



(51) International Patent Classification:

H04L 9/40 (2022.01) H04L 67/14 (2022.01)
H04W 12/06 (2021.01)

(21) International Application Number:

PCT/IB2024/051228

(22) International Filing Date:

09 February 2024 (09.02.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/484,280 10 February 2023 (10.02.2023) US

(71) Applicant: **LENOVO (SINGAPORE) PTE. LTD.**
[SG/SG]; 151 Lorong Chuan #02-01, New Tech Park
556741 (SG).

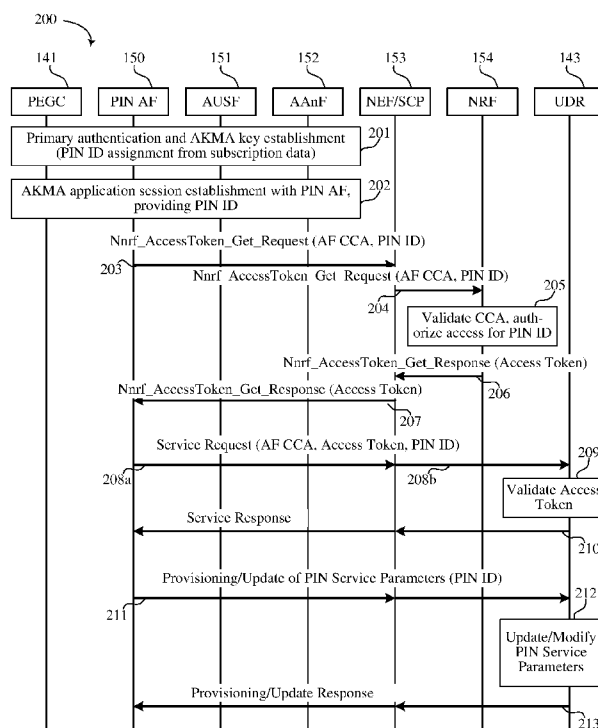
(72) Inventors: **KUNZ, Andreas**; Rheingaustrasse 8, 68526
Ladenburg (DE). **BASKARAN, Sheeba Backia Mary**;
Frankenweg 23, 61381 Friedrichsdorf (DE).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,
KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA,
NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO,
RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, CV,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST,

(54) Title: METHOD TO AUTHORIZE AN APPLICATION FUNCTION FOR A PERSONAL INTERNET OF THINGS NETWORK

FIG. 2



(57) Abstract: Aspects of the present disclosure relate to devices and methods for a core network system to enable a remote device to wireless communication with appropriate authorization using radio access technology and protocols to access a data repository. An application function provided by the core network system acts as a service communication proxy (SCP) to receive a validated access token to provision or update the data repository with service parameters and a network identity associated with the remote device to access data maintained by the data repository. Embodiments provide for PIN application function authorization: (i) without mutual authentication; (ii) by indirect communication with delegated discovery; or (iii) within Authentication and Key Management for Applications (AKMA) application establishment.

SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)*

METHOD TO AUTHORIZE AN APPLICATION FUNCTION FOR A PERSONAL INTERNET OF THINGS NETWORK

PRIORITY APPLICATION

[0001] This application claims priority to U.S. Provisional Application No. 63/484,280, filed February 10, 2023, the contents of which are fully incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates to wireless communications, and more specifically to application function authorization for wireless communication by a remote device to a network device.

BACKGROUND

[0003] A wireless communications system may include one or multiple network communication devices, including base stations, which may be otherwise known as an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. Each network communication device, such as a base station, may support wireless communications for one or multiple user communication devices, which may be otherwise known as user equipment (UE), or other suitable terminology. The wireless communications system may support wireless communications with one or multiple user communication devices by utilizing resources of the wireless communications system (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers). Additionally, the wireless communications system may support wireless communications across various radio access technologies including third generation (3G) radio access technology, fourth generation (4G) radio access technology, fifth generation (5G) radio access technology, and other suitable radio access technologies beyond 5G (e.g., sixth generation (6G)).

[0004] The Internet of things (IoT) describes physical objects with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. IoT devices are

individually addressable and wirelessly connect to form an IoT network, such as a personal IoT network in a home or worn by a person. The wireless links between the IoT devices may use various wireless technologies and protocols, such as low power, short range technologies used in personal access networks (PAN) in a home or worn on a person. To increase the functionality and capabilities of a personal IoT network (PIN), one or more PIN elements of the PIN may have gateway capabilities to wirelessly communicate with a radio access network (RAN) using a radio access technology (RAT).

SUMMARY

[0005] The present disclosure relates to methods, apparatuses, and systems providing a core network system that enables a remote device to wireless communicate using radio access technology and protocols with appropriate authorization by an application function to access a data repository. An application function provided by the core network system acts as a service communication proxy (SCP) to receive a validated access token to provision or update the data repository with service parameters and a network identity associated with the remote device to access data maintained by the data repository. Embodiments provide for PIN application function authorization: (i) without mutual authentication; (ii) by indirect communication with delegated discovery; or (iii) within Authentication and Key Management for Applications (AKMA) application establishment. In particular embodiments, the remote device is a personal Internet of Things network element with gateway capabilities (PEGC) and the application function is a personal Internet of Things network (PIN) application function.

[0006] Some implementations of the method and apparatuses described herein may include a method for wireless communication at a core network system. In one or more embodiments, the method may include authenticating, by an authentication function provided by the core network system, a network identity associated with a remote device. The method may include establishing, by an application function provided by the core network system and via a transceiver communicatively connected to the core network system, an application session with the remote device. The method may include sending, from the application

function to a repository function provided by the core network system, an access token request. The access token request includes a client credential assertion and the network identity. The access token request prompts a repository function provided by the core network system to validate the access token request and return an access token to the core network system. The method may include sending, by the core network system, a service request comprising the access token to a data repository, prompting validation of the access token by the data repository prior to providing access to data in the data repository. The method may include accessing the data repository, by the application function using the access token, to provision or update network service parameters and a network identity of the remote device at the data repository. In response the data repository takes an action to validate the access token. The method may include receiving, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository.

[0007] Some implementations of the method and apparatuses described herein may include a method for wireless communication at a core network system. In one or more embodiments, the method may include receiving, by an authentication function provided by the core network system and via a transceiver of the core network system, an application session establishment request from a remote device. The method may include authenticating, by an authentication function, a network identity associated with a remote device. The method may include enabling, by the authentication function, an application function provided by the core network system to request an application key for an application session using the network identity and an application function identity. The method may include receiving, by the application function, an access token required to access a data repository. The method may include responding, by the application function via the transceiver, to the remote device that the application session is established. The method may include sending, from the application function to the data repository, an access token request. The access token request includes the access token, the application function identity, and the network identity. The access token request prompts the data repository to provision or update network service parameters and a network identity of the remote device at the data repository. The method may include receiving, by the application function, a response message from the data

repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] **FIG. 1** is an example of a wireless communications system enabling wireless communication between base stations and user devices including a personal Internet of Things network (PIN), in accordance with aspects of the present disclosure.

[0009] **FIG. 2** is a communication diagram showing communications exchanges between a PIN element having a gateway capability (PEGC), functions provided by a core network system, and a data repository, the communication exchanges for providing PIN application function authorization without mutual authentication, in accordance with aspects of the present disclosure.

[0010] **FIG. 3** is a communication diagram showing communications exchanges between a PEGC, functions provided by the core network system, and the data repository, the communication exchanges for providing PIN application function authorization for indirect communication with delegated discovery, in accordance with aspects of the present disclosure.

[0011] **FIG. 4** is a communication diagram showing the communication exchanges between a PEGC, functions provided by the core network system, and the data repository, the communication exchanges for providing PIN application function authorization within Authentication and Key Management for Applications (AKMA) application establishment, in accordance with aspects of the present disclosure.

[0012] **FIG. 5** illustrates a block diagram of a network system that supports providing one or more functions of core network system to support PIN application function authorization, in accordance with aspects of the present disclosure.

[0013] **FIG. 6** illustrates a flowchart of a method for wireless communication performed by a network system for PIN application function authorization either: (i) without mutual

authentication or (ii) by indirect communication with delegated discovery, in accordance with aspects of the present disclosure.

[0014] FIG. 7 illustrates a flowchart of a method performed by a network system performing a core network function for PIN application function authorization within AKMA application establishment, in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0015] Wireless communication support for personal Internet of Things networks (PIN) includes providing solutions for authorization aspects of different elements in the PIN. However, a PIN application function (AF), or application server, is not currently addressed for how a PIN element can access PIN data in a unified data repository (UDR). From a security point of view, the scope of access granted to an AF needs to be restricted to the level of certain PIN element with gateway capabilities (“PEGCs”) or PINs and needs to be subject to permissions and consent granted by resource owners. As currently specified, authorization of exposure capabilities is defined on a rather general level. Authorization is based on operator policies using the identity of the AF as well as the “OAuth” authorization mechanism. No details about handling of permissions or providing consent to a specific application function are defined.

[0016] One attempt to address the authorization aspects has been incompletely described by assuming that the authorization from a Network Exposure Function (NEF) is enough to provide access to the UDR. This should not be the case, based on the principle that the service producer (UDR) should verify the access token from the service consumer, such as the PIN AF. Therefore, other solutions are required to ensure that the PIN AF only access the correct PIN resources in the UDR.

[0017] In summary, the present disclosure addresses the issue of how to restrict an AF which is associated with a certain PIN to only modify the resources for this particular PIN and not for another PIN. Embodiments of the present disclosure provide for PIN application function authorization: (i) without mutual authentication; (ii) by indirect communication with delegated discovery; or (iii) within Authentication and Key Management for Applications

(AKMA) application establishment. The basic assumption of all embodiments is that Authentication and Key Management for Applications (AKMA) is used to create a secure application layer connection between the PEGC and the PIN AF. The PEGC behaves as a user equipment (UE) towards the Fifth Generation Core (5GC) and sends the PIN identity (ID) to the PIN AF during application session establishment. The PIN AF then, after retrieval of the PIN ID, requests an access token from a Network Repository Function (NRF) to access the data stored in the UDR for the particular PIN ID. The NRF authorizes the request, taking into account the PIN ID. In another embodiment, the Access Token is already indirectly requested by the AKMA Anchor Function (AAnF) during application session establishment.

