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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 August 2020 (20.08.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/167582 A1

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

(21) International Application Number:
PCT/US2020/017038

(22) International Filing Date:
06 February 2020 (06.02.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/274,999 13 February 2019 (13.02.2019) US

(71) Applicant: **SAUDI ARABIAN OIL COMPANY** [SA/SA]; 1 Eastern Avenue, Dhahran, 31311 (SA).

(71) Applicant *(for US only)*: **ARAMCO SERVICES COMPANY** [US/US]; 1200 Smith Street, Two Allen Building, Houston, Texas 77002 (US).

(72) Inventors: **ALZAHRANI, Abdullah**; c/o Saudi Arabian Oil Company, 1 Eastern Avenue, Dhahran, 31311 (SA). **ALOMARI, Ibrahim**; c/o Saudi Arabian Oil Company, 1 Eastern Avenue, Dhahran, 31311 (SA). **ABUBEKER, Jewahir**; c/o Saudi Arabian Oil Company, 1 Eastern Avenue, Dhahran, 31311 (SA). **AYOUB, Hassan**; c/o Saudi Arabian Oil Company, 1 Eastern Avenue, Dhahran, 31311 (SA). **ALHAZMI, Meshal**; c/o Saudi Arabian Oil Company, 1 Eastern Avenue, Dhahran, 31311 (SA).

(74) Agent: **LEASON, David** et al.; LEASON ELLIS LLP, One Barker Avenue, Fifth Floor, White Plains, New York 10601 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM,

(54) Title: SYSTEM AND METHOD FOR PROVISIONING NON-ENTERPRISE CLIENT DEVICES WITH ACCESS CREDENTIALS

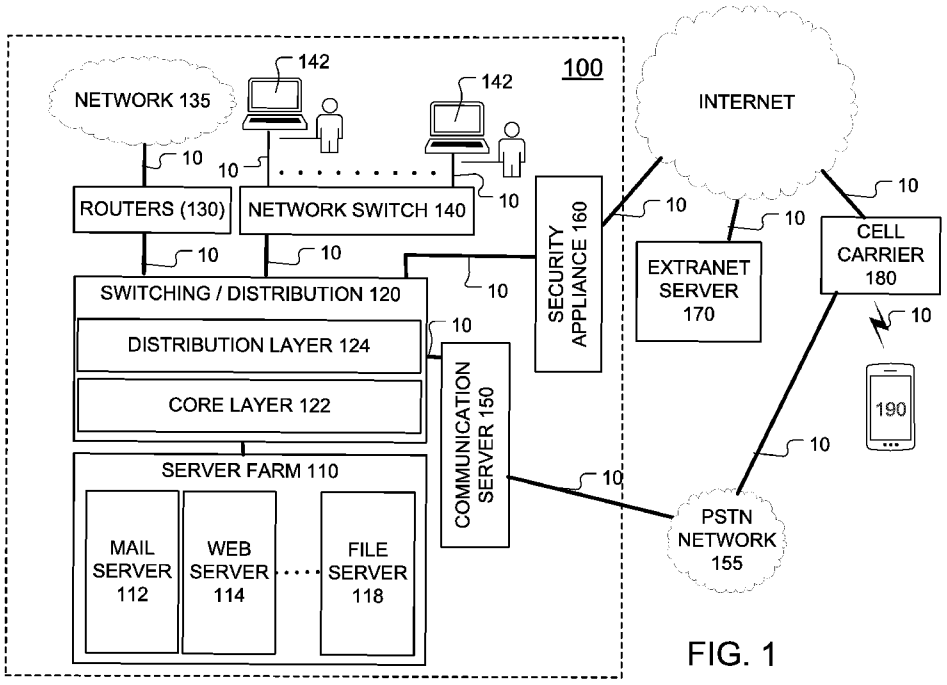

FIG. 1

(57) **Abstract:** A system, a method, or a computer program for provisioning a non-enterprise client device with access to an extranet enterprise domain. The system includes an enterprise client device connected to an intranet, a provisioner that receives an extranet registration request from the enterprise client device, an active directory connected to the intranet, a database that stores a non-enterprise client record populated with the non-enterprise client data, a primary transmission system connected to the intranet that transmits a portion of the non-enterprise client data and a linkage message outside of the intranet, and a secondary transmission system connected to the intranet and configured to transmit to an access message outside of the intranet, wherein the provisioner generates a unique permanent identification ID_{INDEX} for the non-enterprise client record.

[Continued on next page]

WO 2020/167582 A1

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

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEM AND METHOD FOR PROVISIONING NON-ENTERPRISE CLIENT DEVICES WITH ACCESS CREDENTIALS

CROSS-REFERENCE TO PRIOR APPLICATION

[0001] The present application claims priority to U.S. Patent Application No. 16/274,999, titled SYSTEM AND METHOD FOR PROVISIONING NON-ENTERPRISE CLIENT DEVICES WITH ACCESS CREDENTIALS, filed on February 13, 2019 with the U.S. Patent and Trademark Office, which is hereby incorporated by reference in its entirety.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates to a system, a method, and a computer program for provisioning non-enterprise client devices with credentials to securely access a network website.

BACKGROUND OF THE DISCLOSURE

[0003] Non-public enterprise network systems are continuously under attack. The attacks are not always direct, but frequently involve attacks made possible through non-enterprise client devices. These non-enterprise client devices may not have any awareness that they are serving as vehicles in attempts by unscrupulous individuals to breach network security and access proprietary information on the enterprise network systems, or in some way adversely impact or affect the enterprise network system. Numerous retailer enterprise network systems have recently been breached through non-enterprise client devices, such as, for example, vendor point-of-sale (PoS) communicating devices that had access to the enterprise network systems.

[0004] There exists a need for a technology solution that restricts access to an enterprise network system while providing non-enterprise client devices with access to network resources. The disclosure provides a technology solution that meets the foregoing need.

SUMMARY OF THE DISCLOSURE

[0005] The disclosure provides a novel technology solution, including a method, a system, and a computer program for provisioning non-enterprise client devices to access an extranet enterprise domain.

[0006] According to an aspect of the disclosure, a system is provided that provisions a non-enterprise client device with access to an extranet enterprise domain. The system comprises:

an enterprise client device connected to an intranet; a provisioner that receives an extranet registration request from the enterprise client device and parses enterprise client data and non-enterprise client data from the extranet registration request; an active directory connected to the intranet and having an enterprise client record associated with the enterprise client data; a database that stores a non-enterprise client record populated with the non-enterprise client data; a primary transmission system connected to the intranet that transmits a portion of the non-enterprise client data and a linkage message outside of the intranet; and a secondary transmission system connected to the intranet and configured to transmit to an access message outside of the intranet, wherein the provisioner generates a unique permanent identification ID_{INDEX} for the non-enterprise client record. The provisioning system can further comprise a registration application programming interface that receives the linkage message from the provisioner and generates an email message, including an activation link.

[0007] The portion of the non-enterprise client data can comprise a non-enterprise email address and an automatic number identification for a non-enterprise client device.

[0008] The provisioner can generate the linkage message and the access message.

[0009] The provisioner can perform an outbound call through the intranet firewall to the registration application programming interface. The outbound call can comprise a representational state transfer (REST) application programming interface call.

[0010] The linkage message can be sent to a non-enterprise client device in an email message.

[0011] The access message can be sent in an SMS text message to the non-enterprise client device.

[0012] The active directory can comprise a lightweight directory access protocol (LDAP) directory. The provisioner can query the active directory in response to the extranet registration request to locate the enterprise client record.

[0013] The registration application programming interface can receive the non-enterprise client identifier ID_{INDEX} for the non-enterprise client. The registration application programming interface can receive the portion of the non-enterprise client data.

[0014] According to a further aspect of the disclosure, a method is provided for provisioning a non-enterprise client device with access to an extranet enterprise domain. The method comprises: receiving an extranet registration request from an enterprise client device connected to an intranet; parsing enterprise client data and non-enterprise client data from the extranet registration request; querying an active directory for an enterprise client record based on the enterprise client data, the active directory being connected to the intranet; storing the

non-enterprise client data in a non-enterprise client record; generating a unique permanent identification ID_{INDEX} for the non-enterprise client record; transmitting by a primary transmission system a portion of the non-enterprise client data outside of the intranet; and transmitting by a secondary transmission system an access message outside of the intranet, the secondary transmission system being different than the primary transmission system.

[0015] The method can comprise: generating a linkage message based on the non-enterprise client data; and transmitting the linkage message outside of the intranet.

[0016] The method can comprise transmitting the access message to a non-enterprise client device, wherein the access message can comprise an SMS text message.

[0017] The method can comprise receiving the portion of the non-enterprise client data at a registration application programming interface and/or receiving the linkage message at a registration application programming interface.

[0018] The method can comprise: generating an electronic mail message by the registration application programming interface; and sending the electronic mail message to the non-enterprise client device, wherein the electronic mail message can include an activation link.

[0019] The transmitting the linkage message can comprise sending an electronic mail message to a non-enterprise client device.

[0020] According to a further aspect of the disclosure, a non-transitory computer readable storage medium storing non-enterprise client device provisioning instructions for causing a non-enterprise client device to be provisioned to access an extranet enterprise domain. is provided that includes a computer program, which when executed by one or more computing devices, the provisioning instructions comprising the steps of: receiving an extranet registration request from an enterprise client device connected to an intranet; parsing enterprise client data and non-enterprise client data from the extranet registration request; querying an active directory for an enterprise client record based on the enterprise client data, the active directory being connected to the intranet; storing the non-enterprise client data in a non-enterprise client record; generating a unique permanent identification IDINDEX for the non-enterprise client record; transmitting by a primary transmission system a portion of the non-enterprise client data outside of the intranet; and transmitting by a secondary transmission system an access message outside of the intranet, the secondary transmission system being different than the primary transmission system. The provisioning instructions can comprise the steps of: generating a linkage message based on the non-enterprise client data; or transmitting the linkage message outside of the intranet; or transmitting the access message to a non-enterprise client device, wherein the access message can comprise an SMS text message; or receiving the

portion of the non-enterprise client data at a registration application programming interface; or receiving the linkage message at a registration application programming interface; or generating an electronic mail message by the registration application programming interface; or sending the electronic mail message to the non-enterprise client device, wherein the electronic mail message can include an activation link.

[0021] Additional features, advantages, and embodiments of the disclosure may be set forth or apparent from consideration of the detailed description and drawings. Moreover, it is to be understood that the foregoing summary of the disclosure and the following detailed description and drawings provide non-limiting examples that are intended to provide further explanation without limiting the scope of the disclosure as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] The accompanying drawings, which are included to provide a further understanding of the disclosure, are incorporated in and constitute a part of this specification, illustrate embodiments of the disclosure and together with the detailed description serve to explain the principles of the disclosure. No attempt is made to show structural details of the disclosure in more detail than may be necessary for a fundamental understanding of the disclosure and the various ways in which it may be practiced.

