



(51) International Patent Classification:

H04W 76/11 (2018.01) H04L 12/06 (2006.01)

(21) International Application Number:

PCT/IB2023/052314

(22) International Filing Date:

10 March 2023 (10.03.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/319,895 15 March 2022 (15.03.2022) 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, 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.

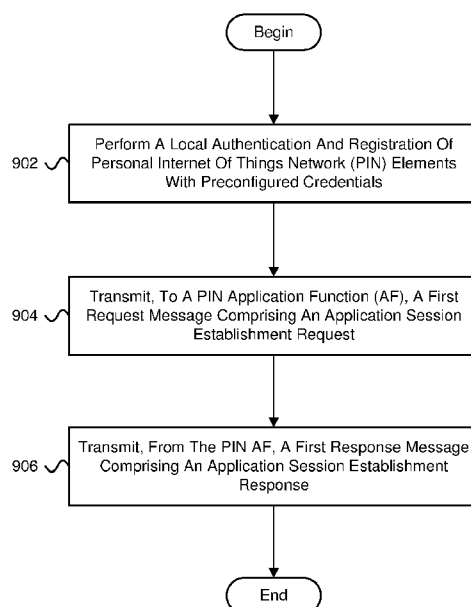
(84) Designated States (unless otherwise indicated, for every

kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, 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,

(54) Title: ESTABLISHING AN APPLICATION SESSION CORRESPONDING TO A PIN ELEMENT

900

FIG. 9



(57) Abstract: Apparatuses, methods, and systems are disclosed for establishing an application session corresponding to a personal internet of things network ("PIN") element. One method (900) includes performing (902), at a first network device, a local authentication and registration of PIN elements with preconfigured credentials. The method (900) includes transmitting (904), to a PIN application function ("AF"), a first request message including an application session establishment request. The method (900) includes transmitting (906), from the PIN AF, a first response message including an application session establishment response.

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))*

ESTABLISHING AN APPLICATION SESSION CORRESPONDING TO A PIN ELEMENT

FIELD

[0001] The subject matter disclosed herein relates generally to wireless communications
5 and more particularly relates to establishing an application session corresponding to a personal
internet of things network (“PIN”) element.

BACKGROUND

[0002] In certain wireless communications networks, PIN elements may be used. In such
networks, communication between PIN elements may be limited.

BRIEF SUMMARY

[0003] Methods for establishing an application session corresponding to a PIN element are
disclosed. Apparatuses and systems also perform the functions of the methods. One embodiment
of a method includes performing, at a first network device, a local authentication and registration
of PIN elements with preconfigured credentials. In some embodiments, the method includes
15 transmitting, to a PIN application function (“AF”), a first request message including an application
session establishment request. In certain embodiments, the method includes transmitting, from
the PIN AF, a first response message including an application session establishment response.

[0004] One apparatus for establishing an application session corresponding to a PIN
element includes a first network device. In some embodiments, the apparatus includes a processor.
20 In various embodiments, the apparatus includes a transceiver coupled to the processor. In certain
embodiments, the processor performs a local authentication and registration of PIN elements with
preconfigured credentials. In some embodiments, the transceiver transmits, to a PIN AF, a first
request message including an application session establishment request. In various embodiments,
the transceiver transmits, from the PIN AF, a first response message including an application
25 session establishment response.

[0005] Another embodiment of a method for establishing an application session
corresponding to a PIN element includes receiving, at a PIN AF from a first network device, a first
request message including an application session establishment request. In some embodiments,
the method includes transmitting, to a second network device, a second request message including
30 a Naanf_AKMA_ApplicationKey_Get request. In certain embodiments, the method includes
receiving, from the second network device, a first response message including a
Naanf_AKMA_ApplicationKey_Get response. The first response message includes a list of
managed PIN element identifiers (“IDs”) and their corresponding binding policies. In various

embodiments, the method includes transmitting, to the first network device, a second response message including an application session establishment response.

[0006] Another apparatus for establishing an application session corresponding to a PIN element includes a PIN AF. In some embodiments, the apparatus includes a processor. In various
5 embodiments, the apparatus includes a transceiver coupled to the processor. In certain embodiments, the transceiver receives, from a first network device, a first request message including an application session establishment request. In some embodiments, the transceiver transmits, to a second network device, a second request message including a Naanf_AKMA_ApplicationKey_Get request. In various embodiments, the transceiver receives,
10 from the second network device, a first response message including a Naanf_AKMA_ApplicationKey_Get response. In certain embodiments, the first response message includes a list of managed PIN element IDs and their corresponding binding policies. In some embodiments, the transceiver transmits, to the first network device, a second response message including an application session establishment response.

15 [0007] A further embodiment of a method for establishing an application session corresponding to a PIN element includes performing, at a PIN element, a local authentication and registration of the PIN element with preconfigured credentials. In some embodiments, the method includes sending a request to a first network device for sending data to a second device outside the local network.

20 [0008] A further apparatus for establishing an application session corresponding to a PIN element includes a PIN element. In some embodiments, the apparatus includes a transceiver. In various embodiments, the apparatus includes a processor coupled to the transceiver. In certain embodiments, the transceiver performs a local authentication and registration of the PIN element with preconfigured credentials. In some embodiments, the transceiver sends a request to a first
25 network device for sending data to a second device outside the local network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] A more particular description of the embodiments briefly described above will be rendered by reference to specific embodiments that are illustrated in the appended drawings. Understanding that these drawings depict only some embodiments and are not therefore to be
30 considered to be limiting of scope, the embodiments will be described and explained with additional specificity and detail through the use of the accompanying drawings, in which:

[0010] Figure 1 is a schematic block diagram illustrating one embodiment of a wireless communication system for establishing an application session corresponding to a PIN element;

[0011] Figure 2 is a schematic block diagram illustrating one embodiment of an apparatus that may be used for establishing an application session corresponding to a PIN element;

[0012] Figure 3 is a schematic block diagram illustrating one embodiment of an apparatus that may be used for establishing an application session corresponding to a PIN element;

5 [0013] Figure 4 is a schematic block diagram illustrating one embodiment of a system including PIN elements;

[0014] Figure 5 is a schematic block diagram illustrating one embodiment of a system for an authentication and key management for applications (“AKMA”) anchor function (“AAnF”) provisioning at primary authentication;

10 [0015] Figure 6 is a schematic block diagram illustrating one embodiment of a system for PIN AF provisioning at application session establishment;

[0016] Figure 7 is a schematic block diagram illustrating one embodiment of a system for a PIN element binding policy update;

15 [0017] Figure 8 is a schematic block diagram illustrating one embodiment of a system for binding PIN elements inside and outside a PIN;

[0018] Figure 9 is a flow chart diagram illustrating one embodiment of a method for establishing an application session corresponding to a PIN element; and

[0019] Figure 10 is a flow chart diagram illustrating another embodiment of a method for establishing an application session corresponding to a PIN element; and

20 [0020] Figure 11 is a flow chart diagram illustrating a further embodiment of a method for establishing an application session corresponding to a PIN element.