[0018] In particular, in a first embodiment, the PIN AF either communicates directly with the NRF or via a Network Exposure Function (NEF) acting as Service Communication Proxy (SCP) (“NEF/SCP”). The PIN AF is taking the role of the NF service consumer and the UDR the role of the NF service producer. The NRF authorizes the request, taking into account the PIN ID and provides an access token back to the PIN AF, which can be then used to access the UDR.

[0019] In a second embodiment, the PIN AF communicates with the NRF via an NEF, acting as a SCP. The PIN AF takes the role of the NF service consumer and the UDR the role of the NF service producer. The NRF authorizes the request, taking into account the PIN ID and provides an access token to the NEF. The NEF, acting as a SCP, sends the service request with access token and PIN ID to the UDR. The PIN AF can then directly, via NEF, access the UDR after authorization.

[0020] In a third embodiment, the access token is generated during the AKMA application session key establishment procedure and provided to the PIN AF, together with the AKMA related information. The PIN AF then can access the UDR, via NEF, including the access token and PIN ID.

[0021] In one aspect, a personal Internet of Things network (PIN) application function is defined within an apparatus. The apparatus includes a transceiver and a processor coupled to the transceiver. The processor and the transceiver are configured to cause the apparatus to perform a method for application function authorization. The method includes establishment

of an application session with a remote device, such as a PEGC, having an associated PIN Identity. The method includes sending an access token request to a first network function, such as NEF/NRF, including a client credentials assertion of the apparatus and the PIN Identity. The method includes receiving, in response to the access token request, a response message including an access token to access a second network function, such as the UDR. The method includes sending a service request message to the second network function, such as the UDR, including the client credentials assertion of the apparatus, the PIN identity and the access token. The method includes receiving a service response message, indicating the successful authorization of the apparatus at the second network function. The method includes sending a provisioning or update message, to the second network function, including the PIN identity and the PIN service parameters that should be updated or modified in the second network function. The method includes receiving a response message indicating the successful action in the second network function.

[0022] FIG. 1 illustrates an example of a wireless communications system **100** enabling wireless communication between base stations and user devices while mitigating cross-link interference between base stations, in accordance with aspects of the present disclosure. The wireless communications system **100** may include one or more network devices **102**, one or more UEs **104**, a core network **106**, and a packet data network **109**. The wireless communications system **100** may support various radio access technologies. In some implementations, the wireless communications system **100** may be a 4G network, such as an LTE network or an LTE-Advanced (LTE-A) network. In some other implementations, the wireless communications system **100** may be a 5G network, such as a New Radio (NR) network. In other implementations, the wireless communications system **100** may be a combination of a 4G network and a 5G network. The wireless communications system **100** may support radio access technologies beyond 5G, or other suitable radio access technology including Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20. Additionally, the wireless communications system **100** may support technologies, such as time division multiple access (TDMA), frequency division multiple access (FDMA), or code division multiple access (CDMA), etc.

[0023] The one or more network devices **102** may be dispersed throughout a geographic region to form the wireless communications system **100**. One or more of the network devices **102** described herein may be, may include, or may be referred to as a network node, a base station, a network element, a radio access network (RAN), a base transceiver station, an access point, a NodeB, an eNodeB (eNB), a next-generation NodeB (gNB), a network device, or other suitable terminology. A network device **102** and a UE **104** may communicate via a communication link **108**, which may be a wireless or wired connection. For example, a network device **102** and a UE **104** may wirelessly communicate (e.g., receive signaling, transmit signaling) over a user to user (Uu) interface.

[0024] A network device **102** may provide a geographic coverage area **110** for which the network device **102** may support services (e.g., voice, video, packet data, messaging, broadcast, etc.) for one or more UEs **104** within the geographic coverage area **110**. For example, a network device **102** and a UE **104** may support wireless communication of signals related to services (e.g., voice, video, packet data, messaging, broadcast, etc.) according to one or multiple radio access technologies. In some implementations, a network device **102** may be moveable, for example, a satellite **107** associated with a non-terrestrial network and communicating via a satellite link **111**. In some implementations, different geographic coverage areas **110** associated with the same or different radio access technologies may overlap, but the different geographic coverage areas **110** may be associated with different network devices **102**. Information and signals described herein may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0025] The one or more UEs **104** may be dispersed throughout a geographic region of the wireless communications system **100**. A UE **104** may include or may be referred to as a mobile device, a wireless device, a remote device, a remote unit, a handheld device, or a subscriber device, or some other suitable terminology. In some implementations, the UE **104** may be referred to as a unit, a station, a terminal, or a client, among other examples.

Additionally, or alternatively, the UE **104** may be referred to as an Internet-of-Things (IoT) device, an Internet-of-Everything (IoE) device, or machine-type communication (MTC) device, among other examples. In some implementations, a UE **104** may be stationary in the wireless communications system **100**. In some other implementations, a UE **104** may be mobile in the wireless communications system **100**.

[0026] In an example, according to aspects of the present disclosure, a network device **102b** may provide a geographic coverage area **110a** for which the network device **102b** may support services UEs **104** that are personal IoT network (PIN) elements **140a – 140n** (e.g., smart home appliance, personal audiovisual output device, sensor, etc.). PIN elements **140a – 140z** and PIN element with gateway capabilities (PEGC) **141** are communicatively coupled in PIN **142** using one or more wireless or wired networking technologies and protocols. In an example, PIN **142** is linked using a low power wireless technology. PEGC **141** is wirelessly connectable to network device **102b** for communication services supported by core network **106** and information services supported by packet network **109**, such as cloud storage service provided by unified data storage (UDR) **143**.

[0027] The one or more UEs **104** may be devices in different forms or having different capabilities. Some examples of UEs **104** are illustrated in **FIG. 1**. A UE **104** may be capable of communicating with various types of devices, such as the network devices **102**, other UEs **104**, or network equipment (e.g., the core network **106**, the packet data network **109**, a relay device, an integrated access and backhaul (IAB) node, or another network equipment), as shown in **FIG. 1**. Additionally, or alternatively, a UE **104** may support communication with other network devices **102** or UEs **104**, which may act as relays in the wireless communications system **100**.

[0028] A UE **104a** may also be able to support wireless communication directly with other UEs **104b** over a communication link **112**. For example, a UE **104** may support wireless communication directly with another UE **104** over a device-to-device (D2D) communication link. In some implementations, such as vehicle-to-vehicle (V2V) deployments, vehicle-to-everything (V2X) deployments, or cellular-V2X deployments, the communication link **112** may be referred to as a sidelink. For example, a UE **104a** may support wireless

communication directly with another UE **104b** over a PC5 interface. PC5 refers to a reference point where the UE **104a** directly communicates with another UE **104b** over a direct channel without requiring communication with the network device **102a**.

[0029] A network device **102** may support communications with the core network **106**, or with another network device **102**, or both. For example, a network device **102** may interface with the core network **106** through one or more backhaul links **114** (e.g., via an S1, N2, or another network interface). The network devices **102** may communicate with each other over the backhaul links **114** (e.g., via an X2, Xn, or another network interface). In some implementations, the network devices **102** may communicate with each other directly (e.g., between the network devices **102**). In some other implementations, the network devices **102** may communicate with each other indirectly (e.g., via the core network **106**). In some implementations, one or more network devices **102** may include subcomponents, such as an access network entity, which may be an example of an access node controller (ANC). An ANC may communicate with the one or more UEs **104** through one or more other access network transmission entities, which may be referred to as a radio heads, smart radio heads, or transmission and reception points (TRPs).

[0030] In some implementations, a network entity or network device **102** may be configured in a disaggregated architecture, which may be configured to utilize a protocol stack physically or logically distributed among two or more network entities or network devices **102**, such as an integrated access backhaul (IAB) network, an open RAN (O-RAN) (e.g., a network configuration sponsored by the O-RAN Alliance), or a virtualized RAN (vRAN) (e.g., a cloud RAN (C-RAN)). For example, a network entity or network device **102** may include one or more of a central unit (CU), a distributed unit (DU), a radio unit (RU), a RAN Intelligent Controller (RIC) (e.g., a Near-Real Time RIC (Near-RT RIC), a Non-Real Time RIC (Non-RT RIC)), a Service Management and Orchestration (SMO) system, or any combination thereof.

[0031] An RU may also be referred to as a radio head, a smart radio head, a remote radio head (RRH), a remote radio unit (RRU), or a transmission and reception point (TRP). One or more components of the network entities or network devices **102** in a disaggregated RAN

architecture may be co-located, or one or more components of the network entities or network devices **102** may be located in distributed locations (e.g., separate physical locations). In some implementations, one or more network entities or network devices **102** of a disaggregated RAN architecture may be implemented as virtual units (e.g., a virtual CU (VCU), a virtual DU (VDU), a virtual RU (VRU)).

[0032] Split of functionality between a CU, a DU, and an RU may be flexible and may support different functionalities depending upon which functions (e.g., network layer functions, protocol layer functions, baseband functions, radio frequency functions, and any combinations thereof) are performed at a CU, a DU, or an RU. For example, a functional split of a protocol stack may be employed between a CU and a DU such that the CU may support one or more layers of the protocol stack and the DU may support one or more different layers of the protocol stack. In some implementations, the CU may host upper protocol layer (e.g., a layer 3 (L3), a layer 2 (L2)) functionality and signaling (e.g., Radio Resource Control (RRC), service data adaptation protocol (SDAP), Packet Data Convergence Protocol (PDCP). The CU may be connected to one or more DUs or RUs, and the one or more DUs or RUs may host lower protocol layers, such as a layer 1 (L1) (e.g., physical (PHY) layer) or an L2 (e.g., radio link control (RLC) layer, medium access control (MAC) layer) functionality and signaling, and may each be at least partially controlled by the CU.

[0033] Additionally, or alternatively, a functional split of the protocol stack may be employed between a DU and an RU such that the DU may support one or more layers of the protocol stack and the RU may support one or more different layers of the protocol stack. The DU may support one or multiple different cells (e.g., via one or more RUs). In some implementations, a functional split between a CU and a DU, or between a DU and an RU may be within a protocol layer (e.g., some functions for a protocol layer may be performed by one of a CU, a DU, or an RU, while other functions of the protocol layer are performed by a different one of the CU, the DU, or the RU).

