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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2019 (24.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/017865 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04L 12/14* (2006.01)
H04L 29/06 (2006.01) *H04M 15/00* (2006.01)

(21) International Application Number:
PCT/US2017/042315

(22) International Filing Date:
17 July 2017 (17.07.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **SONY MOBILE COMMUNICATIONS INC.** [JP/JP]; 4-12-3 Higashi-Shinagawa, Shinagawa-ku, Tokyo, Tokyo 140-0002 (JP).

(71) Applicant *(for LC only)*: **SONY MOBILE COMMUNICATIONS (USA) INC.** [US/US]; Agent - Capitol Services Inc., 615 South DuPont Highway, Dover, Delaware 19901 (US).

(72) Inventor: **MELLQVIST, Anders**; Nya Vattentornet, 221 88 Lund (SE).

(74) Agent: **GALIN, M., David**; Tucker Ellis, LLP, 950 Main Avenue, Suite 1100, Cleveland, Ohio 44113 (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, 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, 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,

WO 2019/017865 A1

(54) Title: APPLICATION-LEVEL SERVICE CREDENTIALS FOR NETWORK ACCESS AUTHENTICATION

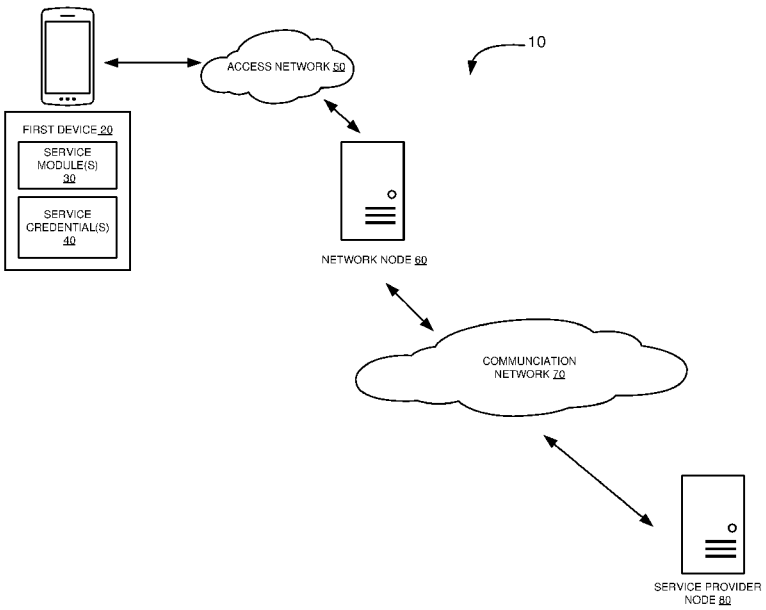

FIGURE 1

(57) Abstract: A system for providing network access/connectivity authorization via presentation and authentication of service credentials by a service provider. As such, network connectivity is established for a specific service and is solely predicated/determined by the service provider, such that the service provider controls which entities/users are authorized to connect to the network, and thus use the service, and, in some embodiments, allows for the service control to control the duration of the network connectivity/service session and/or the amount of data consumed during the duration of the network connectivity/service session.

[Continued on next page]

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))*

APPLICATION-LEVEL SERVICE CREDENTIALS FOR NETWORK ACCESS AUTHENTICATION

FIELD OF THE INVENTION

[0001] The present invention is generally directed to digital communication and, more specifically, network connectivity.

BACKGROUND

[0002] In the current network communication environments, when a device, such as mobile terminal or the like, is turned-on, the device searches for and is connected to a network. The network to which the device is connected may be associated with a wireless communication network provider (*e.g.*, the user of the device possesses a data plan with a cellular service provider, an Internet service provider (ISP) or the like). Subsequently, when a user wants to start using an application-level service, the application requests network connectivity and, since the device is already connected to the network, network connectivity is provided to the application/service. In this current model, in which network connectivity is independent of services provided, it is difficult for a user to assess how network connectivity is associated with the services provider. In this regard, network providers typically offer monthly data rate plans based on different maximum data consumption levels (*e.g.*, 5 gigabytes per month or the like). If the user is merely using the data plan to consume web page content, the user is unlikely to exhaust the maximum data level. Conversely, if the user is using the data plan to consume multimedia content (*e.g.,* video streaming or the like), the maximum data level is likely to be exhausted after a few hours of consuming the multimedia content. As the number of connected devices dramatically increases, the drawbacks associated with this type of model become readily apparent. It is unrealistic for the user to make correct estimations as to the amount of data consumed by the multiple different services used by the user, especially when those services are consumed on an array of different devices, some of which may be outside of the user's data plan.

[0003] Additionally, in the current network communication environment most devices, such as mobile telephones or the like, are personal devices, which means use of the device is limited to one specific user. However, as more and more devices become network compatible (*i.e.,* Internet-connected devices and the like) many of these devices may be conducive to having their use shared amongst various different users (*e.g.*, different family members, different

employees of a business or the like). However, if network connectivity (*i.e.*, the data plan) is associated with one user, there is no means to apportion the data plan to other users who may use the shared device and, equally important, may use the device for services that are more (or less) data intensive than the user associated with the data plan.

[0004] From the service provider perspective, they rely on their users to have network connectivity to access the services offered. However, the ability of the users to have network connectivity is unpredictable because the ability to provide network connectivity lies on the network providers. In this regard, if the user has exhausted their monthly data allocation or have failed to pay their network provider bill, they may be prevented from receiving network access and, thus prevented from accessing network services. Moreover, if the device being used is a shared device or is a device being used temporarily, the user may not be authorized to use the network connection or otherwise prefer not to access the service using another user's data plan.

BRIEF SUMMARY

[0005] Therefore, a need exists to develop alternative systems, apparatus, methods for providing network access/connectivity and, more specifically, network access-connectivity that is tied to the service/application being used.

[0006] The following presents a simplified summary of one or more embodiments in order to provide a basic understanding of such embodiments. This summary is not an extensive overview of all contemplated embodiments, and is intended to neither identify key or critical elements of all embodiments, nor delineate the scope of any or all embodiments. Its sole purpose is to present some concepts of one or more embodiments in a simplified form as a prelude to the more detailed description that is presented later.

[0007] Embodiments of the present invention address the above needs and/or achieve other advantages by providing methods, apparatus, systems or the like which serve to tie network connectivity to service providers. In this regard, according to embodiments of the invention, network connectivity occurs in response to a user requesting a service as opposed to current models, in which the device is already attached/connected to the network prior to requesting the service. As such, the present invention enables service providers to take full control over connecting devices to a network, such that the service provider can control one or more of (*i*) which users or, in some embodiments which devices, get access to the network (and, thus the

service), (*ii*) limitations/restrictions on how much of the service is provided to the user during the network connectivity session, (*iii*) the rates charged to the user for the service and the like.

[0008] A method for obtaining network connectivity defines first embodiments of the invention. The method includes obtaining, at a first device, a service credential signed by a service provider of a service and used for network authorization. The method further includes communicating the service credential to the service provider, via a network node, in order to obtain network connectivity for the service. Additionally, the method includes obtaining network connectivity for at least the service from the network node. The network connectivity is based on the service provider verifying the service credential and providing network connectivity authorization.

[0009] In specific embodiments of the method, obtaining the network connectivity may further include obtaining the network connectivity (*i*) exclusively for the service, or (*ii*) for the service and at least one other service or function on the device requiring a network connection (*e.g.,* a general network connection for all of the services/functions of the device requiring such). In specific embodiments of the method, obtaining the service credential further includes obtaining the service credential associated with a user (*i.e.*, a user-specific service credential).

[0010] In other embodiments of the method, obtaining the service credential further includes communicating a service credential request to the service provider, and, in response to communicating the service credential request, receiving the service credential from the service provider. In such embodiments of the method, communicating the service credential request and receiving the service credential occur via (*i*) a bootstrap-type network connection or (*ii*) a second device in communication with the first device.

[0011] In still further related embodiments the method includes, prior to communicating the service credential, attaching a device signature associated with the first device to the service credential.

[0012] In yet other specific embodiments the method includes selecting a communication network for the network connectivity based on at least one of (*i*) a signal quality of signals, each signal received from one of a plurality of communication networks, and (*ii*) one or more predetermined business rules.

[0013] In further specific embodiments of the method, obtaining the network connectivity further includes obtaining the network connectivity according to one or more

service parameters, whereby the service provider selects the one or more service parameters. In such embodiments the method may further include receiving an indication of at least one of the one or more service parameters.

[0014] A device configured for obtaining network connectivity defines second embodiments of the invention. The device includes a processor and a memory in communication with the processor. The device further includes a service module stored in the memory and executable by the processor. The service module is configured to obtain a service credential signed by a service provider of the service and used for network authorization. The device further includes a network module stored in the memory and executable by the processor. The network module is configured to communicate the service credential to a service provider node via a network node in order to obtain network connectivity for at least the service. The service module is further configured to obtain network connectivity for at least the service from the network node. The network connectivity is based on the service provider node verifying the service credential and providing network authorization.

[0015] In specific embodiments of the device, the service module is further configured to obtain the network connectivity (*i*) exclusively for the service, or (*ii*) for the service and at least one other service or function on the device requiring a network connection (*e.g.*, a general network connection for all of the services/functions of the device requiring such).

[0016] In further embodiments of the device the service module is further configured to obtain the service credential associated with a user.

[0017] In other specific embodiments of the device the service module is further configured to obtain the service credential by communicating a service credential request to the service provider node, and, in response to communicating the service credential request, receive the service credential from the service provider node.

[0018] In still further specific embodiments the device includes a digital signature module stored in the memory, executable by the processor and configured to, prior to communicating the service credential, attach a device signature associated with the first device to the service credential.

[0019] In additional specific embodiments of the device includes a network selection module stored in the memory and executable by the processor. The network selection module is configured to select a communication network for the network connectivity based on at least one

of (*i*) a signal quality of signals, each signal received from one of a plurality of communication networks, and (*ii*) one or more predetermined business rules.

[0020] Moreover, in further specific embodiments of the device, the service module is further configured to obtain the network connectivity according to one or more service parameters obtained from the service provider node.

[0021] A method for providing, by a service provider node network connectivity authorization defines third embodiments of the invention. The method includes receiving, a service credential signed by the service provider and verifying, the service credential. The method further includes, in response to verifying the service credential, communicating a network connectivity authorization to a network node.

[0022] In specific embodiments of the method, communicating the network connectivity authorization further includes communicating the network connectivity authorization that provides a network connection either (*i*) exclusively for the service, or (*ii*) for the service and at least one other service or function on the device requiring a network connection (*e.g.*, a general network connection for all of the services/functions of the device requiring such).

[0023] In still further specific embodiments of the method, receiving the service credential further includes receiving the service credential associated with a user and, in such embodiments, the method further includes verifying, by the service provider node, the user.

[0024] In yet other specific embodiment of the method, receiving the service credential further includes receiving the service credential signed by a first device and, in such embodiments, the method further includes, verifying the first device.

[0025] In additional specific embodiments the method includes obtaining one or more service parameters associated with the network connectivity and communicating the one or more service parameters to the network node. In such embodiments of the method obtaining the service parameters may further include obtaining the services parameters, wherein at least one of the service parameters are specific to a user. In other related embodiments of the method, obtaining the one or more service parameters further includes obtaining the service parameters based on at least one of (*i*) a user profile, (*ii*) a first device profile, and (*iii*) one or more business rules. The service parameters may include, but are not limited to, at least one of (*i*) a maximum time for the network connectivity, (*ii*) a maximum amount of data transmitted during the network

connectivity and (*iii*) a maximum percentage of a subscription allotment that can be used for the network connectivity.

[0026] An apparatus configured for providing network connectivity authorization defines fourth embodiments of the invention. The apparatus includes a processor and a memory in communication with the processor. The apparatus further includes a network connectivity authorization module stored in the memory and executable by the processor. The network connectivity authorization module is configured to (*i*) receive a service credential signed by the service provider, (*ii*) verify the service credential, and (*iii*) in response to verifying the service credential, communicate a network connectivity authorization to a network node.

[0027] In specific embodiments of the apparatus, the network connectivity authorization module is further configured to communicate a network connectivity authorization that provides a network connection (*i*) exclusively for the service, or (*ii*) for the service and at least one other service or function on the device requiring a network connection (*e.g.*, a general network connection for all of the services/functions of the device requiring such).

[0028] In specific embodiments of the apparatus the network connectivity authorization module is further configured to receive the service credential associated with a user, and verify the user.

[0029] In still further specific embodiments of the apparatus the network connectivity authorization module is further configured to receive the service credential signed by a first device, and verify the first device.