[0023] FIG. 1 shows a block diagram of an example of an enterprise network system that is constructed according to the principles of the disclosure.

[0024] FIG. 2 depicts the Open Systems Interconnection (OSI) model.

[0025] FIG. 3 shows a block diagram of an example of a provisioning system for provisioning non-enterprise clients, which is constructed according to the principles of the disclosure.

[0026] FIG. 4 shows an example of an extranet provisioning process that can be carried out by the provisioning system in FIG. 3.

[0027] FIG. 5 shows an example of an extranet client registration process that can be carried out by the provisioning system in FIG. 3.

[0028] FIG. 6 shows an example of a registration updating process that can be carried out by the provisioning system in FIG. 3.

[0029] FIG. 7 shows an example of a connectivity flow for provisioning a non-enterprise client device by the provisioning system in FIG. 3.

[0030] FIG. 8 shows an example a display screen that can be generated and displayed as a GUI on a display of an enterprise client device in the enterprise network system in FIG. 1.

[0031] The present disclosure is further described in the detailed description that follows.

DETAILED DESCRIPTION OF THE DISCLOSURE

[0032] The disclosure and the various features and advantageous details thereof are explained more fully with reference to the non-limiting embodiments and examples that are described and/or illustrated in the accompanying drawings and detailed in the following description. It should be noted that features illustrated in the drawings are not necessarily drawn to scale, and features of one embodiment may be employed with other embodiments as those skilled in the art would recognize, even if not explicitly stated herein. Descriptions of well-known components and processing techniques may be omitted so as to not unnecessarily obscure the embodiments of the disclosure. The examples used herein are intended merely to facilitate an understanding of ways in which the disclosure may be practiced and to further enable those skilled in the art to practice the embodiments of the disclosure. Accordingly, the examples and embodiments herein should not be construed as limiting the scope of the disclosure. Moreover, it is noted that like reference numerals represent similar parts throughout the several views of the drawings.

[0033] FIG. 1 shows a non-limiting embodiment of an enterprise network system 100 that is constructed according to the principles of the disclosure. The enterprise network system 100 can include a server farm 110, switching and distribution layers 120, one or more routers 130, one or more network switches 140, a communication server 150, and a security appliance 160, all of which can be interconnected by communication links 10 and located behind a firewall. The enterprise network system 100 can include one or more modems (not shown) configured for one or more cellular network standards, including, for example, GSM, WiMAX, LTE-TDD/ TD-LTE, LTE Advanced (E-UTRA), LTE Advanced Pro, HiperMAN, Mobile WiMAX, Flash-OFDM, iBurst, CDMA2000, HSPA, UMTS, WiDEN, GPRS, CDPD, D-AMPS, NMT, AMPS, or the like, or any other modulating/demodulating device that can facilitate transmission of short message services (SMS) messages, or the like, over the public switched telephone network (PSTN), the public land mobile network (PLMN), or the like. The enterprise network system can include an SMS gateway (not shown).

[0034] The enterprise network system 100 can be configured such that enterprise client identity information is not stored nor made available in any way outside of the intranet, thereby providing enhanced network security that minimizes potential breaches to the system.

[0035] The server farm 110 can include a plurality of servers, including a mail server 112, a web server 114, and a file server 118. The communication server 150, which is preferably

located on the intranet, can be located in the server farm 110. The intranet can include all of the foregoing and a firewall to protect against threats and breach attempts made against the enterprise network system 100.

[0036] The security appliance 160 can include hardware, firmware, or software that provides malware protection, application visibility and control, reporting, secure mobility, and protection against threats that can arise during connection to non-enterprise devices (such as, e.g., computing devices that are external to the intranet) or the Internet. The security appliance 160 includes a firewall. The security appliance 160 can include a primary transmission system. The primary transmission system can include, for example, Internet message handling services (MHS) that transfer electronic mail messages between communicating devices on the intranet with communicating devices external to the intranet. The MHS can include, for example, a message transfer agent or mail transfer agent (MTA), a mail relay, or the like. The primary transmission system can include a message delivery agent (MDA).

[0037] The switching and distribution layers 120 can include a core layer 112 and a distribution layer 124. The core layer 112 can include one or more layers of switching devices (not shown) that connect the server farm 110 to the distribution layer 124. The distribution layer 124 can include one or more layers of switching devices (not shown) that connect the core layer 122 to the one or more routers 130, the one or more network switches 140, the communication server 150, or the security appliance 160. The switching and distribution layers 120 can include one or more routers (not shown).

[0038] The router(s) 130 can be connected to a network 135 by a communication link 10. The router(s) 130 can include a firewall (not shown). The network switch(es) 140 can be connected to one or more enterprise client devices 142 by one or more associated communication links 10. The network switch(es) 140 can include ethernet switches. Data packets can be securely transported between devices on the intranet.

[0039] The communication server 150 can include a standards-based computing system that can operate as a carrier-grade common platform for a wide range of communications applications and facilitate communication over, for example, the PSTN 155 or the PLMN (not shown). The communication server 150 can include or be connected to an SMS gateway (not shown) that can be connected to one or more modems to transmit SMS messages over the PSTN 155 or the PLMN (not shown). The communication server 150 can include a secondary transmission system. The secondary transmission system can include, for example, an SMS gateway that facilitate SMS traffic between the enterprise network system 100 and communicating devices such as the non-enterprise client device 190.

[0040] Internet message handling services (MHS) that transfer electronic mail messages between communicating devices on the intranet with communicating devices external to the intranet. The MHS can include, for example, a message transfer agent or mail transfer agent (MTA), a mail relay, or the like. The primary transmission system can include a message delivery agent (MDA).

[0041] The enterprise network system 100 can be connected to the Internet over a communication link 10. The enterprise network system 100 can be connected to an extranet server 170 directly over the communication link 10 or via the Internet over one or more communication links 10. The extranet server 170 can host an extranet enterprise domain on the Internet or a non-enterprise network. The extranet enterprise domain can include one or more extranet websites. The extranet enterprise domain can include host applications such as, for example, applications provided by a human resources department that are intended for access by employees and family members of employees who are enterprise clients. The hosted applications can be accessible on or through one or more extranet websites. A non-enterprise client device 190 can be configured to access the Internet over a communication link 10 via, for example, a cellular carrier 180 or Internet service provider (ISP) (not shown). The non-enterprise client device 190 can be provisioned to access the extranet enterprise domain, including, for example, one or more of the extranet websites.

[0042] FIG. 2 shows the seven-layer OSI model. The enterprise network system 100, including the computing devices that are connected to the enterprise network system 100, can operate at any one or more of the seven layers in the OSI model at any instant in time, including the application layer 1, presentation layer 2, session layer 3, transport layer 4, network layer 5, link layer 6, and physical layer 7. The enterprise client devices 142 and non-enterprise client device(s) 190 can operate at any one or more of the seven layers in the OSI model. Each of the enterprise client devices 142 and non-enterprise client device(s) 190 includes a computing device.

[0043] Referring to FIG. 2, the application layer 1 is the OSI layer in a computing device that is closest to the end user. The application layer 1 interacts with software applications in the computing device that implement a communicating component. The application layer 1 can include, for example, a search engine or any other software application which the end user can interact with to carry out a functionality.

[0044] The presentation layer 2 establishes context between software applications, which might use different syntax and semantics. The presentation layer 2 transforms data into a form

that each software application can accept. An operating system is an example of the presentation layer 2.

[0045] The session layer 3 controls the connections between computing devices in a communication system. This layer is responsible for establishing, managing and terminating connections between local and remote applications. The layer can provide for full-duplex, half-duplex, or simplex operations, and is responsible for establishing checkpointing, adjournment, termination, and restart procedures.

[0046] The transport layer 4 provides the functional and procedural mechanisms for transferring variable-length data sequences from a source computing device to a destination computing device, while maintaining quality-of-service (QoS). The transport layer 4 controls the reliability of a given link through flow control, segmentation and desegmentation, and error control. The transport layer 4 can include, for example, tunneling protocols, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

[0047] The network layer 5 provides the functional and procedural mechanisms for transferring data packets from a node on a network to another node on a different network. If the data to be transmitted is too large, the network layer 5 can facilitate splitting the data into a plurality of segments at the node and sending the fragments independently to the other node, where the segments can be reassembled to recreate the transmitted data. The network layer 5 can include one or more layer-management protocols such as, for example, routing protocols, multicast group management, network layer information and error, and network layer address assignment.

[0048] The link layer 6 is responsible for node-to-node transfer between computing devices in a communication system. In IEEE 802 implementations, the link layer 6 is divided into two sublayers, consisting of a medium access control (MAC) layer and a logical link control (LLC) layer. The MAC layer is responsible for controlling how devices in a network gain access to a medium and permission to transmit data. The LLC layer is responsible for identifying and encapsulating network layer protocols, and for controlling error checking and frame synchronization.

[0049] The physical layer 7 includes the hardware that connects the computing systems. The hardware can include for example connectors, cables, switches, and the like, that provide for transmission and reception of instruction and data streams between the computing devices.

[0050] FIG. 3 shows a block diagram of an example of a provisioning system for provisioning client devices that is constructed according to the principles of the disclosure. The provisioning system comprises an intranet provisioning system 210 and an extranet

provisioning system 220. The intranet provisioning system 210 is located behind a firewall (not shown) in the intranet, in the enterprise network system 100 (shown in FIG.1). The extranet provisioning system 220 can be located, for example, in the extranet server 170 or on the Internet, such as, for example, a cloud environment, or on a non-enterprise network.

[0051] The intranet provisioning system 210 includes a provisioner 212. The intranet provisioning system 210 can include an active directory 214, an identity and access management (IAM) system 216, and a database 218. The active directory 214 can be located in the database 218 or elsewhere in the intranet. The database 218 can include a relational database. The database 218 can include a database index. The provisioner 212 can be communicatively connected to the extranet provisioning system 220, the PSTN (or PLMN) 155, and one or more enterprise client devices 142 over communication links 16, 14, and 12, respectively.

[0052] The provisioner 212 can include an intermediary registration provisioning layer (not shown) that receives a non-enterprise client provisioning request over the communication link 12 from the enterprise client device 142 (e.g., at the instruction of an enterprise client). The enterprise client device 142 is located in the intranet, behind the firewall in the enterprise network system 100. The extranet provisioning request can include a request that the non-enterprise client device 190 be provisioned to access the extranet enterprise domain (e.g., website) or to send an invitation to another non-enterprise client device (not shown) to register for provisioning to access the extranet enterprise domain. The enterprise client device 142 can be provided with, for example, a graphic user interface (GUI) through which an enterprise client can request that the non-enterprise client device 190 be provisioned with access to the extranet enterprise domain.