[0034] A CU may be functionally split further into CU control plane (CU-CP) and CU user plane (CU-UP) functions. A CU may be connected to one or more DUs via a midhaul

communication link (e.g., F1, F1-c, F1-u), and a DU may be connected to one or more RUs via a fronthaul communication link (e.g., open fronthaul (FH) interface). In some implementations, a midhaul communication link or a fronthaul communication link may be implemented in accordance with an interface (e.g., a channel) between layers of a protocol stack supported by respective network entities or network devices **102** that are in communication via such communication links.

[0035] The core network **106** may support user authentication, access authorization, tracking, connectivity, and other access, routing, or mobility functions. The core network **106** may be an evolved packet core (EPC), or a 5G core (5GC), which may include a control plane entity that manages access and mobility (e.g., a mobility management entity (MME), an access and mobility management functions (AMF)) and a user plane entity that routes packets or interconnects to external networks (e.g., a serving gateway (S-GW), a Packet Data Network (PDN) gateway (P-GW), or a user plane function (UPF)). In some implementations, the control plane entity may manage non-access stratum (NAS) functions, such as mobility, authentication, and bearer management for the one or more UEs **104** served by the one or more network devices **102** associated with the core network **106**. In example, core network **106** provides functions of PIN Application Function (AF) **150**, Authentication Server Function (AUSF) **151**, Authentication and Key Management for Applications (AKMA) anchor function (or “AAnF”) **152**, Network Exposure Function (NEF) acting as Service Communication Proxy (SCP) (“NEF/SCP) **153**, and Network Repository Function (NRF) **154**.

[0036] The core network **106** may communicate with the packet data network **109** over one or more backhaul links **116** (e.g., via an S1, N2, N2, or another network interface). The packet data network **109** may include an application server **118**. In some implementations, one or more UEs **104** may communicate with the application server **118**. A UE **104** may establish a session (e.g., a protocol data unit (PDU) session, or the like) with the core network **106** via a network entity or network device **102**. The core network **106** may route traffic (e.g., control information, data, and the like) between the UE **104** and the application server **118** using the established session (e.g., the established PDU session). The PDU session may be

an example of a logical connection between the UE **104** and the core network **106** (e.g., one or more network functions of the core network **106**).

[0037] In the wireless communications system **100**, the network entities or network devices **102** and the UEs **104** may use resources of the wireless communications system **100** (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers)) to perform various operations (e.g., wireless communications). In some implementations, the network entities or network devices **102** and the UEs **104** may support different resource structures. For example, the network entities or network devices **102** and the UEs **104** may support different frame structures. In some implementations, such as in 4G, the network entities or network devices **102** and the UEs **104** may support a single frame structure. In some other implementations, such as in 5G and among other suitable radio access technologies, the network entities or network devices or network devices **102** and the UEs **104** may support various frame structures (i.e., multiple frame structures). The network entities or network devices **102** and the UEs **104** may support various frame structures based on one or more numerologies.

[0038] One or more numerologies may be supported in the wireless communications system **100**, and a numerology may include a subcarrier spacing and a cyclic prefix. A first numerology (e.g., $\mu=0$) may be associated with a first subcarrier spacing (e.g., 15 kHz) and a normal cyclic prefix. In some implementations, the first numerology (e.g., $\mu=0$) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., $\mu=1$) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., $\mu=2$) may be associated with a third subcarrier spacing (e.g., 60 kHz) and a normal cyclic prefix or an extended cyclic prefix. A fourth numerology (e.g., $\mu=3$) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., $\mu=4$) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix.

[0039] A time interval of a resource (e.g., a communication resource) may be organized according to frames (also referred to as radio frames). Each frame may have a duration, for example, a 10 millisecond (ms) duration. In some implementations, each frame may include

multiple subframes. For example, each frame may include 10 subframes, and each subframe may have a duration, for example, a 1 ms duration. In some implementations, each frame may have the same duration. In some implementations, each subframe of a frame may have the same duration.

[0040] Additionally, or alternatively, a time interval of a resource (e.g., a communication resource) may be organized according to slots. For example, a subframe may include a number (e.g., quantity) of slots. The number of slots in each subframe may also depend on the one or more numerologies supported in the wireless communications system **100**. For instance, the first, second, third, fourth, and fifth numerologies (i.e., $\mu=0$, $\mu=1$, $\mu=2$, $\mu=3$, $\mu=4$) associated with respective subcarrier spacings of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz may utilize a single slot per subframe, two slots per subframe, four slots per subframe, eight slots per subframe, and 16 slots per subframe, respectively. Each slot may include a number (e.g., quantity) of symbols (e.g., OFDM symbols). In some implementations, the number (e.g., quantity) of slots for a subframe may depend on a numerology. For a normal cyclic prefix, a slot may include 14 symbols. For an extended cyclic prefix (e.g., applicable for 60 kHz subcarrier spacing), a slot may include 12 symbols. The relationship between the number of symbols per slot, the number of slots per subframe, and the number of slots per frame for a normal cyclic prefix and an extended cyclic prefix may depend on a numerology. It should be understood that reference to a first numerology (e.g., $\mu=0$) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[0041] In the wireless communications system **100**, an electromagnetic (EM) spectrum may be split, based on frequency or wavelength, into various classes, frequency bands, frequency channels, etc. By way of example, the wireless communications system **100** may support one or multiple operating frequency bands, such as frequency range designations FR1 (410 MHz – 7.125 GHz), FR2 (24.25 GHz – 52.6 GHz), FR3 (7.125 GHz – 24.25 GHz), FR4 (52.6 GHz – 114.25 GHz), FR4a or FR4-1 (52.6 GHz – 71 GHz), and FR5 (114.25 GHz – 300 GHz). In some implementations, the network entities or network devices **102** and the UEs **104** may perform wireless communications over one or more of the operating frequency

bands. In some implementations, FR1 may be used by the network entities or network devices **102** and the UEs **104**, among other equipment or devices for cellular communications traffic (e.g., control information, data). In some implementations, FR2 may be used by the network entities or network devices **102** and the UEs **104**, among other equipment or devices for short-range, high data rate capabilities.

[0042] FR1 may be associated with one or multiple numerologies (e.g., at least three numerologies). For example, FR1 may be associated with a first numerology (e.g., $\mu=0$), which includes 15 kHz subcarrier spacing; a second numerology (e.g., $\mu=1$), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing. FR2 may be associated with one or multiple numerologies (e.g., at least 2 numerologies). For example, FR2 may be associated with a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., $\mu=3$), which includes 120 kHz subcarrier spacing.

[0043] FIG. 2 is a communication diagram **200** showing communications exchanges between a PIN element having a gateway capability (PEGC), functions provided by a core network system, and a data repository, the communications exchanges for providing PIN application function authorization without mutual authentication. In a first embodiment, PIN AF authorization is provided without mutual authentication. In this embodiment, the PIN AF either communicates directly with the NRF or via an NEF, acting as a SCP. The PIN AF is taking the role of the NF Service Consumer, and the UDR takes the role of the NF Service Producer. The procedure is based on an authorization for indirect communication without delegated discovery procedure. The NRF authorizes the request, taking into account the PIN ID, and provides an Access Token back to the PIN AF, which can be then used to access the UDR.

[0044] At **201**, the PEGC performs primary authentication to the 5GC and may retrieve, during the registration procedure, the PIN ID. Alternatively the PIN ID is already assigned to the PEGC or pre-configured. PEGC and AAnF perform the AKMA key generation as specified.

[0045] At **202**, the PEGC performs a AKMA application session establishment procedure to establish a secure communication between the PEGC and the PIN AF. The PEGC provides the PIN ID to the PIN AF.

[0046] At **203**, the PIN AF sends an access token request (Nnrf_AccessToken_Get Request) to the NEF/SCP. The access token request may additionally include the PIN AF Client Credentials Assertion (CCA) and the PIN ID. The PIN ID may be included in the additional “scope” of the request. If the CCA is included, the NF type of the expected audience in CCA shall contain “RF”.

[0047] At **204**, the NEF/SCP forwards the access token request (Nnrf_AccessToken_Get Request) to the NRF. The request may include the PIN AF CCA and PIN ID.

[0048] At **205**, the NRF authenticates the PEGC, also taking the PIN ID into account. The NRF issues an access token and uses the PIN AF NF Instance ID as the subject of the access token.

[0049] At **206**, the NRF sends the access token to the NEF/SCP in an access token response (Nnrf_AccessToken_Get Response).

[0050] At **207**, the NEF/SCP forwards the access token response (Nnrf_AccessToken_Get Response) to the PIN AF, including the access token.

[0051] At **208a**, the PIN AF sends the service request to the NEF/SCP. The service request includes the access token received at **207** and may include the PIN AF CCA and the PIN ID. If the CCA is included, the “NF” type of the expected audience in CCA shall contain “UDR”. At **208b**, the NEF/SCP forwards the service request to the UDR. The service request includes the access token and may include the PIN AF CCA.

[0052] At **209**, the UDR authenticates the PIN AF and if successful, the UDR validates the access token for data modification associated to the PIN ID.

[0053] At **210**, if the validation of the access token is successful, the UDR sends the service response to the PIN AF via the NEF/SCP.

[0054] At **211**, the PIN AF provisions/updates PIN Service Specific Parameters to the UDR (via NEF) related to the PEGC. The request includes the PIN ID.

[0055] At **212**, the UDR updates the PIN Service Parameters related to the PIN ID.

[0056] At **213**, the UDR sends a response back to the PIN AF via the NEF/SCP. The response may indicate the successful update of the PIN Service Parameters.

[0057] **FIG. 3** is a communication diagram **300** showing communications exchanges between a PEGC, functions provided by the core network system, and the data repository, the communication exchanges for providing PIN application function authorization for indirect communication with delegated discovery, according to a second embodiment. In the second embodiment, PIN AF authorization is provided for indirect communication with delegated discovery. In this embodiment, the PIN AF communicates with the NRF via an NEF, acting as a SCP. The PIN AF is taking the role of the NF service consumer, and the UDR takes the role of the NF service producer. The procedure is based an authorization for indirect communication with delegated discovery procedure. The NRF authorizes the request, taking into account the PIN ID, and provides an access token to the NEF. The NEF/SCP sends the service request with access token and PIN ID to the UDR. The PIN AF can then directly access the UDR after authorization.

[0058] At **201**, the PEGC performs primary authentication to the 5GC and may retrieve during the registration procedure the PIN ID. Alternatively, the PIN ID is already assigned to the PEGC or pre-configured. PEGC and AAnF perform the AKMA key generation as specified.