DETAILED DESCRIPTION

[0021] As will be appreciated by one skilled in the art, aspects of the embodiments may be embodied as a system, apparatus, method, or program product. Accordingly, embodiments may
25 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 all generally be referred to herein as a “circuit,” “module” or “system.” Furthermore, embodiments may take the form of a program product embodied in one or more computer readable storage devices storing machine readable code, computer readable code, and/or
30 program code, referred hereafter as code. The storage devices may be tangible, non-transitory, and/or non-transmission. The storage devices may not embody signals. In a certain embodiment, the storage devices only employ signals for accessing code.

[0022] Certain of the functional units described in this specification may be labeled as modules, in order to more particularly emphasize their implementation independence. For

example, a module may be implemented as a hardware circuit comprising custom very-large-scale integration (“VLSI”) circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic,
5 programmable logic devices or the like.

[0023] Modules may also be implemented in code and/or software for execution by various types of processors. An identified module of code may, for instance, include one or more physical or logical blocks of executable code which may, for instance, be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located
10 together, but may include disparate instructions stored in different locations which, when joined logically together, include the module and achieve the stated purpose for the module.

[0024] Indeed, a module of code may be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices. Similarly, operational data may be identified and illustrated herein
15 within modules, and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different computer readable storage devices. Where a module or portions of a module are implemented in software, the software portions are stored on one or more computer readable storage devices.

[0025] Any combination of one or more computer readable medium may be utilized. The
20 computer readable medium may be a computer readable storage medium. The computer readable storage medium may be a storage device storing the code. The storage device may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, holographic, micromechanical, or semiconductor system, apparatus, or device, or any suitable combination of
25 the foregoing.

[0026] More specific examples (a non-exhaustive list) of the storage device would include the following: an electrical connection having one or more wires, 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 portable compact disc read-
30 only memory (“CD-ROM”), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[0027] Code for carrying out operations for embodiments may be any number of lines and may be written in any combination of one or more programming languages including an object oriented programming language such as Python, Ruby, Java, Smalltalk, C++, or the like, and conventional procedural programming languages, such as the "C" programming language, or the like, and/or machine languages such as assembly languages. The code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network ("LAN") or a wide area network ("WAN"), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0028] Reference throughout this specification to "one embodiment," "an embodiment," or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. Thus, appearances of the phrases "in one embodiment," "in an embodiment," and similar language throughout this specification may, but do not necessarily, all refer to the same embodiment, but mean "one or more but not all embodiments" unless expressly specified otherwise. The terms "including," "comprising," "having," and variations thereof mean "including but not limited to," unless expressly specified otherwise. An enumerated listing of items does not imply that any or all of the items are mutually exclusive, unless expressly specified otherwise. The terms "a," "an," and "the" also refer to "one or more" unless expressly specified otherwise.

[0029] Furthermore, the described features, structures, or characteristics of the embodiments may be combined in any suitable manner. In the following description, numerous specific details are provided, such as examples of programming, software modules, user selections, network transactions, database queries, database structures, hardware modules, hardware circuits, hardware chips, etc., to provide a thorough understanding of embodiments. One skilled in the relevant art will recognize, however, that embodiments may be practiced without one or more of the specific details, or with other methods, components, materials, and so forth. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of an embodiment.

[0030] Aspects of the embodiments are described below with reference to schematic flowchart diagrams and/or schematic block diagrams of methods, apparatuses, systems, and program products according to embodiments. It will be understood that each block of the schematic flowchart diagrams and/or schematic block diagrams, and combinations of blocks in the schematic

flowchart diagrams and/or schematic block diagrams, can be implemented by code. The code may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create
5 means for implementing the functions/acts specified in the schematic flowchart diagrams and/or schematic block diagrams block or blocks.

[0031] The code may also be stored in a storage device that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the storage device produce an article of manufacture including
10 instructions which implement the function/act specified in the schematic flowchart diagrams and/or schematic block diagrams block or blocks.

[0032] The code may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such
15 that the code which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0033] The schematic flowchart diagrams and/or schematic block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of apparatuses,
20 systems, methods and program products according to various embodiments. In this regard, each block in the schematic flowchart diagrams and/or schematic block diagrams may represent a module, segment, or portion of code, which includes one or more executable instructions of the code for implementing the specified logical function(s).

[0034] It should also be noted that, in some alternative implementations, the functions
25 noted in the block may occur out of the order noted in the Figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. Other steps and methods may be conceived that are equivalent in function, logic, or effect to one or more blocks, or portions thereof, of the illustrated Figures.

30 [0035] Although various arrow types and line types may be employed in the flowchart and/or block diagrams, they are understood not to limit the scope of the corresponding embodiments. Indeed, some arrows or other connectors may be used to indicate only the logical flow of the depicted embodiment. For instance, an arrow may indicate a waiting or monitoring period of unspecified duration between enumerated steps of the depicted embodiment. It will also

be noted that each block of the block diagrams and/or flowchart diagrams, and combinations of blocks in the block diagrams and/or flowchart diagrams, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and code.

5 [0036] The description of elements in each figure may refer to elements of proceeding figures. Like numbers refer to like elements in all figures, including alternate embodiments of like elements.

[0037] Figure 1 depicts an embodiment of a wireless communication system 100 for establishing an application session corresponding to a PIN element. In one embodiment, the
10 wireless communication system 100 includes remote units 102 and network units 104. Even though a specific number of remote units 102 and network units 104 are depicted in Figure 1, one of skill in the art will recognize that any number of remote units 102 and network units 104 may be included in the wireless communication system 100.