[0053] The IAM system 216 can manage and control all enterprise client accounts in the intranet in the enterprise network system 100. The IAM system 216 can manage and control all rights, privileges, and policies for each enterprise client in the enterprise network system 100, including rights, privileges and policies relating to the enterprise clients' access to resources in the enterprise network system 100. The IAM system 216 can store the assigned rights, privileges, and policies in an enterprise user profile for each enterprise client, with a unique enterprise client profile being created and managed for each enterprise client in the enterprise network system 100. The IAM system 216 can provide automated enterprise client profile synchronization for all enterprise clients to ensure that enterprise clients have access to only those resources they are intended to have access. For instance, an enterprise client whose

role is that of a network administrator may be granted significantly greater and broader access rights and privileges than an enterprise client whose role is that of, for example, a file clerk.

[0054] A unique permanent identification ID_{INDEX} can be generated for each registered non-enterprise client by the provisioner 212 and then synched to the external non-enterprise client directory hosted in the Internet or non-enterprise network. The ID_{INDEX} can act as a mapper or a link for each created non-enterprise client account in the Internet directory with a valid enterprise client existing in the intranet. After the ID_{INDEX} is created for a non-enterprise client, a linkage message can be created by the provisioner 212 and sent to the non-enterprise client device 190 over the primary transmission system, such as, for example, an email that is sent via the security appliance 160 (shown in FIG. 1) and the Internet to the non-enterprise client device 190. A plurality of linkage messages can be generated for a given enterprise client and sent to associated non-enterprise client devices (not shown). The linkage message can include a registration link that, when selected at the non-enterprise client device 190, can instruct the device to initiate communication with and connect the non-enterprise client device 190 to the extranet provisioning system 220. The initiation and connection can be accomplished through, for example, a web browser on the non-enterprise client device 190. For instance, a non-enterprise client can select the registration link (e.g., by double-clicking on a hyperlink) in an email received from the provisioner 212 and opened on the non-enterprise client device 190, which can instruct the device to launch a web browser and link to a web page hosted by the extranet provisioning system 220.

[0055] After the ID_{INDEX} is created for the non-enterprise client, an access message can be created by the provisioner 212 and sent to the associated non-enterprise client device 190 via a secondary transmission system, such as, for example, the communication link 14 and PSTN 155 (or PLMN, not shown). If multiple linkage messages are created for non-enterprise clients, then an associated number of access messages can be created by the provisioner 212. The access message can include an initial password that is associated with the ID_{INDEX} and sent in, for example, an SMS message to the non-enterprise client device 190. The initial password can include a plurality of alphanumeric characters, a plurality of symbols, a hexadecimal value, or the like. The access message can be sent to the non-enterprise client device 190 concurrently with the linkage message, or at a different time. After the access message is received by the non-enterprise client device 190 and the device has established communication with the extranet provisioning system 212 via the linkage message, a user can interact with the non-enterprise client device 190 to create a non-enterprise client account on, for example, the extranet server 170 (shown in FIG 1) to access the extranet enterprise domain on the extranet

server 170 or the Internet. The non-enterprise client account can include the ID_{INDEX} assigned to the particular non-enterprise client.

[0056] The provisioner 212 can generate a plurality of linkage message and access message pairings to create a group of non-enterprise client accounts, each having a unique ID_{INDEX} and provision each non-enterprise client account in the group with access to the extranet enterprise domain. Each non-enterprise client account can include a non-enterprise client profile that includes predetermined rights, privileges, and policies, so that a particular non-enterprise client can only access portions of the extranet enterprise domain (e.g., applications) permitted under the associated non-enterprise client account. As a result, enterprise clients and non-enterprise clients can be authenticated and authorized to access applications hosted in the extranet enterprise domain, without using or storing any enterprise information outside of the intranet, such as, for example, corporate user related identity details, such as email address, network identification, phone number, automatic number identification (ANI), or the like.

[0057] The extranet provisioning system 220 can include a registration application programing interface (API) suite 2201 and a database 225. The registration API suite 2201 can include an API integration layer 221, a client link layer 223, and a create profile layer 224.

[0058] The extranet provisioning subsystem 220 can be communicatively connected to the non-enterprise client device 190 over a communication link 18 via, for example, an ISP (not shown) or cellular carrier 180 (shown in FIG. 1). The database 225 can store a non-enterprise client directory. The database 225 can be managed and controlled by the registration API Suite 2201 to add, modify, or delete records in the non-enterprise client directory. The database 225 can store a plurality of non-enterprise client records, each one including a data field comprising a non-enterprise email address and a password. The non-enterprise client record can include a non-enterprise user profile. The non-enterprise client record can include the ID_{INDEX} assigned to the non-enterprise client.

[0059] Some or all of the data in the non-enterprise client record can be created and populated by, or at the instruction of the provisioner 212 and communicated to or synched with the external client directory (e.g., Internet client directory) hosted in, for example, the database 225. The ID_{INDEX} can be referenced by the provisioner 212 for the non-enterprise client account in the external client directory.

[0060] FIG. 4 shows an example of an extranet provisioning process 300 according to the principles of the disclosure. Referring to FIGS. 3 and 4, an enterprise client can access an intranet application on the enterprise client device 142 and enter a unique non-enterprise email address and mobile telephone number and select a REGISTER command that instructs the

enterprise client device 142 to send an extranet registration request, which can be received at the provisioner 212 (Step 305). After receiving the extranet registration request, the provisioner 212 can parse the extranet registration request to determine the non-enterprise email address and mobile telephone number entered by the enterprise client at the enterprise client device 142, the enterprise client's user identification (e.g., login identification), the MAC address of the enterprise client device, the enterprise client's enterprise email address, biometric information, or any other information that can be used to accurately identify and authenticate the enterprise client. The parsed information can be used by the intermediary provisioning layer (not shown) in the provisioner 212 to query the active directory 214 to locate an enterprise client record for the particular enterprise client (Step 310). The active directory 214 can include, for example, a Lightweight Directory Access Protocol (LDAP) directory.

[0061] If it is determined that the active directory 214 does not include an enterprise client record for the particular enterprise client (NO at Step 315), then the extranet provisioning process 300 can be terminated. Prior to terminating the process, a message can be generated and sent by the provisioner 212 to the IAM system 216 to reconcile the enterprise client's status and enterprise client record, including the enterprise client profile, in the enterprise network system 100. The reconciliation process can include modifying, creating or deleting an enterprise client record for the particular enterprise client, including any enterprise client profile, as appropriate.

[0062] If it is determined that the active directory 214 includes an enterprise client record for the particular enterprise client (YES at Step 315), then the enterprise client record can be accessed and the rights, privileges and policies in the enterprise client profile can be referenced to determine the appropriate rights, privileges and policies to apply for the non-enterprise client. For instance, only certain areas of the extranet enterprise domain might be made available to the particular enterprise client, or the non-enterprise clients associated with the particular enterprise client. The provisioner 212 can then generate an ID_{INDEX} for the non-enterprise client (Step 320). The ID_{INDEX} can be stored in the database 218. The ID_{INDEX} can be stored in a database table as a database index and used to identify a location of an enterprise client record (or enterprise client profile) associated with the particular non-enterprise client assigned the ID_{INDEX}. The ID_{INDEX} value can include, for example, hexadecimal values, alphanumeric characters, symbols, or the like. The enterprise client record can include the ID_{INDEX}, such as, for example, the database 218, or the enterprise client record and ID_{INDEX} can be stored at different locations on the intranet. The provisioner 212 can also generate an initial extranet password (Step 325).

[0063] After the ID_{INDEX} and initial extranet password are generated (Steps 320 and 325), a non-enterprise client record can be created (or updated, if previously created) by the provisioner 212 and populated with the ID_{INDEX}, non-enterprise email address, mobile telephone number, automatic number identification (ANI), and initial extranet password and stored locally on the intranet, such as, for example, in the database 218 (Step 330). Alternatively, the enterprise client record can be populated with the ID_{INDEX}, non-enterprise email address, mobile telephone number, automatic number identification (ANI), and initial extranet password. According to a non-limiting embodiment, the database 218 can include a relational database comprising at least three separate database regions, including, for example, an enterprise region that includes the enterprise client records, an extranet region that includes non-enterprise client records, and a database index that includes ID_{INDEX} values that can be referenced to identify corresponding enterprise client records and non-enterprise client records for each ID_{INDEX} value.

[0064] After the provisioning request has been processed and completed on the intranet, the provisioner 212 can perform an outbound call through the intranet firewall to the registration API suite 2201 using, for example, a Representational State Transfer (REST) API (Step 335) and transfer the non-enterprise client data, including the ID_{INDEX} value, the non-enterprise email address, the mobile telephone number, ANI and the initial extranet password to the registration API suite 2201 (Step 340). The communication between the provisioner 212 and registration API suite 2201 can be carried out using a platform such as, for example, the SAP NetWeaver Process Integration (SAP PI) platform in SAP's enterprise application integration (EAI) software, to facilitate the exchange of information between the intranet provisioning system 210 and the extranet provisioning system 220. The registration API suite 2201 can include a library of whitelisted IP addresses that can be referenced to verify that the data packets received in the call actually came from the provisioner 212. This can be done, for example, by parsing the source IP address from the data packets and comparing the IP address to the IP address in the library for the intranet (for example, the IP address for the provisioner 212). The provisioner 212 can include a computing device that has a static IP address.

[0065] After sending the non-enterprise client data (Step 340), the provisioner 212 can generate and send an access message to the non-enterprise client device 190 that is associated with the mobile telephone number or ANI (Step 345). The non-enterprise client data can include the linkage message to be sent to the non-enterprise client device 190. The access message sent to the client device 190 can include an SMS text message that is sent over the

PSTN network 155, or PLMN, or the Internet, or the like. The message can include the initial extranet password associated with the mobile telephone number or ANI.

[0066] Optionally, a determination can be made whether extranet provisioning of the non-enterprise client 190 has been completed (Step 350), otherwise this step can be omitted and the non-enterprise client record updated (Step 355). The determination can be based on, for example, the delivery of the access message to the non-enterprise client device 190 or the receipt of a confirmation message from the registration API suite 2201 that provisioning of the client device 190 was completed. If a determination is made that the provisioning of the non-enterprise client has been completed (YES at Step 350), then the non-enterprise client record can be updated (Step 355), otherwise the process can wait (NO at Step 350) until a determination is made that the non-enterprise client has been provisioned.