[0059] At **202**, the PEGC performs a AKMA application session establishment procedure to establish a secure communication between the PEGC and the PIN AF. The PEGC provides the PIN ID to the PIN AF.

[0060] At **203**, the PIN AF sends service request to the NEF/SCP. The service request may additionally include the PIN AF CCA and the PIN ID. The PIN ID may be included in the additional “scope” of the request. If the CCA is included, the NF type of the expected audience in CCA shall contain “NRF” and “UDR”.

[0061] At **204**, the NEF/SCP sends an access token request (Nnrf_AccessToken_Get Request) to the NRF. The request may include the PIN AF CCA and PIN ID.

[0062] At **205**, the NRF authenticates the PEGC, also taking the PIN ID into account. The NRF issues an access token and uses the PIN AF NF Instance ID as the subject of the access token.

[0063] At **206**, the NRF sends the access token to the NEF/SCP in an access token response (Nnrf_AccessToken_Get Response).

[0064] At **307**, the NEF/SCP sends the service request to the UDR. The service request includes the access token and may include the PIN AF CCA and PIN ID.

[0065] At **308**, the UDR authenticates the PIN AF, and if successful, the UDR validates the access token for data modification associated to the PIN ID.

[0066] At **309**, if the validation of the access token is successful, the UDR sends the service response to the PIN AF via the NEF/SCP.

[0067] At **311**, the PIN AF provisions/updates PIN Service Specific Parameters to the UDR (via NEF) related to the PEGC. The request includes the PIN ID.

[0068] At **312**, the UDR updates the PIN Service Parameters related to the PIN ID.

[0069] At **313**, the UDR sends a response back to the PIN AF. The response may indicate the successful update of the PIN Service Parameters.

[0070] **FIG. 4** is a communication diagram **400** showing communications exchanges between a PEGC, functions provided by the core network system, and the data repository, the communication exchanges for providing PIN application function authorization within Authentication and Key Management for Applications (AKMA) application establishment, according to a third embodiment. In the third embodiment 3, PIN AF authorization is provided/performed within AKMA application session establishment. In this embodiment, the access token is generated during the AKMA application session key establishment procedure, as specified, and provided to the PIN AF together with the AKMA related information.

[0071] At **401**, the PEGC performs primary authentication to the 5GC and may retrieve during the registration procedure the PIN ID. Alternatively, the PIN ID is already assigned to the PEGC or pre-configured. PEGC and AAnF perform the AKMA key generation as specified.

[0072] At **402**, the PEGC performs a AKMA application session establishment procedure to establish a secure communication between the PEGC and the PIN AF. The PEGC sends an Application Session Establishment Request to the PIN AF including the PIN ID.

[0073] At **403**, the PIN AF selects the AAnF and sends a Naanf_AKMA_ApplicationKey_Get request to AAnF with the A-KID and the PIN ID to request the KAF for the PEGC. The PIN AF also includes its identity (AF_ID) in the request.

[0074] At **404**, the AAnF authorizes the request from the PIN AF and may contact the NRF, NEF, or UDR (**153a**) for an access token. The access token is bound to the PIN AF NF Identity and potentially the PIN ID.

[0075] At **405**, the AAnF derives the AKMA Application Key (KAF) from KAKMA.

[0076] At **406**, the AAnF sends Naanf_AKMA_ApplicationKey_Get response to the PIN AF with Subscription Permanent Identifier (SUPI), KAF and the KAF expiration time, and the access token.

[0077] At **407**, the AF sends the Application Session Establishment Response to the PEGC.

[0078] At **408**, the PIN AF provisions/updates PIN Service Specific Parameters to the UDR (via NEF) related to the PEGC. The request includes the PIN ID and the Access Token received at **406**.

[0079] At **409**, the UDR validates the Access Token and updates the PIN Service Parameters related to the PIN ID.

[0080] At **410**, the UDR sends a response back to the PIN AF. The response may indicate the successful update of the PIN Service Parameters.

[0081] FIG. 5 illustrates an example of a block diagram 500 of a network system 502 that supports wireless communication with a remote device such as PEGC 501 and provides core network functions for PIN application function authentication. The network system 502 may be an example of a distributed system providing combined capabilities of core network 106 and network device 102 (FIG. 1) as described herein. The network system 502 may support wireless communication with one or more network entities or network devices 102, UEs 104, or any combination thereof. The network system 502 may include components for bi-directional communications including components for transmitting and receiving communications, such as a processor 504, a memory 506, a transceiver 508, and an I/O controller 510. In one or more embodiments, the network system 502 may also support or provide a core network function such as PIN AF 150, AUSF 151, AAnF 152, NEF/SCP 153 and NRF 154. Network system 502 is communicatively connected via a network interface 530 and backhaul links 114 to base stations 534. Network system 502 is also communicatively connected via the network interface 530 to the packet network 109 and other core network devices 536. These components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0082] The processor 504, the memory 506, the transceiver 508, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. For example, the processor 504, the memory 506, the transceiver 508, or various combinations or components thereof may support a method for performing one or more of the operations described herein.

[0083] In some implementations, the processor 504, the memory 506, the transceiver 508, or various combinations or components thereof may be implemented in hardware (e.g., in communications management circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA) or other programmable logic device, a discrete gate or transistor logic, discrete hardware components, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present

disclosure. A controller **507** includes the processor **504** that configures the network system **502** to perform the functionality of the present disclosure. The controller **507** is communicatively coupled to the memory **506** to execute program code. Controller **507** may include dedicated memory solely accessible by the processor **504**, that is a portion of memory **506**. In some implementations, the processor **504** and the memory **506** coupled with the processor **504** may be configured to perform one or more of the functions as a controller **507** described herein (e.g., executing, by the processor **504**, instructions stored in the memory **506**). In an example, the processor **504** of a device controller **507** executes a personal IoT network security application **509** for configuring either network system **502** for personal IoT network security. In an example, embodiments of personal IoT network security application **509** provide for PIN application function authorization: (i) without mutual authentication; (ii) by indirect communication with delegated discovery; or (iii) within Authentication and Key Management for Applications (AKMA) application establishment.

[0084] The processor **504** may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some implementations, the processor **504** may be configured to operate a memory array using a memory controller. In some other implementations, a memory controller may be integrated into the processor **504**. The processor **504** may be configured to execute computer-readable instructions stored in a memory (e.g., the memory **506**) to cause the network system **502** to perform various functions of the present disclosure.

[0085] The memory **506** may include random access memory (RAM) and read-only memory (ROM). The memory **506** may store computer-readable, computer-executable code including instructions that, when executed by the processor **504** cause the network system **502** to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. In some implementations, the code may not be directly executable by the processor **504** but may cause a computer (e.g., when compiled and executed) to perform functions described herein. In some implementations, the memory **506** may include, among other things, a basic I/O system

(BIOS) which may control basic hardware or software operation such as the interaction with peripheral components or devices.

[0086] The I/O controller **510** may manage input and output signals for the network system **502**. The I/O controller **510** may also manage peripherals not integrated into the device **M02**. In some implementations, the I/O controller **510** may represent a physical connection or port to an external peripheral. In some implementations, the I/O controller **510** may utilize an operating system such as iOS®, ANDROID®, MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, LINUX®, or another known operating system. In some implementations, the I/O controller **510** may be implemented as part of a processor, such as the processor **504**. In some implementations, a user may interact with the network system **502** via the I/O controller **510** or via hardware components controlled by the I/O controller **510**.

[0087] In some implementations, the network system **502** may include a single antenna **512**. However, in some other implementations, the network system **502** may have more than one antenna **512** (i.e., multiple antennas), including multiple antenna panels or antenna arrays, which may be capable of concurrently transmitting or receiving multiple wireless transmissions. The transceiver **508** may communicate bi-directionally using one or more receivers **515** and one or more transmitters **517**, via the one or more antennas **512**, wired, or wireless links as described herein. For example, the transceiver **508** may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver **508** may also include a modem to modulate the packets, to provide the modulated packets to one or more antennas **512** for transmission, and to demodulate packets received from the one or more antennas **512**.

[0088] The network system **502** may include a scheduler **519** that is communicatively coupled to the controller **507**. In some implementations, the scheduler **519** may be configured to perform various operations (e.g., receiving, monitoring, transmitting) using or otherwise in cooperation with the receiver **515**, the transmitter **517**, or both. For example, the scheduler **519** may receive information from the receiver **515**, send information to the transmitter **517**, or be integrated in combination with the receiver **515**, the transmitter **517**, or both to receive

information, transmit information, or perform various other operations as described herein. Although the scheduler **519** is illustrated as a separate component, in some implementations, one or more functions described with reference to the scheduler **519** may be supported by or performed by a processing subsystem such as controller **507**, the memory **506**, or any combination thereof. For example, the memory **506** may store code, which may include instructions executable by the controller **507** to cause/configure the network system **502** to perform various aspects of the present disclosure as described herein, or the controller **507** and the memory **506** may be otherwise configured to perform or support such operations.

[0089] **FIG. 6** illustrates a flowchart of a method **600** for wireless communication by a network system for PIN application function authorization either: (i) without mutual authentication or (ii) by indirect communication with delegated discovery. The operations of the method **600** may be implemented by a device or its components as described herein. For example, the operations of the method **600** may be performed by one or more network devices such as core network **106** and network device **102** (**FIG. 1**) and network system **502** (**FIG. 5**). In one or more embodiments, the network system supports a core network function such as PIN AF **150**, AUSF **151**, AAnF **152**, NEF/SCP **153** and NRF **154** (**FIG. 1**). In some implementations, the network system may execute a set of instructions to control the function elements of the network system to perform the described functions. Additionally, or alternatively, the network system may perform aspects of the described functions using special-purpose hardware.

[0090] At **605**, the method **600** may include authenticating, by an authentication function provided by the core network system, a network identity associated with a remote device. The operations of **605** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **605** may be performed by a device or system as described with reference to **FIGs. 1** and **5**.