[0038] In one embodiment, the remote units 102 may include computing devices, such as
15 desktop computers, laptop computers, personal digital assistants (“PDAs”), tablet computers, smart phones, smart televisions (e.g., televisions connected to the Internet), set-top boxes, game consoles, security systems (including security cameras), vehicle on-board computers, network devices (e.g., routers, switches, modems), aerial vehicles, drones, or the like. In some embodiments, the remote units 102 include wearable devices, such as smart watches, fitness bands,
20 optical head-mounted displays, or the like. Moreover, the remote units 102 may be referred to as subscriber units, mobiles, mobile stations, users, terminals, mobile terminals, fixed terminals, subscriber stations, UE, user terminals, a device, or by other terminology used in the art. The remote units 102 may communicate directly with one or more of the network units 104 via uplink (“UL”) communication signals. In certain embodiments, the remote units 102 may communicate
25 directly with other remote units 102 via sidelink communication.

[0039] The network units 104 may be distributed over a geographic region. In certain embodiments, a network unit 104 may also be referred to and/or may include one or more of an access point, an access terminal, a base, a base station, a location server, a core network (“CN”), a radio network entity, a Node-B, an evolved node-B (“eNB”), a 5G node-B (“gNB”), a Home
30 Node-B, a relay node, a device, a core network, an aerial server, a radio access node, an access point (“AP”), new radio (“NR”), a network entity, an access and mobility management function (“AMF”), a unified data management (“UDM”), a unified data repository (“UDR”), a UDM/UDR, a policy control function (“PCF”), a radio access network (“RAN”), a network slice selection function (“NSSF”), an operations, administration, and management (“OAM”), a session

management function (“SMF”), a user plane function (“UPF”), an application function, an authentication server function (“AUSF”), security anchor functionality (“SEAF”), trusted non-third generation partnership project (“3GPP”) gateway function (“TNGF”), or by any other terminology used in the art. The network units 104 are generally part of a radio access network that includes one or more controllers communicably coupled to one or more corresponding network units 104. The radio access network is generally communicably coupled to one or more core networks, which may be coupled to other networks, like the Internet and public switched telephone networks, among other networks. These and other elements of radio access and core networks are not illustrated but are well known generally by those having ordinary skill in the art.

[0040] In one implementation, the wireless communication system 100 is compliant with NR protocols standardized in 3GPP, wherein the network unit 104 transmits using an orthogonal frequency division multiplexing (“OFDM”) modulation scheme on the downlink (“DL”) and the remote units 102 transmit on the UL using a single-carrier frequency division multiple access (“SC-FDMA”) scheme or an OFDM scheme. More generally, however, the wireless communication system 100 may implement some other open or proprietary communication protocol, for example, WiMAX, institute of electrical and electronics engineers (“IEEE”) 802.11 variants, global system for mobile communications (“GSM”), general packet radio service (“GPRS”), universal mobile telecommunications system (“UMTS”), long term evolution (“LTE”) variants, code division multiple access 2000 (“CDMA2000”), Bluetooth®, ZigBee, Sigfox, among other protocols. The present disclosure is not intended to be limited to the implementation of any particular wireless communication system architecture or protocol.

[0041] The network units 104 may serve a number of remote units 102 within a serving area, for example, a cell or a cell sector via a wireless communication link. The network units 104 transmit DL communication signals to serve the remote units 102 in the time, frequency, and/or spatial domain.

[0042] In various embodiments, a network unit 104 may perform, at a first network device, a local authentication and registration of PIN elements with preconfigured credentials. In some embodiments, the network unit 104 may transmit, to a PIN AF, a first request message including an application session establishment request. In certain embodiments, the network unit 104 may transmit, from the PIN AF, a first response message including an application session establishment response. Accordingly, the network unit 104 may be used for establishing an application session corresponding to a PIN element.

[0043] In certain embodiments, a network unit 104 may receive, at a PIN AF from a first network device, a first request message including an application session establishment request. In

some embodiments, the network unit 104 may transmit, to a second network device, a second request message including a Naanf_AKMA_ApplicationKey_Get request. In certain embodiments, the network unit 104 may receive, from the second network device, a first response message including a Naanf_AKMA_ApplicationKey_Get response. The first response message includes a list of managed PIN element IDs and their corresponding binding policies. In various embodiments, the network unit 104 may transmit, to the first network device, a second response message including an application session establishment response. Accordingly, the network unit 104 may be used for establishing an application session corresponding to a PIN element.

[0044] In some embodiments, a remote unit 102 and/or a network unit 104 may perform, at a PIN element, a local authentication and registration of the PIN element with preconfigured credentials. In some embodiments, the remote unit 102 and/or the network unit 104 may send a request to a first network device for sending data to a second device outside the local network. Accordingly, the remote unit 102 and/or the network unit 104 may be used for establishing an application session corresponding to a PIN element.

[0045] Figure 2 depicts one embodiment of an apparatus 200 that may be used for establishing an application session corresponding to a PIN element. The apparatus 200 includes one embodiment of the remote unit 102. Furthermore, the remote unit 102 may include a processor 202, a memory 204, an input device 206, a display 208, a transmitter 210, and a receiver 212. In some embodiments, the input device 206 and the display 208 are combined into a single device, such as a touchscreen. In certain embodiments, the remote unit 102 may not include any input device 206 and/or display 208. In various embodiments, the remote unit 102 may include one or more of the processor 202, the memory 204, the transmitter 210, and the receiver 212, and may not include the input device 206 and/or the display 208.

[0046] The processor 202, in one embodiment, may include any known controller capable of executing computer-readable instructions and/or capable of performing logical operations. For example, the processor 202 may be a microcontroller, a microprocessor, a central processing unit ("CPU"), a graphics processing unit ("GPU"), an auxiliary processing unit, a field programmable gate array ("FPGA"), or similar programmable controller. In some embodiments, the processor 202 executes instructions stored in the memory 204 to perform the methods and routines described herein. The processor 202 is communicatively coupled to the memory 204, the input device 206, the display 208, the transmitter 210, and the receiver 212.

[0047] The memory 204, in one embodiment, is a computer readable storage medium. In some embodiments, the memory 204 includes volatile computer storage media. For example, the memory 204 may include a RAM, including dynamic RAM ("DRAM"), synchronous dynamic

RAM (“SDRAM”), and/or static RAM (“SRAM”). In some embodiments, the memory 204 includes non-volatile computer storage media. For example, the memory 204 may include a hard disk drive, a flash memory, or any other suitable non-volatile computer storage device. In some embodiments, the memory 204 includes both volatile and non-volatile computer storage media.