[0067] FIG. 5 shows an example of an extranet client registration process, according to the principles of the disclosure. Referring to FIGS. 3-5, after the non-enterprise client data is sent to the registration API suite 2201 from the provisioner 212 (Step 340 in FIG. 4), the registration API suite 2201 receives the non-enterprise client data (Step 342) and automatically generates and sends a linkage message (e.g., in an email) to the non-enterprise client device 190 that includes a unique activation link (Step 360). The activation link can be set to expire after a set time (for example, 48 hours). If the linkage message is opened and the activation link activated, then a call signal can be generated and sent from the non-enterprise client device 190 and received at the registration API suite 2201 (YES at Step 365), otherwise the registration API suite 2201 can wait until the set time has expired, at which the process can be terminated (NO at Step 365).

[0068] When the call signal is received from the non-enterprise client device 190, the registration API suite 2201 can open or create a communication session with the non-enterprise client device 190 such as, for example, by means of a web browser, and provide a GUI with data entry fields for the non-enterprise client to input a username, the initial extranet password previously provided in the access message in Step 345 (Step 370). After the non-enterprise client enters the requested data in the entry fields of the GUI, the entered data can be received at the registration API 2201 (Step 375), where it is parsed and used to populate or update the extranet non-enterprise client directory (Step 380). The session can then be terminated (Step 385). At this point, a provisioning complete confirmation signal can be sent to the provisioner 212.

[0069] FIG. 6 shows an example of a registration updating process 400, according to the principles of the disclosure. Referring to FIGS. 3 and 6, where a change is made to an

enterprise client record, such as, for example, where an enterprise client (e.g., an employee) is terminated, has a job reassignment, or any right, privilege, or policy is changed in any way for the particular enterprise client, an enterprise client status change request can be received by the provisioner 212 (Step 410). A query can be generated and sent to identify and retrieve the enterprise client record that is associated with the particular enterprise client (Step 420). A determination can be made whether the enterprise client is an active enterprise client by, for example, querying the active directory 214 (Step 430).

[0070] If it is determined that the enterprise client is no longer an active enterprise client (e.g., the enterprise client is a former employee who resigned, was terminated, or otherwise is no longer an employee) (NO at Step 430), then the provisioner 212 can perform an outbound call through the intranet firewall to the registration API suite 2201 using, for example, a REST API (Step 440) and send one or more ID_{INDEX} values associated with the particular, former enterprise client, which the registration API suite 2201 can use to identify the corresponding extranet non-enterprise client record(s) and delete the record(s), thereby terminating access to the extranet enterprise domain by the non-enterprise clients associated with the received ID_{INDEX} values. The registration API suite 2201 can confirm deletion of the record(s) (Step 450).

[0071] If it is determined that the enterprise client is an active enterprise client, but a change has been made to the enterprise client record, such as, for example, a change in the enterprise client's job, access rights, privileges, policies, or the like, or the enterprise client has initiated a change to the extranet enterprise domain access rights of one or more non-enterprise clients (YES at Step 430), then the provisioner 212 can perform an outbound call through the intranet firewall to the registration API suite 2201 (Step 460) and send an ID_{INDEX} value for each non-enterprise client associated with the enterprise client, as well as an email address and mobile telephone number (or ANI) data for each non-enterprise client (Step 470), so that the associated non-enterprise client record(s) can be updated. The registration API suite 2201 can confirm updating of the non-enterprise client record(s) (Step 480).

[0072] FIG. 7 shows an example of a connectivity flow for provisioning a non-enterprise client device, according to an embodiment of the disclosure, including Steps 305 through 375 discussed above.

[0073] FIG. 8 shows an example a display screen that can be generated and displayed as a GUI on the display of the enterprise client device 142 (shown in FIG. 1) through which an enterprise client can request that the non-enterprise client device 190 be provisioned with access to the extranet enterprise domain. The GUI can include enterprise client entry fields,

including a non-enterprise email address, a mobile phone number (or ANI) and a registration command, which can be displayed as, for example, a radio button. An ID_{INDEX} value (e.g., "75bf3332-8595-4c0e-b8bd-0fcd4278ff6b") may be assigned to each non-enterprise client associated with the particular enterprise client. The GUI can include non-enterprise client entry fields for all non-enterprise clients associated with that enterprise client. The GUI can be populated with all non-enterprise client names retrieved from the enterprise client record or non-enterprise client accounts associated with that enterprise client record, and entry fields for each non-enterprise client account, including a non-enterprise email address, a mobile phone number (or ANI), and one or more command fields (e.g., "INVITE," "RESEND ACTIVATION," "EDIT," "DELETE," "RESET LOGIN DETAILS," or the like).

[0074] In the example shown in FIG. 8, three non-enterprise client accounts are associated with a particular enterprise user record, including "John Doe," "Jane Doe," and "John Smith." In this non-limiting example, the non-enterprise client names can be retrieved automatically from beneficiary data (e.g., from a corporate life insurance policy), dependent data (e.g., from tax data), family member data (e.g., from corporate records), or any other data previously provided from by the enterprise client and identified as beneficiaries, dependents, family members, or the like. Alternatively, the non-enterprise client names can be entered by the enterprise client via the enterprise client device 142 (shown in FIG. 1).

[0075] The non-enterprise client John Doe can be a family member (e.g., a child of the enterprise user) for whom the enterprise client has not requested provisioning access to the extranet enterprise domain. The enterprise client record can include a field that indicates that an extranet registration request was never received from the enterprise client for John Doe. In this instance, an "INVITE" command field (e.g., radio button) can be displayed. If the enterprise client selects the "INVITE" command on the enterprise client device 142, the device will generate and transmit a registration request to the provisioner 212 (shown in FIG. 3), including identifying information for that enterprise client device 142, a timestamp, identifying information for the enterprise client (e.g., user identification), identifying information for that non-enterprise client (e.g., "John Doe"), and any other information that can be used to verify and authenticate that enterprise client or enterprise client device 142.

[0076] The non-enterprise client Jane Doe can be a family member (e.g., an adult child of the enterprise user) for whom the enterprise client previously requested provisioning access to the extranet enterprise domain, but the non-enterprise client never completed the extranet registration process discussed above (shown in FIG. 5). The enterprise client record can include a field that indicates that a registration request was received from the enterprise client

for Jane Doe and processed by the provisioner 212. The record field can indicate whether a linkage message and/or an access message was sent to a non-enterprise client device associated with Jane Doe. In this instance, a plurality of command fields can be displayed (e.g., as radio buttons), including "RESEND ACTIVATION," "EDIT," and "DELETE" commands. If the enterprise client selects the "RESEND ACTIVATION" command on the enterprise client device 142, the device will generate and transmit a registration request resend instruction to the provisioner 212 (shown in FIG. 3), including identifying information for that enterprise client device 142, a timestamp, identifying information for the enterprise client (e.g., user identification), identifying information for that non-enterprise client (e.g., "Jane Doe"), and any other information that can be used to verify and authenticate that enterprise client or enterprise client device 142.

[0077] If the enterprise client selects the "EDIT" command on the enterprise client device 142, the device will generate and transmit an edit request instruction to the provisioner 212 (shown in FIG. 3), including any edited data in the email address and phone number (or ANI) fields, as well as identifying information for that enterprise client device 142, a timestamp, identifying information for the enterprise client (e.g., user identification), identifying information for that non-enterprise client (e.g., "Jane Doe"), and any other information that can be used to verify and authenticate that enterprise client or enterprise client device 142.

[0078] If the enterprise client selects the "DELETE" command on the enterprise client device 142, the device will generate and transmit a delete request instruction to the provisioner 212 (shown in FIG. 3), including identifying information for that enterprise client device 142, a timestamp, identifying information for the enterprise client, identifying information for the non-enterprise client (e.g., "Jane Doe"), and any other information that can be used to verify and authenticate that enterprise client or enterprise client device 142. After receiving the delete request instruction from the enterprise client device 142, the provisioner 212 can send a follow-up instruction to an appropriate subsystem (not shown) in the intranet to follow up with the enterprise client, in case any changes need to be made to enterprise records associated with that enterprise client (e.g., beneficiary data, dependent data, family member data, or the like).

[0079] The non-enterprise client John Smith can be a family member (e.g., a spouse of the enterprise user) for whom access to the extranet enterprise domain was previously provisioned. The enterprise client record can include a field that indicates that the non-enterprise client John Smith is active. In this instance, a plurality of command fields can be displayed (e.g., as radio buttons), including "RESEND LOGIN DETAILS," "EDIT," and "DELETE" commands. If the enterprise client selects the "EDIT" or "DELETE" command, the enterprise client device

142 will generate and transmit an edit request or a delete request to the provisioner 212, as discussed above. If the enterprise client selects the "RESEND LOGIN DETAILS" command on the enterprise client device 142, the device will generate and transmit a resend login details request to the provisioner 212 (shown in FIG. 3), including identifying information for that enterprise client device 142, a timestamp, identifying information for the enterprise client, identifying information for that non-enterprise client (e.g., "John Smith"), and any other information that can be used to verify and authenticate that enterprise client or enterprise client device 142. This command can be useful where the non-enterprise client John Smith changed his email address or phone number (or ANI). Upon receiving the resend login details request from the enterprise client device 142, the provisioner 212 can initiate the process discussed above (e.g., shown in FIG. 4).

[0080] A computer readable medium can be provided containing a computer program, which when executed on one or more of the computing devices in the intranet provisioning system 210 or extranet provision system 220, cause the processes shown in FIGS. 4-6, the connectivity flow shown in FIG. 7, and display screen in FIG. 8 to be carried out. The computer program can be tangibly embodied in the computer readable medium, comprising one or more program instructions, code segments, or code sections for performing each of the Steps 305 through 355 in FIG. 3 (and FIG. 7), Steps 342 through 385 in FIG. 5 (and FIG. 7), Steps 410 through 480 in FIG. 6, and displaying the GUI in FIG. 8, when executed by the one or more computing devices in the intranet provisioning system 210 or extranet provisioning system 220.

[0081] The terms "a," "an," and "the," as used in this disclosure, means "one or more," unless expressly specified otherwise.

[0082] The term "communicating device," as used in this disclosure, means any hardware, firmware, or software that can transmit or receive data packets, instruction signals or data signals over a communication link. The hardware, firmware, or software can include, for example, a telephone, a smart phone, a personal data assistant (PDA), a smart watch, a tablet, a computer, a software defined radio (SDR), or the like, without limitation. The communicating device can be portable or stationary.

