executing on client device 101 associated with the (first) service provider. Short-range transceiver 105 is associated with the user.

[0085] At block 610, application 102 may cause client device 101 to display a user data access request screen (such as shown in, and described above with reference to, FIG. 4). The user data access request screen may include an instruction to tap short-range transceiver 105 with/against client device 101 to initiate a data access key request. As described above with reference to FIG. 4, short-range transceiver 420 (and, hence, short-range transceiver 105) may be a contactless card.

[0086] At block 620, a tap action may be detected between short-range transceiver 105 and client device 101.

[0087] At block 630, user token 107 may be received from short-range transceiver 105. Receiving user token 107 may be in response to the tap action of block 620. User token 107 may include a user identifier. In some example embodiments, user token 107 may include a user key associated with the user.

[0088] At block 640, user token 107 and a service provider token (associated with the service provider) may be transmitted to server 110 along with data access key request, to obtain a key for decrypting the encrypted personal user data received (or to be received) from short-range transceiver 105. Transmission of user token 107, the service provider token and the data access key request to server 110 may be in response to the tap action of block 620.

[0089] At block 650, a data access key may be received from server 110.

[0090] At block 660, the encrypted personal user data may be received from short-range transceiver 105. As discussed above, the encrypted personal user data may be received at any time during the process.

[0091] At block 670, the data access key may be used to decrypt the encrypted personal user data. As discussed above, in some embodiments, application 102 may cause the display of the personal user data on client device 101. In some embodiments, application 102 may be permitted to store the personal user data on client device 101 for retrieval on a time-limited, or limited number of uses, basis.

[0092] FIG. 6B is a flowchart illustrating a method of data access control 600 according to one or more example embodiments, with reference to components and features described above, including but not limited to the figures and associated description. The features described in FIG. 6B may be in addition to the features referenced in FIG. 6A. The description of blocks referenced in FIG. 6A will not be repeated here. As described above

with reference to FIG. 6A, data access control method 600 may be carried out by application 102 executing on client device 101 associated with the (first) service provider. Short-range transceiver 105 is associated with the user.

[0093] Memory located on short-range transceiver 105 (such as memory 302 shown in FIG. 4) may contain basic user data, such as name, gender, and date of birth. This basic user data could be a subset of the types of data contained in the personal user data, or may be additional data, and/or may be data that is unlikely to change (or less likely to change over time than other types of personal user data). In some example embodiments, such as when personal user data includes health data, the basic user data could include certain aspects of health data, such as, for example, height, weight, allergies, prescriptions, DNR instructions, etc. The types of information that may be included in basic user data may be selectable by the user.

[0094] Basic user data may be stored in short-range transceiver memory 302 and may, e.g., be located in specific memory location or in a data file identified by file name.

[0095] The basic user data may be encrypted with a key such that it may be decrypted with a basic service provider key that may be available to service providers. The basic service key may be different from the data access key required to descript personal user data 305. In one or more embodiments a basic service provider key may be available to service providers and valid for a limited period of time, such as, e.g., a daily, weekly, monthly or other basis. The basic service provider key may be common for all personnel associated with a particular service provider entity. The basic service provider key may be stored in database 130, or may be generated by the system based on the identity of the service provider. Storing the basic service provider key (or generating the key) by the system and pushing the key to

the client device provides a way of controlling access and permits access to be logged and tracked for auditing purposes.

[0096] At block 690, a basic service provider key is received from the server. The basic service provider key may be requested and/or obtained at any time, according to arrangements or protocols that the service provider (or service provider entity) may have with system 100. For example, client device 101 may transmit to server 110 a request for the basic service provider key at intervals when a new key becomes available (e.g., daily, weekly, monthly or other basis). Receiving the basic service provider key does not require the service provider to be in the vicinity of short-range transceiver 105, and the basic service provider key may be requested or received independently of any tap action with short-range transceiver 105.

[0097] At block 692, the basic service provider key may be stored in memory located in client device 101, allowing for later recall and use of the basic service provider key by the service provider at a later time.

[0098] At block 694, encrypted basic user information may be received from short-range transceiver 105. This may be in response to a tap action between short-range transceiver 105 and client device 101, or otherwise may be received at any time once short-range transceiver 105 is present within range of a short-range wireless communication field of client device 101.

[0099] At block 696, the basic service provider key may be used to decrypt the encrypted basic user data. Application 102 may cause the display of the basic user data on client device 101. In some embodiments, application 102 may be permitted to store the basic user data on client device 101 for retrieval on a time-limited, or limited number of uses, basis. In an

example embodiment, the basic user data may be stored on transceiver 105 in an unencrypted format. In an example embodiment, the basic user data may be received by client device 101 in an unencrypted form and accessed without the need for a basic service provider key. Whether the basic user data is stored or provided in an unencrypted format may be determined by the user.

[00100] FIG. 7A is a flowchart illustrating a method of data access control 700 according to one or more example embodiments, with reference to components and features described above, including but not limited to the figures and associated description. Data access control method 700 may be carried out by processor 120 in communication with, via server 110, client device 101 associated with the first service provider and/or client device 103 associated with the second service provider.

[00101] At block 710 a data access key request may be received, along with user token 107 and a service provider token (associated with the first service provider), from client device 101 associated with a first service provider, requesting a data access key to enable decryption of encrypted personal user data. Token 107 may include a user identifier. In some example embodiments, token 107 may include a user key associated with the user. In some example embodiments, the service provider token may include a first service provider key.

[00102] At block 720, the sender of the data access key request may be identified as the first service provider based on the service provider token. In some example embodiments, when the service provider token includes the first service provider key associated with the first service provider, the first service provider key may be used to authenticate the first service provider.

[00103] At block 730, the user may be identified based on received user token 107. In some example embodiments, when token 107 includes the user key associated with the user, the user key may be used to authenticate the user.

[00104] At block 740, the processor may verify that the first service provider is authorized to receive access to the personal user data (and thus authorized to obtain the data access key). Authorization may be based on the identity of the service provider, or the identity of the user, or both, and may include retrieval of information from database 130.

[00105] At block 750, a data access key may be sent to client device 101 associated with the service provider. As described above, the data access key may be stored in database 130, or may be generated based on the user key, on the first service provider key, or on a combination of the user key and the first service provider key.

[00106] FIG. 7B is a flowchart illustrating a method of data access control 701 according to one or more example embodiments, with reference to components and features described above, including but not limited to the figures and associated description. The features described in FIG. 7B may be in addition to the features referenced in FIG. 7A. The description of blocks referenced in FIG. 7A will not be repeated here. As described above with reference to FIG. 7A, data access control method 700 may be carried out by processor 120 in communication with, via server 110, client device 101 associated with the first service provider and/or client device 103 associated with the second service provider.

[00107] According to the method in FIG. 7B, block 750 (referenced in FIG. 7A) is not carried out in the sequence shown in FIG. 7A. Instead, with reference to FIG. 7B, at block 750' it is determined that two person approval is required for service provider access to personal user data.

[00108] At block 760, a notice is sent to client 101 associated with the first service provider that two person approval requires that a second service provider must approve the data access key request.

[00109] At block 765, a data access key request may be received from client device 103 associated with the second service provider, along with a user token and a second service provider token. The second service provider token may include a second service provider key.

[00110] At block 770, it may be determined that the data access key request from client device 103 of the second service provider corresponds to the data access key request previously received from client device 101 of the first service provider.

[00111] At block 775, an approval notice may be sent to client device 103 of the second service provider seeking approval of the data access key request made by the first service provider.

[00112] At block 780, an approval message may be received from client device 103 of the second service provider indicating approval, by the second service provider, of the data access key request made by the first service provider.

[00113] At block 785, a data access key may be sent to client device 101 associated with the first service provider. As described above, the data access key may be stored in database 130, or may be generated based on the user key, on the first service provider key, or on a combination of the user key and the first service provider key, or on a combination of the user key, the first service provider key and the second service provider key.