[0030] In yet other specific embodiments of the apparatus the network connectivity authorization module is further configured to obtain one or more service parameters associated with the network connectivity and communicate the one or more service parameters to the network node. In such embodiments of the apparatus the network connectivity authorization module is further configured to obtain the one or more service parameters, wherein at least one of the service parameters are specific to a user. In specific related embodiments the network connectivity authorization module is further configured to obtain the one or more service parameters based on at least one of (*i*) a user profile, (*ii*) a UE profile, and (*iii*) one or more business rules. The service parameters may include, but are not limited to, at least one of (*i*) a maximum time for the network connectivity, (*ii*) a maximum amount of data transmitted during

the network connectivity, and (*iii*) a maximum percentage of a subscription allotment that can be used for the network connectivity.

[0031] Moreover, in other specific embodiments the apparatus includes a service credential provisioning module stored in the memory and executable by the processor. The service credential provisioning module is configured to generate a user-specific service credential.

[0032] A method for establishing, at a network node, network connectivity, defines fifth embodiments of the invention. The method includes receiving, a service credential signed by a service provider associated with a service and communicating the service credential to a service provider node. The method further includes receiving from the service provider node, a network connectivity authorization, and establishing, network connectivity for at least the service based on the network connectivity authorization.

[0033] In specific embodiments of the method, establishing the network connectivity may further include establishing the network connectivity (*i*) exclusively for the service, or (*ii*) for the service and at least one other service or function on the device requiring a network connection (*e.g.,* a general network connection for all of the services/functions of the device requiring such).

[0034] In specific embodiments the method further includes applying one or more service parameters to the network connectivity, wherein the one or more service parameters are received from the service provider node.

[0035] An apparatus for establishing network connectivity defines sixth embodiments of the invention. The apparatus includes a processor and a memory in communication with the processor. The apparatus further includes a network connectivity module stored in the memory and executable by the processor. The network connectivity module is configured to (*i*) receive a service credential signed by a service provider associated with a service, (*ii*) communicate the service credential to a service provider node, (*iii*) receive, from the service provider node, a network connectivity authorization, and (*iv*) establish network connectivity for at least the service based on the network connectivity authorization.

[0036] In specific embodiments of the apparatus, the network connectivity module is further configured to establish the network connectivity (*i*) exclusively for the service, or (*ii*) for the service and at least one other service or function on the device requiring a network

connection (*e.g.*, a general network connection for all of the services/functions of the device requiring such).

[0037] In specific embodiments of the apparatus, the network connectivity module is further configured to apply one or more service parameters to the network connectivity, wherein the one or more service parameters are received from the service provider node.

[0038] Thus, objects, features, aspects and advantages of the present invention include, but are not limited to, using service-issued credentials to tie network access/connectivity to the service provider as opposed to the network provider. In this regard, the present invention allows for network access/connectivity rates to be assigned to the service provider, which means, in turn, that the service provider can charge the user based on the user's access/use of the service (*i.e.*, the time spent using the service, the amount of data consumed while using the service or the like).

[0039] Additional objects, features, aspects and advantages of the present invention provide for the service to issue user-specific credentials, such that service use parameters can be applied on a per-user basis and service usage can be measured on a per-user basis and, as such, service usage/network connectivity rates can be apportioned on a per-user basis.

[0040] In still further objects, features, aspects and advantages of the present invention provide for service credentials that are configured to authenticate the device on which the service is being accessed, as such it is possible to allot or apportion service usage/network connectivity rates based on the device that is using the service.

[0041] In additional objects, features, aspects and advantages of the present invention the service-requesting device and/or the user are capable of determining/selecting which network to associate with the service based on communication parameters and/or business parameters. Further, such determination/selection may occur dynamically, at the time the service is requested so as to optimize the communication and/or business concerns.

[0042] Moreover, objects, features, aspects and advantages of the present invention provide for the service provider to restrict or otherwise limit the amount of services or time allotted for usage based one or more of (*i*) which user is requesting the services, (*ii*) which device is requesting the services and (*iii*) other criteria that the service provider deems appropriate,

[0043]

[0044] Various other objects, features, aspects, and advantages of the present invention will become more apparent from the following detailed description of preferred embodiments of the invention.

[0045] The features, functions, and advantages that have been discussed may be achieved independently in various embodiments of the present invention or may be combined with yet other embodiments, further details of which can be seen with reference to the following description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0046] Having thus described embodiments of the invention in general terms, reference will now be made the accompanying drawings, wherein:

Figure 1 provides a schematic diagram illustrating a system for implementing service credentials for network access authentication, in accordance with an embodiment of the invention;

Figure 2 provides a signaling diagram of a method for provisioning service credentials to a network-accessible device, in accordance with alternate embodiments of the invention;

Figure 3 provides a signaling diagram of a method for authenticating service credentials for authorizing service-level network connectivity, in accordance with an embodiment of the invention;

Figure 4 provides a flow diagram of a method for requesting and receiving service-level network connectivity at a user equipment, in accordance with an embodiment of the invention;

Figure 5 provides a flow diagram of a method for verifying service credentials and providing network access authorization at a service provider node, in accordance with an embodiment of the invention;

Figure 6 provides a flow diagram of a method for providing network connectivity on a service-level basis through use of service credential verification, in accordance with an embodiment of the invention;

Figure 7 provides a block diagram of a user equipment configured for requesting and receiving service-level network connectivity at a user equipment, in accordance with embodiments of the present invention;

Figure 8 provides a block diagram of a service provider node configured for verifying service credentials and providing network access authorization, in accordance with embodiments of the present invention; and

Figure 9 provides a block diagram of a network node for providing network connectivity on a service level basis through use of service credential verification, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0047] Embodiments of the present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all, embodiments of the invention are shown. Indeed, the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like numbers refer to like elements throughout.

[0048] As will be appreciated by one of skill in the art in view of this disclosure, the present invention may be embodied as an apparatus (*e.g.*, a system, computer program product, and/or other device), a method, or a combination of the foregoing. Accordingly, embodiments of the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, *etc.*), or an embodiment combining software and hardware aspects that may generally be referred to herein as a "system." Furthermore, embodiments of the present invention may take the form of a computer program product comprising a computer-usable storage medium having computer-usable program code/computer-readable instructions embodied in the medium.

[0049] Any suitable computer-usable or computer-readable medium may be utilized. The computer usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device. More specific examples (*e.g.*, a non-exhaustive list) of the computer-readable medium would include the following: an electrical connection having one or more wires; a tangible medium such as a portable computer diskette, a hard disk, a time-dependent access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or

Flash memory), a compact disc read-only memory (CD-ROM), or other tangible optical or magnetic storage device.

[0050] Computer program code/computer-readable instructions for carrying out operations of embodiments of the present invention may be written in an object oriented, scripted or unscripted programming language such as JAVA, PERL, SMALLTALK, C++ or the like. However, the computer program code/computer-readable instructions for carrying out operations of the invention may also be written in conventional procedural programming languages, such as the "C" programming language or similar programming languages.

[0051] Embodiments of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods or apparatuses (the term “apparatus” including systems and computer program products). It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a particular machine, such that the instructions, which execute by the processor of the computer or other programmable data processing apparatus, create mechanisms for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0052] These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instructions, which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0053] The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational events to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions, which execute on the computer or other programmable apparatus, provide events for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks. Alternatively, computer program implemented events or acts may be combined with operator or human implemented events or acts in order to carry out an embodiment of the invention.

[0054] As the phrase is used herein, a processor may be "configured to" perform a certain function in a variety of ways, including, for example, by having one or more general-purpose circuits perform the function by executing particular computer-executable program code embodied in computer-readable medium, and/or by having one or more application-specific circuits perform the function.

[0055] Thus, embodiments of the invention provide for tying network connectivity to service providers. In this regard, according to embodiments of the invention, network connectivity occurs in response to a user requesting a service as opposed to current models, in which the device is already attached/connected to the network prior to requesting the service and the service uses the pre-existing connection for the service. As such, the present invention enables service providers to take full control over connecting devices to a network, such that the service provider can control one or more of (*i*) which users or, in some embodiments which devices, receive access to the network (and, thus the service), (*ii*) limitations/restrictions on how much of the service is provided to the user/device during the network connectivity session, (*iii*) the rates charged to the user for the service access and the like.

[0056] Specifically, the present invention employs service credentials which are provisioned to a device by a service provider on a per-service and a per-user basis. Once a user requests a service (*i.e.*, launches a module and provides user credentials), the service credential is fetched from device memory (typically a secured storage environment) and communicated to the service provider via a network access node. The service provider verifies the service credential, identifies the user as a valid service subscriber and notifies the network access node of network connectivity authorization. In response, the network access node establishes a network connection that is restricted solely for use by the service. In specific embodiments of the invention, the network connectivity is mapped directly to a single service. In such embodiments of the invention, the service provider can control service parameters on a per-user and, in some embodiments, per-device basis. Additionally, mapping network connectivity directly to a service allows for different network billing practices to be implemented, in which users only pay for the services they use. In addition, since network connectivity is tied to a specific user, the present invention allows for billing practices that are capable of partitioning payment based on which user accessed the service. In other embodiments of the invention, the network connectivity that is provided is not service-specific but rather provides for general network connectivity. Such

general network connectivity allows a user of the device to not only access the service associated with the connectivity but also perform other network functions (*e.g.*, access other network-based services, browse the Internet, send/receive Short Message Service (SMS) messages and the like).

[0057] In specific embodiments of the invention, the service credentials may take the form of a digital token. A digital token generally uses a limited amount of memory for storage and a limited amount of processing power to read the contents of the token. For example, while service credentials may comprise a lengthy set of data, the digital token stores a short-form identifier that corresponds to a specific set of data (*i.e.*, a specific credential). The credential provisioning entity (*e.g.*, service provider) associates the short-form identifier with the digital token and the corresponding set of data/credential, such that, when the digital token is presented to the verifying entity (*e.g.*, service provider) the short-form identifier is used to determine the service credential corresponding to the short-form identifier.

[0058] Referring to **Figure 1** a schematic diagram is shown of a system 10 for implementing service-specific network access/connectivity, in accordance with embodiments of the present invention. The system includes device 20, access network node 60 and service provide node 80. Device 20 is in communication with access network node 60 via access network 50 and access network node 60 is in communication with service provider node 80 via communication network 70. The communication network 70 may be a wired and/or wireless communication network including, but not limited to, a local area network (LAN), such as a WI-FI network or the like, a cellular network (including evolution of 3rd Generation Partnership Project (3GPP) releases, 5th Generation (5G) releases, Long Term Evolution (LTE) or the like.

[0059] The device 20 may comprise any device configured for network connectivity that utilizes services, otherwise referred to as, service modules or "apps", requiring network connectivity. While in the illustrated example of **Figure 1** the device 20 is shown to be a mobile terminal, device 20 is not limited to being "mobile" (*i.e.*, the device may be a substantially stationary device, such as a PC, an Internet-of-Things (IOT) device, or the like). For example, the device may comprise a speaker, a multimedia viewing device, a smart telephone, or the like.

[0060] Device 20 stores one or more service modules 30 that are configured for network connectivity and, in specific embodiments of the invention service-specific network connectivity. Service modules 30 are also referred to as service application, or more generally, service "apps". In such embodiments of the invention, the network connectivity that is established is specific to

the associated service module 30, such that the network connectivity is established once a service is requested and is terminated once the service session is ended. In other embodiments of the invention, the network connectivity is not service-specific, but rather is general network connectivity that allows the user to use the network connection for other network services implemented on the device. Such network connectivity is made possible by use of service credential(s) 40 otherwise referred to herein as a digital data structure, which is used as a means of obtaining authorization, at the service provider node 80, for network connectivity.

[0061] Specifically, according to embodiments of the present invention, first device 20, obtains the service credential 40 (specific means for obtaining a service credential are described in relation to **Figure 2** discussed *infra.*) for a service that requires network connectivity and stores the service credential 40 in a secured storage area. The service credential 40 is digitally signed (*i.e.*, encoded, encrypted or the like) by the service provider, such that, only the service provider, in possession of a private PKI (Public Key Infrastructure), can read the signature (*i.e.*, decode, decrypt or the like). In response to first device 20 requesting a service (*e.g.*, launching a service module 30 or the like), the service credential 40 is fetched from the secure storage area and communicated to the network node 60, via the access network 50, as part of a connection request. Based on the service credential 40, the access node 60 identifies the service provider associated with the service credential 40, and forwards the service credential 40 to the service provider node 80 via the communication network 70. The service provider node 80, for example, verifies or otherwise authenticates the service credential 40 and, in response to verifying the service credential 40, grants authorization for network connectivity and communicates such to the network node 60 via the communication network 70. Subsequently, the network node 60 establishes network connectivity for the device 20 service module based on the authorization for network connectivity provided by the service provider node 80. In specific embodiments of the invention, the network node 60 establishes the network connectivity specifically for the service module 30.

