



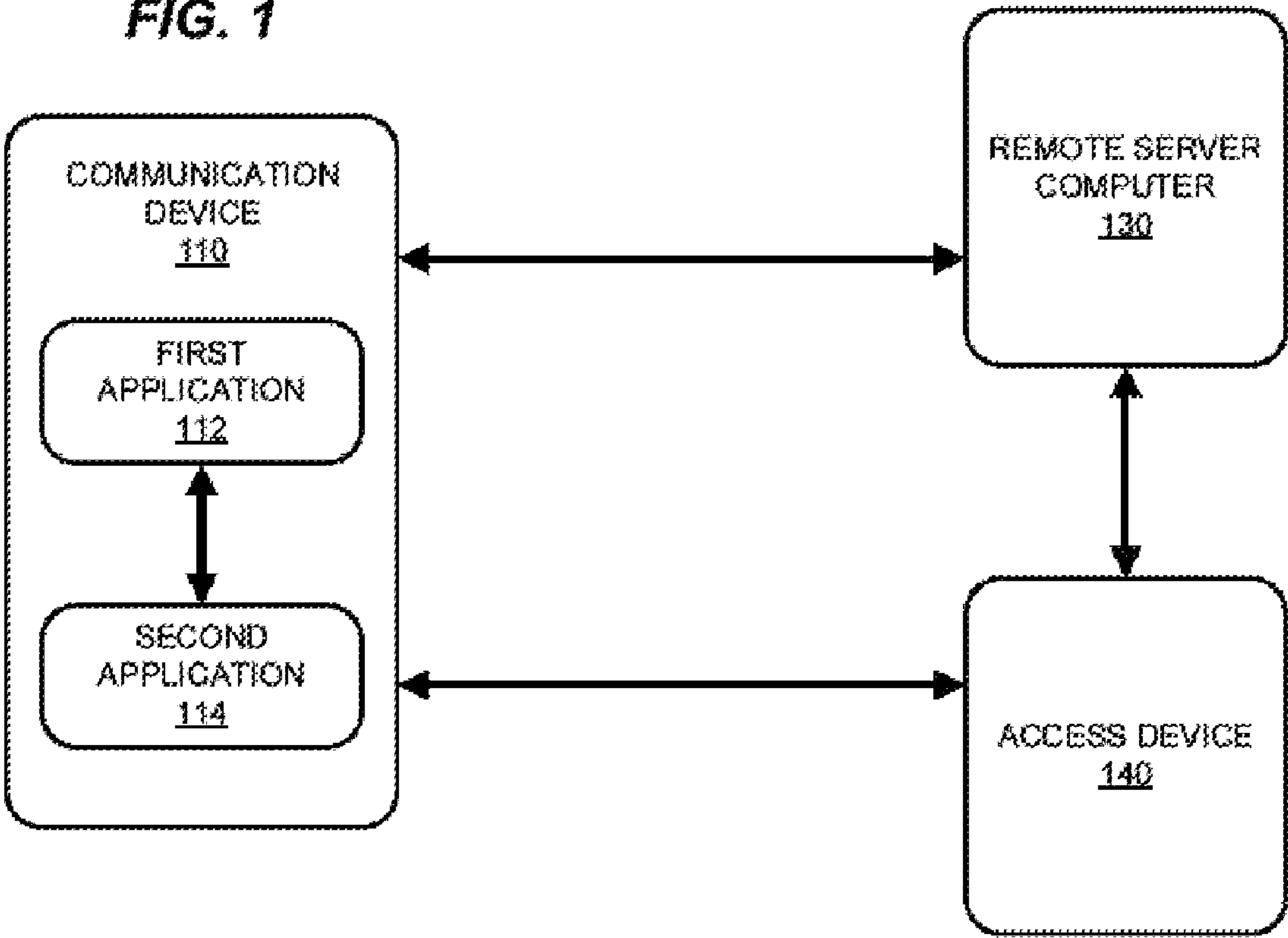
(12) **DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION**

(13) **A1**

<p>(86) Date de dépôt PCT/PCT Filing Date: 2017/01/09</p> <p>(87) Date publication PCT/PCT Publication Date: 2017/07/13</p> <p>(85) Entrée phase nationale/National Entry: 2018/06/22</p> <p>(86) N° demande PCT/PCT Application No.: US 2017/012767</p> <p>(87) N° publication PCT/PCT Publication No.: 2017/120605</p> <p>(30) Priorité/Priority: 2016/01/07 (US62/276,167)</p>	<p>(51) Cl.Int./Int.Cl. <i>H04L 29/06</i> (2006.01)</p> <p>(71) Demandeur/Applicant: VISA INTERNATIONAL SERVICE ASSOCIATION, US</p> <p>(72) Inventeurs/Inventors: CHANDOOR, MADHURI, US; CHITALIA, JALPESH, US; PETKOV, GUEORGUI, US; NOSSEIR, MOHAMED, US; BANSAL, PARVEEN, US; BELLENGER, THOMAS, US; LAW, SIMON, US...</p> <p>(74) Agent: BERESKIN & PARR LLP/S.E.N.C.R.L.,S.R.L.</p>
---	--

(54) Titre : SYSTEMES ET PROCEDES DE FOURNITURE DE PUSH POUR DISPOSITIF
(54) Title: SYSTEMS AND METHODS FOR DEVICE PUSH PROVISIONING

FIG. 1



(57) Abrégé/Abstract:
Techniques for provisioning access data may include receiving, by a first application installed on a communication device, user input selecting an account to provision to a second application installed on the communication device. The first application may

(57) **Abrégé(suite)/Abstract(continued):**

invoke the second application and send a session identifier (ID) to the second application. The second application may send a user ID associated with the second application, a device ID, and the session ID to the first application. The first application may then generate encrypted provisioning request data and send the encrypted provisioning request data to the second application. The second application may send the encrypted provisioning request data to a remote server computer to request access data that can be used to access a resource. The second application may receive the access data provided by the remote server computer based on validation of the encrypted provisioning request data.

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
13 July 2017 (13.07.2017)



(10) International Publication Number
WO 2017/120605 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:

PCT/US2017/012767

(22) International Filing Date:

9 January 2017 (09.01.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/276,167 7 January 2016 (07.01.2016) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: **CHANDOOR, Madhuri**; 3036 Silverland Drive, San Jose, California 95135 (US). **CHITALIA, Jalpesh**; 900 Metro Center Boulevard, Foster City, California 94401 (US). **PETKOV, Gueorgui**; 5860 Sterling Greens Circle, Pleasanton, California 94566 (US). **NOSSEIR, Mohamed**; 4610 Mira Loma Street, Castro Valley, California 94546 (US). **BANSAL, Parveen**; 139 Landsdowne Loop, San Ramon, California 94582 (US). **BELLENGER, Thomas**; 161 10th Avenue, San Mateo, California 94401 (US). **LAW, Simon**; 2803 Toro Drive, San Mateo, California 94403 (US).

(74) Agents: **DAVE, Urmil** et al.; Kilpatrick Townsend & Stockton LLP, 1100 Peachtree Street, #2800, Atlanta, Georgia 30309 (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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

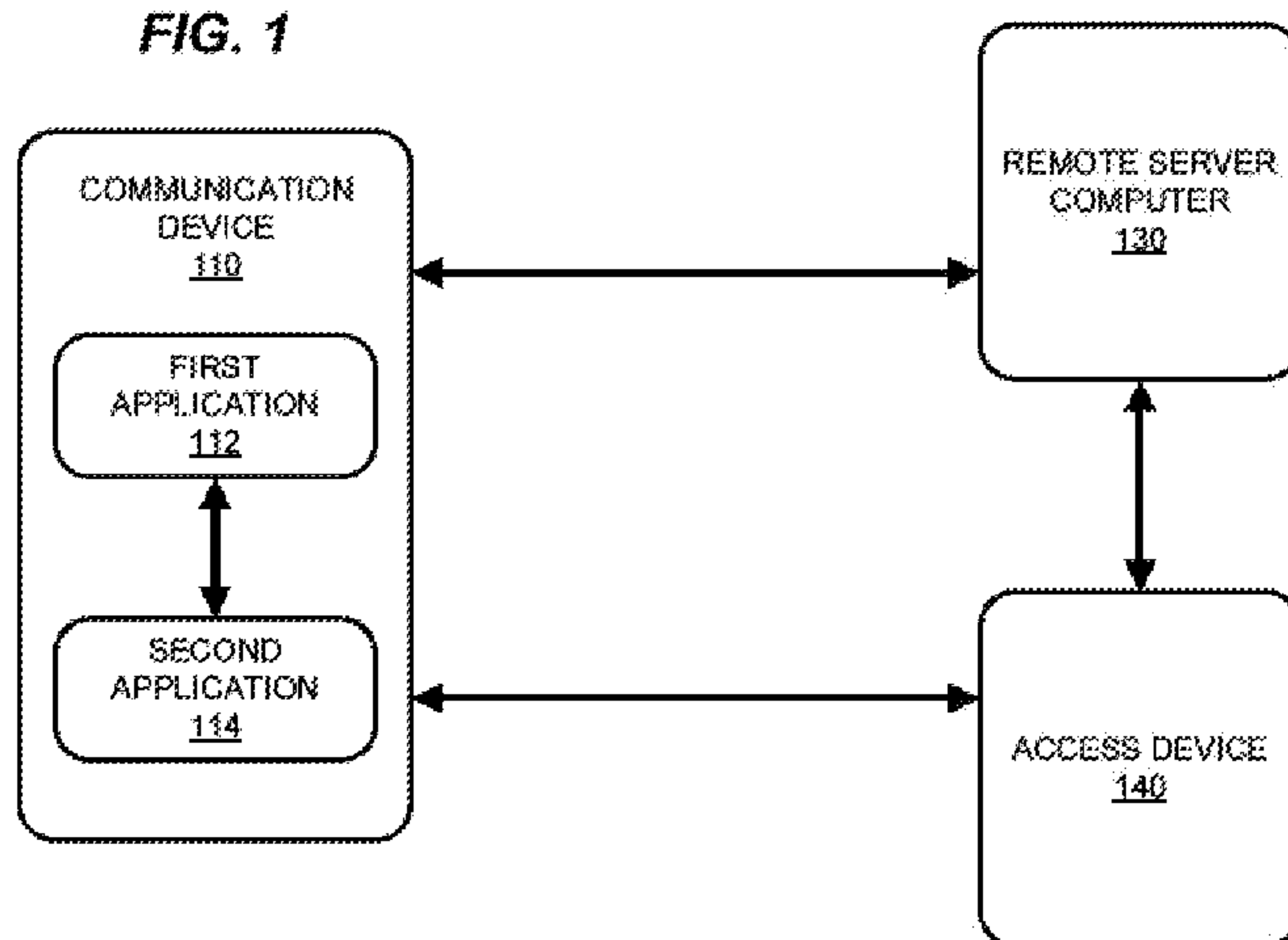
(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,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

Published:

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

(54) Title: SYSTEMS AND METHODS FOR DEVICE PUSH PROVISIONING

FIG. 1



(57) Abstract: Techniques for provisioning access data may include receiving, by a first application installed on a communication device, user input selecting an account to provision to a second application installed on the communication device. The first application may invoke the second application and send a session identifier (ID) to the second application. The second application may send a user ID associated with the second application, a device ID, and the session ID to the first application. The first application may then generate encrypted provisioning request data and send the encrypted provisioning request data to the second application. The second application may send the encrypted provisioning request data to a remote server computer to request access data that can be used to access a resource. The second application may receive the access data provided by the remote server computer based on validation of the encrypted provisioning request data.