[00114] FIG. 7C is a flowchart illustrating a method of data access control 702 according to one or more example embodiments, with reference to components and features described

above, including but not limited to the figures and associated description. The features described in FIG. 7C may be in addition to the features referenced in FIGs. 7A or 7B. The description of blocks referenced in FIGs. 7A and 7B will not be repeated here. As described above with reference to FIGs. 7A and 7B, data access control method 700 may be carried out by processor 120 in communication with, via server 110, client device 101 associated with the first service provider and/or client device 103 associated with the second service provider.

[00115] At block 790, a request for a basic service provider key is received from client device 101. As discussed above, the basic service provider key may be requested at any time, according to arrangements or protocols that the service provider (or service provider entity) may have with system 100. Requesting the basic service provider key does not require the service provider to be in the vicinity of short-range transceiver 105, and the basic service provider key may be sent to client device 101 independently of any tap action with short-range transceiver 105.

[00116] At block 792, the processor may verify that the service is authorized to receive access to basic user data (and thus authorized to obtain a basic service provider key). Authorization may be based on the identity of the service provider, and may include retrieval of information from database 130.

[00117] At block 794, a basic service provider key may be sent to client device 101 associated with the service provider. The service provider key may be stored in database 130, or may be generated by the system based on the identity of the service provider.

[00118] FIG. 8 shows a diagram illustrating a data access control system 800 according to one or more example embodiments. FIG. 8 references similar components of example

embodiment system 100 as illustrated in FIG. 1A, and description of those components will not be repeated here. In addition to components relating to system 100 as illustrated in FIG. 1A and described above, system 800 may include a data repository 801. Data repository 801 may include a database having some or all of the same or similar structure, functionality or features as described above for database 130. Data repository may also include or incorporate a server having some or all of the same or similar structure, functionality or features as described above for server 110. Data repository may also include or incorporate a processor having some or all of the same or similar structure, functionality or features as described above for processor 120. Data repository is configured to store personal user data, such as personal user data of the type described above with respect to personal user data 305 in FIG. 3. Data repository may store the personal user data in an encrypted format, or may encrypt the personal user data before sending to an authorized service provider. Data repository 801 may be operated by the same or related entity as operating system 100, or may be operated by a third party.

[00119] In operation, system 800 may carry out all or many of the same functions as performed by the components of system 100, as described above, for handling a request for a data access key to access personal user data. Once system 800 verifies that the service provider is authorized to receive access to personal user data, processor 120 may generate a link to the data repository where the personal user data is stored. In an example embodiment, processor 120 may provide information (such as, e.g., an electronic address for data repository 801) in addition to or instead of the link to data repository 801.

[00120] Processor 120 may retrieve a data access key or generate a data access key as described above (including, e.g., generated based on the user key or based on the user key

and service provider key). Processor 120 may send to client device 101 the data access key and the link to data repository 801 where the personal user data may be located. Upon receiving the data access key and the link to data repository 801, client device 101 may then retrieve the encrypted personal user data from data repository 801, based on the link. For example, client device 101 may transmit to data repository 801, via the link, a request for the encrypted personal user data and receive the encrypted personal user data from data repository 801. Once client device 101 has obtained the encrypted personal user data, client device 101 may use the data access key to decrypt the encrypted personal user data. Once the personal user data is decrypted, client device 101 may access and use the personal user data as described above.

[00121] In some example embodiments, data repository 801 may store the same personal user data as stored on transceiver 105. In some example embodiments, the personal user data is stored in data repository 801 instead of being stored on transceiver 105. In some example embodiments, personal user data may be stored in data repository 801, and only a limited set of user data (such as, for example, basic user data) may be stored on transceiver 105. In some example embodiments, the personal user data stored in data repository 801 may be updated. The updated personal user data may be stored in data repository 801 and transmitted to client device 101 upon request for the personal user data.

[00122] The description of embodiments in this disclosure provides non-limiting representative examples referencing figures and numerals to particularly describe features and teachings of different aspects of the disclosure. 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 disclosure. The description of embodiments should facilitate understanding of the disclosure 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 disclosure

[00123] Throughout the specification and the claims, 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.

[00124] 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.

[00125] 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.

[00126] 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.

[00127] 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 data access control system, comprising:

a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider;

a server configured for data communication with a client device associated with the service provider via a network;

a contactless card associated with the user, the contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet, a user token, and personal user data associated with the user, wherein the personal user data is encrypted using the user key;

a client application comprising instructions for execution on the client device, the client application configured to:

in response to a tap action between the contactless card and the client device: receive the user token from the contactless card, and transmit to the server a service provider token, the user token, and a request for a data access key, wherein the service provider token is associated with the service provider;

receive from the server the data access key;

receive from the contactless card the encrypted personal user data; and

using the data access key, decrypt the encrypted personal user data;

and,

a processor in data communication with the server and the database, the processor configured to:

receive from the client device the service provider token, the user token, and the request for the data access key;

identify the service provider based on the service provider token;

identify the user based on the user token;

verify that the service provider is authorized to receive access to the personal user data;

retrieve the user key from the database;

generate the data access key from the user key; and

transmit to the client device the data access key.

2. The data access control system of claim 1, wherein the user token comprises the user key, and the processor is further configured to authenticate the user based on the user key.

3. The data access control system of claim 1, wherein the service provider token comprises the service provider key, and the processor is further configured to authenticate the service provider based on the service provider key.

4. The data access control system of claim 1, wherein:

the service provider token comprises the service provider key; and

the data access key is generated from the user key and the service provider key.

5. The data access control system of claim 1, wherein the client application is further configured to display the decrypted personal user data on the client device.

6. The data access control system of claim 5, wherein the client application is further configured to:

store the data access key on the client device; and

only display the decrypted personal user data on the client device if the data access key remains stored on the client device.

7. The data access control system of claim 1, wherein:

the memory of the contactless card further stores basic user data associated with the user, the basic user data encrypted with a basic service provider key; and

the client application is further configured to:

receive from the contactless card the encrypted basic user data; and

using the basic service provider key, decrypt the encrypted basic user data.

8. The data access control system of claim 7, wherein the client application is further configured to:

receive from the server the basic service provider key; and

store the basic service provider key in a memory of the client device.

9. The data access control system of claim 8, wherein:

the client application is further configured to transmit to the server a request for the basic service provider key, the request for the basic service provider key being independent of the tap action between the contactless card and the client device; and

the processor is further configured to:

verify that the service provider is authorized to receive the basic service provider key; and

transmit to the client device the basic service provider key.

10. The data access control system of claim 9, wherein the basic service provider key is valid only for a predetermined period of time.

11. A method for controlling data access, comprising:

establishing a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a first service provider key associated with a service provider;

receiving from a first client device associated with the service provider, via a network, a service provider token and a request for a data access key to access personal user data stored on a contactless card associated with the user, the personal user data encrypted using the user key, the request generated in response to a tap action between the contactless card and the first client device, the request accompanied by a user token stored on the contactless card;

identifying the service provider based on the service provider token;

identifying the user based on the user token;

verifying that the service provider is authorized to receive access to personal user data stored on the contactless card;

retrieving the user key from the database;

generating the data access key based on the user key; and

transmitting to the first client device the data access key.

12. The method of claim 11, wherein the user token includes the user key, the method further comprising authenticating the user based on the user key.

13. The method of claim 11, wherein the service provider token comprises the first service provider key, the method further comprising authenticating the service provider based on the first service provider key.

14. The method of claim 13, wherein the data access key is generated based on the user key and the first service provider key.

15. The method of claim 13, further comprising receiving from a second client device a second service provider key, wherein the data access key is generated based on the user key, the first service provider key and the second service provider key.

16. The method of claim 15, wherein the second service provider key is transmitted by the second client device in response to a tap action between the contactless card and the second client device.

17. The method of claim 11, wherein the database further stores updated personal user data associated with the user, the method further comprising:

encrypting the updated personal user data using the user key; and

transmitting to the first client device the encrypted updated personal user data.