[0091] At **610**, the method **600** may include establishing, by an application function provided by the core network system and via a transceiver communicatively connected to the core network system, an application session with the remote device. The operations of **610** may be performed in accordance with examples as described herein. In some

implementations, aspects of the operations of **610** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[0092] At **615**, the method **600** may include sending, from the application function to a repository function provided by the core network system, an access token request comprising a client credential assertion and comprising the network identity, prompting a repository function provided by the core network system to validate the access token request and return an access token to the core network system. The operations of **615** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **615** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[0093] At **620**, the method **600** may include sending, by the core network system, a service request comprising the access token to a data repository, prompting validation of the access token by the data repository to access data in the data repository. The operations of **620** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **620** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[0094] At **625**, the method **600** may include accessing the data repository, by the application function using the access token, to provision or update network service parameters and a network identity of the remote device at the data repository. The operations of **625** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **625** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[0095] At **630**, the method **600** may include receiving, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository. The operations of **630** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **630** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[0096] According to one or more aspects of the present disclosure, in one or more embodiments, the application function is a personal internet of things network (PIN) application function. The network identity is a PIN identity (ID). The remote device is a PIN element with gateway capabilities. In one or more particular embodiments, establishing the application session includes communicating the PIN ID from the PIN application function to the authentication function comprising an authentication server function (AUSF) and an authentication and key management for applications anchor function (AAnF). In one or more particular embodiments, the repository function comprises a network repository function (NRF). The data repository is a unified data repository (UDR).

[0097] In one or more embodiments, the method **600** includes providing a network exposure function (NEF) serving as a service communication proxy (SCP) between the application function and the NRF. In one or more particular embodiments, in response to receiving the access token from the NRF via the NEF, the method **600** further includes sending, from the application function, the service request to the UDR to prompt validation of the access token. In one or more particular embodiments, in response to receiving the access token from the NRF, the method **600** further includes sending, from the NRF, the service request to the UDR to prompt validation of the access token.

[0098] **FIG. 7** illustrates a flowchart of a method **700** for wireless communication by a network system for PIN application function authorization within Authentication and Key Management for Applications (AKMA) application establishment. The operations of the method **700** may be implemented by a device or its components as described herein. For example, the operations of the method **700** may be performed by one or more network devices such as core network **106** and network device **102** (**FIG. 1**) and network system **502** (**FIG. 5**). In one or more embodiments, the network system supports a core network function such as PIN AF **150**, AUSF **151**, AAnF **152**, NEF/SCP **153** and NRF **154** (**FIG. 1**). In some implementations, the network system may execute a set of instructions to control the function elements of the network system to perform the described functions. Additionally, or alternatively, the network system may perform aspects of the described functions using special-purpose hardware.

[0099] At **705**, the method **700** may include receiving, by an authentication function provided by the core network system and via a transceiver of the core network system, an application session establishment request from a remote device. The operations of **705** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **705** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00100] At **710**, the method **700** may include authenticating, by the authentication function, a network identity associated with a remote device. The operations of **710** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **710** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00101] At **715**, the method **700** may include enabling, by the authentication function, an application function provided by the core network system to request an application key for an application session using the network identity and an application function identity. The operations of **715** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **715** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00102] At **720**, the method **700** may include receiving, by the application function, an access token required to access a data repository. The operations of **720** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **720** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00103] At **725**, the method **700** may include responding, by the application function via the transceiver, to the remote device that the application session is established. The operations of **725** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **725** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00104] At **730**, the method **700** may include sending, from the application function to the data repository, the access token request comprising the access token, the application function identity, and the network identity, prompting a data repository to provision or update network service parameters and a network identity of the remote device at the data repository. The operations of **730** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **730** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00105] At **735**, the method **700** may include receiving, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository. The operations of **735** may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of **735** may be performed by a device or system as described with reference to **FIGs. 1 and 5**.

[00106] According to one or more aspects of the present disclosure, in one or more embodiments, the application function is a personal internet of things network (PIN) application function. The network identity comprises a PIN identity (ID). The remote device is a PIN element with gateway capabilities. In one or more embodiments, the authentication function is an authentication server function (AUSF) and an authentication and key management for applications anchor function (AAnF). In one or more embodiments, at least one of a network repository function (NRF) and a network exposure function (NEF) provided by the core network system assign the access token to the application function and the remote device. In one or more embodiments, the data repository is a united data repository (UDR) that assigns the access token to the application function and the remote.

[00107] The various illustrative blocks and components described in connection with the disclosure herein may be implemented or performed with a general-purpose processor, a DSP, an ASIC, a CPU, an FPGA or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but in the alternative, the processor may be any processor, controller,

microcontroller, or state machine. A processor may also be implemented as a combination of computing devices (e.g., a combination of a DSP and a microprocessor, multiple microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration).

[00108] The functions described herein may be implemented in hardware, software executed by a processor, firmware, or any combination thereof. If implemented in software executed by a processor, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Other examples and implementations are within the scope of the disclosure and appended claims. For example, due to the nature of software, functions described herein may be implemented using software executed by a processor, hardware, firmware, hardwiring, or combinations of any of these. Features implementing functions may also be physically located at various positions, including being distributed such that portions of functions are implemented at different physical locations.

[00109] Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer. By way of example, and not limitation, non-transitory computer-readable media may include RAM, ROM, electrically erasable programmable ROM (EEPROM), flash memory, compact disk (CD) ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium that may be used to carry or store desired program code means in the form of instructions or data structures and that may be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor.

[00110] Any connection may be properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are

included in the definition of computer-readable medium. Disk and disc, as used herein, include CD, laser disc, optical disc, digital versatile disc (DVD), floppy disk and Blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above are also included within the scope of computer-readable media.

[00111] As used herein, including in the claims, “or” as used in a list of items (e.g., a list of items prefaced by a phrase such as “at least one of” or “one or more of”) indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase “based on” shall not be construed as a reference to a closed set of conditions. For example, an example step that is described as “based on condition A” may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase “based on” shall be construed in the same manner as the phrase “based at least in part on”. Further, as used herein, including in the claims, a “set” may include one or more elements.

[00112] The terms “transmitting,” “receiving,” or “communicating,” when referring to a network entity, may refer to any portion of a network entity (e.g., a base station, a CU, a DU, a RU) of a RAN communicating with another device (e.g., directly or via one or more other network entities).

[00113] The description set forth herein, in connection with the appended drawings, describes example configurations and does not represent all the examples that may be implemented or that are within the scope of the claims. The term “example” used herein means “serving as an example, instance, or illustration,” and not “preferred” or “advantageous over other examples.” The detailed description includes specific details for the purpose of providing an understanding of the described techniques. These techniques, however, may be practiced without these specific details. In some instances, known structures and devices are shown in block diagram form to avoid obscuring the concepts of the described example.

[00114] The description herein is provided to enable a person having ordinary skill in the art to make or use the disclosure. Various modifications to the disclosure will be apparent to a person having ordinary skill in the art, and the generic principles defined herein may be applied to other variations without departing from the scope of the disclosure. Thus, the disclosure is not limited to the examples and designs described herein but is to be accorded the broadest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A network system comprising:

a transceiver;

memory that stores core network program code that defines at least three core functions comprising an authentication function, an application function, and repository function; and

at least one processor communicatively connected to the transceiver and the memory and that configures the network system to:

authenticate, by the authentication function, a network identity associated with a remote device;

establish, by the application function via the transceiver, an application session with the remote device;

send, from the application function to the repository function, an access token request comprising a client credential assertion and comprising the network identity, prompting the repository function to validate the access token request and return an access token to the at least three core functions;

send, by the at least three core functions, a service request comprising the access token to a data repository, prompting validation of the access token by the data repository to access data in the data repository;

access the data repository, by the application function using the access token, to provision or update network service parameters and a network identity of the remote device at the data repository; and

receive, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository.

2. The network system of claim 1, wherein:
 - the application function comprises a personal internet of things network (PIN) application function;
 - the network identity comprises a PIN identity (ID); and
 - the remote device comprises a PIN element with gateway capabilities.
3. The network system of claim 2, wherein, in establishing the application session, the at least one processor: configures the network system to communicate the PIN ID from the PIN application function to the authentication function comprising an authentication server function (AUSF) and an authentication and key management for applications anchor function (AAnF).
4. The network system of claim 3, wherein:
 - the repository function comprises a network repository function (NRF); and
 - the data repository comprises a unified data repository (UDR).
5. The network system of claim 4, wherein the at least three core functions comprise a network exposure function (NEF) serving as a service communication proxy (SCP) between the PIN application function and the NRF.
6. The network system of claim 5, wherein, in response to receiving the access token from the NRF via the NEF, the application function sends the service request to the UDR to prompt validation of the access token.
7. The network system of claim 5, wherein, in response to receiving the access token from the NRF, the NEF sends the service request to the UDR to prompt validation of the access token.

8. A network system comprising:
- a transceiver;
 - memory that stores core network program code that defines at least two core functions comprising an authentication function and an application function; and
 - at least one processor communicatively connected to the transceiver and the memory and that configures the network system to:
 - receive, by the authentication function via the transceiver, an application session establishment request from a remote device;
 - authenticate, by the authentication function, a network identity associated with a remote device;
 - enable, by the authentication function, the application function to request an application key for an application session using the network identity and an application function identity;
 - receive, by the application function, an access token required to access a data repository;
 - respond, by the application function via the transceiver, to the remote device that the application session is established;
 - send, from the application function to the data repository, the access token request comprising the access token, the application function identity, and the network identity, prompting a data repository to provision or update network service parameters and a network identity of the remote device at the data repository; and
 - receive, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository.
9. The network system of claim 8, wherein:
- the application function comprises a personal internet of things network (PIN) application function;
 - the network identity comprises a PIN identity (ID); and
 - the remote device comprises a PIN element with gateway capabilities.

10. The network system of claim 8, wherein the authentication function comprises an authentication server function (AUSF) and an authentication and key management for applications anchor function (AAnF).

11. The network system of claim 8, wherein the at least two core network functions comprise at least one of a network repository function (NRF) and a network exposure function (NEF) that assign the access token to the application function and the remote device.

12. The network system of claim 8, wherein the data repository comprises a united data repository (UDR) that assigns the access token to the application function and the remote device.