[0062] In specific embodiments of the invention, the service credential 40 is user-specific (*i.e.*, the service credential is issued to a single user), as well as, service-specific. As such, the service providers control network connectivity for the service on a per-user basis. This means that the user is required to be authorized for network connectivity (*e.g.*, have a valid subscription for the service) in order for the service provider to issue the service

credential 40 to the user. Subsequently, verification of the service credential 40 by the service provider node 80, requires verification that the user has a valid subscription.

[0063] As such, the present invention provides for the service provider to be the gateway for network connectivity. In other words, the service provider, through requiring presentation of service provider-issued service credential 40, controls which devices and/or users are granted network connectivity and, in specific embodiments, service-specific network connectivity. From a business perspective, this means that the service providers are responsible for any fees associated with the network connection/access, with such fees being passed along to the users (*i.e.*, service subscribers). Unlike the present model in which the users purchase a data plan from the network providers (ISPs (Internet Service Providers), wireless communication service providers, *etc*.) regardless of the type of services consumed by the user, the present invention is capable of mapping the service to the network connectivity and, in doing so, allows for the user to only be charged, by the service provider, for actual services consumed.

[0064] Moreover, by providing for service-level network connectivity on a *per-user basis*, the present invention allows for devices 20 to be shared amongst more than one user and for service consumption to be apportioned to the different users, accordingly. This means that, unlike current models in which data plans are associated with a single user, the present invention allows for different users of a shared or common (*i.e.*, non-personal) device 20 to use a service available on the device 20 and be apportioned the fees associated with the service used.

[0065] **Figure 2** provides a signaling diagram of a method 100 for provisioning a service credential on a device, in accordance with embodiments of the present invention. At Event 140, a service module 30 communicates a service credential request along with user credentials (*e.g.*, username and/or passcode, or the like) to a service credential provisioning module 130 at the service provider node 80. In certain instances, the device 20 may have a pre-existing network connection which can be used to communicate the service credential request. In other instances, in which first device 20 is device without current network connectivity (*e.g.*, a new/out-of-the-box device or the like), the device may be configured for limited network connectivity to perform initial configuration steps (*e.g.*, download certain service modules, request and receive service credential 40, or the like). In other instances, in which the service module 30 is currently installed on the device 20 (*e.g.*, pre-loaded on a new device or the like), the service module may include a generic credential/token that allows for the limited network connectivity, such as to

request and receive service credential 40 or the like. These methodologies are commonly referred to in the art as performing a bootstrap-type network connection.

[0066] In other embodiments of the invention (not depicted in **Figure 2**), the device 20 may obtain the service credential through a tethering mode with another device (*i.e.*, the other device, which currently has network connectivity, communicates the service credential request on behalf of device 20, receives the service credential, and then communicates the service credential to device 20 via a physical connection or via a short-range wireless technique (*e.g.*, Bluetooth® or the like).

[0067] At Event 150, the service credential provisioning module generates service credential 40, which, in specific embodiments of the invention, is a user-specific service credential. As previously noted, in specific embodiments of the invention, the service credential is digitally signed (*i.e.*, encoded, encrypted or the like) by the service provider, such that, only the service provider, in possession of a private PKI (Public Key Infrastructure), can verify the service credential (*i.e.*, decode, decrypt or the like using the private PKI). At Event 160, the service credential is communicated from the service provider node 70 to the first device 20 and, more specifically, to the service module 30 residing on the first device 20.

[0068] At Event 170, the service module 30, forwards the service credential 40 to a secure storage environment 180 within the first device 20. The secure storage environment 180 may be a stand-alone secure memory unit/device within the first device or, as configured, a secure portion of the general memory unit/device within the first device. It should be noted that first device 20 may have multiple different security credentials 40 stored in the secure storage environment 140. For example, secure storage environment 140 may store at least one service credential for each service module 30 configured for service-specific network connectivity and may further store an individual service credential 30 for each user of an individual service module 30.

[0069] Referring to **Figure 3** a flow diagram is illustrated of a method 200 for requesting and receiving service-specific network connectivity, in accordance with embodiments of the present invention. At Event 210, the service module 30 requests network connectivity to the network module 220. In specific embodiments, the request is initiated by a user launching the associated service module 30, which, in some embodiments, is configured for service-specific network connectivity and entering user credentials (*i.e.*, username and/or passcode). As

previously discussed, in certain embodiments of the invention, the network connectivity request is specific to the service and the user (*i.e.*, the request includes the user credentials or some user identifier), while in other embodiments of the invention, the network connectivity request may be for general network connectivity (*i.e.*, connectivity that allows other services to use the connection)

[0070] In current network communication environments, when application module requests network connectivity the device is already attached to a network (*i.e.*, the device has previously presented the network with subscriber credentials stored in a SIM (Subscriber Identity Module) or the like). The application makes a request to the operating system for a specific URL (Universal Resource Locator)/service address associated with a service provider server, and the operating system provides the service with a requisite socket for the connection. However, according to the present invention, either a pre-existing connection does not exist at the time service module 30 requests network connectivity or, in the event that a pre-existing network connection does exist, the service module 30 is configured to ignore the existing network connection and request service-specific network connectivity.

[0071] In receipt of the network connectivity request, the network module 220 fetches the service credential 40 by sending, at Event 230, a service credential request to the secure storage environment 180 and, in response to the request, at Event 240, the service credential; typically specific to (*i*) the service and (*ii*) the user requesting the service, is retrieved from the secure storage environment 180. In optional embodiments of the invention, the service credentials may also be digitally signed (encoded, encrypted or the like) by the device to indicate the device-type and/or manufacturer. Such device signing may be on a per-service basis, and, as such, the device signing may occur in response to the service credential request at the time of retrieval (*i.e.*, the service credential request may be configured to additionally require signing by the device). In specific embodiments of the invention, the service provider may have a need to know the identity of the device (*i.e.*, device type/model, manufacturer or the like). For example, in one specific scenario, the service provider may have an agreement with the device manufacturer that offers a discount in network rates for connections being established with devices they manufacture or certain types/models of their devices. At Event 250, the service provider-signed and, optionally, device-signed service credential is communicated from the secure storage environment 180 to the network module 220.

[0072] At Event 260, the network module 220 communicates a connectivity request to the network node 60 which includes the service credential 40. Unlike conventional connectivity requests, which include subscriber credentials retrieved from the SIM or the like, the connectivity request of the present invention includes the service-signed (and, in some embodiments, additional device-signed) service credentials as opposed to subscriber credentials. In optional embodiments of the invention, the network module 220 is configured to select a communication network for the network connectivity. The communication network may be a wide area network, *e.g.*, a cellular network and/or a local area network, e.g., WI-FI® or the like. The selection of the network may be based on at least one of (*i*) signal quality of signals received from different communication networks, and/or (*ii*) one or more predetermined business rules.

[0073] At Event 280, the network authentication application 270, forwards the service credentials 40 to the server provider node. At Event 300, the network connectivity authorization module 290 is configured to verify the service credential 40. Verification of the service credential 40 includes verification the service provider signature (*i.e.*, applying the private PKI to decode or decrypt the service credential 40 to insure that the service credentials have not been tampered with or otherwise changed) and, in specific embodiments, verifying the device signature as a means of identifying the device type and/or manufacturer. Moreover, verification of the service credential 40 includes applying business logic to match the service credential to the user (*i.e.*, insuring that the user to whom the service credential was issued has a valid service subscription or the like).

[0074] In optional embodiments of the invention, in addition to verifying the service credential 40, service parameters associated with the service session may be obtained or otherwise selected. Service parameters may be based on information stored in a (*i*) a user profile, (*ii*) a device profile and/or (*iii*) business rules. Thus, in accordance with specific embodiments of the invention service parameters may be user-specific and/or device-specific. Service parameters may include, but are not limited to, restrictions/limitations on the length/duration of the service session (*i.e.*, the maximum length (units of time) or amount of data (units of data) that can be consumed during the service session before the session expires). In the event that the service session exceeds a service parameter that is a restriction/limitation on the length/duration of the service session, the network connectivity (*i.e.*, the service session) may be configured to terminate. In other embodiments of the invention, in response to the service session

approaching the service parameter limitation of session length, the device 20 communicates a request for an extended session to the service provider node 80 via the network node 60, which prompts the service provider node 80 to re-verify the service credentials (*i.e.*, issue new service parameters for the extended sessions, which may be the same or different than the initially assigned service parameters). At Event 310, in response to verifying the service credentials 40, the service provider node 80 provides network connectivity authorization and, optionally, any applicable service parameters to the network node 60. According to specific embodiments of the invention, the network connectivity authorization is an indication to the network node 60 that the service provider is obligated to remit payment for the ensuing network connectivity for the service module 30.

[0075] At Event 320, the network connectivity module 270 signals to the network module 220 on the device 20 that a network connection is authorized to be established solely for purposes of the service. In addition, the network connection authorization may include, where applicable, any service parameters applicable to the service session/network connectivity. At Event 330, the network module 220 signals to the service module 30 that the network connectivity is available for service use. In addition, the network connectivity signal may include an indication of the service parameters applied to the service/session/network connectivity. In this regard, the service module 30 may be made aware of the service parameters, such that the service module 30 can notify the service user of the service parameters (*e.g.*, notify the user that a service limitation is approaching or for the service module to initiate a request for extension of the service session/network connectivity or a new request to re-establish network connectivity).

[0076] Referring to **Figure 4** a flow diagram is presented of a method 400 for obtaining network connectivity, in accordance with embodiments of the present invention. At Event 410, a first device obtains a service credential (*e.g.*, digital token, data structure or the like) that is signed by a service provider of an associated service requiring network connectivity. In specific embodiments of the invention, the service credential is not only service-specific but, also, is user-specific. In specific embodiments of the invention, the service credential is obtained by communicating a service credential request to the service provider and, in response, receiving the service credential from the service provider. In such embodiments of the invention, the service credential request and receipt of the service credential may occur by a bootstrap-type

network connection or through a tethering mode communication with another communication device (*i.e.,* a wearable device, a mobile terminal or the like).

[0077] At Event 420, the first device communicates the service credential to the service provider, via a network access node, in order to obtain network connectivity authorization for the service. In specific embodiments of the invention, prior to communicating the service credential, a device signature is attached to the service credential that serves to identify to the service provider the source of the service credentials (*e.g.,* device type, device manufacturer or the like). In specific embodiments, prior to communicating the service credential, a communication network is selected for the network connectivity based on at least one of (*i*) signal quality of signals received from different communication networks and/or (*ii*) one or more predetermined business rules.

[0078] At Event 430, the first device obtains network connectivity for at least the service from the network node. The network connectivity is based on the service provider verifying the service credential and providing network connectivity authorization. In specific embodiments of the invention, the network connectivity is obtained exclusively for the service, while in other embodiments of the invention, the network connectivity is obtained for the service and at least one other service or functions requiring network access that are accessible via the device *(e.g.*, a general network connection that provides network connectivity to all of the services/functions requiring such). In specific embodiments of the invention, in addition to network connectivity one or more service parameters are selected or obtained by the service provider and applied to the network connectivity

[0079] Referring to **Figure 5** a flow diagram is presented of a method 500 for providing network connectivity authorization, in accordance with embodiments of the present invention. At Event 510, a service provider node receives a service credential signed by the service provider. In specific embodiments the service credential is received, via a network node, from device in which a service module is requesting network connectivity. In specific embodiments of the invention, the service credential is associated with a specific user. In other specific embodiments of the method, the service credential is signed by the source/first device as a means of identifying the source of the service credentials.

[0080] At Event 520, the service provider node verifies the service credential as being authentic and, in specific embodiments, verifies the user associated with the service credential

as being valid (*i.e.*, a current service subscriber) and/or the device (*i.e.*, source of the service credentials).

[0081] At optional Event 530, the service provider node obtains one or more service parameters associated with the network connectivity. The service parameters may be based on one or more of (*i*) a user profile, (*ii*) a device profile and/or (*iii*) business rules. In specific embodiments of the invention the service parameters are limitations/restrictions of the network connectivity/service session, such as, but not limited to, (*i*) a maximum amount of data that can be transmitted/consumed during the network connectivity/service session, (*ii*) a maximum duration/time for the network connectivity/service session and/or (*iii*) a maximum percentage of a user subscription allotment for the network connectivity/service session.

[0082] At Event 540, the service provider node communicates a network connectivity authorization and, optionally, the service parameters to the network node. In specific embodiments of the invention, the network connectivity authorization may provide for a network connection exclusively for use of the service, while in other embodiments of the invention, the network connectivity is obtained for the service and at least one other service or functions requiring network access that are accessible via the device (*e.g.*, a general network connection that provides network connectivity to all of the services/functions requiring such).