18. A method for controlling data access, comprising:

establishing a database storing information comprising a user identifier and a user key associated with a user, and a service provider identifier and a service provider key associated with a service provider;

providing a contactless card comprising a communications interface, a processor, and a memory, the memory storing an applet and a user token, wherein the communications interface is configured to support at least one of near field communication, Bluetooth, or Wi-Fi, and wherein the contactless card is associated with the user;

providing a client application comprising instructions for execution on a client device associated with the service provider, the client application configured to:

in response to a tap action between the contactless card and the client device: receive the user token from the contactless card, and transmit via a network, to a server, a service provider token, the user token, and a request for a data access key, wherein the service provider token is associated with the service provider;

receive from the server the data access key and a link to a data repository storing encrypted personal user data associated with the user, wherein the data access key is generated based on the user key;

transmit to the data repository, via the link, a request for the encrypted personal user data;

receive from the data repository the encrypted personal user data; and

using the data access key, decrypt the encrypted personal user data;

receiving from the client device, via the network, a service provider token and the request for the data access key to access the personal user data associated with the user, the request accompanied by the user token;

identifying the service provider based on the service provider token;

identifying the user based on the user token;

verifying that the service provider is authorized to receive access to the personal user data associated with the user;

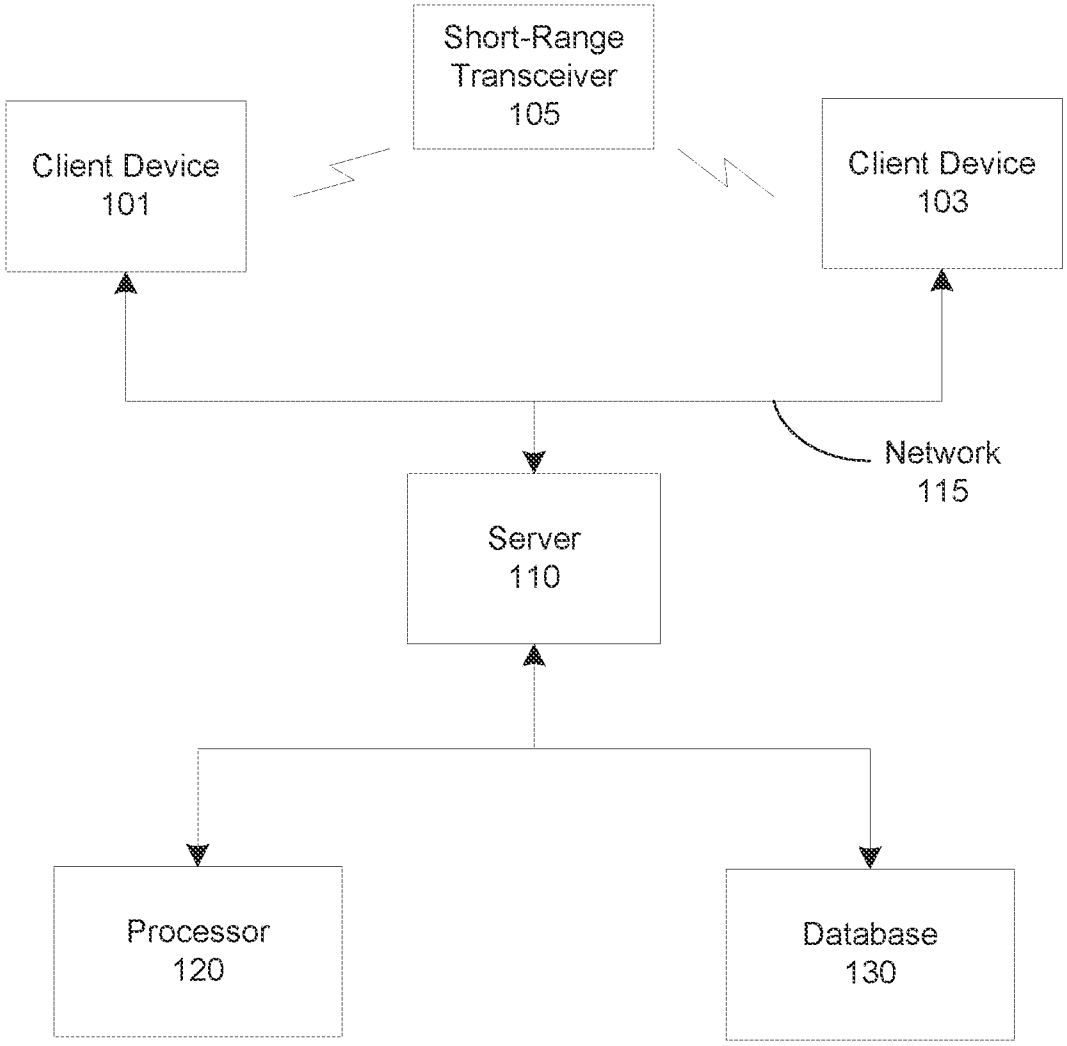
generating the link to the data repository storing the encrypted personal user data;

retrieving the user key from the database;

generating the data access key based on the user key; and

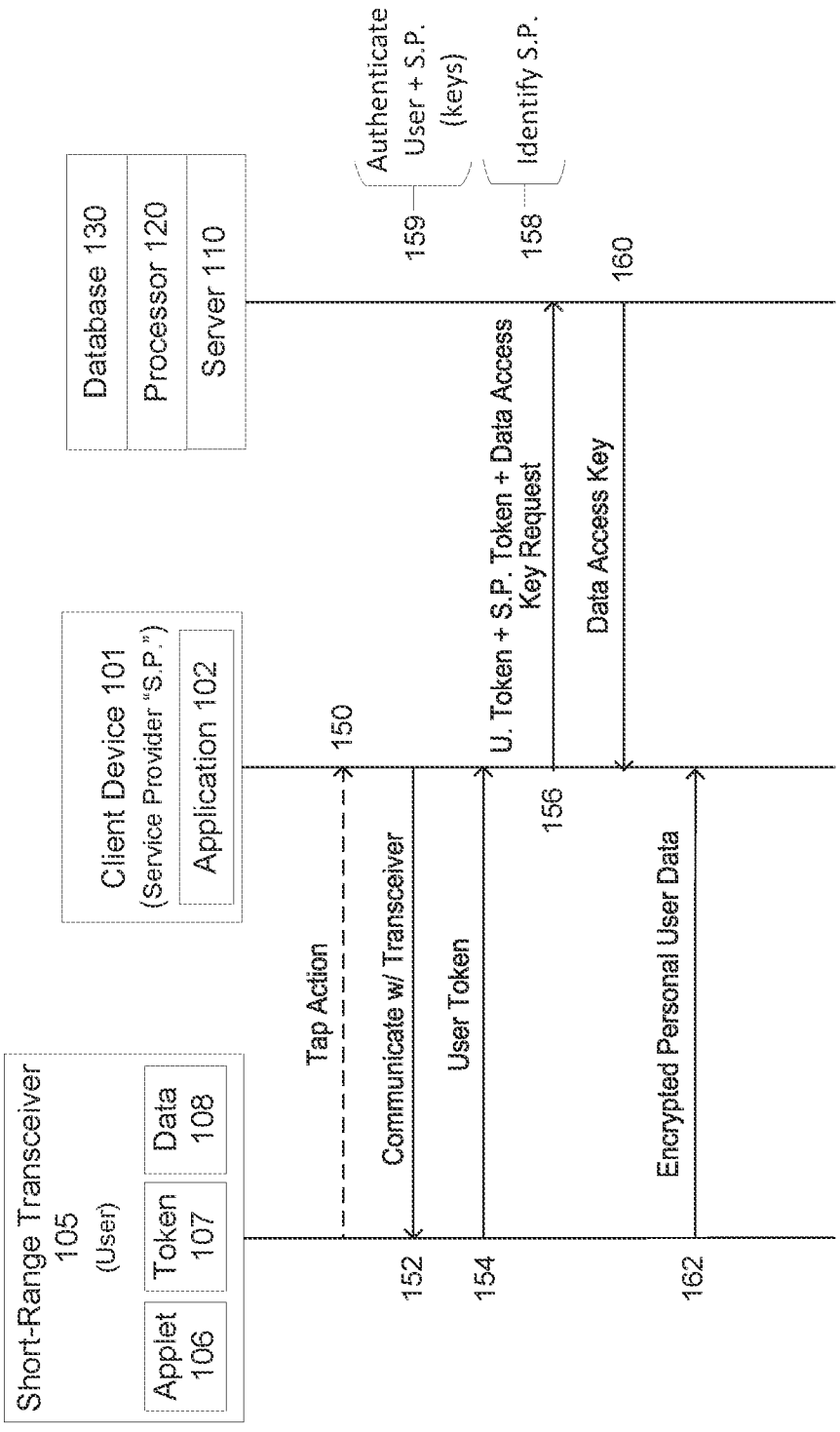
transmitting to the client device the data access key and the link to the data repository storing the encrypted personal user data.