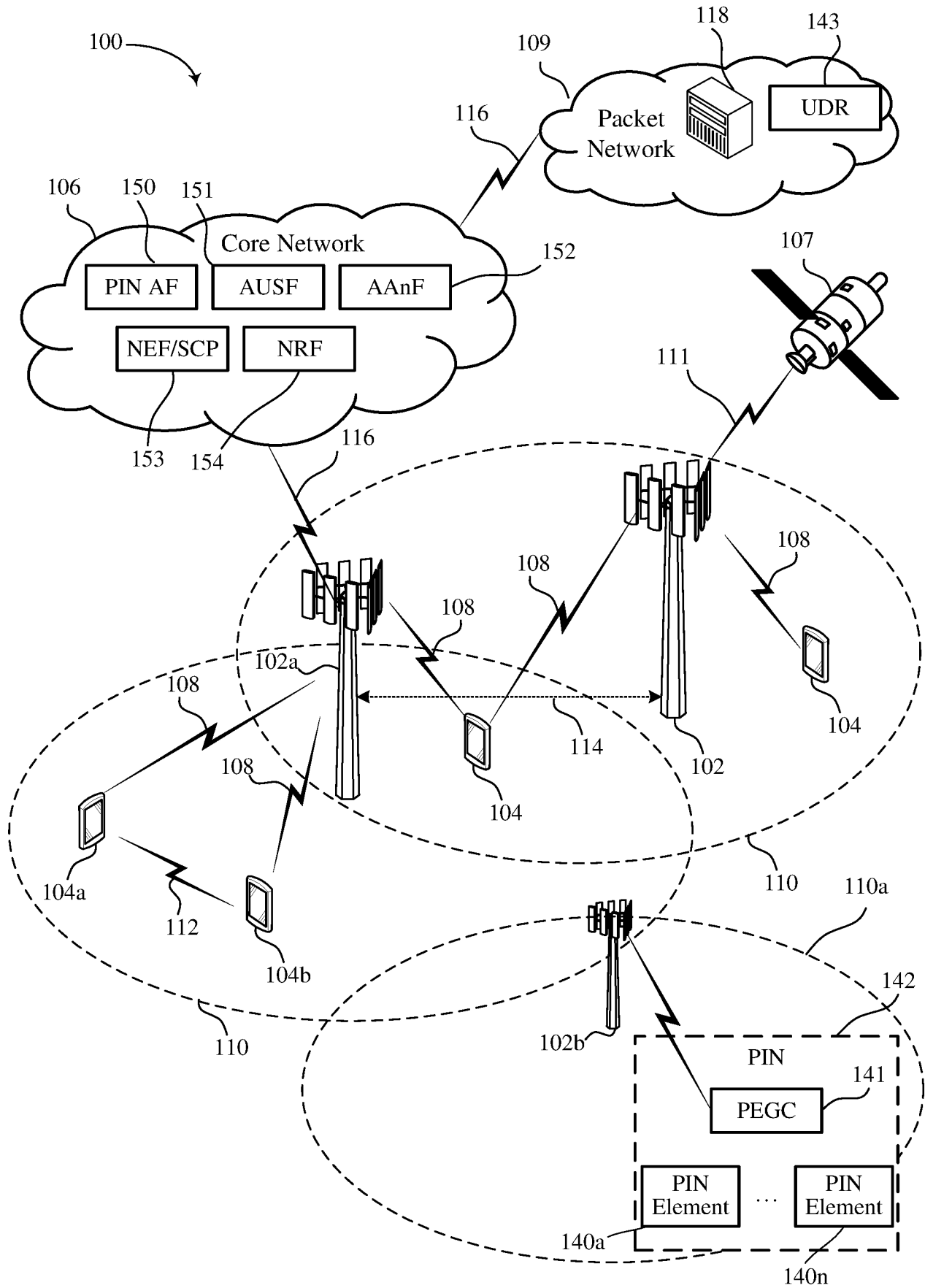
13. A method for communication at a core network system, the method comprising:
- authenticating, by an authentication function provided by the core network system, a network identity associated with a remote device;
 - establishing, by an application function provided by the core network system and via a transceiver communicatively connected to the core network system, an application session with the remote device;
 - sending, from the application function to a repository function provided by the core network system, an access token request comprising a client credential assertion and the network identity, prompting a repository function provided by the core network system to validate the access token request and to return an access token to the core network system;
 - sending, by the core network system, a service request comprising the access token to a data repository, prompting validation of the access token by the data repository to access data in the data repository;
 - accessing the data repository, by the application function using the access token, to provision or update network service parameters and a network identity of the remote device at the data repository; and
 - receiving, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository.
14. The method of claim 13, wherein:
- the application function comprises a personal internet of things network (PIN) application function;
 - the network identity comprises a PIN identity (ID); and
 - the remote device comprises a PIN element with gateway capabilities.
15. The method of claim 14, wherein establishing the application session comprises communicating the PIN ID from the PIN application function to the authentication function comprising an authentication server function (AUSF) and an authentication and key management for applications anchor function (AAnF).

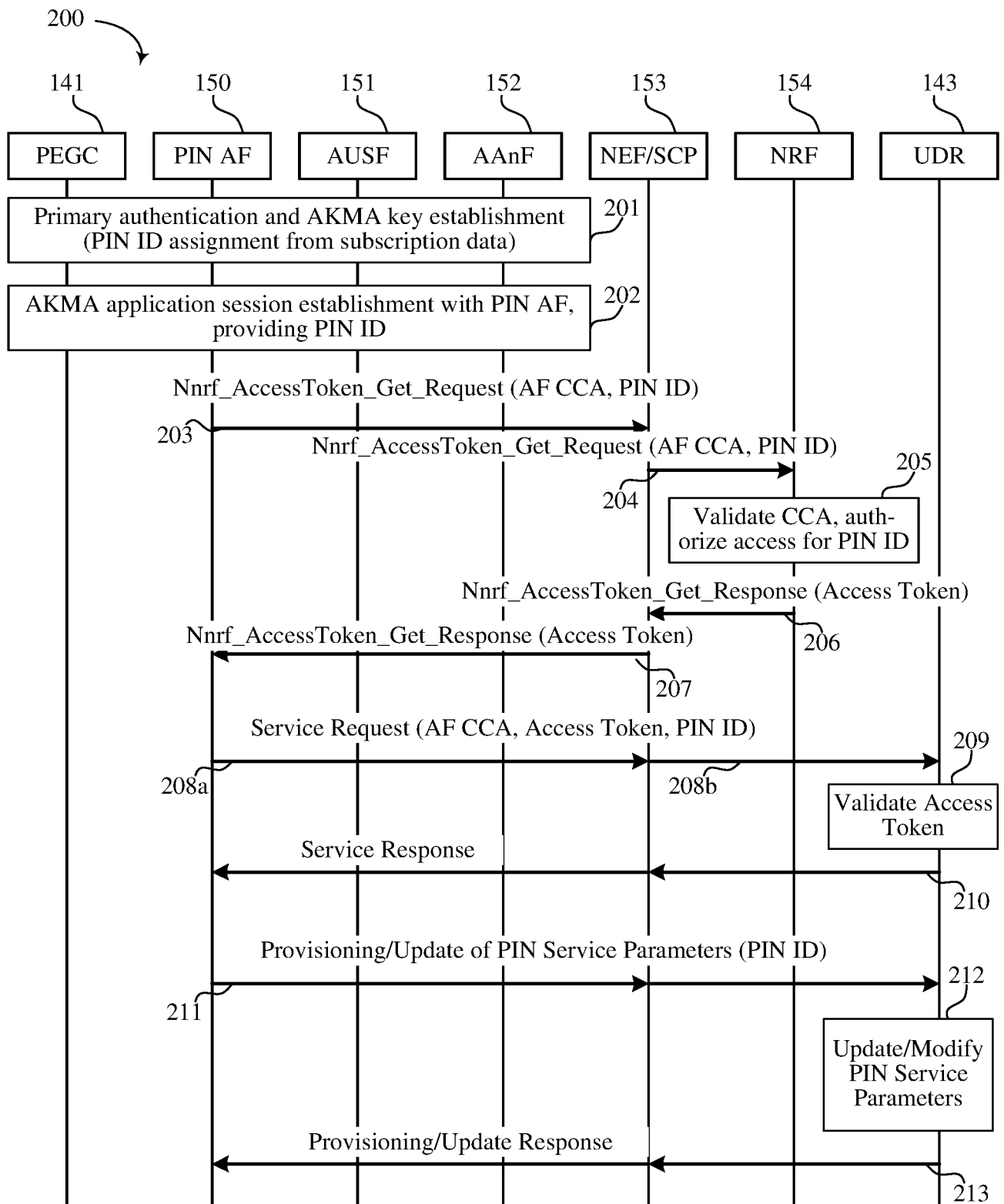
16. The method of claim 15, wherein:
the repository function comprises a network repository function (NRF); and
the data repository comprises a unified data repository (UDR).
17. The method of claim 16, further comprising providing a network exposure function (NEF) serving as a service communication proxy (SCP) between the application function and the NRF.
18. The method of claim 17, further comprising, in response to receiving the access token from the NRF via the NEF, sending, from the application function, the service request to the UDR to prompt validation of the access token.
19. The method of claim 17, further comprising, in response to receiving the access token from the NRF, sending, from the NRF, the service request to the UDR to prompt validation of the access token.
20. A method of communicating by a core network system, the method comprising:
receiving, by an authentication function provided by the core network system and via a transceiver of the core network system, an application session establishment request from a remote device;
authenticating, by the authentication function, a network identity associated with a remote device;
enabling, by the authentication function, an application function provided by the core network system to request an application key for an application session using the network identity and an application function identity;
receiving, by the application function, an access token required to access a data repository;
responding, by the application function via the transceiver, to the remote device that the application session is established;
sending, from the application function to the data repository, the access token request comprising the access token, the application function identity, and the network identity,