[0083] The term "communication link," as used in this disclosure, means a wired and/or wireless medium that conveys data or information between at least two points. The wired or wireless medium can include, for example, a metallic conductor link, a radio frequency (RF) communication link, an Infrared (IR) communication link, an optical communication link, or the like, without limitation. The RF communication link can include, for example, WiFi,

WiMAX, IEEE 802.11, DECT, 0G, 1G, 2G, 3G or 4G cellular standards, Bluetooth, or the like, without limitation.

[0084] The terms "computer" or "computing device," as used in this disclosure, means any machine, device, circuit, component, or module, or any system of machines, devices, circuits, components, modules, or the like, which are capable of manipulating data according to one or more instructions, such as, for example, without limitation, a processor, a microprocessor, a central processing unit, a general purpose computer, a super computer, a personal computer, a laptop computer, a palmtop computer, a notebook computer, a desktop computer, a workstation computer, a server, a server farm, a computer cloud, or the like, or an array of processors, microprocessors, central processing units, general purpose computers, super computers, personal computers, laptop computers, palmtop computers, notebook computers, desktop computers, workstation computers, servers, or the like, without limitation.

[0085] The term "computer-readable medium," as used in this disclosure, means any storage medium that participates in providing data (for example, instructions) that can be read by a computer. Such a medium can take many forms, including non-volatile media and volatile media. Non-volatile media can include, for example, optical or magnetic disks and other persistent memory. Volatile media can include dynamic random access memory (DRAM). Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a CD-ROM, DVD, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH-EEPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read. The computer-readable medium can include a "Cloud," which includes a distribution of files across multiple (e.g., thousands of) memory caches on multiple (e.g., thousands of) computers.

[0086] Various forms of computer readable media can be involved in carrying sequences of instructions to a computer. For example, sequences of instruction (i) can be delivered from a RAM to a processor, (ii) can be carried over a wireless transmission medium, and/or (iii) can be formatted according to numerous formats, standards or protocols, including, for example, WiFi, WiMAX, IEEE 802.11, DECT, 0G, 1G, 2G, 3G, 4G, or 5G cellular standards, Bluetooth, or the like.

[0087] The term "database," as used in this disclosure, means any combination of software and/or hardware, including at least one application and/or at least one computer. The database can include a structured collection of records or data organized according to a database model, such as, for example, but not limited to at least one of a relational model, a hierarchical model,

a network model or the like. The database can include a database management system application (DBMS) as is known in the art. The at least one application may include, but is not limited to, for example, an application program that can accept connections to service requests from clients by sending back responses to the clients. The database can be configured to run the at least one application, often under heavy workloads, unattended, for extended periods of time with minimal human direction.

[0088] The terms "including," "comprising" and variations thereof, as used in this disclosure, mean "including, but not limited to," unless expressly specified otherwise.

[0089] The term "network," as used in this disclosure means, but is not limited to, for example, at least one of a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a personal area network (PAN), a campus area network, a corporate area network, a global area network (GAN), a broadband area network (BAN), a cellular network, the Internet, or the like, or any combination of the foregoing, any of which can be configured to communicate data via a wireless and/or a wired communication medium. These networks can run a variety of protocols not limited to TCP/IP, IRC or HTTP.

[0090] The term "server," as used in this disclosure, means any combination of software and/or hardware, including at least one application and/or at least one computer to perform services for connected clients as part of a client-server architecture. The at least one server application can include, but is not limited to, for example, an application program that can accept connections to service requests from clients by sending back responses to the clients. The server can be configured to run the at least one application, often under heavy workloads, unattended, for extended periods of time with minimal human direction. The server can include a plurality of computers configured, with the at least one application being divided among the computers depending upon the workload. For example, under light loading, the at least one application can run on a single computer. However, under heavy loading, multiple computers can be required to run the at least one application. The server, or any if its computers, can also be used as a workstation.

[0091] The term "transmission," as used in this disclosure, means the conveyance of signals via electricity, acoustic waves, light waves and other electromagnetic emissions, such as those generated with communications in the radio frequency (RF) or infrared (IR) spectra. Transmission media for such transmissions can include coaxial cables, copper wire and fiber optics, including the wires that comprise a system bus coupled to the processor.

[0092] Devices that are in communication with each other need not be in continuous communication with each other, unless expressly specified otherwise. In addition, devices that

are in communication with each other may communicate directly or indirectly through one or more intermediaries.

[0093] Although process steps, method steps, algorithms, or the like, may be described in a sequential order, such processes, methods and algorithms may be configured to work in alternate orders. In other words, any sequence or order of steps that may be described does not necessarily indicate a requirement that the steps be performed in that order. The steps of the processes, methods or algorithms described herein may be performed in any order practical. Further, some steps may be performed simultaneously.

[0094] When a single device or article is described herein, it will be readily apparent that more than one device or article may be used in place of a single device or article. Similarly, where more than one device or article is described herein, it will be readily apparent that a single device or article may be used in place of the more than one device or article. The functionality or the features of a device may be alternatively embodied by one or more other devices which are not explicitly described as having such functionality or features.

[0095] While the disclosure has been described in terms of exemplary embodiments, those skilled in the art will recognize that the disclosure can be practiced with modifications in the spirit and scope of the appended claims. These examples are merely illustrative and are not meant to be an exhaustive list of all possible designs, embodiments, applications, or modifications of the disclosure.

WHAT IS CLAIMED IS:

1. A provisioning system that provisions a non-enterprise client with access to an extranet enterprise domain, the provisioning system comprising:

an enterprise client device connected to an intranet;

a provisioner that receives an extranet registration request from the enterprise client device and parses enterprise client data and non-enterprise client data from the extranet registration request;

an active directory connected to the intranet and having an enterprise client record associated with the enterprise client data;

a database that stores a non-enterprise client record populated with the non-enterprise client data;

a primary transmission system connected to the intranet that transmits a portion of the non-enterprise client data and a linkage message outside of the intranet; and

a secondary transmission system connected to the intranet and configured to transmit to an access message outside of the intranet,

wherein the provisioner generates a unique permanent identification ID_{INDEX} for the non-enterprise client record.

2. The provisioning system of claim 1, wherein the provisioner generates the linkage message and the access message.

3. The provisioning system of claim 1, wherein the linkage message is sent to a non-enterprise client device in an email message.

4. The provisioning system of claim 1, wherein the access message is sent in an SMS text message to the non-enterprise client device.

5. The provisioning system of claim 1, wherein the active directory comprises a lightweight directory access protocol (LDAP) directory.

6. The provisioning system of claim 1, wherein the provisioner queries the active directory in response to the extranet registration request to locate the enterprise client record.

7. The provisioning system of claim 1, further comprising:

a registration application programming interface that receives the linkage message from the provisioner and generates an email message, including an activation link.

8. The provisioning system of claim 7, wherein the provisioner performs an outbound call through the intranet firewall to the registration application programming interface.

9. The provisioning system of claim 7, wherein the outbound call comprises a representational state transfer (REST) application programming interface call.

10. The provisioning system of claim 7, wherein the registration application programming interface receives the non-enterprise client identifier ID_{INDEX} for the non-enterprise client.

11. The provisioning system of claim 7, wherein the registration application programming interface receives the portion of the non-enterprise client data.

12. The provisioning system of claim 1, wherein the portion of the non-enterprise client data comprises a non-enterprise email address and an automatic number identification for a non-enterprise client device.

13. A method for provisioning a non-enterprise client with access to an extranet enterprise domain, the method comprising:

receiving an extranet registration request from an enterprise client device connected to an intranet;

parsing enterprise client data and non-enterprise client data from the extranet registration request;

querying an active directory for an enterprise client record based on the enterprise client data, the active directory being connected to the intranet;

storing the non-enterprise client data in a non-enterprise client record;

generating a unique permanent identification ID_{INDEX} for the non-enterprise client record;

transmitting by a primary transmission system a portion of the non-enterprise client data outside of the intranet; and

transmitting by a secondary transmission system an access message outside of the intranet, the secondary transmission system being different than the primary transmission system.

14. The method of claim 13, further comprising:

generating a linkage message based on the non-enterprise client data; and

transmitting the linkage message outside of the intranet.

15. The method of claim 14, wherein the transmitting the linkage message comprises sending an electronic mail message to a non-enterprise client device.

16. The method of claim 13, further comprising:

transmitting the access message to a non-enterprise client device,

wherein the access message comprises an SMS text message.

17. The method of claim 13, wherein the active directory comprises a lightweight directory access protocol (LDAP) directory.

18. The method of claim 13, further comprising:

receiving the portion of the non-enterprise client data at a registration application programming interface.

19. The method of claim 14, further comprising:

receiving the linkage message at a registration application programming interface.

20. The method of claim 19, further comprising:

generating an electronic mail message by the registration application programming interface; and

sending the electronic mail message to the non-enterprise client device,

wherein the electronic mail message includes an activation link.