[0083] Referring to **Figure 6**, a flow diagram is illustrated of a method 600 for establishing network connectivity, in accordance with embodiments of the present invention. At Event 610, a network access node receives a service credential signed by a service provider that is associated with a corresponding service. At Event 620, the network access node, communicates the service credentials to a service provider node.

[0084] At Event 630, the network node receives a network connectivity authorization from the service provider node and, at Event 640, the network access node establishes network connectivity for at least the service based on the received network connectivity authorization. In specific embodiments of the invention, the network connectivity is established exclusively for the service, while in other embodiments of the invention, the network connectivity is established for the service and at least one other service or functions requiring network access that are accessible via the device *(e.g.*, a general network connection that provides network connectivity to all of the services/functions requiring such).

[0085] Referring to **Figure 7** shown is a block diagram illustrating first device 20 configured for requesting and receiving service-specific network connectivity, in accordance with embodiments of the present invention. In specific embodiments of the invention, the first device 20 may comprise user equipment, such as a mobile terminal or the like. The first device includes a processor 20-2 communicably coupled to such devices as a memory 20-1, user output devices 20-8, user input devices 20-11, a network interface 20-3, and a power source 20-7. The processor 20-2, and other processors described herein, generally includes circuitry for implementing communication and/or logic functions of the first device 20.

[0086] The memory 20-1 is operatively coupled to the processor 20-1. As used herein, memory includes any computer readable medium (as defined herein below) configured to store data, code, or other information. The memory 20-1 may include volatile memory, such as volatile Random Access Memory (RAM) including a cache area for the temporary storage of data. The memory 20-1 may also include non-volatile memory, which can be embedded and/or may be removable. The non-volatile memory can additionally or alternatively include an electrically erasable programmable read-only memory (EEPROM), flash memory or the like. The memory 20-1 can store any of a number of modules, applications which include computer-executable instructions/code executed by the processor 20-2 to implement the functions of the first device 20 described herein.

[0087] For example, the processor 20-2 may include a digital signal processor device, a microprocessor device, and various analog to digital converters, digital to analog converters, and/or other support circuits. Control and signal processing functions of the mobile device 100 are allocated between these devices according to their respective capabilities. The processor 20-2 thus may also include the functionality to encode and interleave messages and data prior to modulation and transmission. The processor 20-2 can additionally include an internal data modem. Further, the processor 20-2 may include functionality to operate one or more software programs/modules/applications, which may be stored in the memory 20-1.

[0088] For example, in specific embodiments of the invention, the processor 20-2 executes service module 30 this is configured to obtain a user and service-specific service credential 40 stored in secured storage environment 180 of memory 20-1. The service credential 40 signed by a service provide and, subsequently obtain network connectivity for the service based on a service provider verifying the service credential and providing network

authorization. In specific embodiments the service module obtains the service credential by communicating a service credential request to a service provider node and, in response, receiving the service credential from the node. In still further embodiments, the service module 30 is configured to obtain the network connectivity according to one or more service parameters that are assigned by the service provider node. In other embodiments of the invention, the processor 20-2 executes network module 220 that is configured to communicate the service credential to the service provider node via a network node in order to obtain network connectivity limited to connectivity for service. In specific embodiments of the invention, the network module 220 may include a network selection module 222 that is configured to select a communication network for the network connectivity. In specific embodiments the selection of the communication network may be based on one or more of (*i*) quality of signals received from various different communication networks (*e.g.*, different types of communication networks and/or different communication network providers) and/or (*ii*) one or more predetermined business rules that dictate use of a communication network based on economic concerns.

[0089] Additionally, memory 20-1 and, in some embodiments, secured storage environment 180 may store device digital signature module 184 that is executed by the processor 20-2 and configured to attach a device signature to the service credentials as a means of identifying the source of the service credentials (*i.e.*, the device from which the credentials are being transmitted) and/or the identity of the device (*i.e.*, the device type and/or device manufacturer).

[0090] The processor 20-2 is configured to use the network interface 20-3 to communicate with one or more other devices on a communication network. In this regard, the network interface 20-3 includes an antenna 20-6 operatively coupled to a transmitter 20-4 and a receiver 20-5 (together a "transceiver"). The processor 20-2 is configured to provide signals to and receive signals from the transmitter 20-4 and receiver 20-5, respectively. The signals may include signaling information in accordance with the air interface standard of the applicable cellular system of a wireless telephone network. In this regard, the first device 20 may be configured to operate with one or more air interface standards, communication protocols, modulation types, and access types. By way of illustration, the first device 20 may be configured to operate in accordance with any of a number of first, second, third, and/or fourth-generation communication protocols and/or the like. For example, the first device 20 may be configured to

operate in accordance with second-generation (2G) wireless communication protocols IS-136 (time division multiple access (TDMA)), GSM (global system for mobile communication), and/or IS-95 (code division multiple access (CDMA)), or with third-generation (3G) wireless communication protocols, such as Universal Mobile Telecommunications System (UMTS), CDMA2000, wideband CDMA (WCDMA) and/or time division-synchronous CDMA (TD-SCDMA), with fourth-generation (4G) wireless communication protocols, Long Term Evolution (LTE) and/or the like. The first device 20 may also be configured to operate in accordance with non-cellular communication mechanisms, such as via a wireless local area network (WLAN) or other communication/data networks.

[0091] As described above, first device 20 has a user interface that is, like other user interfaces described herein, made up of user output devices 20-8 and/or user input devices 20-11. The user output devices 20-8 include a display 20-9 and a speaker 20-10 or other audio device, which are operatively coupled to the processor 20-2. The user input devices 20-11, which allow the first device 20 to receive data from a user, may include any of a number of devices allowing the mobile device 100 to receive data from a user, such as a keypad, keyboard, touch-screen, touchpad, microphone, mouse, joystick, other pointer device, button, soft key, and/or other input device(s).

[0092] The first device 20 further includes a power source 20-7, such as a battery, for powering various circuits and other devices that are used to operate the first device 20.

[0093] Referring to **Figure 8** a block diagram is provided of a service provider node 80 configured for verifying service credentials and providing network access authorization, in accordance with embodiments of the present invention. The service provider node, which may comprise one or more servers, storage units or the like, includes a memory 80-1 and at least one processor 80-2 in communication with the memory 80-1. Memory 80-1 stores credential provisioning module 130 that is configured to provision service credential 40 to a device requesting a service credential. In specific embodiments of the invention, the service credential 40 may take the form of a digital token that stores the service credential as a short-form identifier. In specific embodiments of the invention, the service credential 40 may be user-specific, as well as service specific. User-specific service credential 40 requires that the user to whom the service credential is issued be the presenter of the user credential 40 for the purpose of obtaining network connectivity for the device.

[0094] Memory 80-1 additionally stores network authorization module 290 is configured to (*i*) receive a service credential signed by the service provider, (*ii*) verify the service credential, and (*iii*) in response to verifying the service credential, communicate a network connectivity authorization 294 to a network node. In specific embodiments of the invention, the network connectivity authorization module 290 is further configured to receive the service credential associated with a user, and verify the user. In still further specific embodiments of the invention, the network connectivity authorization module 290 is further configured to receive the service credential signed by a first device, and verify the first device.

[0095] Additionally, in other embodiments of the invention, the network connectivity authorization module 290 is further configured to obtain one or more service parameters 296 associated with the network connectivity and communicate the one or more service parameters 296 to the network node. In such embodiments, the network connectivity authorization module 290 is further configured to obtain the one or more service parameters 296, which are specific to a user. The one or more service parameters 296 may be based on at least one of (*i*) a user profile, (*ii*) a UE profile, and (*iii*) one or more business rules. The service parameters 296 may include, but are not limited to, at least one of (*i*) a maximum time for the network connectivity, (*ii*) a maximum amount of data transmitted during the network connectivity, and (*iii*) a maximum percentage of a subscription allotment that can be used for the network connectivity.

[0096] Referring to **Figure 9** a block diagram is provided of a network node 60 for providing network connectivity on a service level basis through use of service credential verification, in accordance with an embodiment of the present invention. The network node 60 which may comprise one or more servers, storage units or the like, includes a memory 60-1 and at least one processor 60-2 in communication with the memory 60-1. Memory 60-1 stores network connectivity module 270 that is configured to receive a service credential 40 signed by a service provider associated with a service and communicate the service credential 40 to a service provider node,. In response to communicating the service credential 40 to the service provider, the network connectivity module 270 is configured to receive, from the service provider node, a network connectivity authorization 294, and, in specific embodiments service parameters 296 associated with the authorization 294.

[0097] Additionally, network connectivity module 270 is configured to establish network connectivity 274 for at least the service and, in specific embodiments provide

indication of the service parameters, based on the network connectivity authorization. As previous discussed the network connectivity may be exclusive to the service or in other embodiments provide a network connection for the service and one or more other services or functions on the device that require network access (*e.g.*, a general network connection that provides network connectivity to all of the services/functions requiring such).

[0098] Thus, systems, devices, methods, computer program products and the like described above provide for using service-issued credentials to tie network access/connectivity to the service provider as opposed to the network provider. In this regard, the present invention allows for network access/connectivity rates to be assigned to the service provider, which means, in turn, that the service provider can charge the user based on the user's access/use of the service (*i.e.*, the time spent using the service, the amount of data consumed while using the service or the like).

[0099] Each processor, device, apparatus or node described herein generally includes circuitry for implementing audio, visual, and/or logic functions. For example, the processor/device/apparatus/node may include a digital signal processor device, a microprocessor device, and various analog-to-digital converters, digital-to-analog converters, and other support circuits. Control and signal processing functions of the system in which the processor resides may be allocated between these devices according to their respective capabilities. The processor/device/apparatus/node may also include functionality to operate one or more software programs based at least partially on computer-executable program code portions thereof, which may be stored, for example, in a memory.

[00100] Each memory may include any computer-readable medium. For example, memory may include volatile memory, such as volatile random access memory ("RAM") having a cache area for the temporary storage of data. Memory may also include non-volatile memory, which may be embedded and/or may be removable. The non-volatile memory may additionally or alternatively include an EEPROM, flash memory, and/or the like. The memory may store any one or more of pieces of information and data used by the system in which it resides to implement the functions of that system.

[00101] The various features described with respect to any embodiments described herein are applicable to any of the other embodiments described herein. As used herein, the terms data and information may be used interchangeably. Although many embodiments of the present

invention have just been described above, the present invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Also, it will be understood that, where possible, any of the advantages, features, functions, devices, and/or operational aspects of any of the embodiments of the present invention described and/or contemplated herein may be included in any of the other embodiments of the present invention described and/or contemplated herein, and/or vice versa. In addition, where possible, any terms expressed in the singular form herein are meant to also include the plural form and/or vice versa, unless explicitly stated otherwise. As used herein, "at least one" shall mean "one or more" and these phrases are intended to be interchangeable. Accordingly, the terms "a" and/or "an" shall mean "at least one" or "one or more," even though the phrase "one or more" or "at least one" is also used herein. Like numbers refer to like elements throughout.

[00102] As will be appreciated by one of ordinary skill in the art in view of this disclosure, the present invention may include and/or be embodied as an apparatus (including, for example, a system, machine, device, computer program product, and/or the like), as a method (including, for example, computer-implemented process, and/or the like), or as any combination of the foregoing. Accordingly, embodiments of the present invention may take the form of an entirely an entirely software embodiment (including firmware, resident software, micro-code, stored procedures, etc.), an entirely hardware embodiment, or an embodiment combining software, and hardware aspects that may generally be referred to herein as a "system." Furthermore, embodiments of the present invention may take the form of a computer program product that includes a computer-readable storage medium having one or more computer-executable program code portions stored therein. As used herein, a processor, which may include one or more processors, may be "configured to" perform a certain function in a variety of ways, including, for example, by having one or more general-purpose circuits perform the function by executing one or more computer-executable program code portions embodied in a computer-readable medium, and/or by having one or more application-specific circuits perform the function.

[00103] It will be understood that any suitable computer-readable medium may be utilized. The computer-readable medium may include, but is not limited to, a non-transitory computer-readable medium, such as a tangible electronic, magnetic, optical, electromagnetic, infrared, and/or semiconductor system, device, and/or other apparatus. For example, in some

embodiments, the non-transitory computer-readable medium includes a tangible medium such as a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory ("ROM"), an erasable programmable read-only memory ("EPROM" or Flash memory), a compact disc read-only memory ("CD-ROM"), and/or some other tangible optical and/or magnetic storage device.