19. The method of claim 18, wherein the data access key is generated based on the user key and the service provider key.



System 100

FIG. 1A



System 100

FIG. 1B

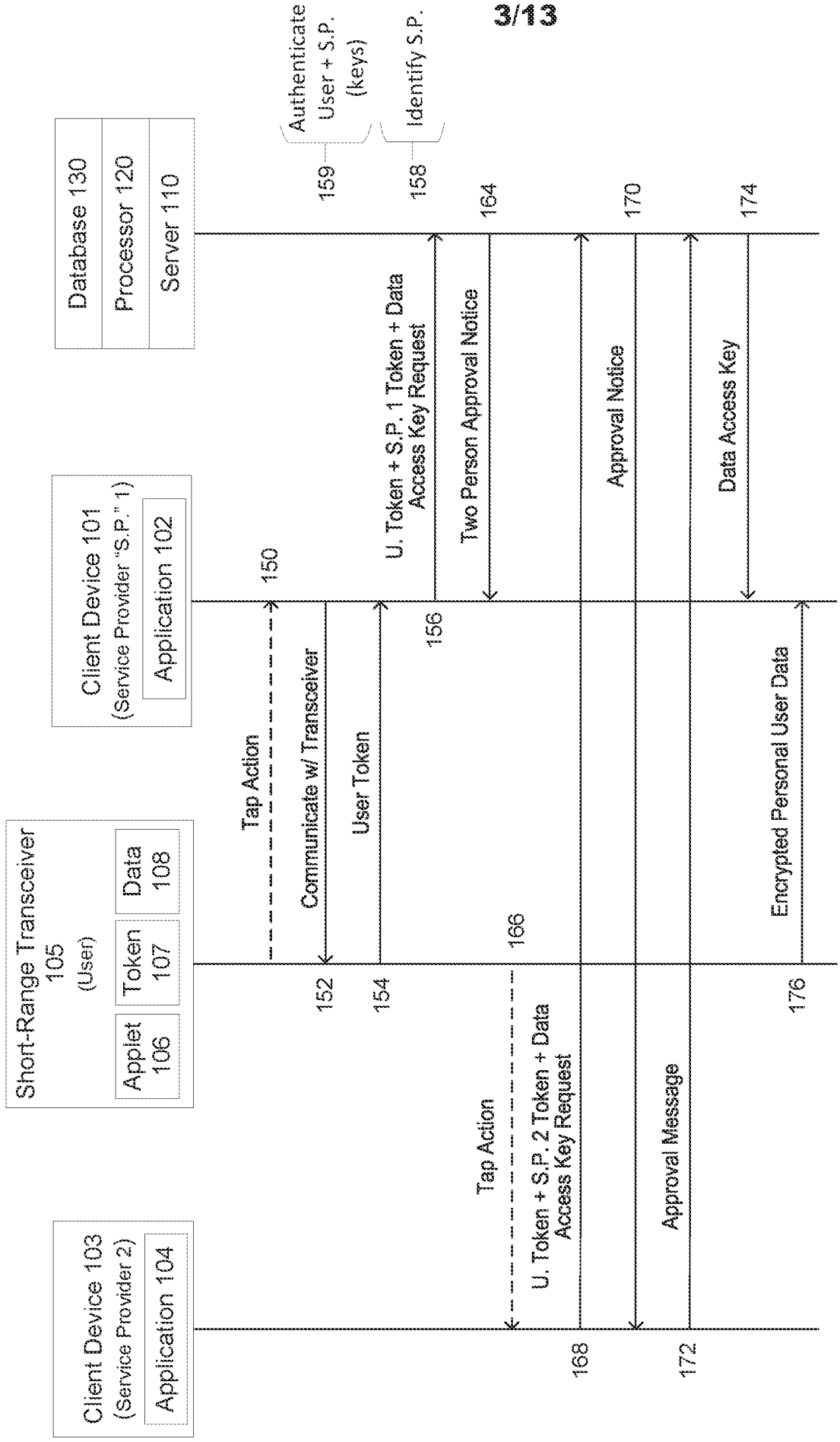

Client Device 103
(Service Provider 2)
Application 104
Short-Range Transceiver
105
(User)
Applet
106
Token
107
Data
108
Client Device 101
(Service Provider "S.P." 1)
Application 102
Database 130
Processor 120
Server 110
Tap Action
150
Communicate w/ Transceiver
152
User Token
154
U. Token + S.P. 1 Token + Data
Access Key Request
156
Authenticate
User + S.P.
(keys)
159
Identify S.P.
158
Two Person Approval Notice
164
Approval Notice
170
Data Access Key
174
Tap Action
166
U. Token + S.P. 2 Token + Data
Access Key Request
168
Approval Message
172
Encrypted Personal User Data
176
System 100

FIG. 1C

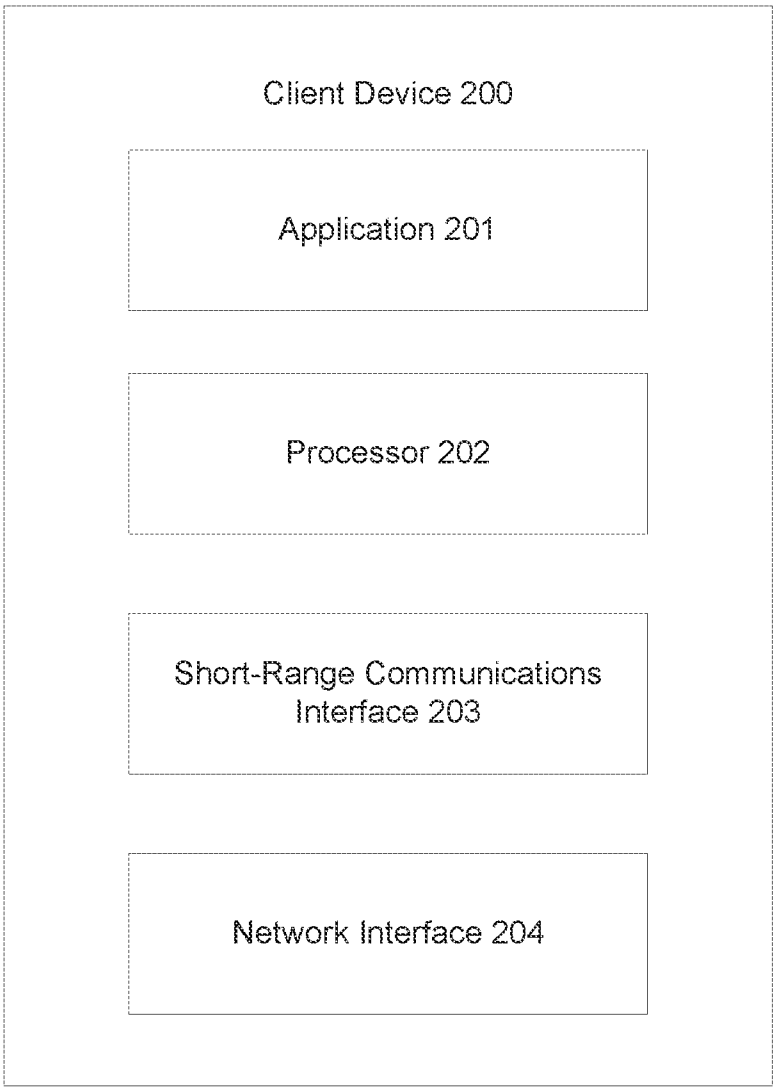

Client Device 200
Application 201
Processor 202
Short-Range Communications Interface 203
Network Interface 204