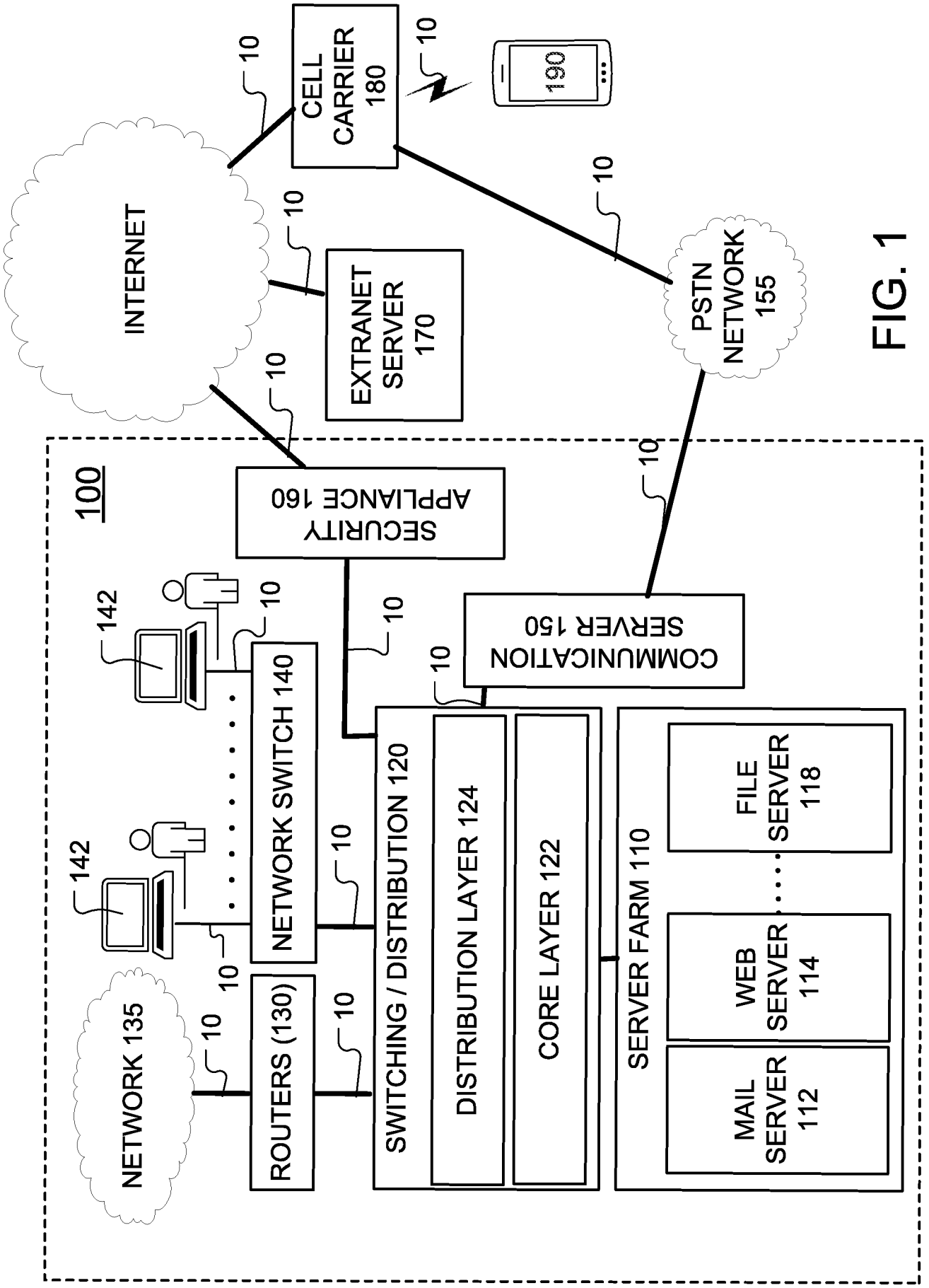
INTERNET
CELL CARRIER 180
190
EXTRANET SERVER 170
PSTN NETWORK 155
100
SECURITY APPLIANCE 160
COMMUNICATION SERVER 150
142
NETWORK SWITCH 140
NETWORK 135
ROUTERS (130)
SWITCHING / DISTRIBUTION 120
DISTRIBUTION LAYER 124
CORE LAYER 122
SERVER FARM 110
FILE SERVER 118
WEB SERVER 114
MAIL SERVER 112
10

FIG. 1

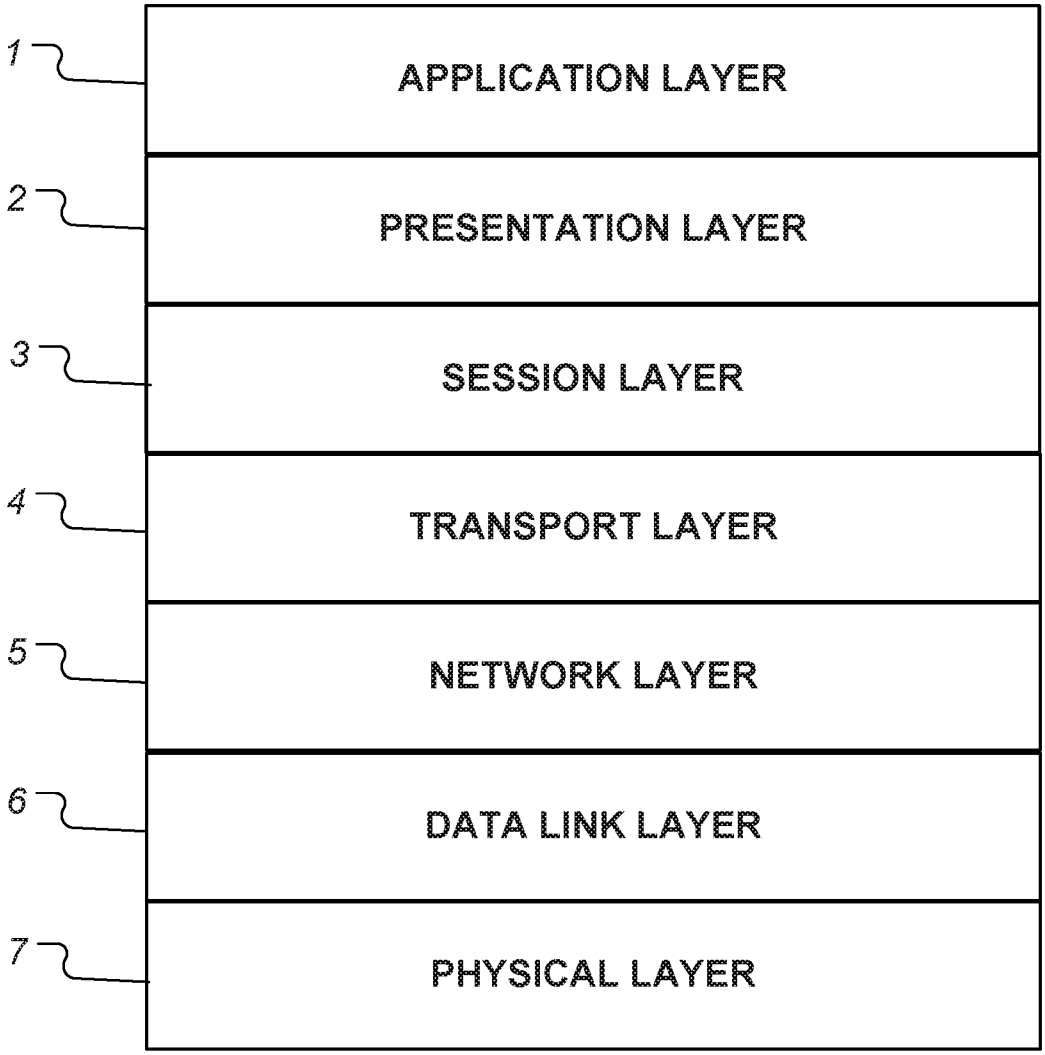
1
APPLICATION LAYER
2
PRESENTATION LAYER
3
SESSION LAYER
4
TRANSPORT LAYER
5
NETWORK LAYER
6
DATA LINK LAYER
7
PHYSICAL LAYER

FIG. 2

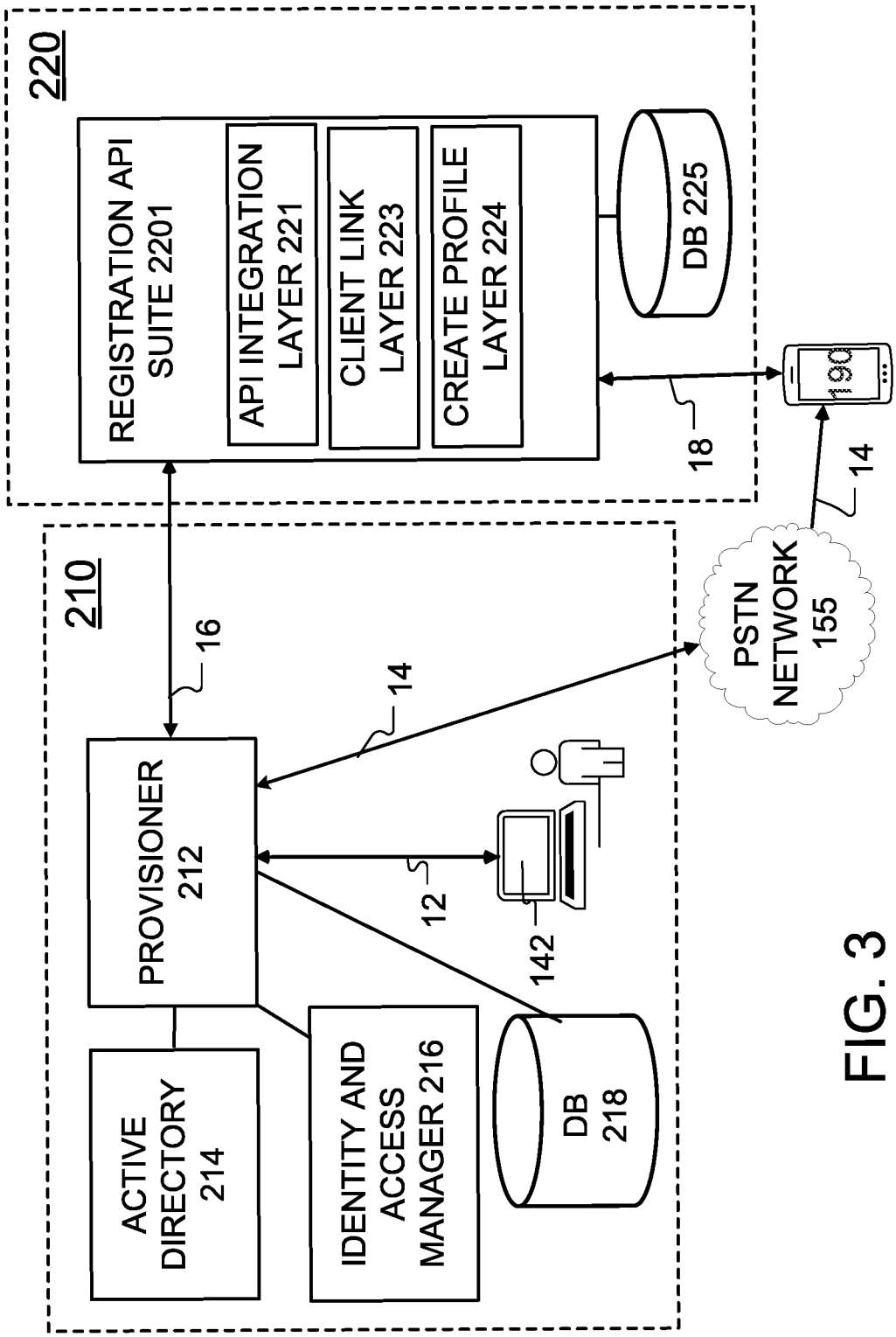
220
REGISTRATION API SUITE 2201
API INTEGRATION LAYER 221
CLIENT LINK LAYER 223
CREATE PROFILE LAYER 224
DB 225
18
190
14
PSTN NETWORK 155
210
16
14
PROVISIONER 212
12
142
ACTIVE DIRECTORY 214
IDENTITY AND ACCESS MANAGER 216
DB 218