WO 2017/120605 A1

SYSTEMS AND METHODS FOR DEVICE PUSH PROVISIONING

BACKGROUND

[0001] Communication devices can be provisioned with access data to allow a user of the communication device to obtain access to a resource. For instance, a remote server associated with the resource provider can transmit the requisite access data to be loaded onto the communication device. In some cases, a communication device can have more than one application installed on the device that allows the user to access the resource. For example, a communication device can have multiple email applications that can each be used to access a particular email account. As another example, a communication device can have multiple transaction applications that can each be used to conduct a transaction using a particular account.

[0002] In order to provision each application with the access data, a user may have to manually enter account identifying information into each individual application to identify the user's account associated with the resource provider. In addition, each application may require a separate authentication process to provision the access data. This can be a cumbersome process that adds unwanted friction to the user experience.

[0003] Some conventional systems may allow one application to request the access data be provisioned onto another application. For example, a first application may request an authentication code from a remote server associated with the resource provider, and provide the authentication code to a second application installed on the communication device. Thereafter, the second application may send the authentication code to the remote server to request the access data. However, such systems may have a security risk in that the access data transmitted from the remote server to the communication device can be susceptible to interception by an unauthorized party. If an unauthorized party comes into possession of the access data, the unauthorized party may use the access data to access the resource without permission from the user.

[0004] Embodiments of the invention address these and other problems individually and collectively.

BRIEF SUMMARY

[0005] Embodiments of the invention can include systems and methods which provide techniques for provisioning access data from a first application to a second application installed on a communication device.

[0006] Some embodiments of the invention are directed to a push provisioning method. The method may include receiving, by a first application installed on a communication device, after a user successfully authenticates to the first application, user input selecting an account to provision to a second application installed on the communication device,. The method may also include, in response to receiving the selection of the account to provision, invoking the second application by the first application and may also include additionally sending a session identifier (ID) to the second application. The first application may use the session ID to accurately track and associate the data sent by the second application, with the user authenticated in the first application.

[0007] The method may further include sending, by the second application, a user ID associated with the second application, a device ID, and the session ID to the first application. The method may additionally include generating, by the first application, encrypted provisioning request data including an account ID of the account to provision, the user ID, and the device ID provided by the second application. The method may further include sending, by the first application, the encrypted provisioning request data to the second application. The method may also include sending, by the second application, the encrypted provisioning request data to a remote server computer, along with the user ID and the device ID associated with the user in the second application. The remote server computer may utilize the user ID, the device ID and the account ID of the second application (requestor) to validate against the user ID, the device ID and the account ID provided by the first application, which are included inside the encrypted portion of the request, ensuring that the end to end exchange of data is secure and is made accessible only to the specified user. The method may further include receiving, by the second application, access data provided by the remote server computer based

on validation of the encrypted provisioning request data. The method may also include provisioning, by the second application, the access data onto the second application.

[0008] Some embodiments of the invention are directed to a communication device configured to perform the above-noted method.

[0009] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 shows a block diagram of a system according to some embodiments of the invention.

[0011] FIG. 2 shows a block diagram of a communication device according to some embodiments of the invention.

[0012] FIG. 3 shows a block diagram of a remote server computer according to some embodiments of the invention.

[0013] FIG. 4 illustrates a flow diagram illustrating a process flow according to some embodiments of the invention.

[0014] FIG. 5 illustrates a flow chart illustrating a process flow according to some embodiments of the invention.

[0015] FIG. 6 illustrates a block diagram of a building access system according to some embodiments of the invention.

[0016] FIG. 7 illustrates a block diagram of a transaction processing system according to some embodiments of the invention.

[0017] FIG. 8 illustrates a block diagram of a computing system according to some embodiments of the invention.

DETAILED DESCRIPTION

[0018] Embodiments of the invention can include systems and methods which provide techniques for provisioning access data from a first application to a second application installed on a communication device. The systems and methods can provide an improved experience for users and parties involved in the provisioning process by allowing one or more applications residing on the communication device to push access data securely to one or more other applications residing on the communication device. In some embodiments, the Identification and Verification (ID&V) process for authenticating the user of one application (e.g., the first application) can be leveraged to provision the access data to another application (e.g., the second application) such that the user can avoid entering information required for access data provisioning in each individual application residing on the mobile device. As such, an additional step up process to authenticate the user can be avoided and thereby reducing friction in the user experience. In some embodiments, the access data being provisioned can be bound to the communication device such that the access data cannot be used with another communication device. In other words, once the access data is provisioned to a particular communication device, any attempts to use the access data from a different communication device to obtain access to the resource associated with the access data will be denied,

[0019] Prior to discussing embodiments of the invention, descriptions of some terms may be helpful in understanding embodiments of the invention.

[0020] A “communication device” may be any electronic device that can be operated by a user to communicate with another device. A communication device may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile (cellular) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other wireless or wired communication medium that may provide access to a network such as the Internet or a private network. Examples of communication devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music

players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), smart appliances, or other network connected devices, etc. A communication device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device - i.e., using the other device as a relay - both devices taken together may be considered a single communication device).

[0021] “Authentication data” may include any data suitable for authenticating a user or communication device. Authentication data may be obtained from a user or a communication device that is operated by the user. Examples of authentication data obtained from a user may include PIN (personal identification number), username/password, biometric data, etc. Examples of authentication data that may be obtained from a communication device may include device serial numbers, hardware secure element identifiers, device fingerprints, phone numbers, IMEI numbers, etc.

[0022] A “remote server computer” may include a powerful computer or cluster of computers accessible via a network. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more communication devices. In some embodiments, a remote server computer can be operated by or associated with a resource provider such as a service provider (e.g., a web service provider), transit or building operator, ticketing operator, payment processing network or organization, etc.

[0023] “Access data” may include any suitable data that can be used to access a resource or create data that can access a resource. In some embodiments, access data may include credentials (e.g., PIN, username/password, passcode, etc.) or account information that can be used to access the resource. For example, the access

data can be login information used for accessing a web service. As another example, the access data can be account information for a payment account. Account information may include an account identifier such as a primary account number (PAN), verification values (e.g., CVV, CVV2, dCVV, dCVV2), or other account data that can be used to verify an account. In some embodiments, access data may be data that can be used to activate account data. For example, in some cases, account information may be stored on a communication device, but may not be activated until specific information is received by the communication device. This specific information may be characterized as access information in some embodiments. In some embodiments, access data can include data that can be used to access a restricted location. Such information may be, for example, ticket information for an event, data to access a building, transit ticket information, etc. In some embodiments, the access data can be pseudo-credentials or pseudo account information such as a token that can be used as a substitute for the real credentials or real account identifier. In contrast to a real credentials or real account identifier which can be used from any device to access a resource, access data in the form of pseudo-credentials or pseudo account information can be bound to a particular communication device such that the access data can only be used from the particular communication device to access the resource.

[0024] A "token" may include a substitute identifier for some information. For example, a transaction token may include an identifier for a transaction account that is a substitute for an account identifier, such as a primary account number (PAN). For instance, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a transaction. The token may also be used to represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be

generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0025] An “application” may be a computer program executable from a communication device that is used to perform one or more tasks. In some embodiments, performing a task may involve using access data to access a resource. Examples of applications may include a browser application to access the Internet, an email application to access an email account, a transit application to access a restricted area, a transaction application to access a payment or banking account to conduct a transaction, etc.

[0026] A “digital wallet” application can be an application that stores information that can be used in a variety of transactions. For example, a digital wallet application can store user profile information, payment information (e.g. PANs or primary account numbers, payment tokens (i.e., PAN substitutes), verification values such as CVVs, etc.), bank account information, and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like.

[0027] A “timestamp” may include data relating to any suitable time. For example, a timestamp may be a time, date, month, year, or any suitable combination of the above. The timestamp element could also be derived from the time, date, month, year, or any suitable combination of the above. An encrypted timestamp element may be a data element that may include an encrypted time, date, month, year, and/or suitable combination of the above.

[0028] An “access device” may be any suitable device for obtaining access to a resource. An access device may generally be located in any suitable location, such as at the entrance of a restricted area or at a location of a merchant. An access device

may be in any suitable form. Some examples of access devices include POS devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a payment device and/or a user communication device.

[0029] An “issuer” may typically refer to a business entity (e.g., a bank) that maintains an account for a user that is associated with a communication device such as an account enrolled in a mobile application installed on a portable communication device. An issuer may also issue account parameters associated with the account to a communication device. An issuer may be associated with a host system that performs some or all of the functions of the issuer on behalf of the issuer.

[0030] An “authorization request message” may be an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to “identification information” including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0031] An “authorization response message” may be an electronic message reply to an authorization request message generated by an issuing financial institution or a

payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0032] A “processor” may refer to any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include CPU comprises at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0033] A “memory” may be any suitable device or devices that can store electronic data. A suitable memory may comprise a computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0034] A “key” may refer to a piece of information that is used in a cryptographic algorithm to transform input data into another representation. A cryptographic algorithm can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data

encryption standard (TOES), data encryption standard (DES), advanced encryption standard (AES), etc.

[0035] FIG. 1 shows a block diagram of a system according to some embodiments of the invention. FIG. 1 shows a communication device 110 in communication with a remote server computer 130. The communication device 110 may store a first application 112 and a second application 114.