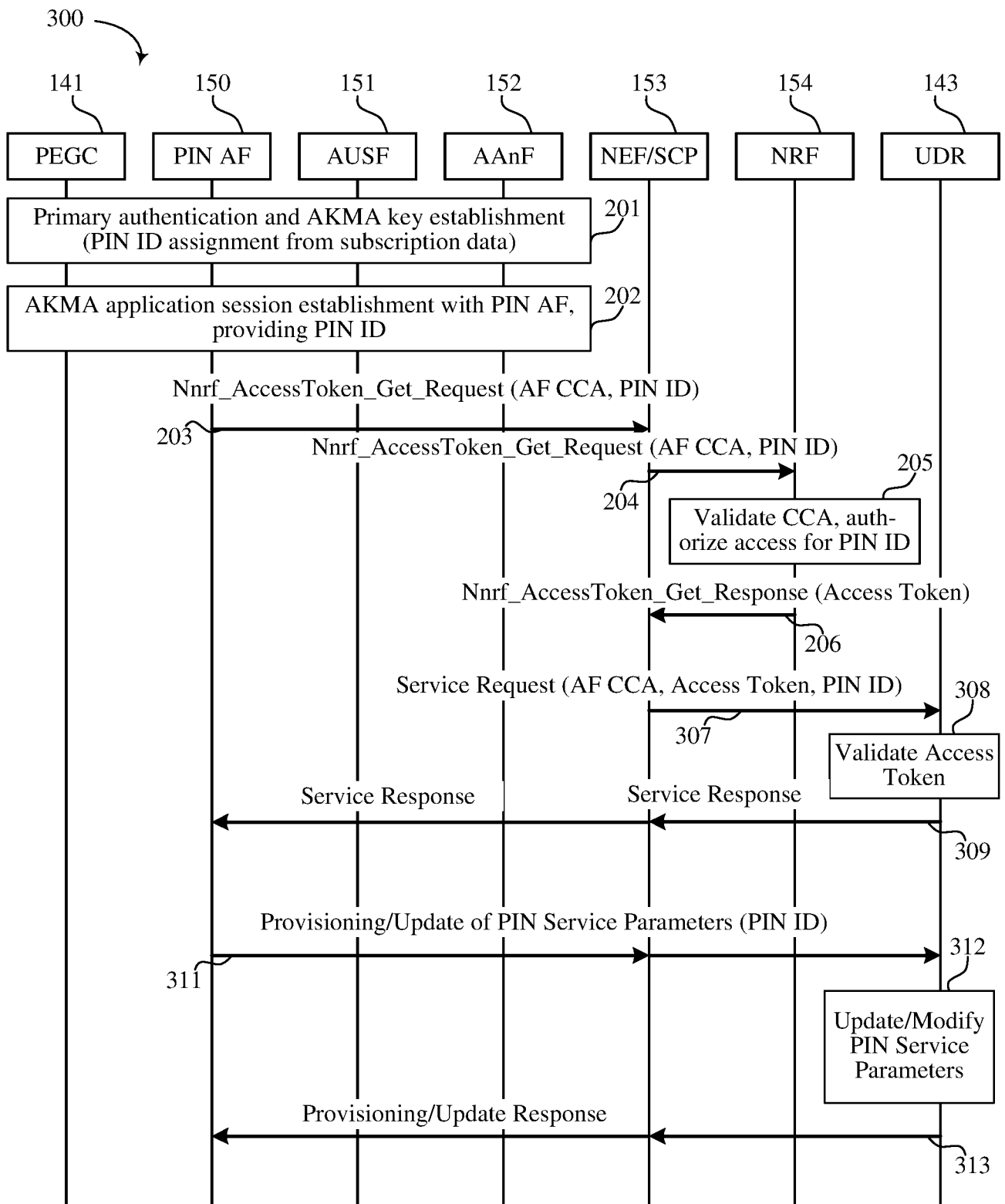
prompting a data repository to provision or update network service parameters and a network identity of the remote device at the data repository; and

receiving, by the application function, a response message from the data repository indicating a successful action by the data repository in validating the access token, enabling the application function to access the data repository.