5 In some embodiments, the memory 204 also stores program code and related data, such as an operating system or other controller algorithms operating on the remote unit 102.

[0048] The input device 206, in one embodiment, may include any known computer input device including a touch panel, a button, a keyboard, a stylus, a microphone, or the like. In some embodiments, the input device 206 may be integrated with the display 208, for example, as a

10 touchscreen or similar touch-sensitive display. In some embodiments, the input device 206 includes a touchscreen such that text may be input using a virtual keyboard displayed on the touchscreen and/or by handwriting on the touchscreen. In some embodiments, the input device 206 includes two or more different devices, such as a keyboard and a touch panel.

[0049] The display 208, in one embodiment, may include any known electronically

15 controllable display or display device. The display 208 may be designed to output visual, audible, and/or haptic signals. In some embodiments, the display 208 includes an electronic display capable of outputting visual data to a user. For example, the display 208 may include, but is not limited to, a liquid crystal display (“LCD”), a light emitting diode (“LED”) display, an organic light emitting diode (“OLED”) display, a projector, or similar display device capable of outputting

20 images, text, or the like to a user. As another, non-limiting, example, the display 208 may include a wearable display such as a smart watch, smart glasses, a heads-up display, or the like. Further, the display 208 may be a component of a smart phone, a personal digital assistant, a television, a table computer, a notebook (laptop) computer, a personal computer, a vehicle dashboard, or the like.

25 [0050] In certain embodiments, the display 208 includes one or more speakers for producing sound. For example, the display 208 may produce an audible alert or notification (e.g., a beep or chime). In some embodiments, the display 208 includes one or more haptic devices for producing vibrations, motion, or other haptic feedback. In some embodiments, all or portions of the display 208 may be integrated with the input device 206. For example, the input device 206

30 and display 208 may form a touchscreen or similar touch-sensitive display. In other embodiments, the display 208 may be located near the input device 206.

[0051] Although only one transmitter 210 and one receiver 212 are illustrated, the remote unit 102 may have any suitable number of transmitters 210 and receivers 212. The transmitter 210

and the receiver 212 may be any suitable type of transmitters and receivers. In one embodiment, the transmitter 210 and the receiver 212 may be part of a transceiver.

[0052] In certain embodiments, the transceiver performs a local authentication and registration of the PIN element with preconfigured credentials. In some embodiments, the transceiver sends a request to a first network device for sending data to a second device outside the local network.

[0053] Figure 3 depicts one embodiment of an apparatus 300 that may be used for establishing an application session corresponding to a PIN element. The apparatus 300 includes one embodiment of the network unit 104. Furthermore, the network unit 104 may include a processor 302, a memory 304, an input device 306, a display 308, a transmitter 310, and a receiver 312. As may be appreciated, the processor 302, the memory 304, the input device 306, the display 308, the transmitter 310, and the receiver 312 may be substantially similar to the processor 202, the memory 204, the input device 206, the display 208, the transmitter 210, and the receiver 212 of the remote unit 102, respectively.

[0054] In certain embodiments, the processor 302 performs a local authentication and registration of PIN elements with preconfigured credentials. In some embodiments, the transceiver transmits, to a PIN AF, a first request message including an application session establishment request. In various embodiments, the transceiver transmits, from the PIN AF, a first response message including an application session establishment response.

[0055] In some embodiments, the transceiver receives, from a first network device, a first request message including an application session establishment request. In some embodiments, the transceiver transmits, to a second network device, a second request message including a Naanf_AKMA_ApplicationKey_Get request. In various embodiments, the transceiver receives, from the second network device, a first response message including a Naanf_AKMA_ApplicationKey_Get response. In certain embodiments, the first response message includes a list of managed PIN element IDs and their corresponding binding policies. In some embodiments, the transceiver transmits, to the first network device, a second response message including an application session establishment response.

[0056] In various embodiments, the transceiver performs a local authentication and registration of the PIN element with preconfigured credentials. In some embodiments, the transceiver sends a request to a first network device for sending data to a second device outside the local network.

[0057] It should be noted that two or more embodiments described herein may be combined together. In certain embodiments, security may be used by a device for authentication,

authorization, data protection, and registration to a mobile core network. In some embodiments, there may be security protection and access control that indicates 1) how a fifth generation system (“5GS”) supports secure protection for communications between personal internet of things (“IoT”) network (“PIN”) elements (e.g., via a PIN element with gateway capabilities (“PEGC”) or
5 via fifth generation core (“5GC”), or for communications between PIN elements and PEGC; and/or 2) gap analysis on how a 5GS supports mitigation of repeated and unauthorized attempts to access PIN elements (e.g., the from internet, or from other PIN elements via a PEGC).

[0058] In various embodiments, for binding PIN elements inside a PIN with those outside in a data network (“DN”), there may be a mechanism to establish communication between PIN
10 elements. In such embodiments, the PIN elements may have 3GPP credentials but may also not have 3GPP credentials. Moreover, there may be direct communication between PIN elements inside and outside a PIN where a PIN element may not have 3GPP credentials.

[0059] In certain embodiments, PIN elements may connect to a non-3GPP network. In some embodiments, there may be different trust relationships with a non-3GPP access network
15 (e.g., trusted, untrusted access) as well as different device capabilities (e.g., devices with 3GPP credentials with non-access stratum (NAS) capabilities, without NAS capabilities, behind a residential gateway or direct connection to the non-3GPP access point (“AP”).

[0060] In some embodiments, there may be a direct communication (e.g., an IP multimedia system (“IMS”) voice and/or video session) with devices that both have 3GPP credentials and are
20 registered in a mobile network. However, the PIN elements may not have 3GPP credentials for a registration to a mobile core network.

[0061] In various embodiments, there may be local registration and/or authentication at a gateway in a personal network for devices with and without 3GPP credentials. In certain embodiments, there may be registration of devices without 3GPP credentials in a 5GC and/or data
25 connectivity for those devices explicitly with operator controlled traffic connection configuration. In some embodiment, devices without 3GPP credentials are limited to a residential gateway and not to end user devices (e.g., PIN elements). In various embodiments, a local binding for a direct communication within a local personal network may be performed and a service request procedure for data access to a DN via a 5GC may be made.