[0036] The remote server computer 130 may be operated by or associated with a resource provider, and can be configured to provision the communication device 110 with access data. It may include a processor and a computer readable medium comprising code which causes the processor to perform any suitable method associated with provisioning the communication device 110 with access data. It may also maintain a database of access data and device identifiers (e.g., an IP or internet protocol address, serial number, IMEI number, or phone number, etc.) for various communication devices provisioned with access data. In some embodiments, remote server computer 130 may provision access data to the first application 112. Provisioning the first application 112 may require the user to manually enter credentials used for the provisioning process (e.g., account information associated with the user of communication device 110). Once provisioned with the access data, the first application 112 may provide the access data to an access device 140 to obtain access to a resource. Access device 140 may forward the access data to remote server computer 130 for verification. In some embodiments, access device 140 can be part of remote server computer 130 (e.g., if the resource being accessed is a web-based service provided by remote server computer 130).

[0037] In accordance with the techniques described herein, the first application 112 can be used to push the access data to the second application 114 installed on communication device 110. In some embodiments, provisioning the second application 114 can be done without requiring the user to reenter the account information used for the provisioning process because the user and the user's account has already been verified by the remote server computer 130 during provisioning of the first application 112. Once provisioned with the access data, the second application 114 may provide

the access data to an access device 140 independently from the first application 112 to obtain access to a resource.

[0038] Each of the entities in FIG. 1 may communicate through any suitable communication channel or communications network. A suitable communications network may be any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like.

[0039] FIG. 2 illustrates a block diagram of a communication device 201, according to some embodiments. Communication device 201 may include device hardware 204 coupled to a memory 202. Device hardware 204 may include a processor 205, a communications subsystem 209, use interface 206, a display screen 207 (which may be part of user interface 206), and an optional contactless interface 208 (e.g., if communication device 201 is a portable communication device or has wireless communication functionalities). Processor 205 can be implemented as one or more integrated circuits (e.g., one or more single core or multicore microprocessors and/or microcontrollers), and is used to control the operation of communication device 201. Processor 205 can execute a variety of programs in response to program code or computer-readable code stored in memory 202, and can maintain multiple concurrently executing programs or processes. Communications subsystem 209 may include one or more RF transceivers and/or connectors that can be used by communication device 201 to communicate with other devices and/or to connect with external networks. User interface 206 can include any combination of input and output elements to allow a user to interact with and invoke the functionalities of communication device 201. In some embodiments, display screen 207 may be part of user interface 206.

[0040] Contactless interface 208 may include one or more RF transceivers to interact with a contactless reader of an access device to access a resource (e.g., to enter a restricted area, to conduct a transaction, etc.). In some embodiments,

contactless interface 208 can be accessed by applications in application environment 210 or operating system 220 to communicate with an access device. In some embodiments, display 207 can also be part of contactless interface 208, and is used, for example, to communication with an access device using QR codes, bar codes, or other optical communication techniques, etc.

[0041] Memory 202 can be a non-transitory computer readable storage medium implemented using any combination of any number of non-volatile memories (e.g., flash memory) and volatile memories (e.g., DRAM, SRAM), or any other computer readable storage medium, or a combination thereof media. Memory 202 may store a OS 220 and an application environment 210 where one or more mobile applications (e.g., applications 212 and 214) to be executed by processor 205 reside.

[0042] According to some embodiments, the first application 212 can be an application associated with and/or provided by a resource provider, and the first application 212 is used to access a resource provided by the resource provider. For example, the first application 212 can be a transit application used to access a restricted area provided by a transit or building operator, an issuer application used to conduct transactions using an account issued by the issuer, or a web-service application used to access a web-based service such as email, photo-sharing, social media, etc. provided by the web-based service provider. When the user of communication device 201 installs the first application 212, the user may initiate an enrollment process with a remote server computer to provision the first application 212 with access data 234 that is used to access the resource associated with the resource provider. The user may be requested to manually enter account information such as a real account identifier to obtain access data 234. In some embodiments, the provisioned access data 234 can be used as a substitute for the real account identifier to obtain access to the resource. For example, the first application 212 can provide the provisioned access data 234 in the form of pseudo-credentials or pseudo-account identifier such as a token to an access device to gain access to the resource.

[0043] In some embodiments, the first application 212 may include an authentication module 238 that is used to authenticate the user to use the first

application 212. For example, the authentication module 238 may request the user to enter a PIN or other user identification information to authenticate the user each time the user attempts to use the first application 212. The authentication module 238 may authenticate the user locally at the communication device 201, or send the user identification information to a remote sever computer to authenticate the user according to the identification and verification (ID&V) requirements of the resource provider.

[0044] The first application 212 may also include an encryption module 236 that is used to encrypt sensitive data provided by the first application 236. For example, during installation or enrollment, the first application 212 can be provided with a shared key or shared secret that is only known to the first application 212 and the remote server computer. The first application 212 can then encrypt communications intended for the remote server computer using the shared key or derivative keys derived from the shared key or shared secret. The remote server computer can then decrypt the communication using the shared key or derivative keys derived from the shared key or shared secret to verify that the communication originated from the first application 212. In some embodiments, encryption module 236 can be part of the OS 220, and the first application 212 may encrypt data by calling the encryption service provided by OS 220.

[0045] In some embodiments, the first application 212 may encrypt data used in a provisioning request (e.g., a PAN) to push access data to another application. The encryption can be performed using JavaScript Object Notation (JSON) techniques such as JSON Web Encryption (JWE) or using any other suitable encryption technique. The JWE techniques may use the shared key or shared secret to encrypt the data. In some embodiments, compact serialization style (e.g., elements separated by “.”) can be used. All fields are can be base 64 and URL Safe encoded. A 256-bit Content Encryption Key (CEK) can also be used. In some embodiments, an AES encryption algorithm such as AES-GCM-256KW algorithm for encryption of the CEK, and a 96-bit Initialization Vector (IV) can be used. An Authentication Tag (e.g., e.g., 128-bits) can also be generated as an additional output of the AES-GCM-256 encryption. String to byte and vice-versa conversions can be performed using UTF-8 charset.

[0046] Communication device 201 may also include a second application 214 that is used to access the same resource accessible by the first application 212. The second application 214 can be a third-party application that is provided by an entity different from the resource provider. In some embodiments, the second application 214 can be a multi-operator transit application that can be used to access various restricted areas associated with multiple transit or building operators, a digital wallet application that can be used to conduct transactions using various account issued by multiple issuers, or a multi-functional web-service application that can be used to access various web-based services provided by multiple web-based service providers (e.g., a digital assistant application that can access multiple email accounts of the user, a social media application that can access multiple social media accounts of the user, etc.).

[0047] According to some embodiments, the first application 212 can be used to provision the access data for accessing the resource to the second application 214. For example, the first application 212 can be used to generate encrypted provisioning request data that is sent to the remote server computer to request access data for the second application 214. The provisioning request data can be encrypted based on a shared key or shared secret known only to the first application and the remote server computer. Since the first application 212 is provided by the resource provider, the first application 212 can be considered a trusted application by the remote server computer. If the remote server computer is able to properly decrypt the provisioning request data and thus verify that the provisioning request data was generated by the trusted first application 212, the remote server can then generate the access data for provisioning to the second application 214. Both the access data provisioned to the first application 212 and the second application 214 can be linked to the same account of the user, and thus allowing either application to access the resource using the same account.

[0048] In some embodiments, although the access data provisioned to the second application 214 is linked to the same account, the access data provisioned to the second application 214 can be the same or different than the access data provisioned to the first application 212. For example, the first application 212 can be provisioned with the real credentials, whereas the second application 214 can be

provisioned with pseudo-credentials or pseudo-account information (e.g., a token that is a substitute for a real account identifier). As another example, both the first application 212 and the second application 214 can be provisioned with the same pseudo-credentials or pseudo-account information. As a further example, the first application 212 can be provisioned with a first pseudo-credentials or a first pseudo-account information, whereas the second application can be provisioned with a second pseudo-credentials or second pseudo-account information that is linked to the same account. In this latter case, the access data provisioned to a particular application can be bound to the specific application such that the access data provisioned to one application cannot be used from another application. In some embodiments, the access data being provisioned can also be bound to the communication device such that the access data cannot be used with another communication device.

[0049] FIG. 3 shows a block diagram of an remote server computer 300 according to some embodiments of the invention. Remote server computer 300 can be operated by or associated with a resource provider that provides a resource accessible from a communication device. For example, remote server computer 300 can be associated with a web-service provider, a transit or building operator, an issuer, a payment processing network or organization, etc. In some embodiments, the remote server computer may provide and/or support an application (e.g., first application 112 or 212) installed on a communication device that is used to access a resource associated with remote server computer 300. The remote server computer 300 may include a processor 310, which may be coupled to a system memory 320 and an external communication interface 330. A computer readable medium 340 may also be operatively coupled to the processor 310. The computer readable medium 340 may comprise a number of software modules including a communication module 342, cryptographic module 346, a validation module 348, and an access data generation module 344.

[0050] The communication module 342 may comprise code that causes the processor 310 to generate messages, forward messages, reformat messages, and/or otherwise communicate with other entities. For example, communication module 342

can be used to facilitate communications between remote server computer 300 and a communication device operated by a user. Communication module 342 may also facilitate communications with access data database 350 (or with a separate computer that has access to access data database 350) to lookup access data information or to write access data generated by remote server computer 300 to the access data database 350.

[0051] The cryptographic module 346 may include any suitable encryption/decryption algorithms to encrypt or decrypt data. For example, the cryptographic module 346 may decrypt an encrypted payload received from a communication device. The encrypted payload may include encrypted provisioning request data generated by an application installed on the communication device. Suitable data encryption algorithms may include DES, triple DES, AES, etc. The cryptographic module 346 may utilize symmetric or asymmetric encryption techniques to encrypt/decrypt and/or verify data. It may also store encryption keys that can be used with such encryption algorithms. For example, a shared key or shared secret can be established between an application installed on the communication device and remote server computer 300, and encrypted communications originating from the application can be decrypted using the shared key or shared secret, or a derivative key derived from the shared information.

[0052] The validation module 348 may comprise code, which causes the processor 310 to validate data from a user's communication device. For example, during provisioning of access data to a communication device, validation module 348 may verify the account information provided in the provisioning request. This may involve verifying that the account information corresponds to a valid account. Validation module 348 may also carry out an ID&V process to verify the user of the communication device. For example, validation module 348 may verify a PIN or other user identifying information requested from the user to authenticate the user. If the information is validated, validation module 348 may request access data generation module 344 to generate access data for provisioning to the communication device.