FIG. 2

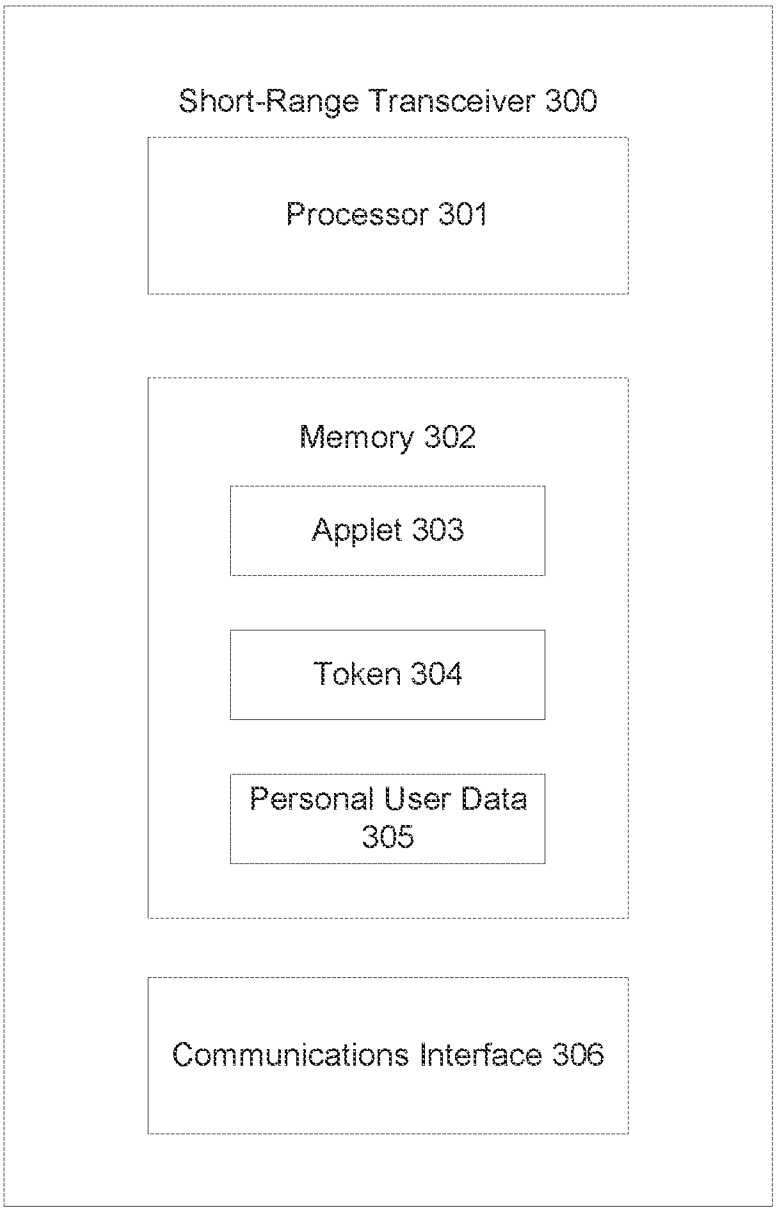