[0062] Figure 4 is a schematic block diagram illustrating one embodiment of a system 400
30 including PIN elements. The system 400 includes a PIN element #A 402 (e.g., motion sensor) that communicates a trigger to a PIN element #B 404 (e.g., surveillance camera). The PIN element #A 402 sends a motion detected (e.g., via locally encrypted commands) signal to a PIN element with management capabilities 406. Further, the PIN element #B 404 sends data to a PIN element with

gateway capabilities 408. Moreover, the PIN element with management capabilities 406 provides a list of registered PIN elements to the PIN element with gateway capabilities 408. Also, the PIN element with management capabilities 406 provides an indication to turn a light switch (e.g., via locally encrypted commands) on to a PIN element #C 410 (e.g., light). The PIN element with gateway capabilities 408 sends information to a 5GC 412, and the 5GC 412 sends information to a PIN element #D 414 (e.g., smartphone). After all PIN elements are locally authenticated and registered, the PIN element with gateway capabilities 408 registers all the local PIN elements in the fifth generation (“5G”) core network (“CN”).

[0063] In certain embodiments there may be: 1) local registration and authentication with PIN elements without 3GPP credentials at a PIN element with management capabilities (“PEMC”) and/or PEGC (“PEMC/PEGC”) in a PIN; 2) registration of the PEMC and/or PEGC in a 5GC including local authenticated PIN elements without 3GPP credentials; 3) registration of PIN elements with 3GPP credentials locally and in the 5GC; 4) binding of local PIN elements; and/or 5) a service request for PIN elements without 3GPP credentials to send data via the 5GC.

[0064] In some embodiments, a PEMC and a PEGC may be collocated as one function within a same entity or may be implemented as two separate functions. The PEMC and/or the PEGC may be considered as a user equipment (“UE”) from the 5GC point of view with additional capabilities (e.g., registration of local PIN elements without 3GPP credentials to the 5GC).

[0065] In a first embodiment, there may be PIN application function (“AF”) provisioning.

[0066] In various embodiments, there may be provisioning of PIN related information at a time of PEMC/PEGC registration to a 5GC which triggers an AKMA key generation procedure. In such embodiments, an AAnF is provided with a list of managed PIN element IDs and operator PIN policies for this PEMC/PEGC in addition to AKMA information.

[0067] Figure 5 is a schematic block diagram illustrating one embodiment of a system 500 for AAnF provisioning at primary authentication. The system 500 includes a PEMC/PEGC 502, an AMF 504, an AUSF 506, a UDM 508, and an AAnF 510. Each of the communications in the system 500 may include one or more messages.

[0068] In a first communication 512, during a primary authentication procedure 514, the AUSF 506 interacts with the UDM 508 to fetch authentication information such as subscription credentials (e.g., authentication and key agreement (“AKA”) authentication vectors) and an authentication method using a Nudm_UEAuthentication_Get request service operation (e.g., the message may include subscription permanent identifier (“SUPI”) and/or subscription concealed identifier (“SUCI”). The address of a PIN AF for binding PIN elements inside a PIN with those

outside a PIN may be preconfigured in the PEMC/PEGC 502 or provisioned during primary authentication.

[0069] In a second communication 516, in a response which may include a Nudm_UEAuthentication_Get response, the UDM 508 may indicate to the AUSF 506 whether
5 AKMA anchor keys need to be generated for the PEMC/PEGC 502. If an AKMA indicator (e.g., AKMA Ind) is included, the UDM 508 may include an RID of the PEMC/PEGC 502 as well as a list of managed PIN element IDs and operator PIN policies for binding PIN elements. An authentication vector ("AV") may also be included in the response.

[0070] If the AUSF 506 receives the AKMA indication from the UDM 508, the AUSF 506
10 stores the K_{AUSF} , and generates 520 the AKMA anchor key (K_{AKMA}) and generates 524 an AKMA key identifier ("ID") ("A-KID") from K_{AUSF} after the primary authentication procedure is successfully completed. Moreover, the PEMC/PEGC 502 generates 518 the K_{AKMA} and generated 522 the A-KID from the K_{AUSF} before initiating communication with an AKMA application function.

[0071] In a third communication 526, after AKMA key material is generated, the AUSF
15 selects the AAnF 510, and sends the generated A-KID, and K_{AKMA} to the AAnF 510 together with the SUPI of the PEMC/PEGC 502 using the Naanf_AKMA_KeyRegistration request service operation. The transmission to the AAnF 510 includes the list of managed PIN elements IDs and the operator PIN policies for binding PIN elements. The AAnF 510 may store the latest
20 information sent by the AUSF. It should be noted that the AUSF 506 need not store any AKMA key material after delivery to the AAnF 510. Moreover, when re-authentication runs, the AUSF 506 generates a new A-KID, and a new K_{AKMA} and sends the new generated A-KID and K_{AKMA} to the AAnF 510. After receiving the new generated A-KID and K_{AKMA} , the AAnF 510 deletes the old A-KID and K_{AKMA} and stores the new generated A-KID and K_{AKMA} .

[0072] In a fourth communication 528, the AAnF 510 sends a response to the AUSF 506
25 using a Naanf_AKMA_AnchorKey_Register response service operation.

[0073] In some embodiments, the A-KID identifies the K_{AKMA} key of a UE. Moreover, the A-KID may be in a network access identifier ("NAI") format (e.g., username@realm). The username part may include an RID and an AKMA temporary UE ID ("A-TID"), and the realm
30 part may include a home network identifier. Further, the A-TID may be derived from K_{AUSF} . The AUSF may use the RID received from the UDM 508 to derive A-KID.

[0074] In various embodiments, K_{AKMA} may be derived from K_{AUSF} . Since K_{AKMA} and A-TID in A-KID are both derived from K_{AUSF} based on a primary authentication run, the K_{AKMA} and A-KID may only be refreshed by a new successful primary authentication. Once a PEMC/PEGC

connects to a PIN AF for establishment of a binding service, the AKMA procedures for the application session establishment may be carried out. The whole communication may also take place via a network exposure function (“NEF”).