[00104] One or more computer-executable program code portions for carrying out operations of the present invention may include object-oriented, scripted, and/or unscripted programming languages, such as, for example, Java, Perl, Smalltalk, C++, SAS, SQL, Python, Objective C, JavaScript, and/or the like. In some embodiments, the one or more computer-executable program code portions for carrying out operations of embodiments of the present invention are written in conventional procedural programming languages, such as the "C" programming languages and/or similar programming languages. The computer program code may alternatively or additionally be written in one or more multi-paradigm programming languages, such as, for example, F#.

[00105] Some embodiments of the present invention are described herein with reference to flowchart illustrations and/or block diagrams of apparatus and/or methods. It will be understood that each block included in the flowchart illustrations and/or block diagrams, and/or combinations of blocks included in the flowchart illustrations and/or block diagrams, may be implemented by one or more computer-executable program code portions. These one or more computer-executable program code portions may be provided to a processor of a general purpose computer, special purpose computer, and/or some other programmable information processing apparatus in order to produce a particular machine, such that the one or more computer-executable program code portions, which execute via the processor of the computer and/or other programmable information processing apparatus, create mechanisms for implementing the steps and/or functions represented by the flowchart(s) and/or block diagram block(s).

[00106] The one or more computer-executable program code portions may be stored in a non-transitory computer-readable medium (*e.g.*, a memory, etc.) that can direct, instruct, and/or cause a computer and/or other programmable information processing apparatus to function in a particular manner, such that the computer-executable program code portions stored in the computer-readable medium produce an article of manufacture including instruction mechanisms

which implement the steps and/or functions specified in the flowchart(s) and/or block diagram block(s).

[00107] The one or more computer-executable program code portions may also be loaded onto a computer and/or other programmable information processing apparatus to cause a series of operational steps to be performed on the computer and/or other programmable apparatus. In some embodiments, this produces a computer-implemented process such that the one or more computer-executable program code portions which execute on the computer and/or other programmable apparatus provide operational steps to implement the steps specified in the flowchart(s) and/or the functions specified in the block diagram block(s). Alternatively, computer-implemented steps may be combined with, and/or replaced with, operator- and/or human-implemented steps in order to carry out an embodiment of the present invention.

[00108] While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other changes, combinations, omissions, modifications and substitutions, in addition to those set forth in the above paragraphs, are possible. Those skilled in the art will appreciate that various adaptations, modifications, and combinations of the just described embodiments can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

CLAIMS:

1. A method (400) performed by a first device for obtaining network connectivity, the method comprising:

obtaining (410) a service credential signed by a service provider of a service and used for network authorization, wherein the service requires network connectivity;

communicating (420) the service credential to the service provider via a network node in order to obtain network connectivity for at least the service; and

obtaining (430) network connectivity for at least the service from the network node, whereby the network connectivity is based on the service provider verifying the service credential and providing network connectivity authorization.

2. The method (400) of Claim 1, wherein obtaining network connectivity further comprises one of (*i*) obtaining network connectivity exclusively for the service, or (*ii*) obtaining network connectivity for the service and for one or more other services or functions accessible via the first device.

3. The method (400) of Claim 1, wherein obtaining a service credential (410) further comprises obtaining the service credential associated with a user.

4. The method (400) of any one of Claims 1-3, wherein obtaining the service credential (410) further comprises communicating a service credential request to the service provider, and, in response to communicating the service credential request, receiving the service credential from the service provider.

5. The method (400) of Claim 4, wherein communicating the service credential request and receiving the service credential occur via (*i*) a bootstrap-type network connection or (*ii*) a second device in communication with the first device.

6. The method (400) of any one of Claims 1-5, further comprising prior to communicating the service credential, attaching a device signature associated with the first device to the service credential.

7. The method (400) of any one of Claims 1-6, further comprising selecting, a communication network for the network connectivity based on at least one of (*i*) a signal quality of signals, each signal received from one of a plurality of communication networks, and (*ii*) one or more predetermined business rules.

8. The method (400) of any one of Claims 1-7, wherein obtaining the network connectivity (430) further comprises obtaining the network connectivity according to one or more service parameters, whereby the service provider selects the one or more service parameters.

9. The method (400) of Claim 8, further comprising receiving an indication of at least one of the one or more service parameters.

10. A device (20) configured for obtaining network connectivity, the device comprising:

a processor (20-2);

a memory (20-1) in communication with the processor (20-2);

a service module (30) stored in the memory (20-1), executable by the processor (20-2) and configured to obtain a service credential (40) signed by a service provider of a service and used for network authorization, wherein the service requires network connectivity; and

a network module (220) stored in the memory (20-1), executable by the processor (20-2) and configured to communicate the service credential (40) to a service provider node (80) via a network node (60) in order to obtain network connectivity for at least the service,

wherein the service module (30) is further configured to obtain network connectivity for at least the service from the network node (60), whereby the network connectivity is based on the service provider node (80) verifying the service credential (40) and providing network authorization.

11. The device (20) of Claim 10, wherein the service module is further configured to obtain network connectivity (*i*) exclusively for the service, or (*ii*) for the service and for one or more other services or functions accessible via the first device.

12. The device (20) of Claim 10, wherein the service module (30) is further configured to obtain the service credential associated with a user.

13. The device (20) of any one of Claims 10-12 wherein the service module (30) is further configured to obtain the service credential (40) by communicating a service credential request to the service provider node (80), and, in response to communicating the service credential request, receive the service credential (40) from the service provider node (80).

14. The device (20) of any one of Claims 10-13, further comprising a digital signature module (184) stored in the memory (20-1), executable by the processor (20-2) and configured to, prior to communicating the service credential, attach a device signature associated with the first device to the service credential.

15. The device (20) of any one of Claims 10-14, further comprising a network selection module (222) stored in the memory (20-1), executable by the processor (20-2) and configured to select a communication network for the network connectivity based on at least one of (*i*) a signal quality of signals, each signal received from one of a plurality of communication networks, and (*ii*) one or more predetermined business rules.

16. The device (20) of any one of Claims 10-15, wherein the service module (30) is further configured to obtain the network connectivity according to one or more service parameters (296), whereby the service provider node (80) obtains the one or more service parameters

17. A method (500) performed by a service provider node for providing network connectivity authorization, the method comprising:

receiving (510), a service credential signed by the service provider and used for network authorization;

verifying (520) the service credential; and

in response to verifying the service credential, communicating (540) a network connectivity authorization for providing a network connection for at least the service to a network node.

18. The method (500) of Claim 17, wherein communicating (540) the network connectivity authorization further comprises communicating (540) the network connectivity authorization for providing the network connection (*i*) exclusively for the service or (*ii*) for the service and for one or more other services or functions accessible via the first device.

19. The method (500) of any one of Claims 17 or 18, wherein receiving the service credential (510) further comprises receiving the service credential associated with a user and wherein the method further comprises verifying, by the service provider node, the user.

20. The method (500) of any one of Claims 17-19, wherein receiving the service credential (510) further comprises receiving the service credential signed by a first device and wherein the method further comprises verifying, by the service provider node, the first device.

21. The method (500) of any one of Claims 17-20, further comprising obtaining (530) one or more service parameters associated with the network connectivity and communicating, by the service provider node, the one or more service parameters to the network node.

22. The method (500) of Claim 21, wherein obtaining the service parameters (530) further comprises obtaining the services parameters, wherein at least one of the service parameters are specific to a user.

23. The method (500) of any one of Claims 17-22, wherein obtaining the one or more service parameters (530) further comprises obtaining the service parameters based on at least one of (*i*) a user profile, (*ii*) a first device profile, and (*iii*) one or more business rules.

24. The method (500) of any one of Claims 17-23, wherein the service parameters include at least one of (*i*) a maximum time for the network connectivity, (*ii*) a maximum amount of data transmitted during the network connectivity and (*iii*) a maximum percentage of a subscription allotment that can be used for the network connectivity.

25. An apparatus (80) configured for providing network connectivity authorization, the apparatus comprising:

a processor (80-2);

a memory (80-1) in communication with the processor (80-2);

a network connectivity authorization (290) module stored in the memory (80-1), executable by the processor (80-2) and configured to (*i*) receive a service credential (40) signed by the service provider and used for network authorization, (*ii*) verify the service credential (40), and (*iii*) in response to verifying the service credential (40), communicate a network connectivity authorization for providing a network connection for at least the service to a network node.

26. The apparatus (80) of Claim 25, wherein the network connectivity authorization (290) module is further configured to communicate the network connectivity authorization for providing a network connection (*i*) exclusively for the service or (*ii*) for the service and for one or more other services or functions accessible via the first device.

27. The apparatus (80) of Claim 25 or 26, wherein the network connectivity authorization module (290) is further configured to receive the service credential associated with a user, and verify the user.

28. The apparatus (80) of any one of Claims 25-27, wherein the network connectivity authorization module (290) is further configured to receive the service credential signed by a first device (20), and verify the first device (20).

29. The apparatus (80) of any one of Claims 25-28, wherein the network connectivity authorization module (290) is further configured to obtain one or more service parameters (296)

associated with the network connectivity and communicate the one or more service parameters to the network node (60).

30. The apparatus (80) of Claim 29, wherein the network connectivity authorization module (290) is further configured to obtain the one or more service parameters (296), wherein at least one of the service parameters (296) are specific to a user.

31. The apparatus (80) of any one of Claims 29-30, wherein the network connectivity authorization module (290) is further configured to obtain the one or more service parameters (296) based on at least one of (*i*) a user profile, (*ii*) a UE profile, and (*iii*) one or more business rules.

32. The apparatus (80) of any one of Claims 29-31, wherein the network connectivity authorization module (290) is further configured to obtain the one or more service parameters (296) including at least one of (*i*) a maximum time for the network connectivity, (*ii*) a maximum amount of data transmitted during the network connectivity, and (*iii*) a maximum percentage of a subscription allotment that can be used for the network connectivity.

33. The apparatus (80) of any one of Claims 25-32, further comprising a service credential provisioning module (130) stored in the memory (80-1), executable by the processor (80-2) and configured to generate a user-specific service credential (40).

34. A method (600) performed by a network node for establishing network connectivity, the method comprising:

receiving (610) from a first device, a service credential signed by a service provider of the service, wherein the service requires network connectivity and wherein the service is provided to the first device;

communicating (620) the service credential to a service provider node;

receiving (630) from the service provider node, a network connectivity authorization for the service; and

establishing (640) network connectivity for at least the service based on the network connectivity authorization.

35. The method (600) of Claim 34 wherein establishing (640) network connectivity further comprises establishing network connectivity (*i*) exclusively for the service or (*ii*) for the service and for one or more other services or functions accessible via the first device.

36. The method (600) of Claim 34 or 35, further comprising applying one or more service parameters to the network connectivity, wherein the one or more service parameters are received from the service provider node.

37. An apparatus (60) for establishing network connectivity, the apparatus comprising:

a processor (60-2);

a memory (60-1) in communication with the processor (60-2);

a network connectivity module (270) stored in the memory (60-1), executable by the processor (60-2) and configured to (*i*) receive a service credential (40) signed by a service provider of a service, wherein the service requires network connectivity and wherein the service is provided to the first device, (*ii*) communicate the service credential (40) to a service provider node (80), (*iii*) receive, from the service provider node (80), a network connectivity authorization for at least the service; and (*iv*) establish network connectivity for at least the service based on the network connectivity authorization.

38. The (60) apparatus of Claim 37, wherein the network connectivity module (270) is further configured to apply one or more service parameters (296) to the network connectivity, wherein the one or more service parameters (296) are received from the service provider node (80).