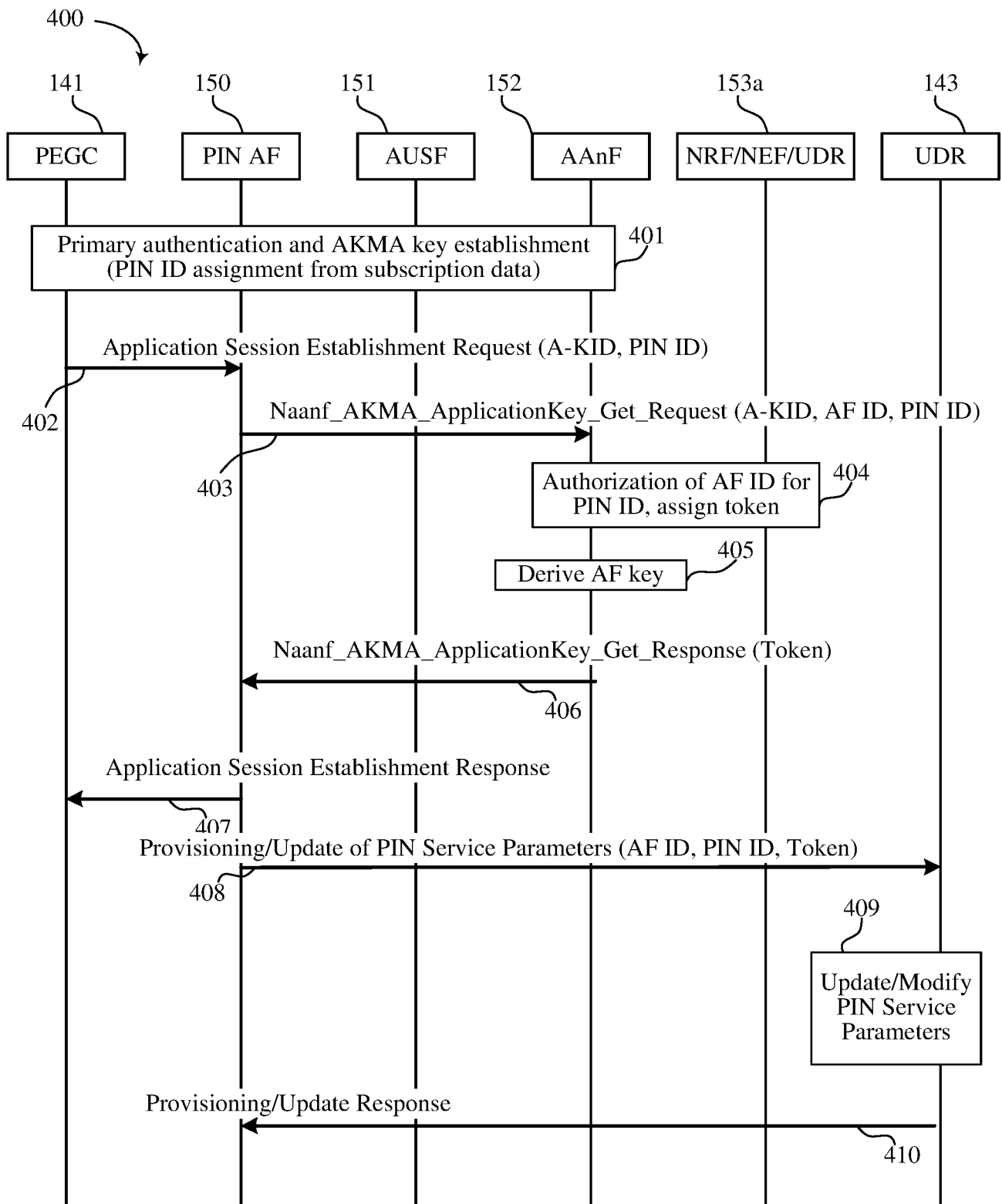
1/7

**FIG. 1**

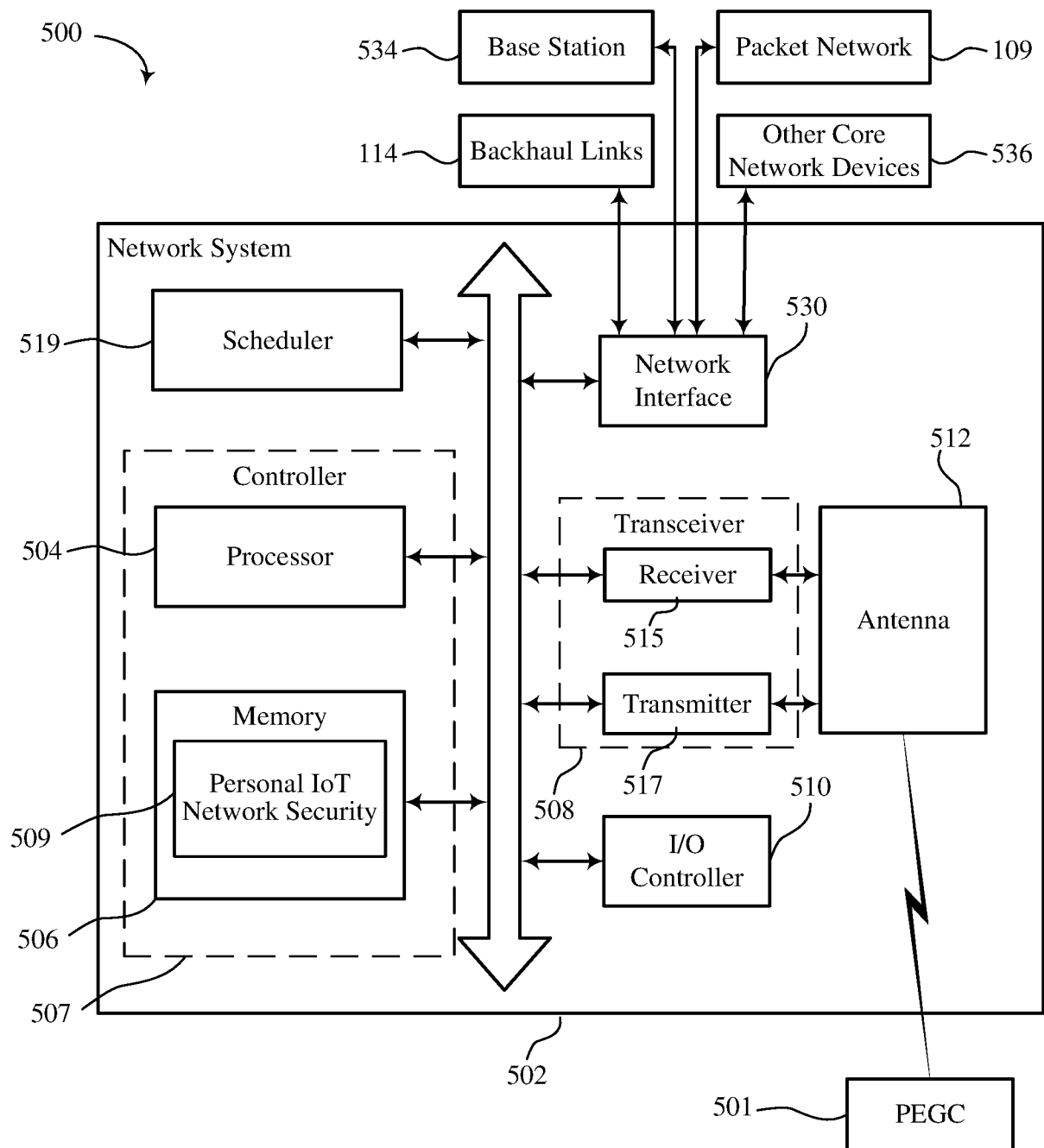
**FIG. 2**

**FIG. 3**

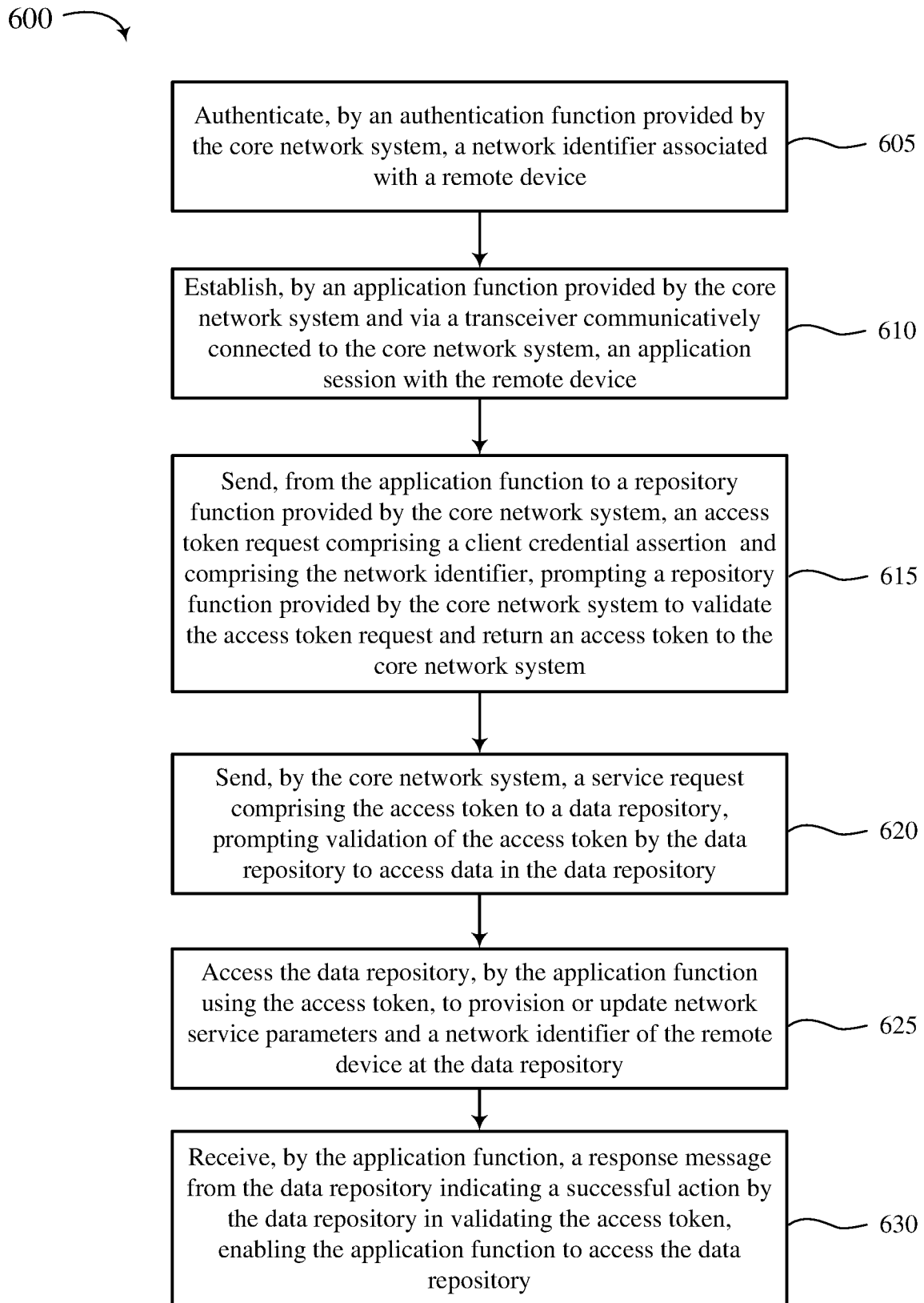
4/7

**FIG. 4**

5/7

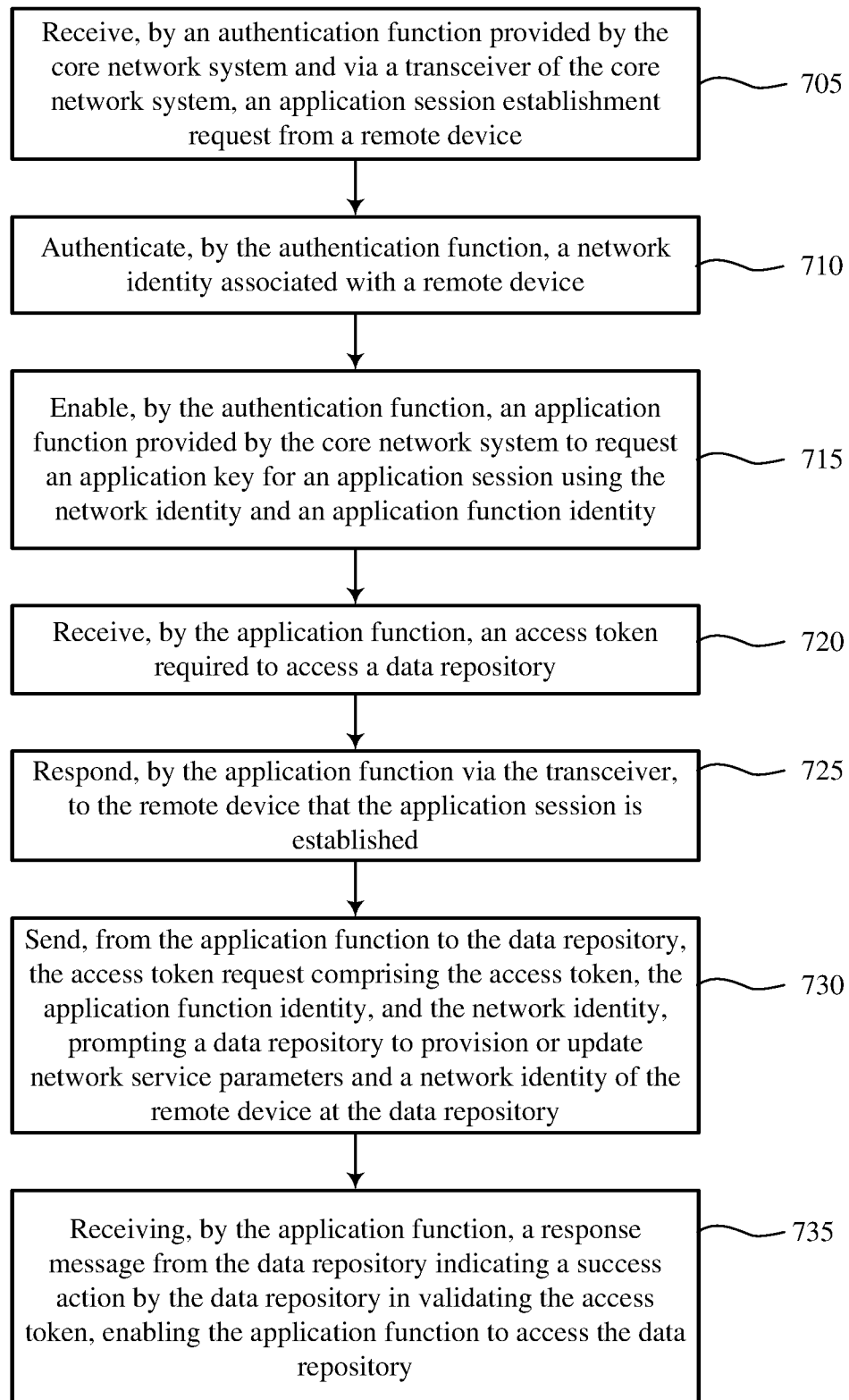
**FIG. 5**

6/7

**FIG. 6**

7/7

700

**FIG. 7**

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2024/051228

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L9/40 H04W12/06 H04L67/14
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04W

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, COMPENDEX, INSPEC, 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 Y	WO 2020/141355 A1 (ERICSSON TELEFON AB L M [SE]) 9 July 2020 (2020-07-09) paragraph [0003] - paragraph [0004] paragraph [0009] - paragraph [0015] paragraph [0050] paragraph [0138] - paragraph [0144] paragraph [0154] - paragraph [0157] figures 1, 2, 3, 12-14 ----- -/--	1, 8, 10-13, 20 2-7, 9, 14-19



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

16 April 2024

Date of mailing of the international search report

26/04/2024

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Cankaya, Sukru

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2024/051228

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on architecture enhancements for Personal IoT Network (PIN) (Release 18)", 3GPP STANDARD; TECHNICAL REPORT; 3GPP TR 23.700-88, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , no. V0.3.0 27 May 2022 (2022-05-27), pages 1-113, XP052182985, Retrieved from the Internet: URL:https://ftp.3gpp.org/Specs/archive/23_series/23.700-88/23700-88-030.zip draft_23700-88-030-rm.docx [retrieved on 2022-05-27] page 16 - page 17 page 37 - page 39 Page 43, "6.6.2.2 PINE authentication and registration" Page 45, "6.7.2 Procedures" Pages 84-85, "6.22.1 Description" -----	2-7, 9, 14-19
A	NOKIA ET AL: "New solution to KI#1: EAP based PIN device authentication using AKMA", 3GPP DRAFT; S3-222571, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG3, no. e-meeting; 20221010 - 20221014 3 October 2022 (2022-10-03), XP052271483, Retrieved from the Internet: URL:https://ftp.3gpp.org/tsg_sa/WG3_Security/TSGS3_108e-AdHoc/Docs/S3-222571.zip S3-222571 pCR solution to KI#1 using AKMA for EAP PIN device authentication.doc [retrieved on 2022-10-03] the whole document -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2024/051228

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2020141355	A1	09-07-2020	NONE