[0075] Figure 6 is a schematic block diagram illustrating one embodiment of a system 600 for PIN AF provisioning at application session establishment. The system 600 includes a PEMC/PEGC 602, an AUSF 604, an AAnF 606, and a PIN AF 608. Each of the communications in the system 600 may include one or more messages.

[0076] In certain embodiments, before communication between the PEMC/PEGC 602 and an AKMA AF (or the PIN AF 708) can start, the PEMC/PEGC 602 and the AKMA AF needs to know whether to use AKMA. This knowledge may be implicit to a specific application on the PEMC/PEGC 602 and the AKMA AF or indicated by the AKMA AF to the PEMC/PEGC 602.

[0077] In a first communication 610, there may be a primary authentication and establishment of K_{AKMA} .

[0078] In a second communication 612, the PEMC/PEGC 602 may generate an AKMA anchor key (K_{AKMA}) and the A-KID from the K_{AUSF} before initiating communication with an AKMA application function (“AF”) and/or PIN AF 608. When the PEMC/PEGC 602 initiates communication with the PIN AF 608, it may include the derived A-KID in an application session establishment request message. The PEMC/PEGC 602 may derive K_{AF} before sending the message or afterwards. The PEMC/PEGC 602 may include its PIN element ID.

[0079] In a third communication 614, if the PIN AF 608 does not have an active context associated with the A-KID, then the PIN AF 608 selects the AAnF 606 and sends a Naanf_AKMA_ApplicationKey_Get request message to the AAnF 606 with the A-KID to request the K_{AF} for the PEMC/PEGC 602. The PIN AF 608 may also include its identity (AF_ID) in the request. In some embodiments, AF_ID consists of a fully qualified domain name (“FQDN”) of the PIN AF 608 and the Ua* security protocol identifier. The Ua* security protocol identifier identifies a security protocol that the PIN AF 608 will use with the PEMC/PEGC 602.

[0080] In various embodiments, the AAnF 606 may check whether the AAnF 606 can provide a service to the PIN AF 608 based on a configured local policy or based on an authorization information or policy provided by a network repository function (“NRF”) using the AF_ID. If it succeeds, the following procedures are executed. Otherwise, the AAnF 606 may reject the procedure. Moreover, the AAnF 606 may verify whether the subscriber is authorized to use AKMA based on the presence of the PEMC/PEGC 602 specific K_{AKMA} key identified by the A-KID. If K_{AKMA} is present in the AAnF 606, the AAnF 606 may continue with step 616. If K_{AKMA} is not present in the AAnF 606, the AAnF 606 may continue with step 618 with an error response.

[0081] The AAnF 606 derives 616 an AKMA application key (K_{AF}) from K_{AKMA} if it does not already have K_{AF} .

[0082] In a fourth communication 618, the AAnF 606 sends a Naanf_AKMA_ApplicationKey_Get response to the PIN AF 608 with SUPI, K_{AF} , a K_{AF} expiration time, a list of managed PIN elements IDs, and/or operator PIN policies for binding PIN elements.

[0083] In a fifth communication 620, the PIN AF 608 sends an application session establishment response to the PEMC/PEGC 602. If the information in step 618 indicates failure of the AKMA key request, the PIN AF 608 may reject the application session establishment by including a failure cause. Afterwards, the PEMC/PEGC 602 may trigger a new application session establishment request with the latest A-KID to the PIN AF 608.

[0084] In a second embodiment, there may be a PEMC/PEGC local policy update at a PIN AF. After the PEMC/PEGC performs an application session establishment procedure and created a protected connection to a PIN AF, the PEMC/PEGC may provide its local authenticated PIN element IDs and its local binding policies to the PIN AF.

[0085] Figure 7 is a schematic block diagram illustrating one embodiment of a system 700 for a PIN element binding policy update. The system 700 includes a PEMC/PEGC 702, an AUSF 704, an AAnF 706, and a PIN AF 708. Each of the communications in the system 700 may include one or more messages.

[0086] In certain embodiments, before communication between the PEMC/PEGC 702 and an AKMA AF (or the PIN AF 708) can start, the PEMC/PEGC 702 and the AKMA AF needs to know whether to use AKMA. This knowledge may be implicit to a specific application on the PEMC/PEGC 702 and the AKMA AF or indicated by the AKMA AF to the PEMC/PEGC 702.

[0087] In a first communication 710, there may be a primary authentication and establishment of K_{AKMA} .

[0088] In a second communication 712, the PEMC/PEGC 702 may generate an AKMA anchor key (K_{AKMA}) and the A-KID from the K_{AUSF} before initiating communication with an AKMA application function ("AF") and/or PIN AF 708. When the PEMC/PEGC 702 initiates communication with the PIN AF 708, it may include the derived A-KID in an application session establishment request message. The PEMC/PEGC 702 may derive K_{AF} before sending the message or afterwards. The PEMC/PEGC 702 may include its PIN element ID.

[0089] In a third communication 714, if the PIN AF 708 does not have an active context associated with the A-KID, then the PIN AF 708 selects the AAnF 706 and sends a Naanf_AKMA_ApplicationKey_Get request message to the AAnF 706 with the A-KID to request

the K_{AF} for the PEMC/PEGC 702. The PIN AF 708 may also include its identity (AF_ID) in the request. In some embodiments, AF_ID consists of a fully qualified domain name ("FQDN") of the PIN AF 708 and the Ua* security protocol identifier. The Ua* security protocol identifier identifies a security protocol that the PIN AF 708 will use with the PEMC/PEGC 702.

5 [0090] In various embodiments, the AAnF 706 may check whether the AAnF 706 can provide a service to the PIN AF 708 based on a configured local policy or based on an authorization information or policy provided by a NRF using the AF_ID. If it succeeds, the following procedures are executed. Otherwise, the AAnF 706 may reject the procedure. Moreover, the AAnF 706 may verify whether the subscriber is authorized to use AKMA based on the presence of the
10 PEMC/PEGC 702 specific K_{AKMA} key identified by the A-KID. If K_{AKMA} is present in the AAnF 706, the AAnF 706 may continue with step 716. If K_{AKMA} is not present in the AAnF 706, the AAnF 706 may continue with step 718 with an error response.

[0091] The AAnF 706 derives 716 an AKMA application key (K_{AF}) from K_{AKMA} if it does not already have K_{AF} .