[0053] In some embodiments, validation module 348 can also be used to verify the access data provided by the communication device when the communication device is attempting to access the resource associated with the service provider. For example, the communication device may provide access data previously provisioned on the communication device to an access device, and the access device may forward the access data (e.g., in an authorization request message) to remote server computer 300. Upon receiving the access data, validation module 348 may query the access data database 350 to determine if the received access data is valid. In some embodiments, if the access data is bound to the communication device, validation module may also verify that the access data was provided by the corresponding communication device. If the received access data is in the form of pseudo-credentials or pseudo-account information, validation module 344 may also retrieve the real credentials or real account information from access data database 350 if such information is needed to authorize access to the resource.

[0054] The access data generation module 344 may include code for implementing an algorithm to generate access data for provisioning to an application of a communication device. Access data generation module 344 can be initiated by validation module 348 to generate the access data upon validation of the provisioning request data. In some embodiments, if the access data being provisioned is in the form of pseudo-credentials or pseudo-account information (e.g., a token), the access data can be generated randomly or be based on the actual credentials or account information. In some embodiments, the access data can be generated by selecting the access data from a list of predefined access data for a particular account. If the access data is generated based on the actual credentials or account information, the access data can be generated by encrypting the credentials or account information using data associated with the provisioning request such as a session ID associated with the request, device ID of the communication device requesting the access data, application ID of the application requesting or being provisioned with the access data, or user ID associated with the user of the communication device, etc., or any combination thereof. For example, a combination of one or more pieces of data from the provisioning request

can be used to generate an encryption key that is used to encrypt the actual credentials or actual account information to generate the access data. In some embodiments, instead of relying on encryption, the access data can be generated by performing one or more mathematical operations on the actual credentials or actual account information. In some embodiments, the mathematical operations may use any combination of the provisioning request data as operands (e.g., adding the device ID to the actual account information, etc.). The access data can also be generated by combining different portions of the actual credentials or account information with portions of any combination of the provisioning request data (e.g., concatenation of different digits or characters from the various pieces of data). In some embodiments, the access data generated by the access data generation module 344 can be written to access data database 350.

[0055] Access data database 350 can be coupled to remote server computer 300 or can be accessible by remote server computer 300 via a separate computer. Access data database 350 can store the access data generated by remote server computer 300 and associate the access data with information that may be needed to validate the access data when the access data is received to request access to a resource. For example, access data database 350 can store the access data together with the real credentials or real account information for which the access data substitutes for. In some embodiments, if the access data is bound to a particular communication device and/or particular application, the access data can be stored together with the device ID of the communication device or application ID of the application that was received as part of the provisioning request data. In this manner, when the access data is received, the access data database 350 can be queried to retrieve the device ID and/or the application ID to validate that the access data is being used with the proper communication device and/or application that was provisioned with the access data.

[0056] FIG. 4 illustrates a flow diagram illustrating a process flow according to some embodiments of the invention. In the process flow illustrated in FIG. 4, a first application 412 installed on a communication device may push access data for provisioning to a second application 414 installed on the communication device. In

some embodiments, the first application 412 can be an application provided by a resource provider such as a web-service application used to access a web-based service such as email, photo-sharing, social media, etc. provided by a web-based service provider, a transit application used to access a restricted area provided by a transit or building operator, an issuer application used to conduct transactions using an account issued by the issuer, etc. In some embodiments, the second application 414 is an application that can be used to access the same resource accessible by the first application 412, and can be provided by a third-party. For example, the second application 414 can be a multi-functional web-service application that can be used to access various web-based services provided by multiple web-based service providers (e.g., a digital assistant application that can access multiple email accounts of the user, a social media application that can access multiple social media accounts of the user, etc.), a multi-operator transit application that can be used to access various restricted areas associated with multiple transit or building operators, a digital wallet application that can be used to conduct transactions using various account issued by multiple issuers, etc.

[0057] At step S402, a user 410 of a communication device may interact with the first application 412 residing on the communication device to initiate provisioning of the access data to the second application 414. The first application 412 may be an application that is already familiar to the user 410 that the user has previously used, and access data for accessing a resource associated with the first application 412 may have already been provisioned to the first application 412 during an initial enrollment process. If user 410 is not already logged on to the first application 412, user 410 may be requested to enter login information such as a PIN or password to authenticate the user. Once the user has successfully logged onto the first application 412, the user can be assumed to be authenticated because the user has already gone through an ID&V process during the initial enrollment process of the first application 412. User 410 may then select the push-provisioning feature of the first application 412 on the user interface of the communication device. The first application 412 may present a list of other applications that the first application 412 can provision access data to. The other

applications may include the second application 414. The user 410 may then select the second application 414 from the list of applications presented by the first application 412.

[0058] At step S404, after the user 410 selects the second application 414 for provisioning, the first application 412 may invoke and launch the second application 414. The first application 412 may send a session identifier (ID) that identifies the current provisioning session to the second application 414. The session ID may be a unique identifier (e.g., a random number, counter value, etc.) that may be short lived and may be uniquely associated with the user's account associated with the first application 412. In some embodiments, the session ID is generated by the first application 412 or can be provided to the first application 412 by the remote server computer 430. The first application 412 may use the session ID to track and associate the data sent by the second application 414 with the user authenticated in the first application 412.

[0059] At step S406, the second application 414 may request the user 410 to enter login information such as a user ID associated with the second application 414 if the user has not already logged in. In some embodiments, the login request by the second application 414 may be in the form of a "pop-up" window that may appear while the first application 412 is still opened. In some embodiments, the second application 414 may temporarily appear on the display of the communication device to accept the user's login information, and then the user may be returned to the first application 412. At step S408, the user 410 may enter login information such as a user ID associated with the second application 414 to login to the second application 414. At step S410, the login information is provided to the second application 414.

[0060] At step S412, if the user successfully logs into the second application 414, the second application 414 may send the user ID of the user associated with the second application 414, a device ID identifying the communication device, and the session ID to the first application 412. The user ID may identify the user 410 that logged in to the second application 414 in step S408. The device ID may be a unique device ID associated with the communication device 410. In some embodiments, the device ID

may uniquely identify the specific installation of the second application 414 on the communication device 410. The session ID may be the session ID received by the second application 414 from the first application 412 in step S404. In some embodiments, the second application 414 may also send an application ID that uniquely identifies the second application 414 to the first application 412.

[0061] After the second application sends the user ID, device ID, and session ID to the first application 412, the first application may generate an encrypted provisioning request by encrypting provisioning request data. The provisioning request data being encrypted may include an account ID (e.g., a PAN) of the account for which the access data is being provisioned to the second application 414. The account ID is available to the first application 412 because the account used for accessing the resource has previously been provisioned to the first application 412. The provisioning request data being encrypted may also include the, user ID, and the device ID received by the first application 412 from the second application 414. In some embodiments, provisioning request data being encrypted may also include the session ID and/or application ID of the second application 414. The encrypted provisioning request data may also include a timestamp indicating when the encrypted provisioning request was generated.

[0062] At step S414, after the first application 412 generates the encrypted provisioning request, the first application 412 may send the encrypted provisioning request including the encrypted provision request data to the second application 414. In some embodiments, the first application 412 may also provide an unencrypted application ID of the first application 412 to the second application 414. In some embodiments, the first application 412 may also provide an authentication indicator that indicates whether the user has been authenticated by the first application 412.

[0063] At step S416, after the first application 412 provides the encrypted provisioning request to the second application 414, the second application 414 may send the encrypted provisioning request to the remote server computer 430 for validation of the provisioning request. In some embodiments, the second application 414 may send the unencrypted application ID of the first application 412 together with the encrypted provisioning request to the remote server computer 430 such that the

remote server computer 430 can retrieve the appropriate key or shared secret to decrypt the encrypted provisioning request. In some embodiments, the second application 414 may also send the authentication indication to the remote server computer 430. The second application 414 may send the encrypted provisioning request to the remote server computer 430 via an enrollment Application Program Interface (API).

[0064] Upon receiving the encrypted provisioning request, the remote server computer 430 may validate and/or verify the data in the encrypted provisioning request. The remote server computer 430 may decrypt the encrypted provisioning request using a shared key or shared secret known to the remote server computer 430 and the first application 412 to access the data elements (e.g., any one or more of account ID, user ID, device ID, session ID, timestamp, application ID, etc.) within the encrypted provisioning request. The remote server computer 430 can verify that the encrypted provisioning request was generated by the first application 412 if the remote server computer 430 can properly decrypt the provisioning request. If the remote server computer 430 verifies that the encrypted provisioning request was generated by the first application 412, the remote server computer 430 can continue with the validation process because the first application 412 is a trusted application of the remote server computer 430. If the remote server computer 430 determines that the encrypted provisioning request did not originate from the first application 412, the remote server computer 430 may terminate the provisioning session.

[0065] The remote server computer 430 may then analyze and validate the data elements within the decrypted provisioning request. The validation may include analyzing the timestamp in the decrypted provisioning data. For example, the timestamp may be compared to a current time at which the remote server computer 430 received the encrypted provisioning data from the second application 414. The remote server computer 430 may validate the provisioning request if the difference between the current time and the time indicated by the timestamp is less than a predefined time threshold. For example, if the difference is less than 20 minutes, the remote server computer 430 may validate the provisioning request. In some embodiments, if the

session ID was provided by the remote server computer 430, the timestamp can be omitted from the provisioning request, and the remote server computer 430 can determine if the provisioning request was received within the predefined time threshold by comparing the time at which the remote server computer 430 provided the session ID to the first application 412 and the time at which the provisioning request was received. The validation may also include determining whether the account ID corresponds to a valid account ID associated with the first application 412 and the resource provider, that the user ID is a valid user ID for the second application 414, and/or that the device ID corresponds to a valid communication device on which the first application 412 was installed.

[0066] In some embodiments, if the authentication indicator indicating whether the user has been authenticated by the first application 412 is provided to the remote server computer 430, the remote server computer 430 can determine whether any additional step-up authentication is required. For example, if the authentication process of the first application 412 meets the requirements of the ID&V process of the resource provider, and the authentication indicator indicates that the user has been successfully authenticated by the first application 412, then no additional step-up authentication may be necessary, and the remote server computer 430 can provision access data to the second application 412 without requiring the user to manually enter any additional authentication information.