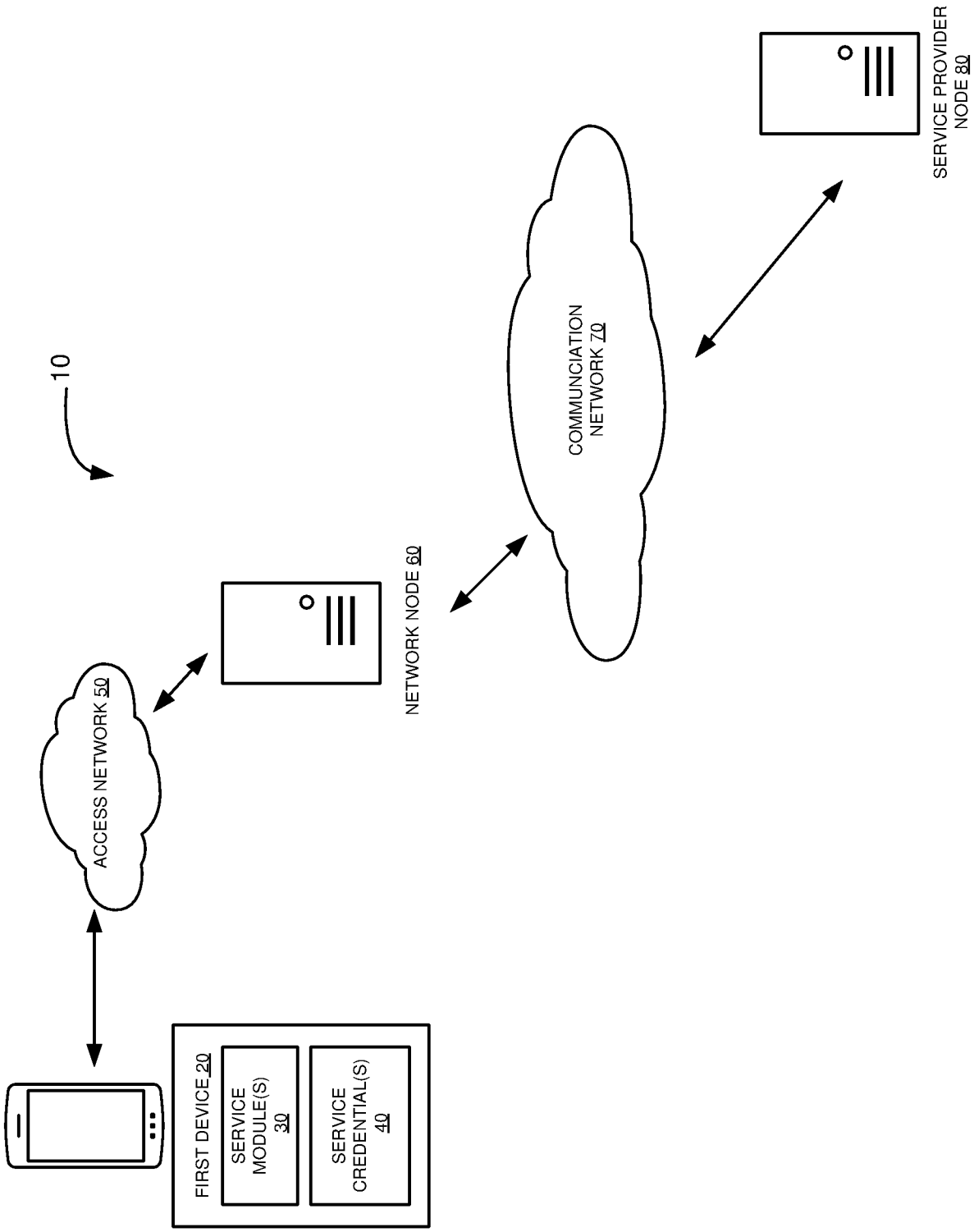
10
FIRST DEVICE 20
SERVICE MODULE(S) 30
SERVICE CREDENTIAL(S) 40
ACCESS NETWORK 50
NETWORK NODE 60
COMMUNICATION NETWORK 70
SERVICE PROVIDER NODE 80

FIGURE 1

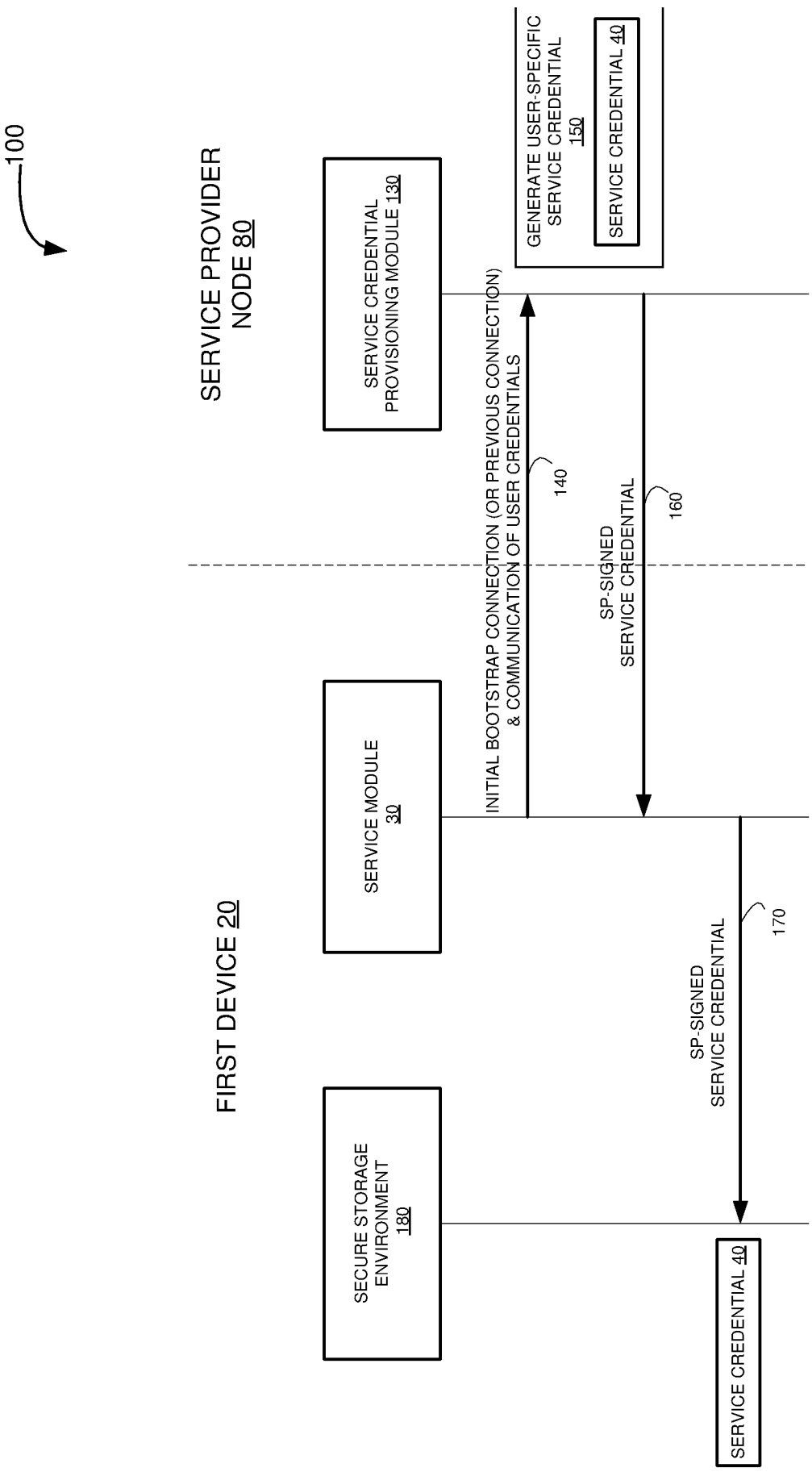
100
SERVICE PROVIDER NODE 80
SERVICE CREDENTIAL PROVISIONING MODULE 130
GENERATE USER-SPECIFIC SERVICE CREDENTIAL 150
SERVICE CREDENTIAL 40
INITIAL BOOTSTRAP CONNECTION (OR PREVIOUS CONNECTION) & COMMUNICATION OF USER CREDENTIALS
140
SP-SIGNED SERVICE CREDENTIAL
160
FIRST DEVICE 20
SERVICE MODULE 30
SECURE STORAGE ENVIRONMENT 180
SP-SIGNED SERVICE CREDENTIAL
170
SERVICE CREDENTIAL 40

FIGURE 2

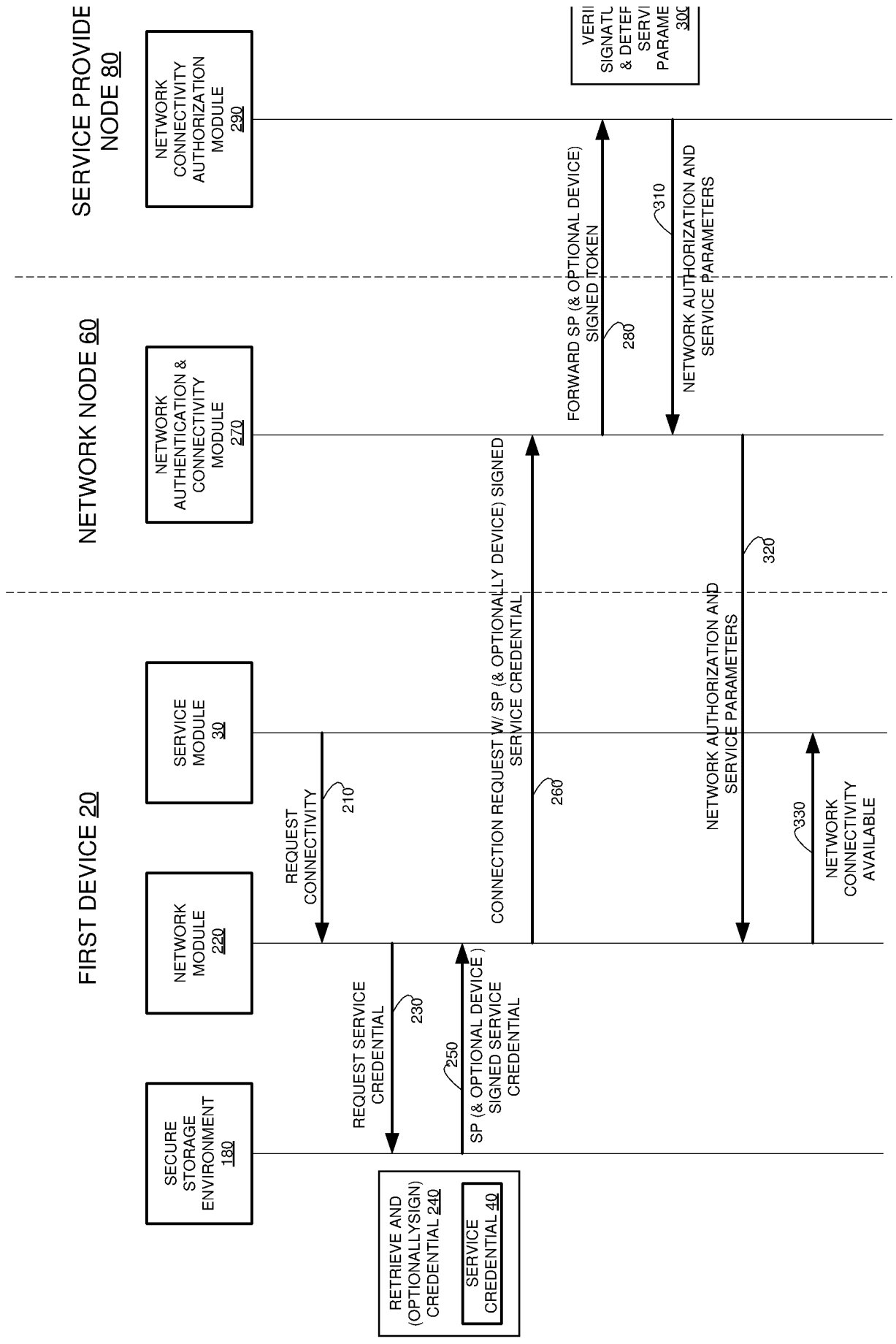
200
FIRST DEVICE 20
NETWORK NODE 60
SERVICE PROVIDE NODE 80
SECURE STORAGE ENVIRONMENT 180
NETWORK MODULE 220
SERVICE MODULE 30
NETWORK AUTHENTICATION & CONNECTIVITY MODULE 270
NETWORK CONNECTIVITY AUTHORIZATION MODULE 290
RETRIEVE AND (OPTIONALLYSIGN) CREDENTIAL 240
SERVICE CREDENTIAL 40
REQUEST SERVICE CREDENTIAL
230
SP (& OPTIONAL DEVICE) SIGNED SERVICE CREDENTIAL
250
REQUEST CONNECTIVITY
210
CONNECTION REQUEST W/ SP (& OPTIONALLY DEVICE) SIGNED SERVICE CREDENTIAL
260
FORWARD SP (& OPTIONAL DEVICE) SIGNED TOKEN
280
NETWORK AUTHORIZATION AND SERVICE PARAMETERS
310
NETWORK AUTHORIZATION AND SERVICE PARAMETERS
320
NETWORK CONNECTIVITY AVAILABLE
330
VERII SIGNATL & DETEF SERVI PARAME 300