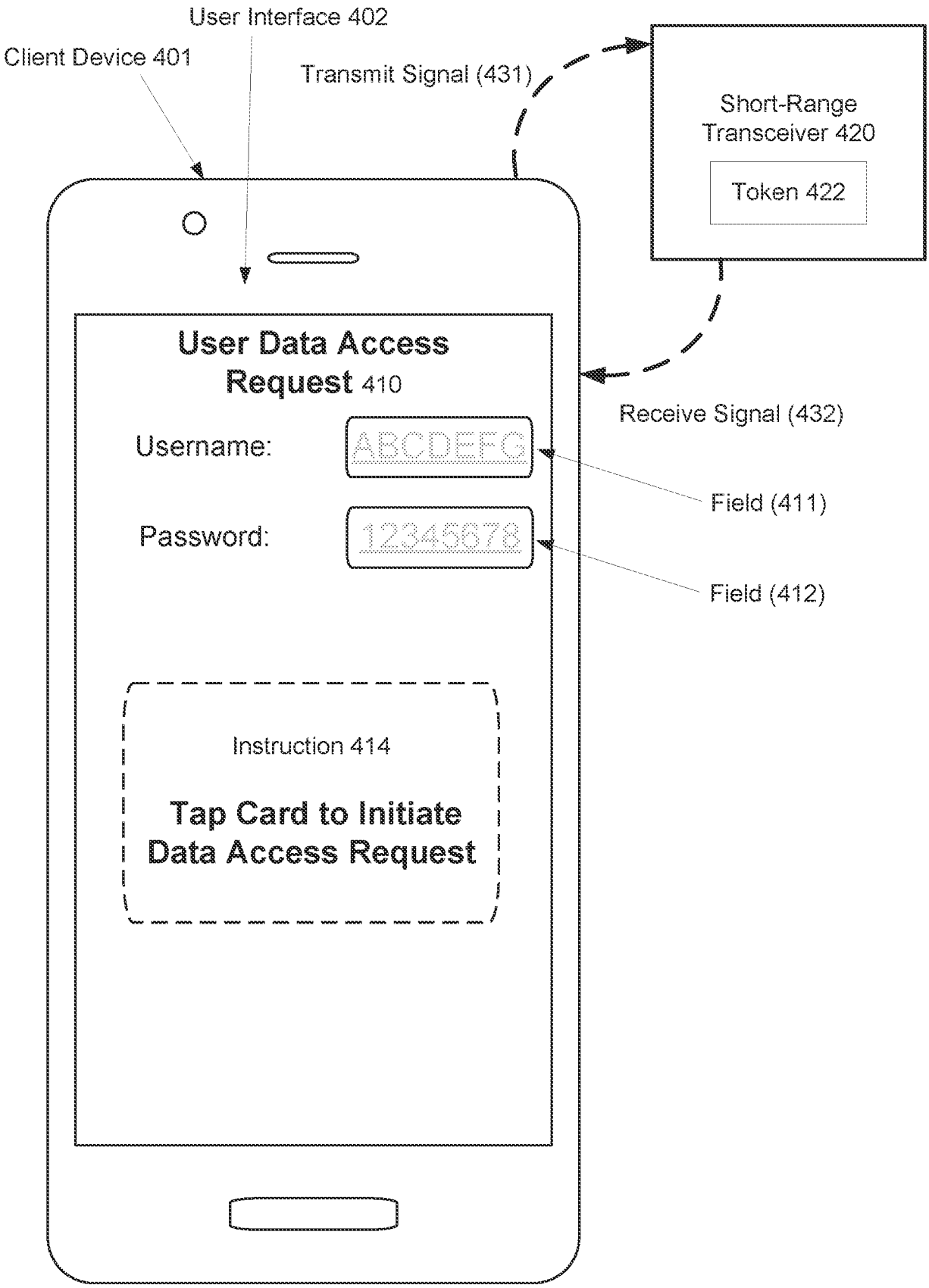
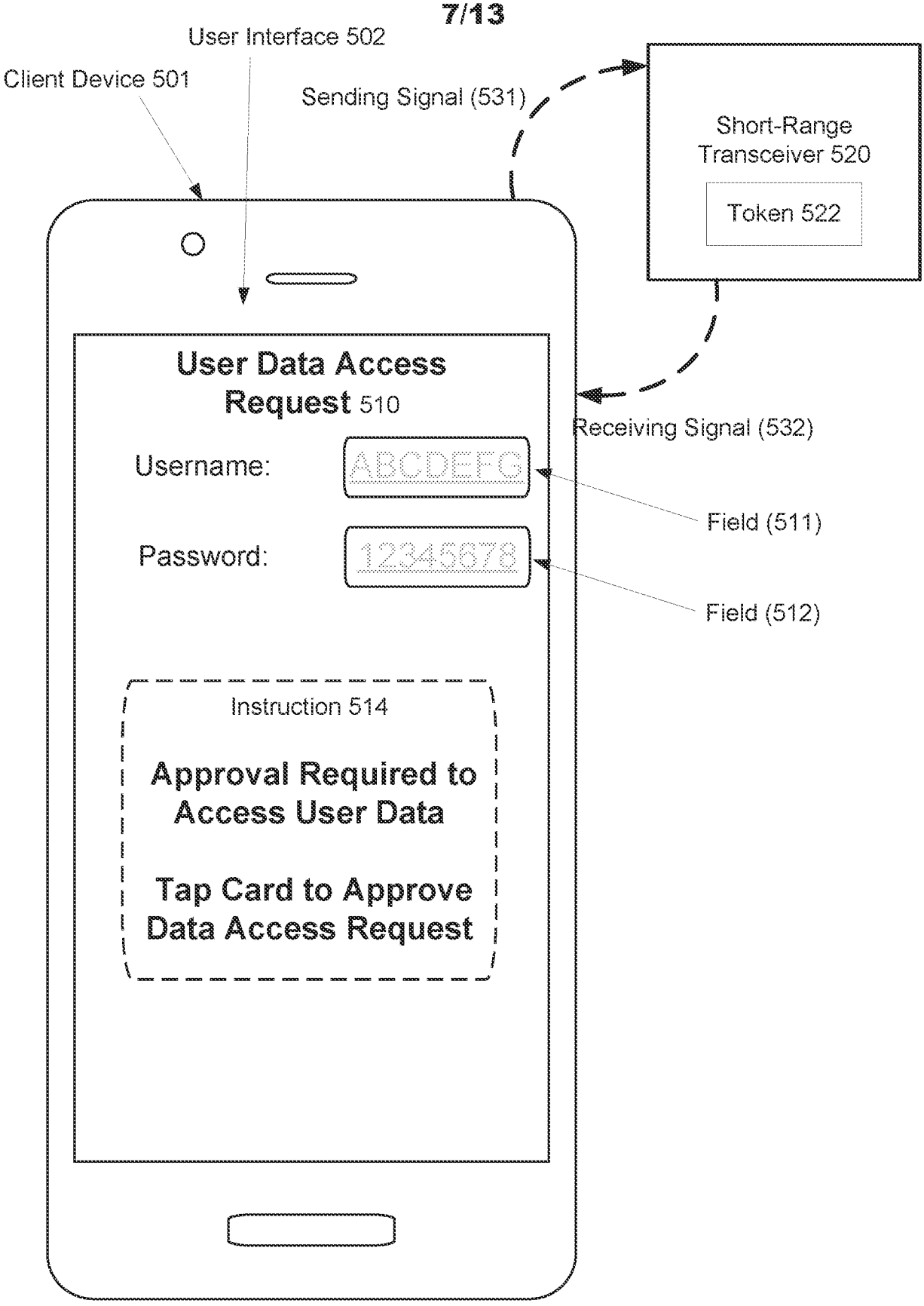