[0067] After the remote server computer 430 validates the provisioning request, the remote server computer 430 may generate access data that the second application 414 can use to access a resource, and send the access data to the second application 414 at step S418. For example, the access data may include user credential data that the second application 414 can use to access a service associated with the first application 412 and/or the remote server computer 430. In some embodiments, the access data may include a token that is a substitute for the account ID. For example, if the account ID is a primary account number (PAN), the access data may include a token that is a substitute for the PAN and can be used to conduct transactions. In some embodiments, the access data can be bound to the communication device 410

and may not be used with a different communication device. For example, the access data can be linked to the device ID received in the provisioning request. In this manner, if an attempt to access the resource using the access data is received from a communication device with a different device ID, the access to the resource can be denied. In contrast to conventional push provisioning techniques that may not bound the access data to a device ID, the techniques described herein can prevent the access data from being used by an unauthorized party if the access data is intercepted by the unauthorized party during the provisioning process.

[0068] Upon receiving the access data, the second application 414 can complete the provisioning process, for example, by storing the access data in a secured memory location accessible by the second application 414. Thereafter, the second application 414 can provide the access data, for example, to an access device to gain access to the resource associated with the access data. At step S420, the second application 414 may then, either directly or via the first application 412, display or present a success message to the user 410 via the user interface of the communication device 410 to indicate that the second application 414 has been successfully provisioned with the access data. At step S422, the second application 414 can redirect the user 410 back to the first application 412, and the first application 412 may also display a success message to indicate that the provisioning process has completed.

[0069] FIG. 5 illustrates a flow diagram illustrating a process flow 500 according to some embodiments of the invention. Process flow 500 can be used for pushing access data by a first application to a second application.

[0070] At block 502, a first application installed on a communication device may receive user input selecting an account to provision to a second application installed on the communication device. At block 504, in response to receiving the selection of the account to provision, the first application may invoke the second application and send a session identifier (ID) to the second application. At block 506, the second application may send a user ID associated with the second application, a device ID, and the session ID to the first application. At block 508, the first application may generate encrypted provisioning request data including an account ID of the account to provision,

the user ID, and the device ID. In some embodiments, the encrypted provision request data may also include other data elements such as the session ID. At block 510, the first application may send the encrypted provisioning request data to the second application. At block 512, the second application may send the encrypted provisioning request data to a remote server computer associated with a resource provider to request access data that can be used to access the resource.

[0071] At block 514, the second application receives the access data provided by the remote server computer based on validation of the encrypted provisioning request data. In some embodiments, the validation of the encrypted provisioning request data may include decrypting the received encrypted provisioning request data using a key associated with the first application to determine that the encrypted provisioning request data was generated by the first application. In some embodiments, the encrypted provisioning request data may include a timestamp, and the validation of the encrypted provisioning request data may include determining whether a difference between a time at which the encrypted provision request data was received by the remote server computer and the time indicated in the timestamp is within a predefined time threshold. In some embodiments, the validation of the encrypted provisioning request data may include determining that the account ID is a valid account ID associated with first application.

[0072] At block 516, the second application provisions the access data onto the second application. In some embodiments, the access data may include user credential data that the second application can use to access a service associated with the first application. In some embodiments, the access data can be a token that is a substitute for the account ID. In some embodiments, the access data may allow a user of the communication device to access a building. In some embodiments, the access data provided by the remote server computer can be bound to the communication device and cannot be used with a different communication device.

[0073] FIG. 6 illustrates a building access system including a communication device that is provisioned with access data and that can allow a user to access a location such as a building, according to some embodiments. The communication

device 630 can be provisioned with access data according to the techniques described herein and be operated by a user 610. The communication device 630 can interact with the access device 640 and pass access data to the access device 640 (e.g., by launching the application provisioned with the access data). The access device 640 may locally verify the received access data or it may communicate with a remotely located authentication server computer (not shown). The remotely located authentication server computer may verify that the access data is authentic and may transmit a signal indicating this back to the access device 640. The access device 640 may then proceed to let the user 610 enter the building 620.

[0074] FIG. 7 illustrates a transaction processing system that includes a communication device 710 such as a mobile device provisioned with access data to allow a user to access an account to pay for a good or service at a merchant. A user 701 that can operate a communication device 710. The user 701 may use the communication device 710 to pay for a good or service at a merchant. The merchant may operate a merchant computer 750 and/or an access device 740. The merchant may communicate with an issuer computer 730 via an acquirer computer 720 and a payment processing network 760.

[0075] The payment processing network 760 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The payment processing network may use any suitable wired or wireless network, including the Internet.

[0076] A transaction flow using a communication device 710 at an access device 740 (e.g. POS location) can be described as follows. A user 701 presents his or her communication device 710 to an access device 740 to pay for an item or service (e.g.,

by launching an application provisioned with access data to initiate communication with access device 740). The communication device 710 and the access device 740 can interact such that access data from the communication device 710 (e.g. PAN, a token, verification value(s), expiration date, etc.) is received by the access device 740 (e.g. via contact or contactless interface). The merchant computer 750 may then receive this information from the access device 740 via a communication interface. The merchant computer 750 may then generate an authorization request message that includes the information received from the access device 740 (i.e. access data) along with additional transaction information (e.g. a transaction amount, merchant specific information, etc.) and electronically transmits this information to an acquirer computer 720. The acquirer computer 720 may then receive, process, and forward the authorization request message to a payment processing network 760 for authorization.

[0077] Prior to the occurrence of a credit or debit-card transaction, the payment processing network 760 may have an established protocol with each issuer on how the issuer's transactions are to be authorized. In some cases, such as when the transaction amount is below a threshold value, the payment processing network 760 may be configured to authorize the transaction based on information that it has about the user's account without generating and transmitting an authorization request message to the issuer computer 730. In other cases, such as when the transaction amount is above a threshold value, the payment processing network 760 may receive the authorization request message, determine the issuer associated with the access data provided by communication device 710, and forward the authorization request message for the transaction to the issuer computer 730 for verification and authorization. Once the transaction is authorized, the issuer computer 730 may generate an authorization response message (that may include an authorization code indicating the transaction is approved or declined) and transmit this electronic message via its communication interface to payment processing network 760. The payment processing network 760 may then forward the authorization response message to the acquirer computer 720, which in turn may then transmit the electronic message to

comprising the authorization indication to the merchant computer 750, and then to the access device 740.

[0078] At the end of the day or at some other suitable time interval, a clearing and settlement process between the merchant computer 750, the acquirer computer 720, the payment processing network 760, and the issuer computer 730 may be performed on the transaction.

[0079] FIG. 8 is a high level block diagram of a computer system that may be used to implement any of the entities or components described above. The subsystems shown in FIG. 8 are interconnected via a system bus 875. Additional subsystems include a printer 874, keyboard 878, system memory 872, and monitor 876, which is coupled to display adapter 882. Peripherals and input/output (I/O) devices, which couple to I/O controller 871. For example, the external interface 822 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner, via an input/output port 877. The interconnection via system bus 875 allows the central processor 873 to communicate with each subsystem and to control the execution of instructions from system memory 872 or the storage device(s) 879, as well as the exchange of information between subsystems. The system memory 872 and/or the storage device(s) may be embodied by a computer-readable medium.

[0080] Embodiments of the invention have a number of advantages. For example, as noted above, in embodiments of the invention, a second application (which can be an untrusted application) may be provisioned with access data by making the request for the access data using a trusted first application associated with an authorizing entity (e.g., remote server computer associated with an issuer of an account). The authorizing entity can be confident that the request for the access data is authentic since the application is a trusted application. Also, the use of the above-described techniques allow for an improved user experience since a step-up authentication step may be bypassed when provisioning the access data for use with the second application. The provisioning process may also include providing a device identifier to the authorizing entity when requesting the access data. In this manner, the

access data can be bound to the communication device, and cannot be used with a different device.

[0081] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention using hardware and a combination of hardware and software.

[0082] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer-readable medium, such as a random access memory (RAM), a read-only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer-readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0083] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art.

[0084] It should be understood that the methods and processes in accordance with some embodiments may perform one or more of the steps in a different order than those described herein, include one or more additional steps not specially described, omit one or more steps, combine one or more steps into a single step, split up one or more steps into multiple steps, and/or any combination thereof.

[0085] It should also be understood that one or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0086] As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1 1. A communication device comprising:
2 a processor; and
3 a non-transitory computer readable medium coupled to the processor,
4 wherein the non-transitory computer readable medium comprises code executable by
5 the processor for implementing a method comprising:
6 receiving, by a first application installed on the communication
7 device, user input selecting an account to provision to a second application
8 installed on the communication device;
9 in response to receiving the selection of the account to provision,
10 invoking, by the first application, the second application and sending a session
11 identifier (ID) to the second application;
12 sending, by the second application, a user ID associated with the
13 second application, a device ID, and the session ID to the first application;
14 generating, by the first application, encrypted provisioning request
15 data including an account ID of the account to provision, the user ID, and the
16 device ID;
17 sending, by the first application, the encrypted provisioning request
18 data to the second application;
19 sending, by the second application, the encrypted provisioning
20 request data to a remote server computer;
21 receiving, by the second application, access data provided by the
22 remote server computer based on validation of the encrypted provisioning
23 request data; and
24 provisioning, by the second application, the access data onto the
25 second application.

1 2. The communication device of claim 1, wherein the access data
2 provided by the remote server computer is bound to the communication device and
3 cannot be used with a different communication device.

1 3. The communication device of claim 1, wherein the validation of the
2 encrypted provisioning request data includes decrypting the received encrypted
3 provisioning request data using a key associated with the first application to determine
4 that the encrypted provisioning request data was generated by the first application.

1 4. The communication device of claim 1, wherein the encrypted
2 provisioning request data includes a timestamp, and the validation of the encrypted
3 provisioning request data includes determining whether a difference between a time at
4 which the encrypted provision request data was received by the remote server
5 computer and the time indicated in the timestamp is within a predefined time threshold.

1 5. The communication device of claim 1, wherein the validation of the
2 encrypted provisioning request data includes determining that the account ID is a valid
3 account ID associated with first application.

1 6. The communication device of claim 1, wherein the access data
2 includes user credential data that the second application uses to access a service
3 associated with the first application.

1 7. The communication device of claim 1, wherein the access data is a
2 token that is a substitute for the account ID.

1 8. The communication device of claim 1, wherein the first application
2 is an issuer application and the second application is an digital wallet application.

1 9. The communication device of claim 1, wherein the account ID is a
2 primary account number (PAN).