15 [0092] In a fourth communication 718, the AAnF 706 sends a Naanf_AKMA_ApplicationKey_Get response to the PIN AF 708 with SUPI, K_{AF} , a K_{AF} expiration time, a list of managed PIN elements IDs, and/or operator PIN policies for binding PIN elements.

[0093] In a fifth communication 720, the PIN AF 708 sends an application session
20 establishment response to the PEMC/PEGC 702. If the information in step 718 indicates failure of the AKMA key request, the PIN AF 708 may reject the application session establishment by including a failure cause. Afterwards, the PEMC/PEGC 702 may trigger a new application session establishment request with the latest A-KID to the PIN AF 708.

[0094] In a sixth communication 722, after the PEMC/PEGC 702 established a secure
25 connection with the PIN AF 708 based on the K_{AF} , the PEMC/PEGC 702 provides a PIN session binding policy request that may include a PEMC/PEGC PIN element ID, locally authenticated PIN element IDs, and local binding policies for the PIN AF 708.

[0095] The PIN AF 708 stores 724 the locally authenticated PIN element IDs and the local
30 binding policies and matches them with the list of managed PIN elements IDs and the operator PIN policies for the binding.

[0096] In a seventh communication 726, the PIN AF 708 acknowledges the PIN session binding request from the PEMC/PEGC 702 with a PIN session binding policy response.

[0097] In a third embodiment, there may be direct communication establishment between PIN elements inside and outside of a PIN. In such embodiments, there may be binding and linking

of two or more PIN elements together for a direct communication. A pre-requisite for this may be that the PIN element behind a PEMC/PEGC is registered to a PIN AF on behalf of the PEMC/PEGC or directly if the PIN element has 3GPP credentials and is able to perform an AKMA registration.

5 [0098] Figure 8 is a schematic block diagram illustrating one embodiment of a system 800 for binding PIN elements inside and outside a PIN. The system 800 includes a PIN element #B 802, a PEMC/PEGC 804, a PIN AF 806, and a PIN element #D 808 in DN. Each of the communications in the system 800 may include one or more messages.

[0099] The PEMC/PEGC 804 and the PIN Element #D 808 in the DN outside the PIN
10 perform 810 and 812 primary authentication and the establishment of K_{AKMA} for PIN services.

[0100] In a first communication 814 and in a second communication 816, the PEMC/PEGC 804 and the PIN element #D 808 perform an application session establishment procedure respectively (e.g., as described in the first embodiment and the second embodiment).

[0101] In a third communication 818, the PIN element #B 802 sends a request to send data
15 to PIN element #D 808 to the PEMC/PEGC 804.

[0102] The PEMC/PEGC 804 performs 820 a local authorization and checks whether the PIN Element #B 802 is locally authenticated and whether it is allowed to send data to the target PIN Element #D 808 based on the local configured policies or based on the operator managed policies.

20 [0103] In a fourth communication 822, the PEMC/PEGC 804 sends a data request to the PIN AF 806 including a A-TID of the PEMC/PEGC 804, a PEGC PIN element ID, and a target PIN element #D ID. The PEMC/PEGC 804 may be an endpoint of the communication from the PIN AF 806 point of view in case the PIN Element #B 802 does not have the capability to support the termination of the end to end communication. The PEMC/PEGC 804 may include the source
25 PIN element #B ID to indicate the origination of the request.

[0104] The PIN AF 806 checks 824 whether the target PIN element #D 808 is registered at the PIN AF 806 and checks the previously provisioned policies from the PEMC/PEGC 804 and the operator policies from an AAnF whether the PEMC, PEGC, and/or PIN element #B 802 is authorized to connect directly to the target PIN element #D 808. The PIN AF 806 derives a direct
30 communication key K_{DC} . The root key K_{root} which is input to the K_{DF} for the key derivation of the K_{DC} can be based on the keys available in the PIN AF 806, e.g., the PEMC, PEGC, and/or PIN element #B 802 or the target PIN element #D 808 session key K_{AF} or a concatenation of both keys K_{AF} as input root key. As an additional input to the K_{DF} , the following parameters may be used: IDs of the PIN elements to be paired (e.g., here PEMC, PEGC PIN element ID, PIN element #B

802, PIN element #D 808), but there may be more than two paired PIN elements), a NONCE, which may be a random number, a counter, and so forth. The PIN AF 806 generates an access token which is used to mutually authenticate the two PIN elements among each other. The access token may be an OAuth token or any other token. In the simplest case, it may be a sufficient long random number.

[0105] In a fifth communication 826, the PIN AF 806 sends the security key K_{DC} and the access token to the PEMC/PEGC 804 in a protected paring request message.

[0106] In a sixth communication 828, the PEMC/PEGC 804 may terminate the secure binding on the behalf of the PIN element #B 802, in case the PIN element #B 802 does not have the capabilities for it. In that case, the PEMC/PEGC 804 did not include the PIN element #B ID in the request in step 822. Otherwise, if the PIN element #B 802 is capable to terminate the end-to-end with the PIN element #D 808, then the PEMC/PEGC 804 forwards the security key K_{DC} and the access token to the PIN element #B 802.

[0107] In a seventh communication 830, the PIN AF 806 sends the security key K_{DC} and the access token to the PIN element #D 808 in a protected paring request message. The request includes the PEMC/PEGC 804 address and may include the PIN element #B ID.

[0108] In an eighth communication 832, the PEMC/PEGC 804 and/or PIN element #B and #D perform authentication between them by sending either the access token and verify it or performing a mutual exchange: the PEMC/PEGC 804 and/or PIN element #B sends an authentication message to PIN element #D 808, including a hash (e.g., secure hash algorithm ("SHA") 1 ("SHA1"), SHA 2 ("SHA2"), or SHA 3 ("SHA3") with their variants) of the access token and its PIN element ID. PIN element #D 808 receives the message and also performs a hash over the access token and the PEMC/PEGC 804 and/or PIN element #B ID (e.g., received previously from the PIN AF 806) and compares it with the value received from the PEMC/PEGC 804 and/or PIN element #B 802. If identical, the PIN element #D 808 sends also an authentication response with the hash of the access token and the PIN element #D ID, the receiving PEMC/PEGC 804 and/or PIN elements #B 802 then also computes the hash and compares it with the received one. Then the PEMC/PEGC 804 and/or PIN element #B 802 sets up a secure connection with the security key K_{DC} . This can be done either with an internet protocol ("IP") security ("IPsec") standalone ("SA") establishment or using a block cipher, for example.