Short-Range Transceiver 300
Processor 301
Memory 302
Applet 303
Token 304
Personal User Data 305
Communications Interface 306

FIG. 3



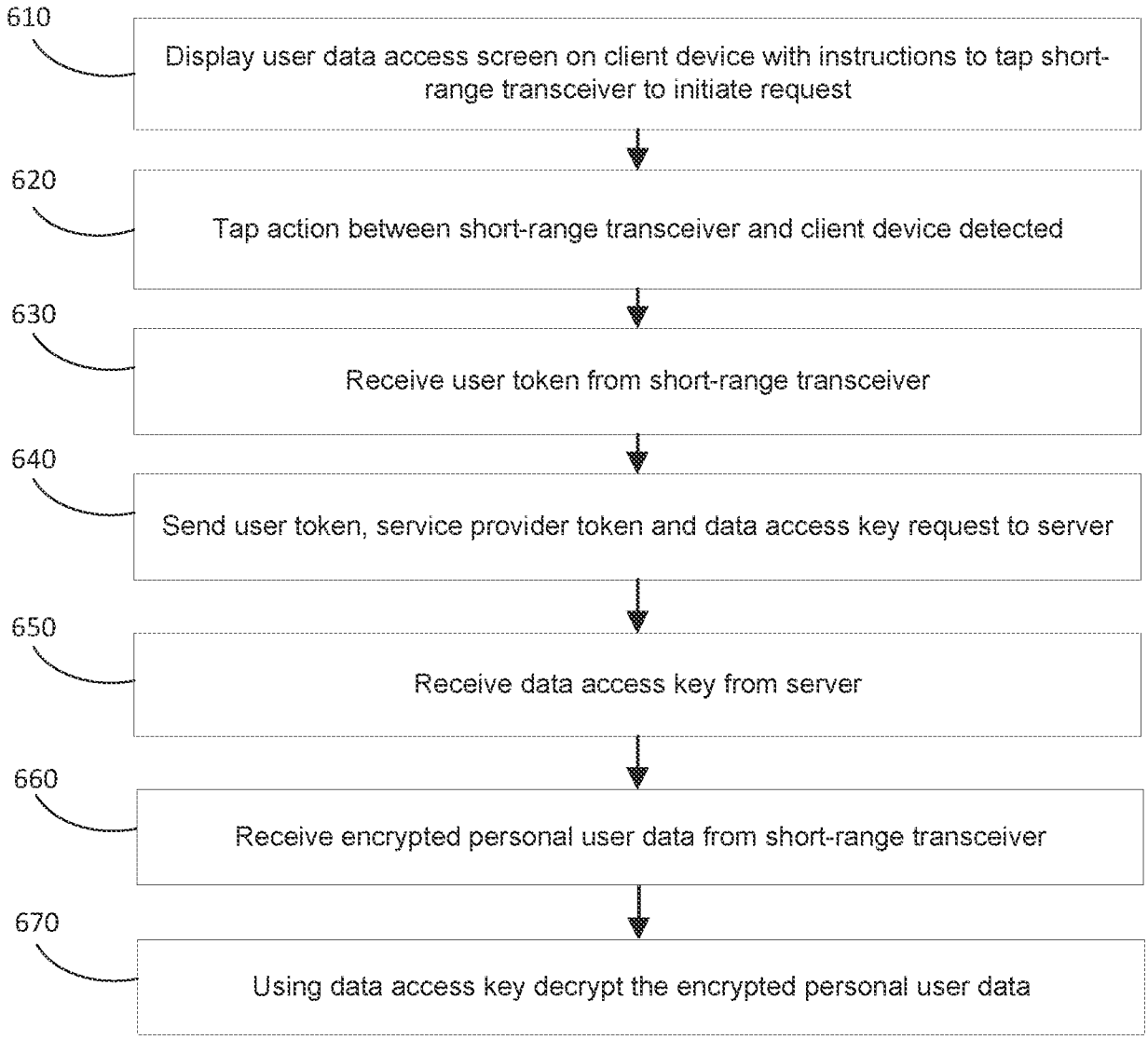
Client Device Interaction 400

FIG. 4



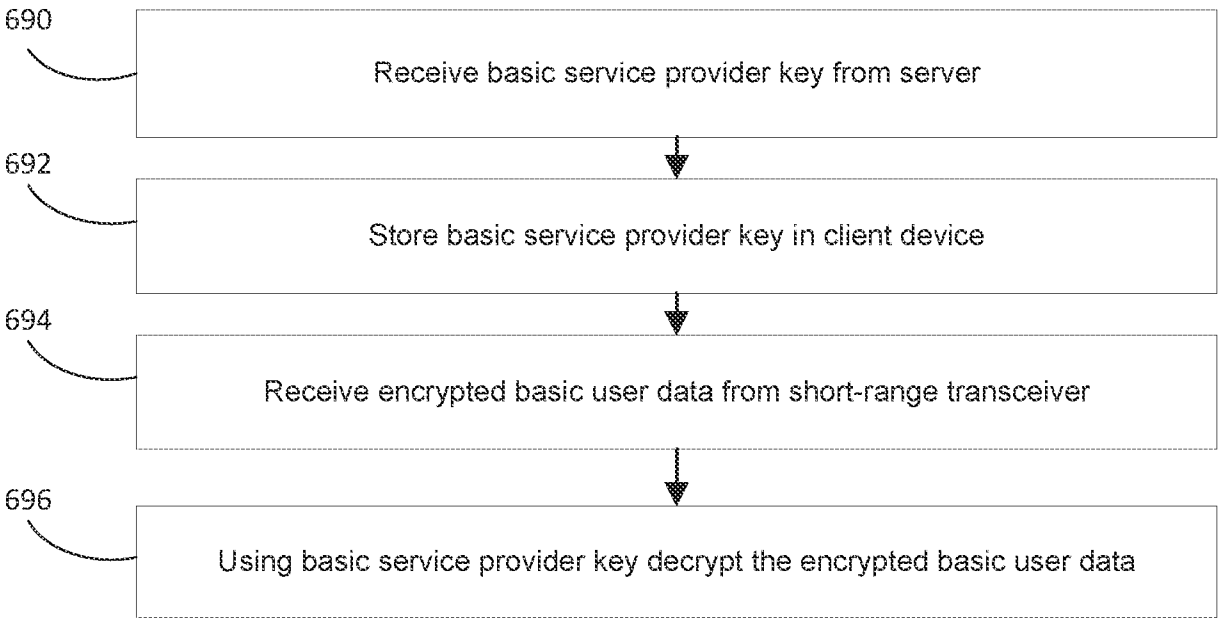
Client Device Interaction 500

FIG. 5


610
Display user data access screen on client device with instructions to tap short-range transceiver to initiate request
620
Tap action between short-range transceiver and client device detected
630
Receive user token from short-range transceiver
640
Send user token, service provider token and data access key request to server
650
Receive data access key from server
660
Receive encrypted personal user data from short-range transceiver
670
Using data access key decrypt the encrypted personal user data

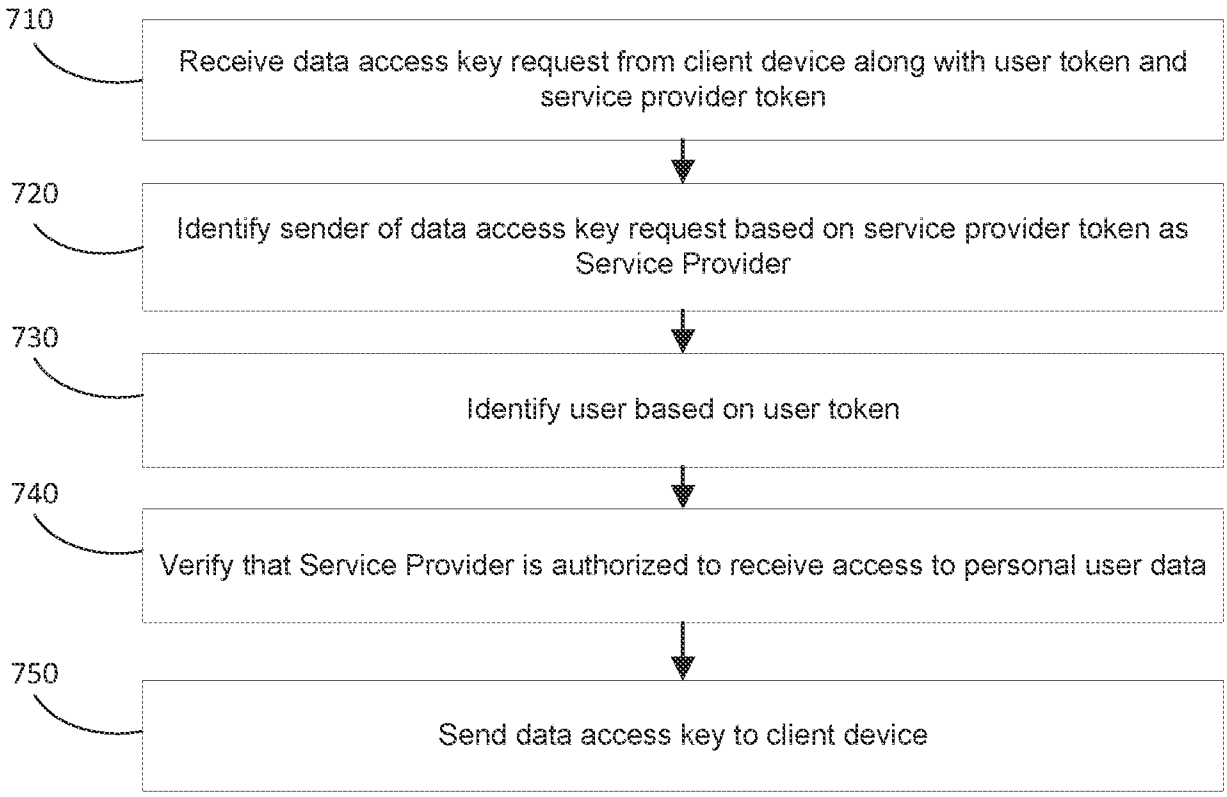
600

FIG. 6A


690
Receive basic service provider key from server
692
Store basic service provider key in client device
694
Receive encrypted basic user data from short-range transceiver
696
Using basic service provider key decrypt the encrypted basic user data