1 10. The communication device of claim 1, wherein the access data
2 allows a user of the communication device to access a building.

1 11. A method comprising:
2 receiving, by a first application installed on a communication device, user
3 input selecting an account to provision to a second application installed on the
4 communication device;
5 in response to receiving the selection of the account to provision, invoking,
6 by the first application, the second application and sending a session identifier (ID) to
7 the second application;
8 sending, by the second application, a user ID associated with the second
9 application, a device ID, and the session ID to the first application;
10 generating, by the first application, encrypted provisioning request data
11 including an account ID of the account to provision, the user ID, and the device ID;
12 sending, by the first application, the encrypted provisioning request data to
13 the second application;
14 sending, by the second application, the encrypted provisioning request
15 data to a remote server computer;
16 receiving, by the second application, access data provided by the remote
17 server computer based on validation of the encrypted provisioning request data; and
18 provisioning, by the second application, the access data onto the second
19 application.

1 12. The method of claim 11, wherein the access data provided by the
2 remote server computer is bound to the communication device and cannot be used with
3 a different communication device.

1 13. The method of claim 11, wherein the validation of the encrypted
2 provisioning request data includes decrypting the received encrypted provisioning
3 request data using a key associated with the first application to determine that the
4 encrypted provisioning request data was generated by the first application.

1 14. The method of claim 11, wherein the encrypted provisioning
2 request data includes a timestamp, and the validation of the encrypted provisioning

3 request data includes determining whether a difference between a time at which the
4 encrypted provision request data was received by the remote server computer and the
5 time indicated in the timestamp is within a predefined time threshold.

1 15. The method of claim 11, wherein the validation of the encrypted
2 provisioning request data includes determining that the account ID is a valid account ID
3 associated with first application.

1 16. The method of claim 11, wherein the access data includes user
2 credential data that the second application uses to access a service associated with the
3 first application.

1 17. The method of claim 11, wherein the access data is a token that is
2 a substitute for the account ID.

1 18. The method of claim 11, wherein the first application is an issuer
2 application and the second application is an digital wallet application.

1 19. The method of claim 11, wherein the account ID is a primary
2 account number (PAN).

1 20. The method of claim 11, wherein the access data allows a user of
2 the communication device to access a building.