FIG. 3

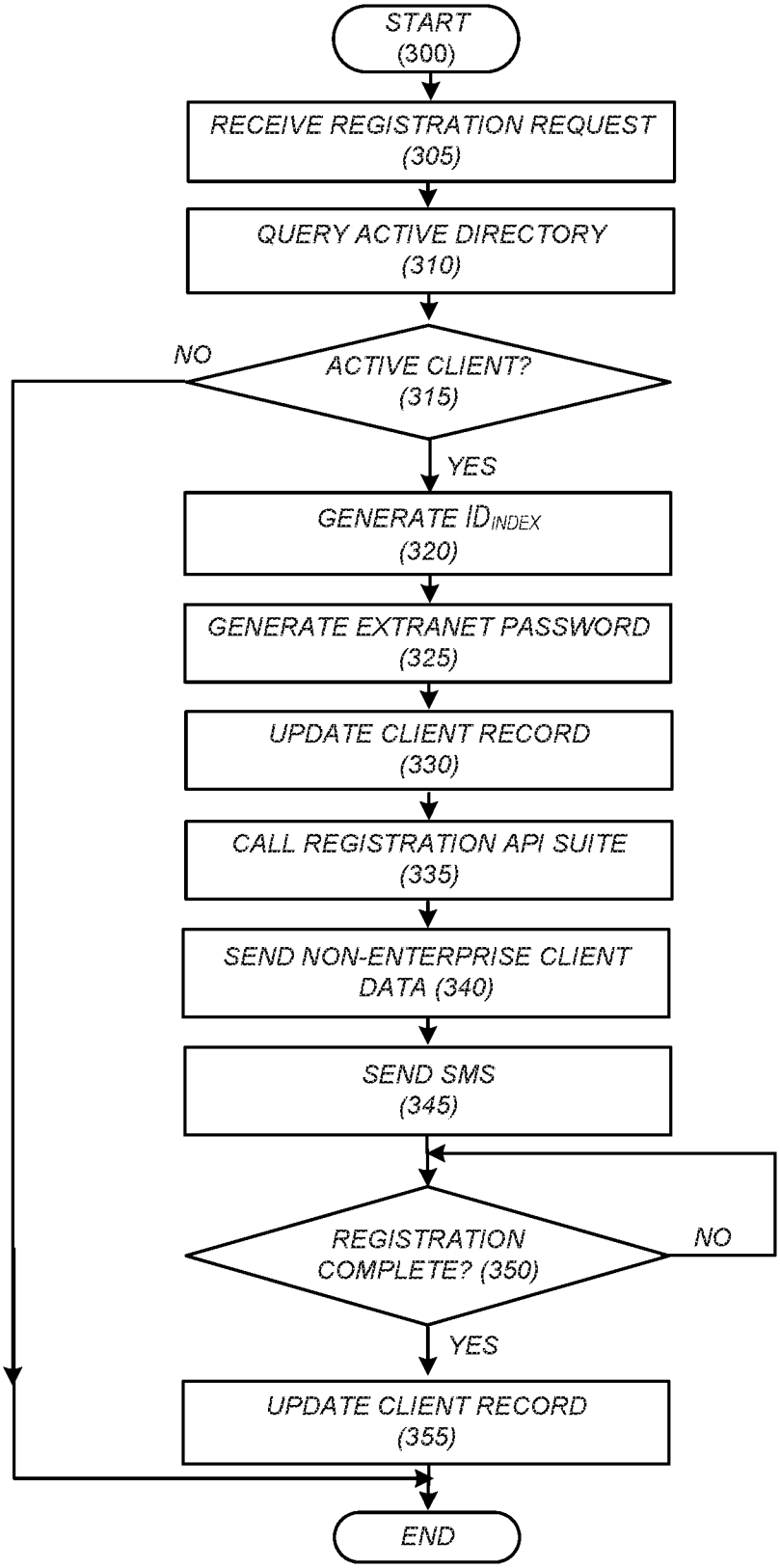
START
(300)
RECEIVE REGISTRATION REQUEST
(305)
QUERY ACTIVE DIRECTORY
(310)
NO
ACTIVE CLIENT?
(315)
YES
GENERATE ID_{INDEX}
(320)
GENERATE EXTRANET PASSWORD
(325)
UPDATE CLIENT RECORD
(330)
CALL REGISTRATION API SUITE
(335)
SEND NON-ENTERPRISE CLIENT DATA (340)
SEND SMS
(345)
REGISTRATION COMPLETE? (350)
NO
YES
UPDATE CLIENT RECORD
(355)
END

FIG. 4

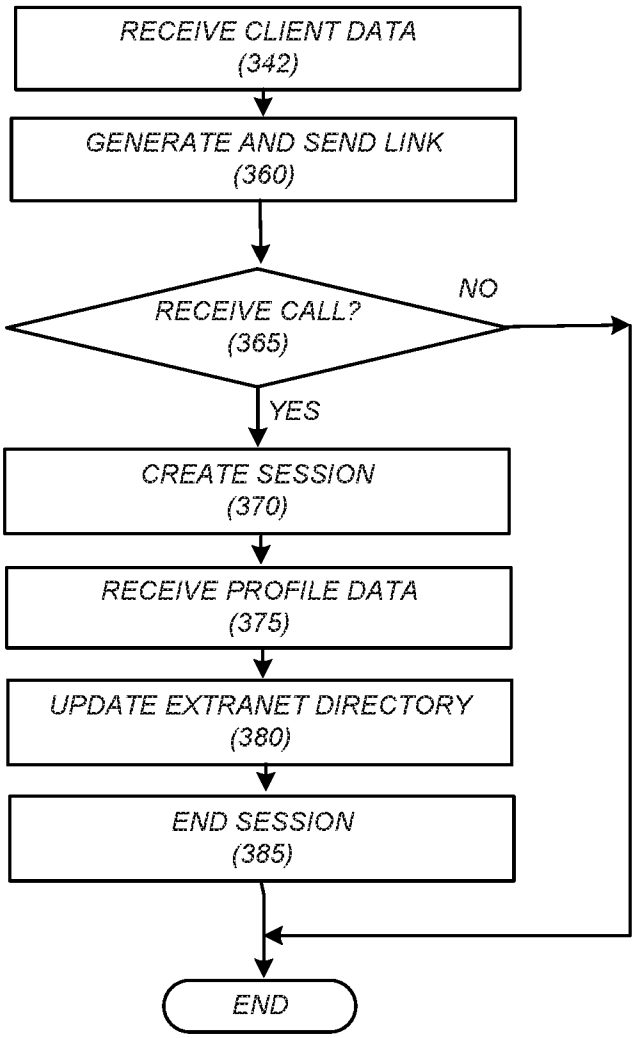
RECEIVE CLIENT DATA
(342)
GENERATE AND SEND LINK
(360)
RECEIVE CALL?
(365)
NO
YES
CREATE SESSION
(370)
RECEIVE PROFILE DATA
(375)
UPDATE EXTRANET DIRECTORY
(380)
END SESSION
(385)
END

FIG. 5

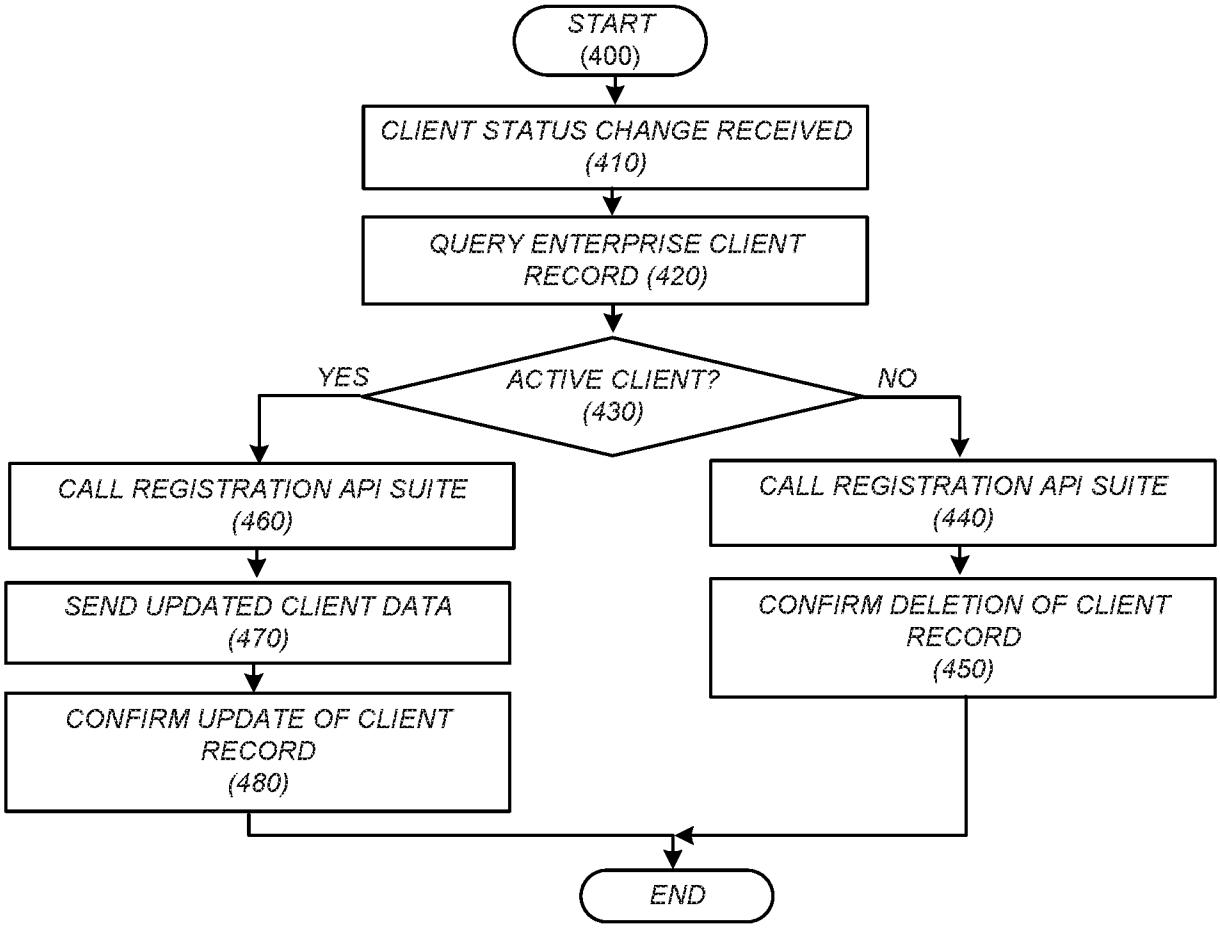
START
(400)
CLIENT STATUS CHANGE RECEIVED
(410)
QUERY ENTERPRISE CLIENT
RECORD (420)
ACTIVE CLIENT?
(430)
YES
NO
CALL REGISTRATION API SUITE
(460)
SEND UPDATED CLIENT DATA
(470)
CONFIRM UPDATE OF CLIENT
RECORD
(480)
CALL REGISTRATION API SUITE
(440)
CONFIRM DELETION OF CLIENT
RECORD
(450)
END