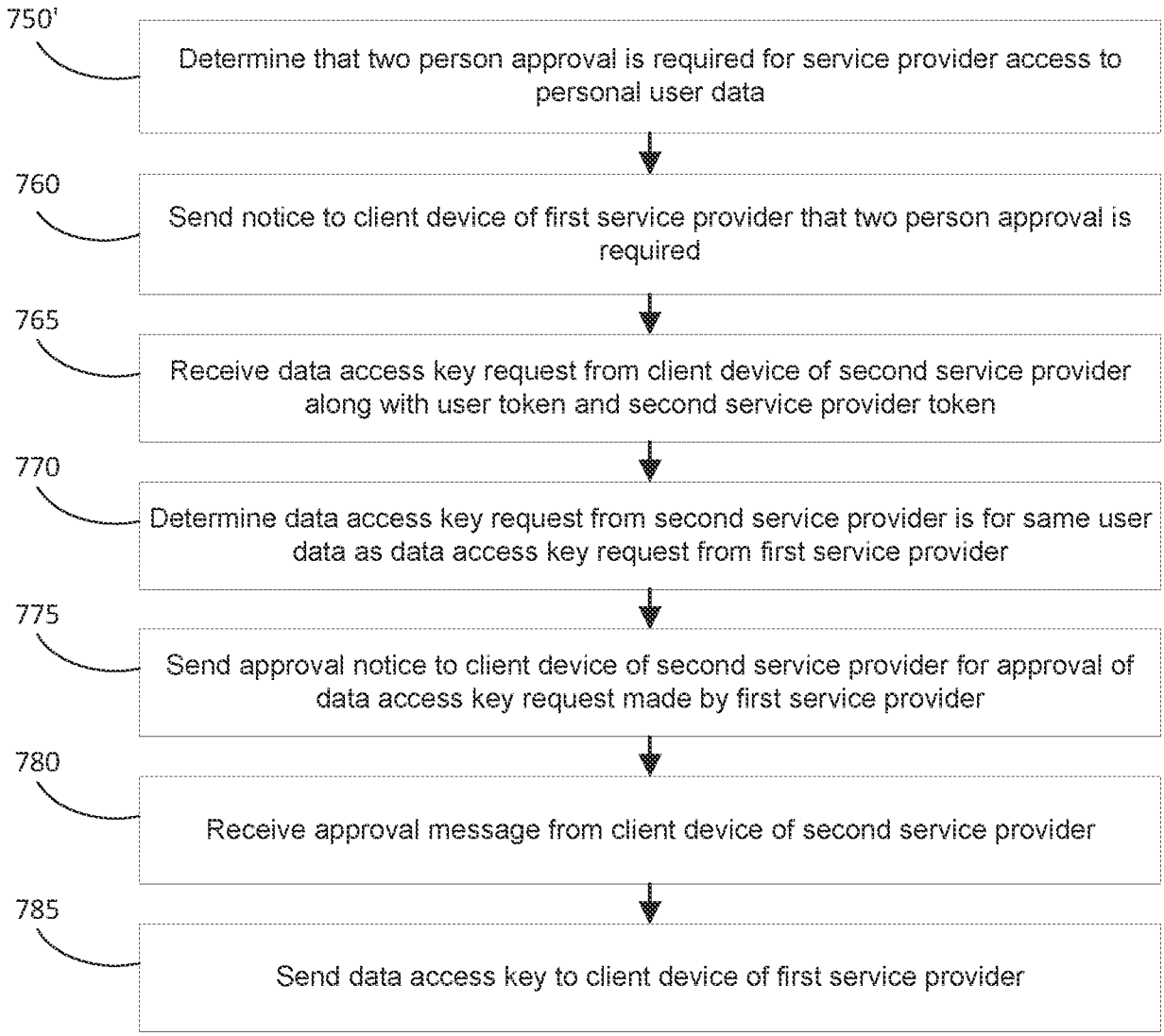
600

FIG. 6B


710
Receive data access key request from client device along with user token and service provider token
720
Identify sender of data access key request based on service provider token as Service Provider
730
Identify user based on user token
740
Verify that Service Provider is authorized to receive access to personal user data
750
Send data access key to client device

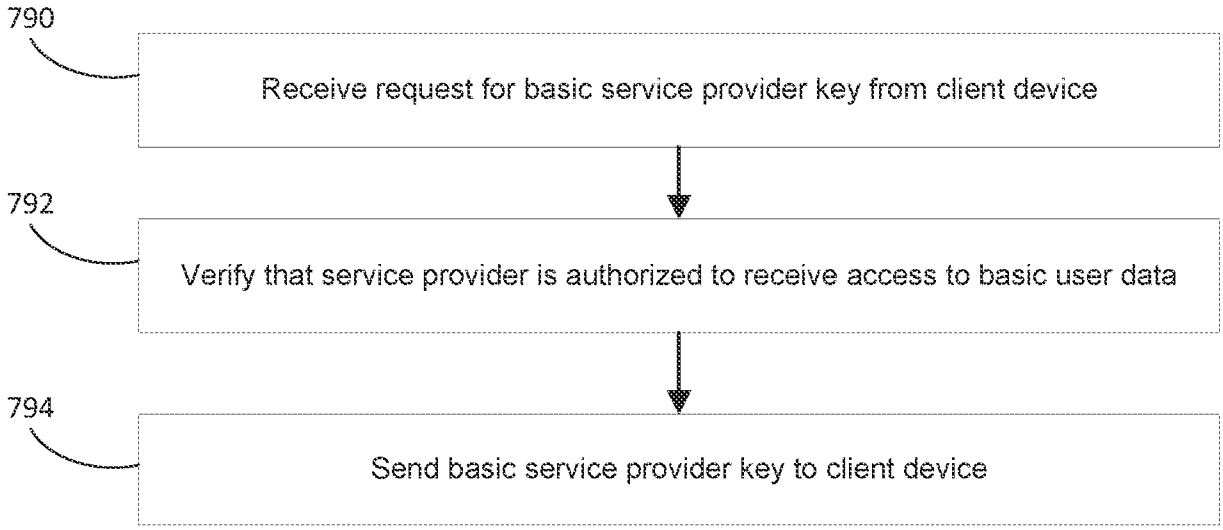
700

FIG. 7A


750'
Determine that two person approval is required for service provider access to personal user data
760
Send notice to client device of first service provider that two person approval is required
765
Receive data access key request from client device of second service provider along with user token and second service provider token
770
Determine data access key request from second service provider is for same user data as data access key request from first service provider
775
Send approval notice to client device of second service provider for approval of data access key request made by first service provider
780
Receive approval message from client device of second service provider
785
Send data access key to client device of first service provider

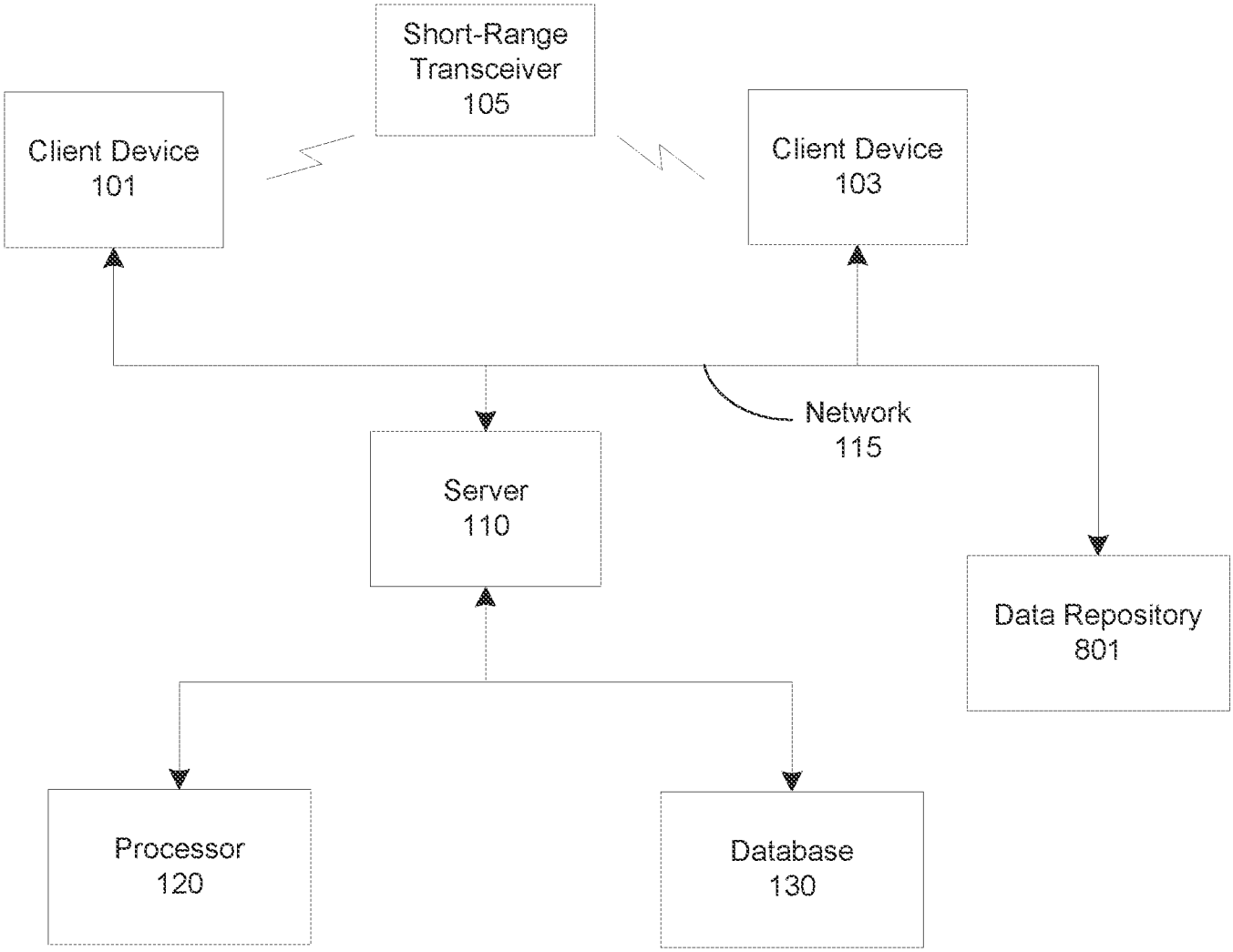
701

FIG. 7B


790
Receive request for basic service provider key from client device
792
Verify that service provider is authorized to receive access to basic user data
794
Send basic service provider key to client device

702

FIG. 7C



System 800

FIG. 8