FIGURE 3

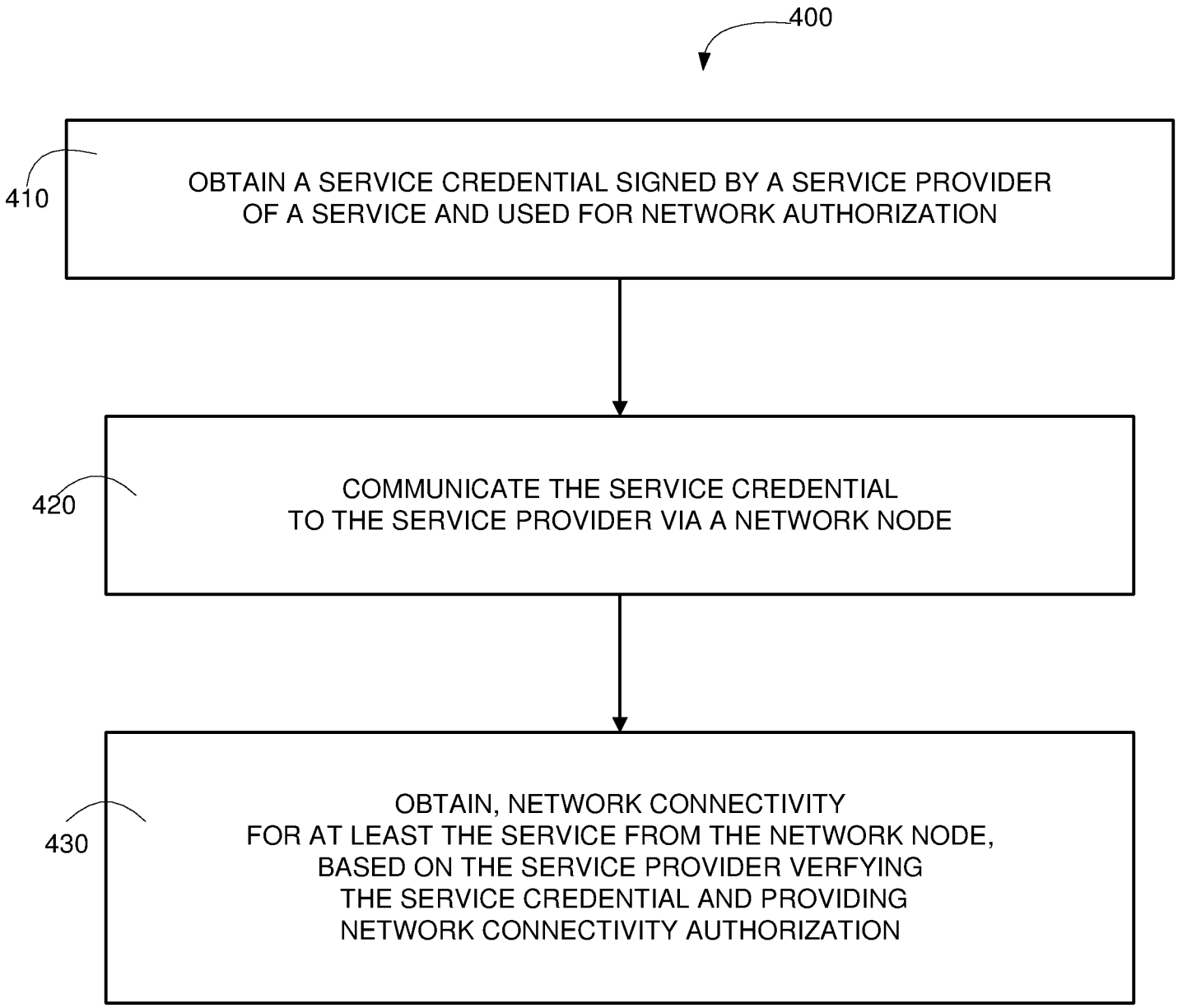
400
410
OBTAIN A SERVICE CREDENTIAL SIGNED BY A SERVICE PROVIDER OF A SERVICE AND USED FOR NETWORK AUTHORIZATION
420
COMMUNICATE THE SERVICE CREDENTIAL TO THE SERVICE PROVIDER VIA A NETWORK NODE
430
OBTAIN, NETWORK CONNECTIVITY FOR AT LEAST THE SERVICE FROM THE NETWORK NODE, BASED ON THE SERVICE PROVIDER VERFYING THE SERVICE CREDENTIAL AND PROVIDING NETWORK CONNECTIVITY AUTHORIZATION

FIGURE 4

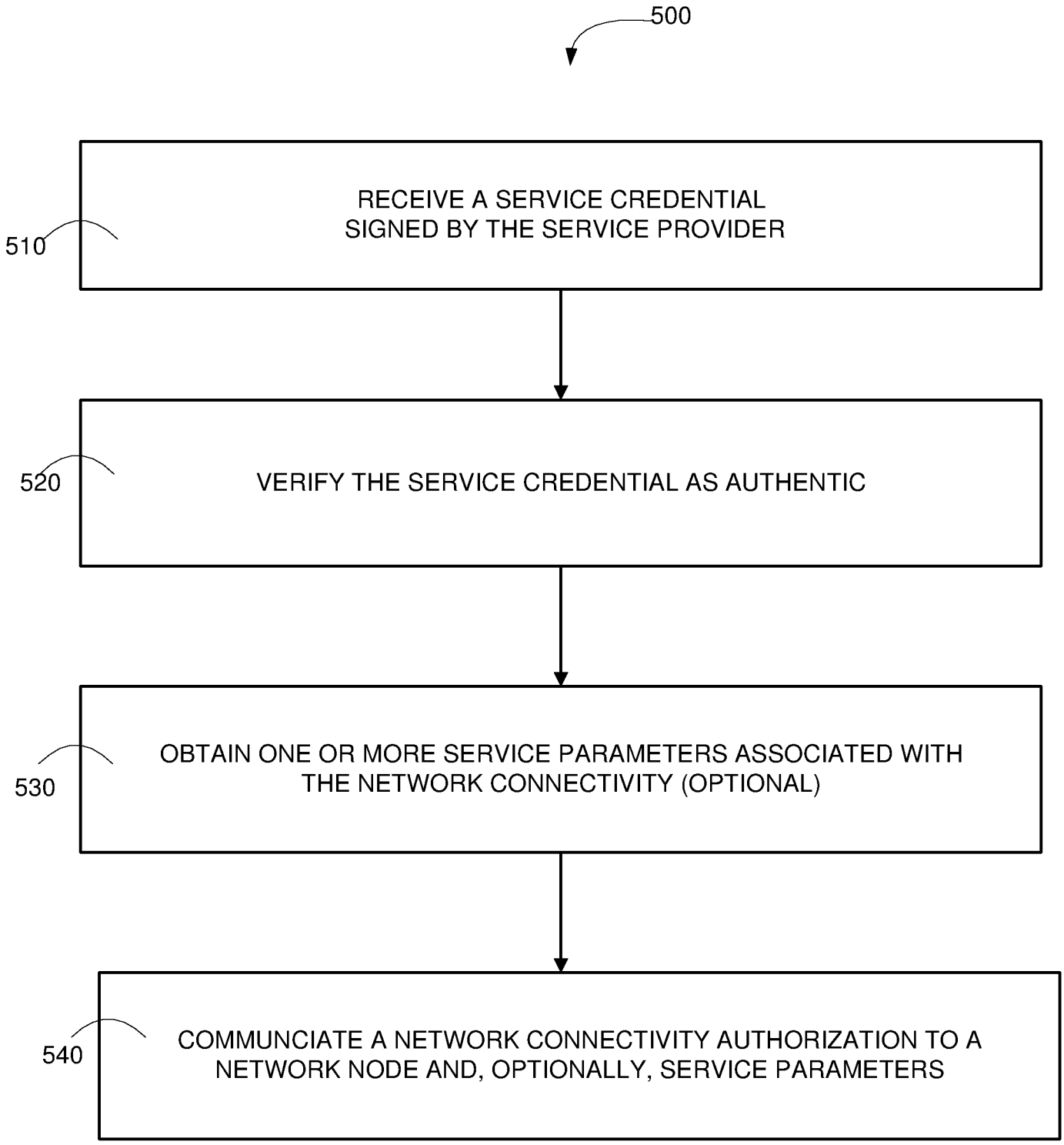
500
RECEIVE A SERVICE CREDENTIAL SIGNED BY THE SERVICE PROVIDER
510
VERIFY THE SERVICE CREDENTIAL AS AUTHENTIC
520
OBTAIN ONE OR MORE SERVICE PARAMETERS ASSOCIATED WITH THE NETWORK CONNECTIVITY (OPTIONAL)
530
COMMUNCIATE A NETWORK CONNECTIVITY AUTHORIZATION TO A NETWORK NODE AND, OPTIONALLY, SERVICE PARAMETERS
540

FIGURE 5

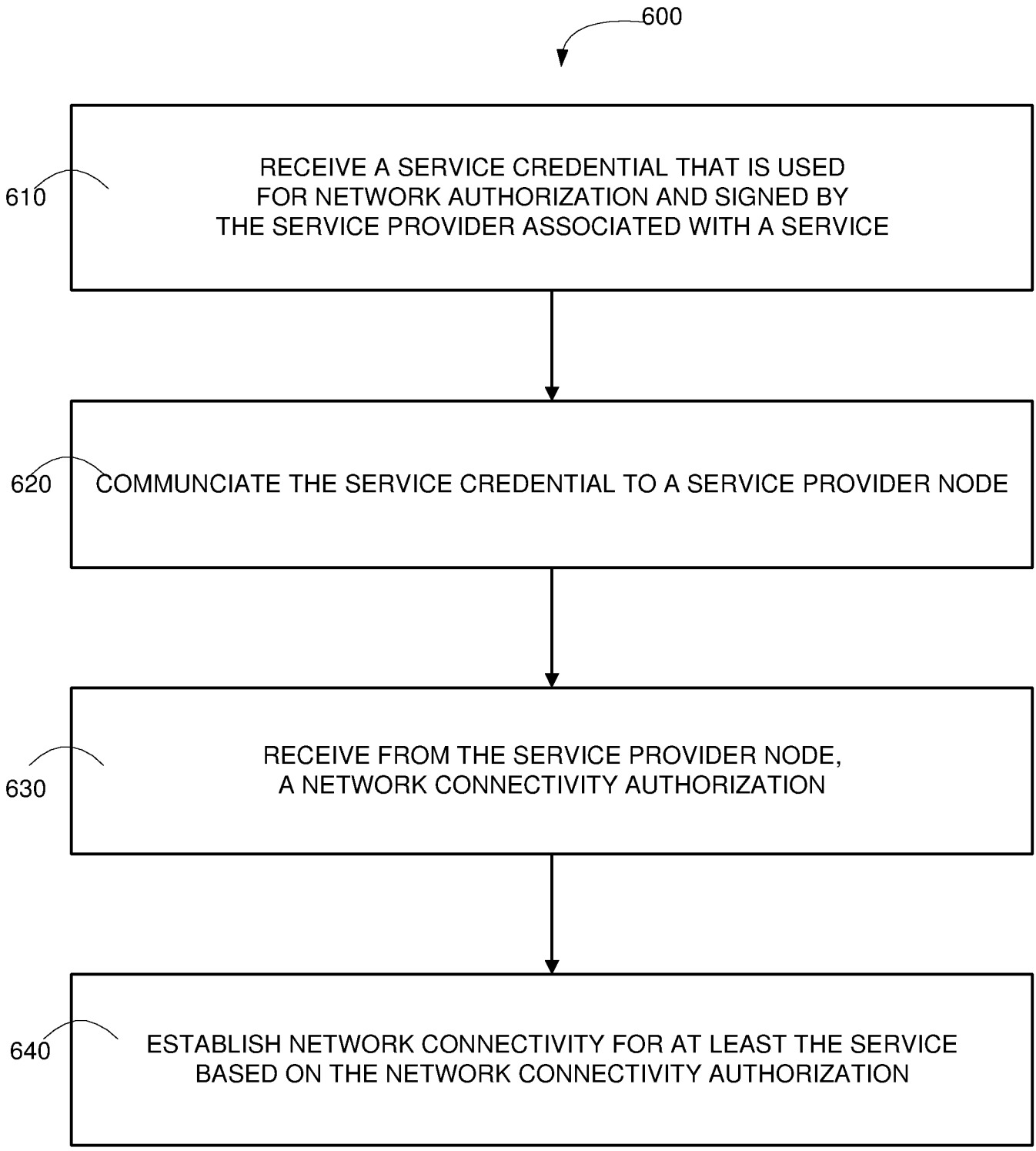
600
610
RECEIVE A SERVICE CREDENTIAL THAT IS USED FOR NETWORK AUTHORIZATION AND SIGNED BY THE SERVICE PROVIDER ASSOCIATED WITH A SERVICE
620
COMMUNCIATE THE SERVICE CREDENTIAL TO A SERVICE PROVIDER NODE
630
RECEIVE FROM THE SERVICE PROVIDER NODE, A NETWORK CONNECTIVITY AUTHORIZATION
640
ESTABLISH NETWORK CONNECTIVITY FOR AT LEAST THE SERVICE BASED ON THE NETWORK CONNECTIVITY AUTHORIZATION