1

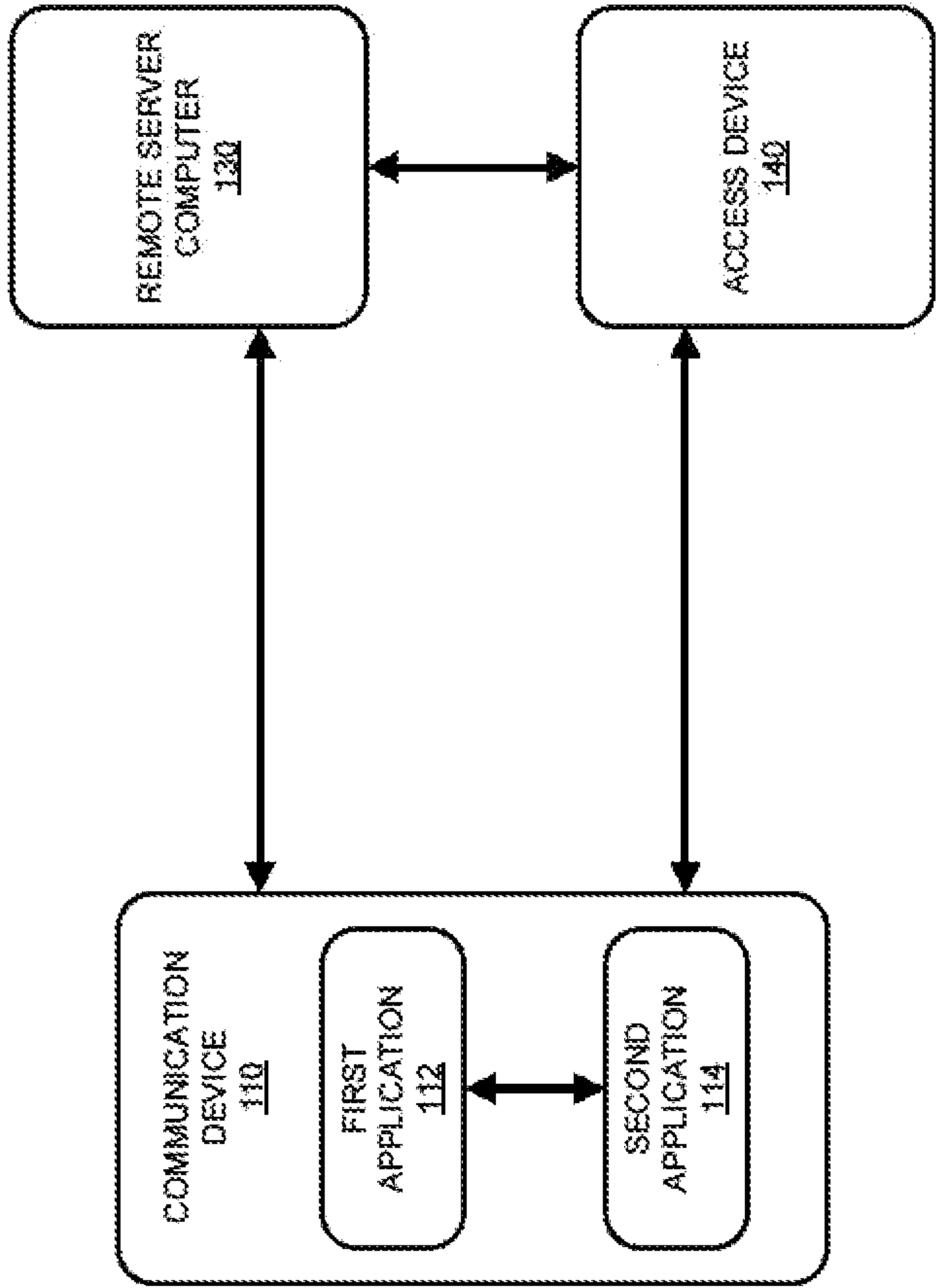


FIG. 1

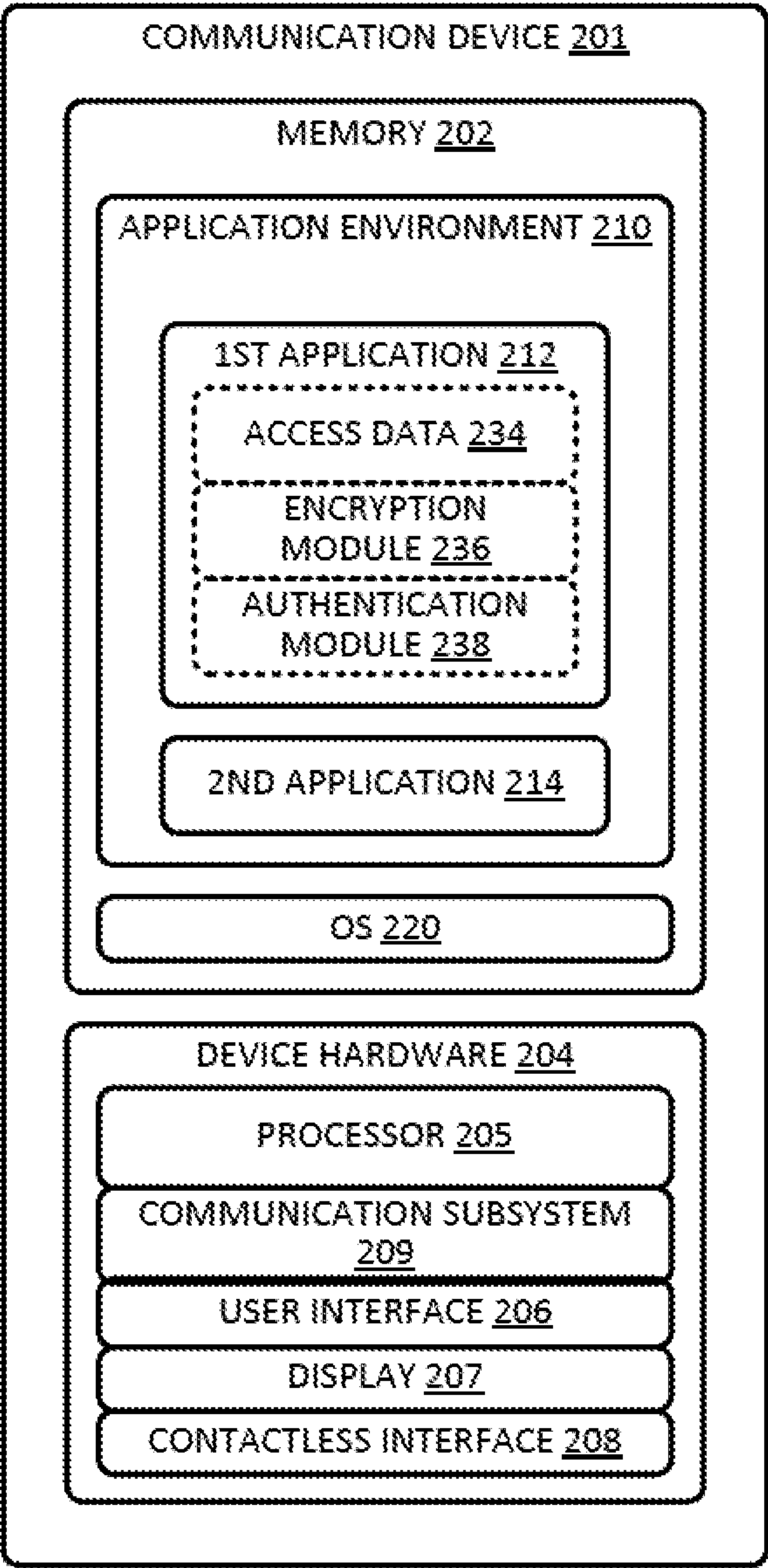


FIG. 2

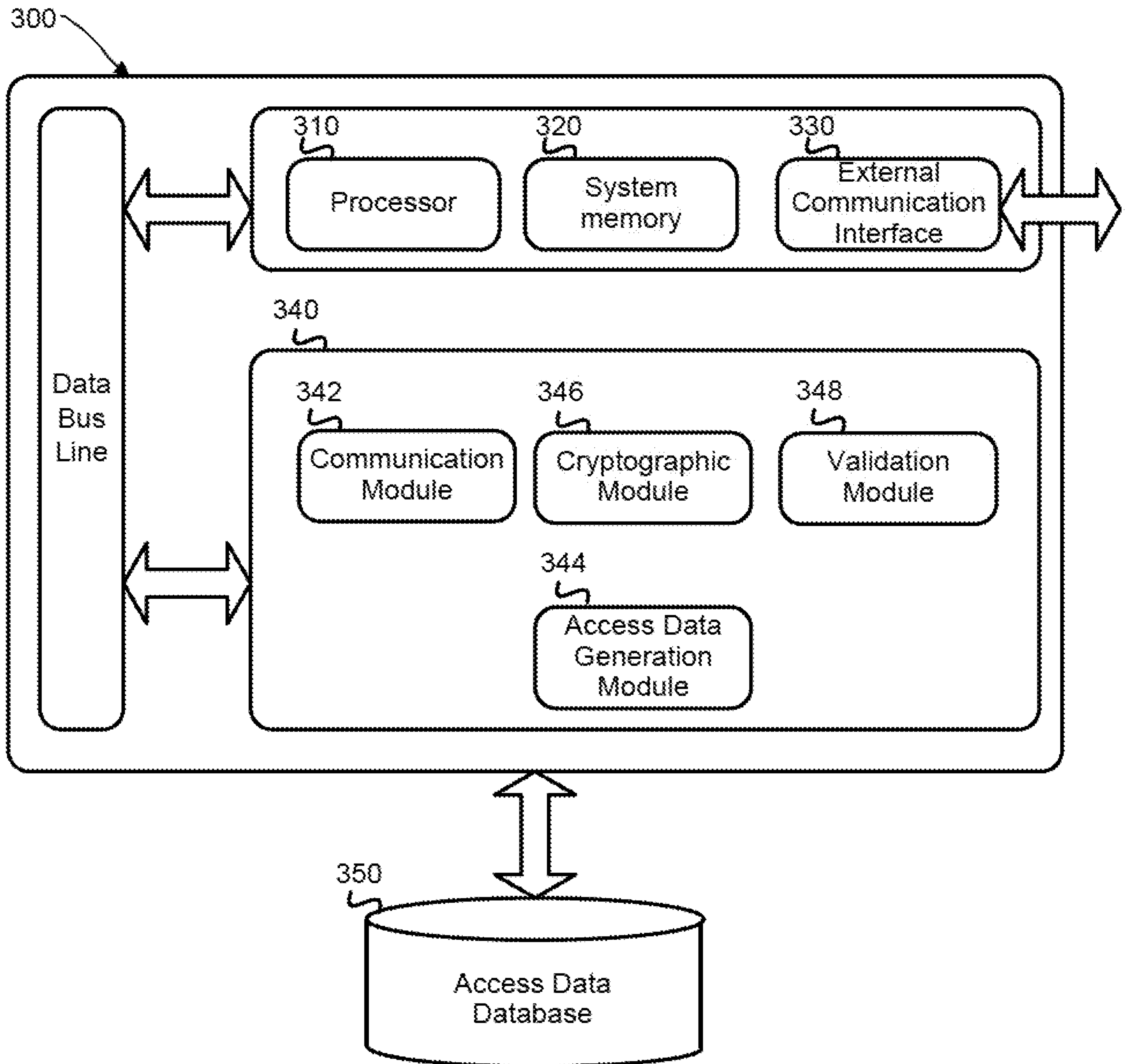


FIG. 3

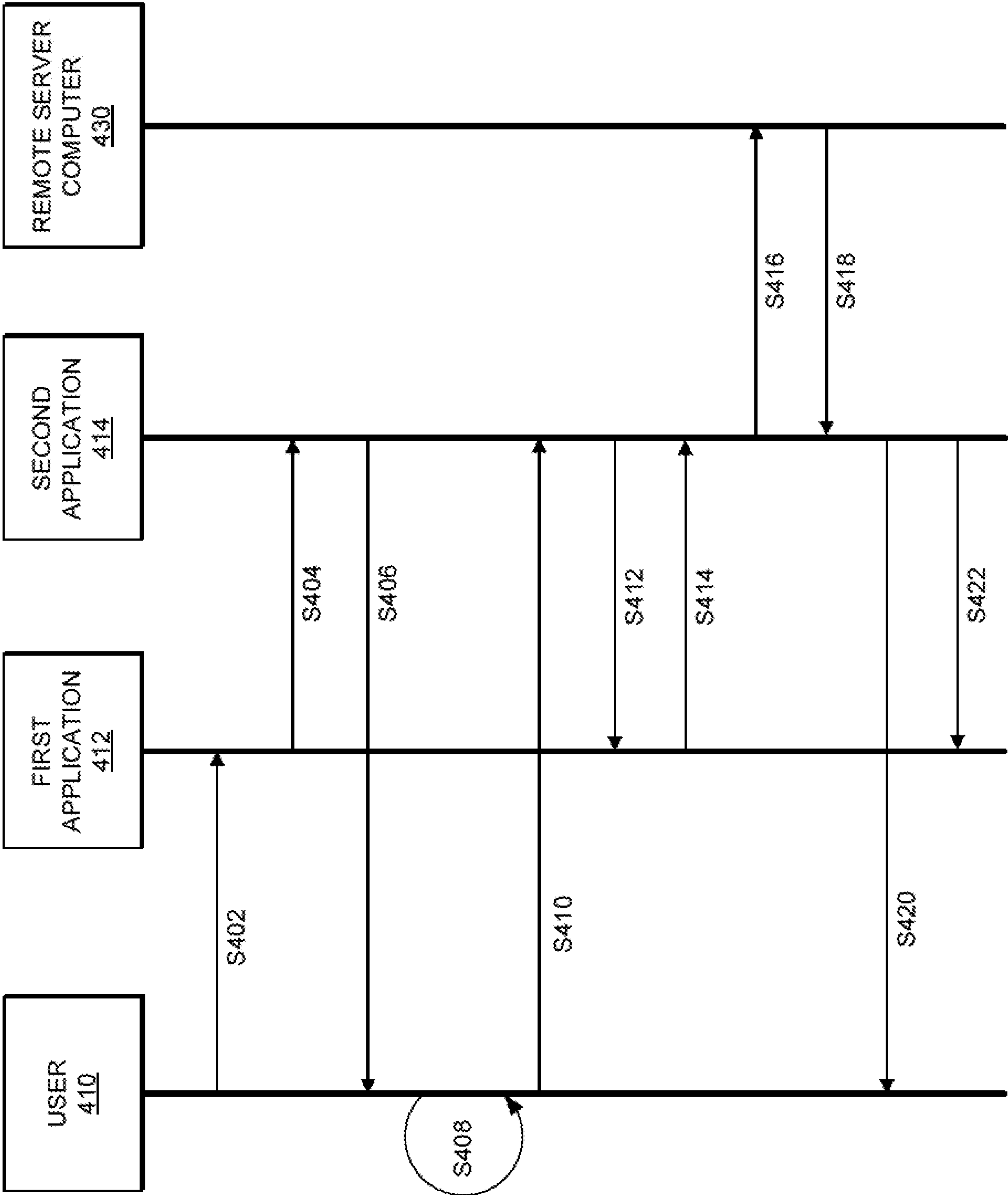


FIG. 4

5 / 8