FIG. 6

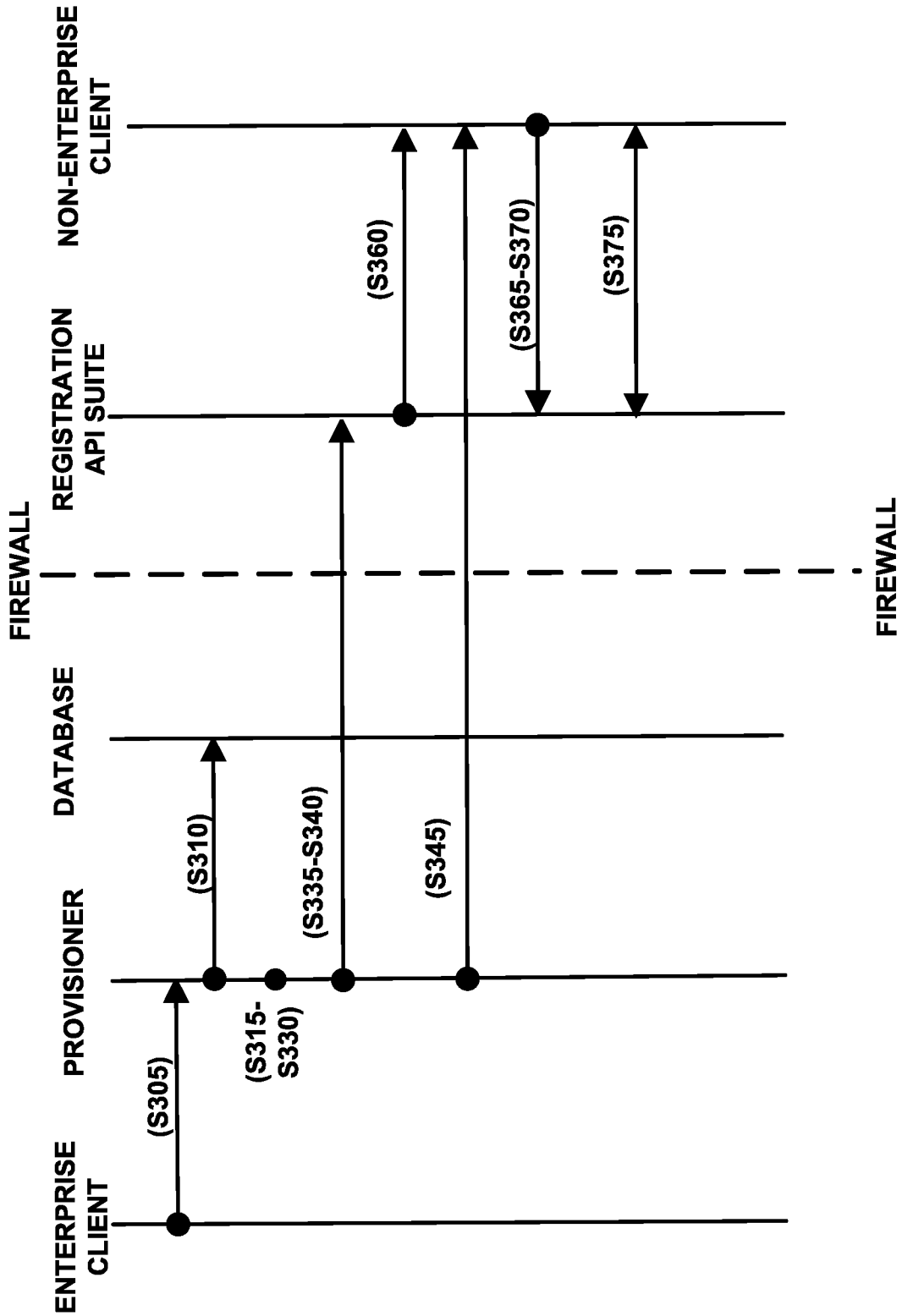
ENTERPRISE CLIENT
PROVISIONER
DATABASE
REGISTRATION API SUITE
NON-ENTERPRISE CLIENT
FIREWALL
FIREWALL
(S305)
(S315-S330)
(S310)
(S335-S340)
(S345)
(S360)
(S365-S370)
(S375)

FIG. 7

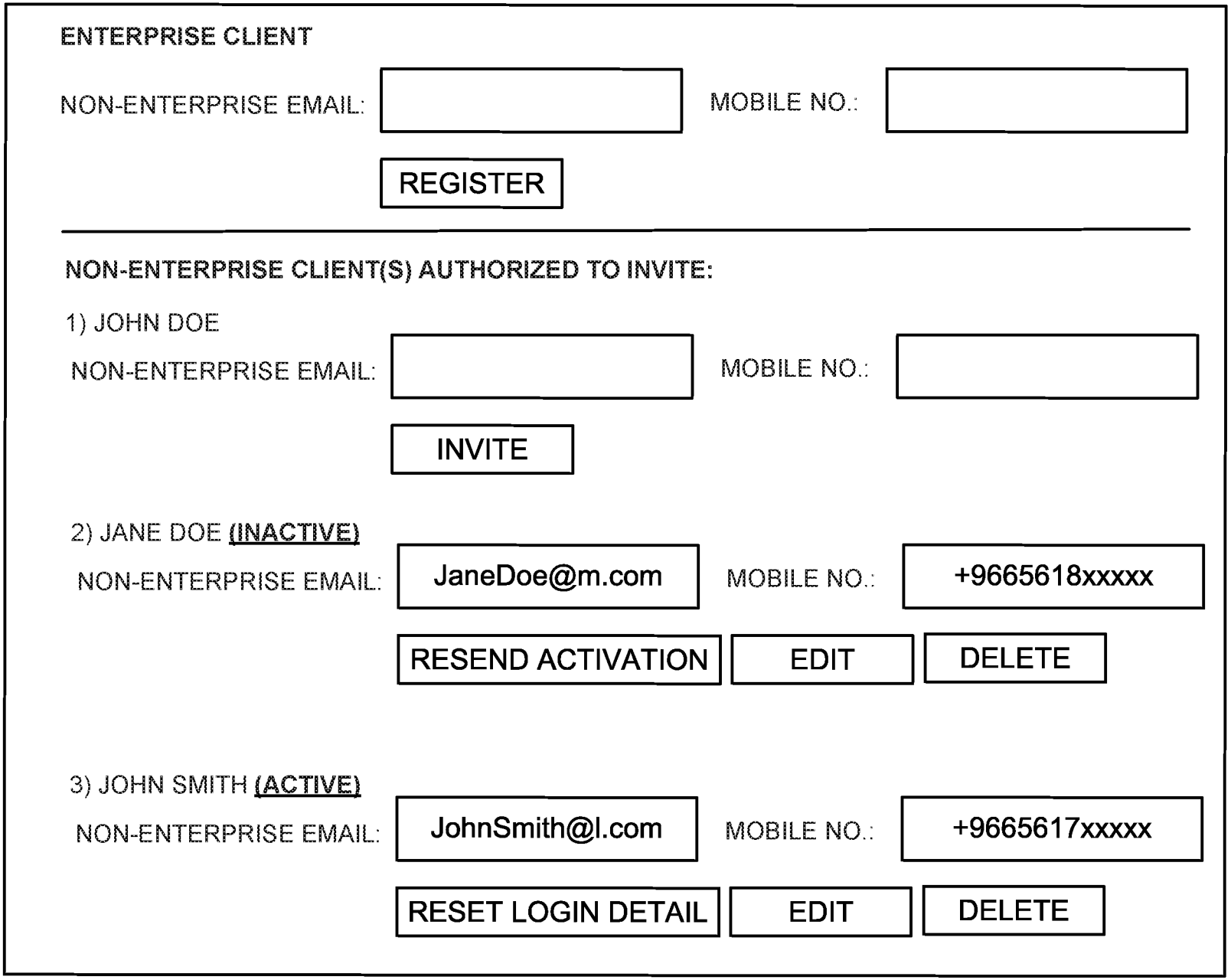
ENTERPRISE CLIENT
NON-ENTERPRISE EMAIL:
MOBILE NO.:
REGISTER
NON-ENTERPRISE CLIENT(S) AUTHORIZED TO INVITE:
1) JOHN DOE
NON-ENTERPRISE EMAIL:
MOBILE NO.:
INVITE
2) JANE DOE (INACTIVE)
NON-ENTERPRISE EMAIL:
JaneDoe@m.com
MOBILE NO.:
+9665618xxxxx
RESEND ACTIVATION
EDIT
DELETE
3) JOHN SMITH (ACTIVE)
NON-ENTERPRISE EMAIL:
JohnSmith@l.com
MOBILE NO.:
+9665617xxxxx
RESET LOGIN DETAIL
EDIT
DELETE

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/017038

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/227667 A1 (LUNDBLADE LAURENCE [US]) 29 August 2013 (2013-08-29) paragraph [0032] - paragraph [0072]; figures 1-9	1-20
A	US 2007/220154 A1 (EL HUSSEINI AHMAD M [US] ET AL) 20 September 2007 (2007-09-20) paragraph [0018] - paragraph [0055]	1-20
A	US 2006/123234 A1 (SCHMIDT DONALD E [US] ET AL) 8 June 2006 (2006-06-08) paragraph [0027] - paragraph [0107]	1-20

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

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 April 2020	04/08/2020

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hou, Jie

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2020/017038

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013227667 A1	29-08-2013	AR 050394 A1	25-10-2006
		AU 2004285255 A1	12-05-2005
		BR PI0415916 A	26-12-2006
		CA 2543987 A1	12-05-2005
		CN 1875564 A	06-12-2006
		EP 1680884 A2	19-07-2006
		JP 4616268 B2	19-01-2011
		JP 2007510235 A	19-04-2007
		KR 20060107798 A	16-10-2006
		NZ 546717 A	30-06-2008
		PE 20050854 A1	18-10-2005
		RU 2322763 C2	20-04-2008
		TW 200517971 A	01-06-2005
		US 2005097330 A1	05-05-2005
		US 2012030742 A1	02-02-2012
		US 2013227667 A1	29-08-2013
		WO 2005043334 A2	12-05-2005
US 2007220154 A1	20-09-2007	NONE	
US 2006123234 A1	08-06-2006	CN 1787435 A	14-06-2006
		US 2006123234 A1	08-06-2006