FIGURE 6

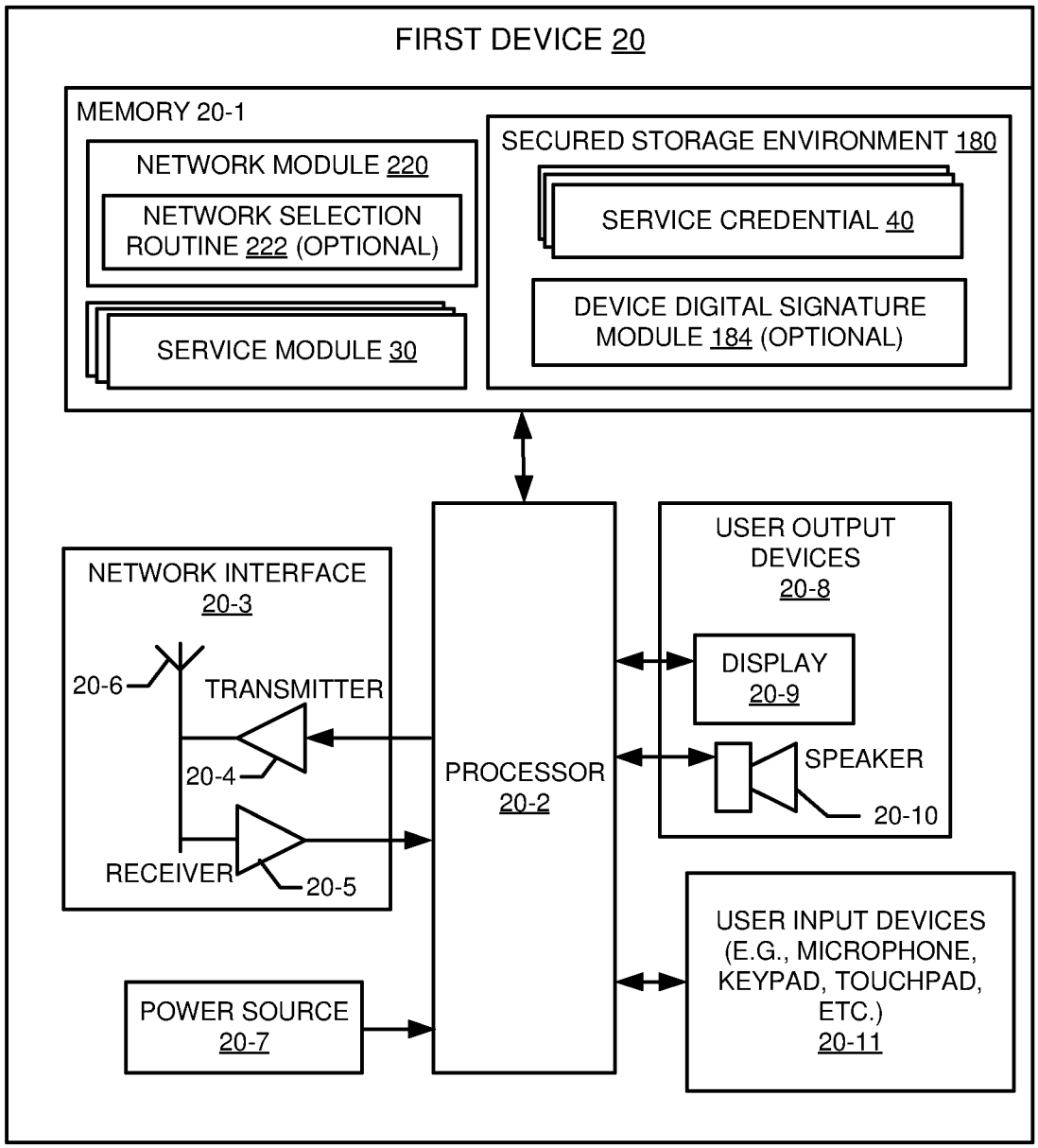
FIRST DEVICE 20
MEMORY 20-1
NETWORK MODULE 220
NETWORK SELECTION ROUTINE 222 (OPTIONAL)
SERVICE MODULE 30
SECURED STORAGE ENVIRONMENT 180
SERVICE CREDENTIAL 40
DEVICE DIGITAL SIGNATURE MODULE 184 (OPTIONAL)
NETWORK INTERFACE 20-3
20-6
TRANSMITTER
20-4
RECEIVER
20-5
PROCESSOR 20-2
USER OUTPUT DEVICES 20-8
DISPLAY 20-9
SPEAKER
20-10
USER INPUT DEVICES (E.G., MICROPHONE, KEYPAD, TOUCHPAD, ETC.) 20-11
POWER SOURCE 20-7

FIGURE 7

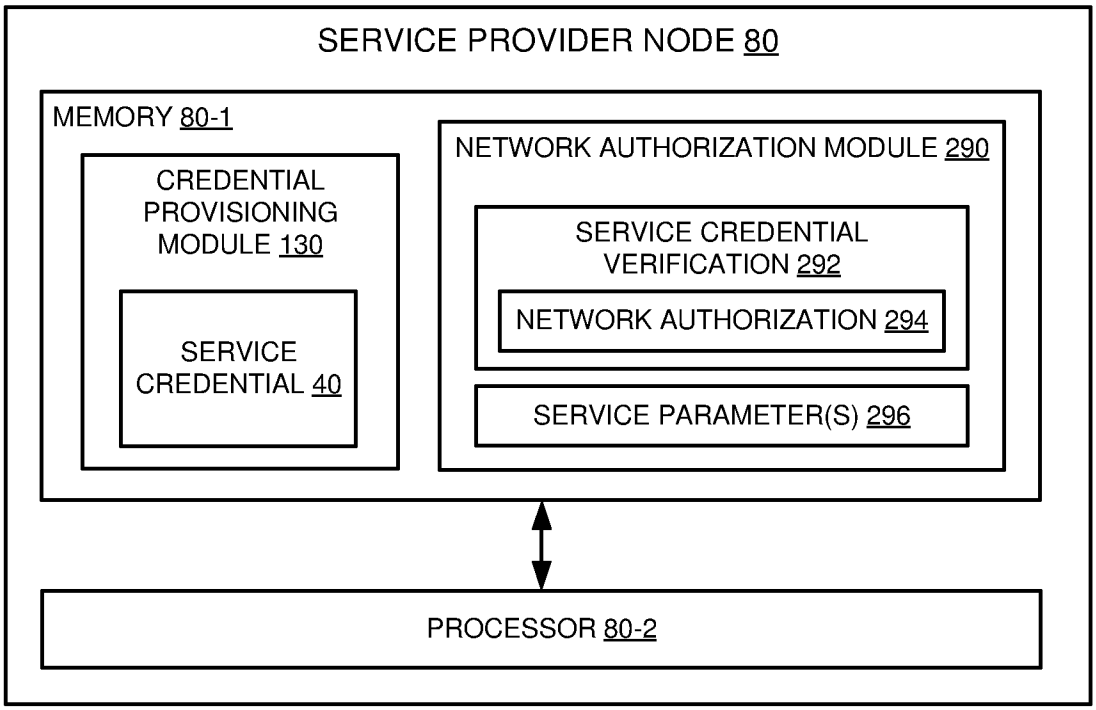

FIGURE 8

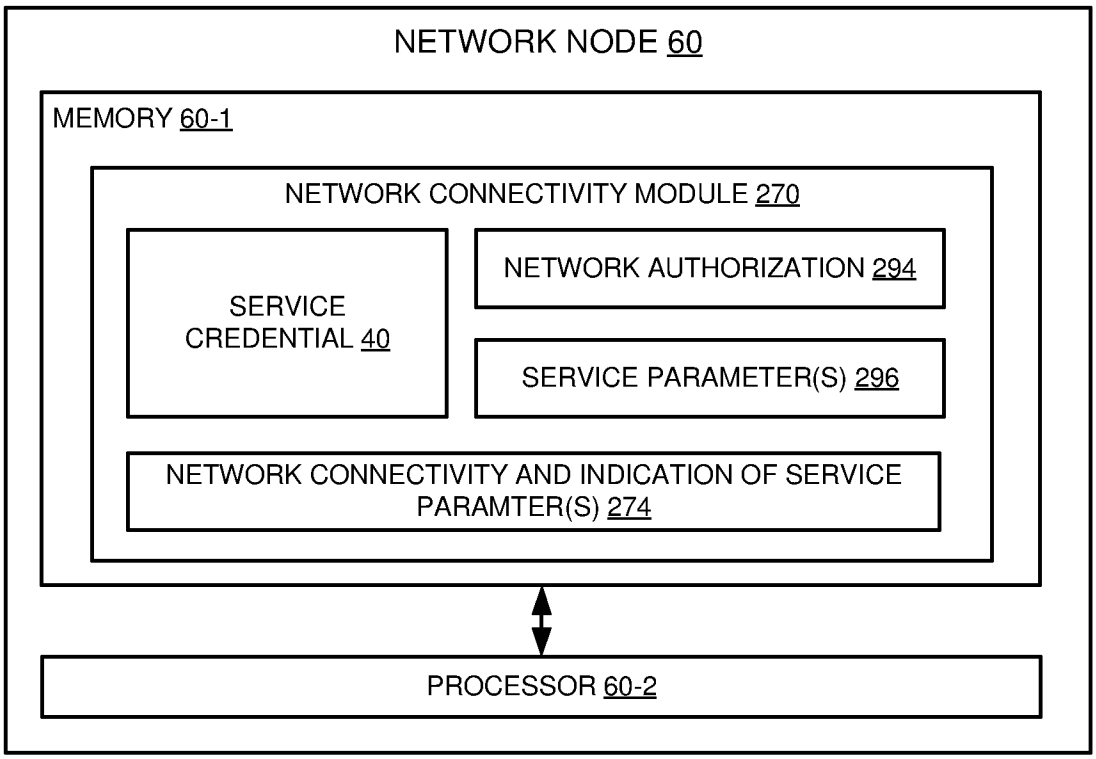

FIGURE 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/042315

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06
ADD. H04L29/06 H04L12/14 H04M15/00

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)
H04W H04L H04M

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 2016/277191 A1 (LEE SOO BUM [US] ET AL) 22 September 2016 (2016-09-22) paragraph [0003] - paragraph [0021] paragraph [0043] - paragraph [0057] paragraph [0077] paragraph [0084] claims 1-50 figures 1, 8A, 8B, 14, 18, 19	1-38

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
19 March 2018	26/03/2018

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	Bakdi, Idir

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/042315

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/262021 A1 (LEE SOO BUM [US] ET AL) 8 September 2016 (2016-09-08) paragraph [0002] - paragraph [0013] paragraph [0029] - paragraph [0035] paragraph [0046] paragraph [0059] - paragraph [0062] paragraph [0078] paragraph [0176] - paragraph [0179] claims 1-45 figures 1, 5, 8A-8C	1-38
A	US 2016/044484 A1 (CHO SONG YEAN [KR] ET AL) 11 February 2016 (2016-02-11) paragraph [0002] - paragraph [0009] paragraph [0028] - paragraph [0031] paragraph [0064] - paragraph [0068] paragraph [0076] - paragraph [0083] paragraph [0094] - paragraph [0099] claims 1-4, 8-11 figures 2, 5, 9-12, 16	1-38

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/042315

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016277191 A1	22-09-2016	CN 107409136 A	28-11-2017
		EP 3272099 A1	24-01-2018
		KR 20170110157 A	10-10-2017
		TW 201644292 A	16-12-2016
		US 2016277191 A1	22-09-2016
		WO 2016148903 A1	22-09-2016
US 2016262021 A1	08-09-2016	AU 2016229439 A1	10-08-2017
		CN 107431701 A	01-12-2017
		EP 3266180 A1	10-01-2018
		KR 20170106490 A	20-09-2017
		KR 20180004310 A	10-01-2018
		TW 201644250 A	16-12-2016
		US 2016262021 A1	08-09-2016
		US 2017230829 A1	10-08-2017
		WO 2016144516 A1	15-09-2016
US 2016044484 A1	11-02-2016	CN 103460729 A	18-12-2013
		CN 107103486 A	29-08-2017
		EP 2670174 A2	04-12-2013
		JP 6158095 B2	05-07-2017
		JP 2014505438 A	27-02-2014
		JP 2017121079 A	06-07-2017
		KR 20120100719 A	12-09-2012
		US 2013316674 A1	28-11-2013
		US 2015156027 A1	04-06-2015
		US 2015156337 A1	04-06-2015
		US 2016044484 A1	11-02-2016
		WO 2012102594 A2	02-08-2012