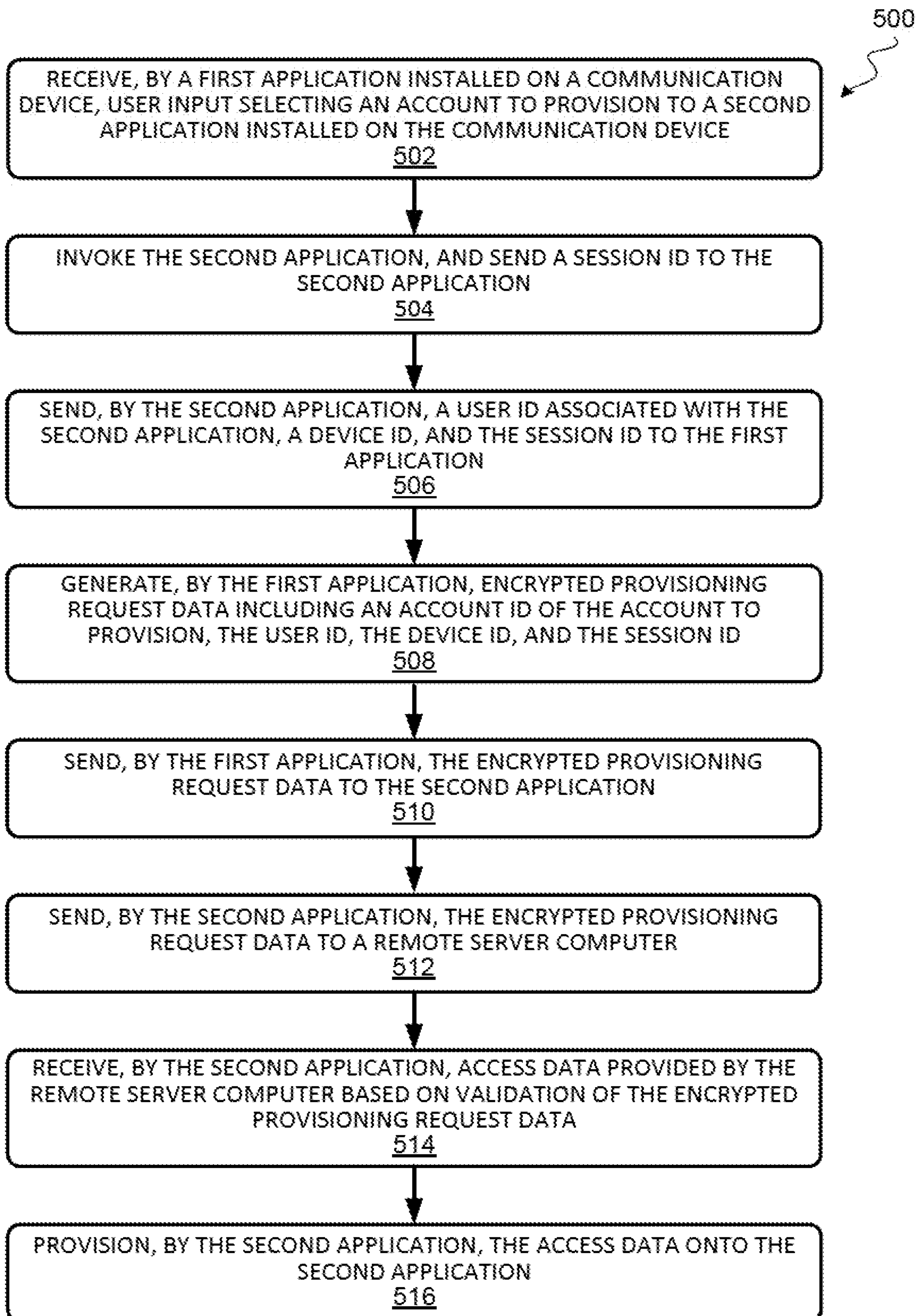


FIG. 5

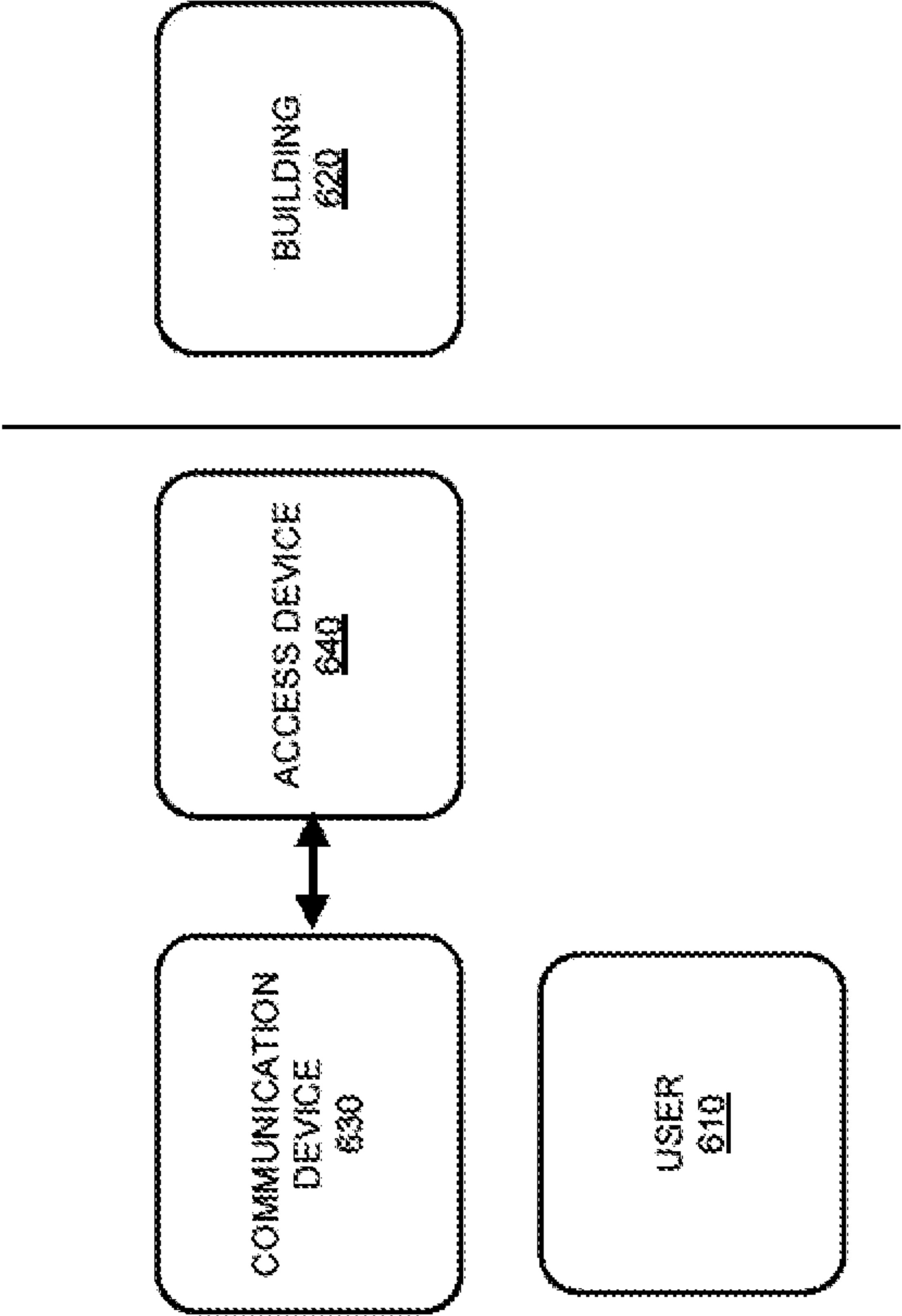


FIG. 6

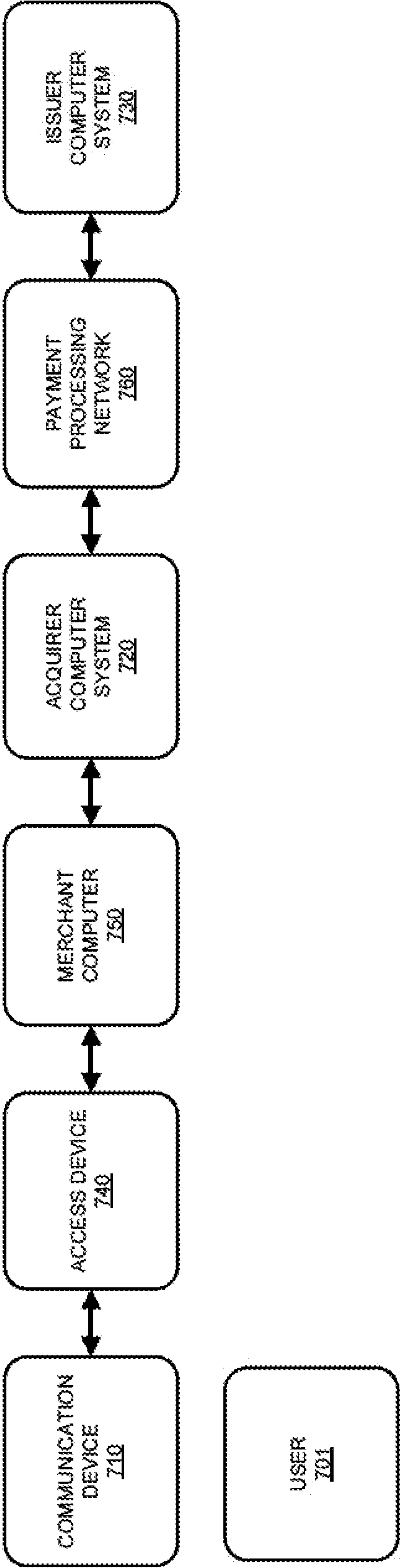


FIG. 7

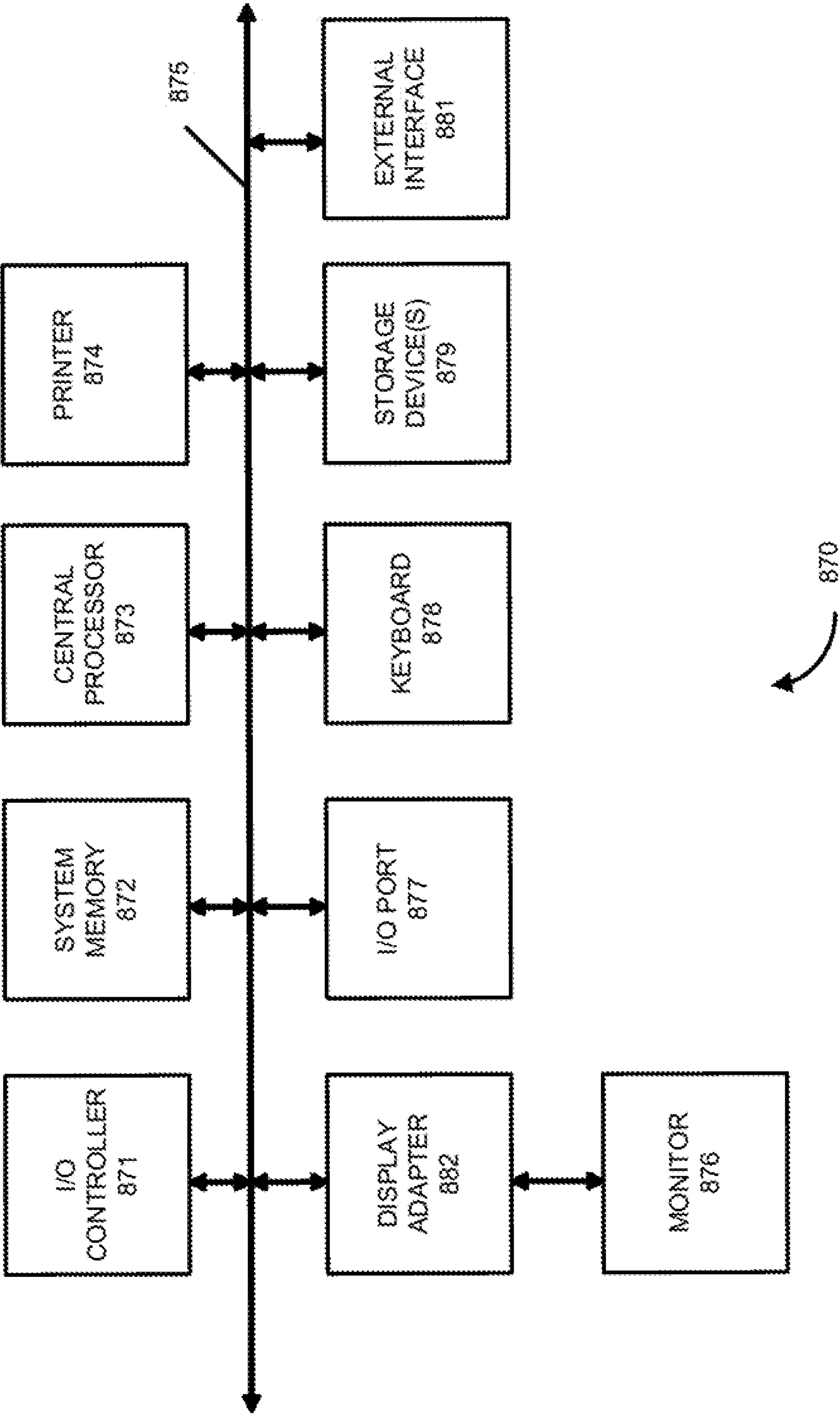


FIG. 8

FIG. 1