[0109] In a ninth communication 834, a data response acknowledgment may be transmitted.

[0110] Figure 9 is a flow chart diagram illustrating one embodiment of a method 900 for establishing an application session corresponding to a PIN element. In some embodiments, the method 900 is performed by an apparatus, such as the network unit 104. In certain embodiments,

the method 900 may be performed by a processor executing program code, for example, a microcontroller, a microprocessor, a CPU, a GPU, an auxiliary processing unit, a FPGA, or the like.

[0111] In various embodiments, the method 900 includes performing 902, at a first network device, a local authentication and registration of PIN elements with preconfigured credentials. In some embodiments, the method 900 includes transmitting 904, to a PIN AF, a first request message including an application session establishment request. In certain embodiments, the method 900 includes transmitting 906, from the PIN AF, a first response message including an application session establishment response.

[0112] In certain embodiments, the method 900 further comprises transmitting, to the PIN AF, a second request message comprising a PIN session binding policy request, wherein the second request message comprises a list of authenticated PIN element IDs and corresponding binding policies. In some embodiments, the method 900 further comprises receiving, from the PIN AF, a second response message comprising a PIN session binding policy response. In various embodiments, the method 900 further comprises receiving a data send request from a locally registered PIN element.

[0113] In one embodiment, the method 900 further comprises transmitting, to the PIN AF, a third request message comprising a data request message an A-TID of the first network device, a (PEGC) PIN element ID, a target PIN element ID, a source PIN element ID, or some combination thereof. In certain embodiments, the method 900 further comprises receiving, from the PIN AF, a third response message comprising a data response message comprising a direct communication key (K_{DC}) and an access token.

[0114] In some embodiments, the method 900 further comprises transmitting a data send response to the locally registered PIN element, the data send response comprising the K_{DC} and the access token. In various embodiments, the first network device comprises a (PEGC), a (PEMC), or a combination thereof.

[0115] Figure 10 is a flow chart diagram illustrating another embodiment of a method 1000 for establishing an application session corresponding to a PIN element. In some embodiments, the method 1000 is performed by an apparatus, such as the network unit 104. In certain embodiments, the method 1000 may be performed by a processor executing program code, for example, a microcontroller, a microprocessor, a CPU, a GPU, an auxiliary processing unit, a FPGA, or the like.

[0116] In various embodiments, the method 1000 includes receiving 1002, at a PIN AF from a first network device, a first request message including an application session establishment

request. In some embodiments, the method 1000 includes transmitting 1004, to a second network device, a second request message including a Naanf_AKMA_ApplicationKey_Get request. In certain embodiments, the method 1000 includes receiving 1006, from the second network device, a first response message including a Naanf_AKMA_ApplicationKey_Get response. The first
5 response message includes a list of managed PIN element IDs and their corresponding binding policies. In various embodiments, the method 1000 includes transmitting 1008, to the first network device, a second response message including an application session establishment response.

[0117] In certain embodiments, the method 1000 further comprises receiving, from the first network device, a third request message comprising a PIN session binding policy request,
10 wherein the third request message comprises a list of authenticated PIN element IDs and corresponding binding policies. In some embodiments, the method 1000 further comprises storing the list of authenticated PIN element IDs and their corresponding binding policies. In various embodiments, the method 1000 further comprises matching the list of managed PIN element IDs and their corresponding binding policies to the list of authenticated PIN element IDs and their
15 corresponding binding policies.

[0118] In one embodiment, the method 1000 further comprises transmitting, to the first network device, a third response message comprising a PIN session binding policy response. In certain embodiments, the method 1000 further comprises receiving, from the first network device, a data request message, wherein the data request message comprises an A-TID of the first network
20 device, a (PEGC) PIN element ID, a target PIN element ID, a source PIN element ID, or some combination thereof. In some embodiments, the method 1000 further comprises determining a binding of source PIN elements and target PIN elements.

[0119] In various embodiments, the method 1000 further comprises determining a binding of two or more locally registered PIN elements. In one embodiment, the method 1000 further
25 comprises deriving a direct communication key (K_{DC}) and an access token.

[0120] In certain embodiments, the method 1000 further comprises transmitting, to the first network device, a protected pairing request message including the K_{DC} and the access token. In some embodiments, the second network device comprises an AKMA anchor function (AAnF).

[0121] Figure 11 is a flow chart diagram illustrating a further embodiment of a method
30 1100 for establishing an application session corresponding to a PIN element. In some embodiments, the method 1100 is performed by an apparatus, such as the remote unit 102 and/or the network unit 104. In certain embodiments, the method 1100 may be performed by a processor executing program code, for example, a microcontroller, a microprocessor, a CPU, a GPU, an auxiliary processing unit, a FPGA, or the like.

[0122] In various embodiments, the method 1100 includes performing 1102, at a PIN element, a local authentication and registration of the PIN element with preconfigured credentials. In some embodiments, the method 1100 includes sending 1104 a request to a first network device for sending data to a second device outside the local network.

5 [0123] In certain embodiments, the method 1100 further comprises receiving a pairing request message from the first network device, the pairing request message comprises a direct communication key (K_{DC}), an access token, at least one target PIN element identifier, a PIN element address associated with at least one second network device, or some combination thereof. In some embodiments, the method 1100 further comprises computing an authentication value
10 using a hash function, the access token, and the at least one target PIN element identifier. In various embodiments, the method 1100 further comprises transmitting an authentication request to the at least one second network device, and the authentication request comprises an authentication value.

[0124] In one embodiment, the method 1100 further comprises receiving an authentication
15 request comprising an authentication value from a network device with the at least one PIN element identifier from the pairing request message. In certain embodiments, the method 1100 further comprises computing an authentication value using a hash function, the access token, and the at least one PIN element identifier, and comparing the authentication value with the authentication value received from the network device with the at least one PIN element identifier
20 from the pairing request message. In some embodiments, the method 1100 further comprises setting up the secure connection by deriving a security key (K_{DC}).

[0125] In one embodiment, an apparatus comprises a first network device. The apparatus further comprises: a processor; and a transceiver coupled to the processor, wherein: the processor performs a local authentication and registration of PIN elements with preconfigured credentials;
25 the transceiver transmits, to a PIN AF, a first request message comprising an application session establishment request; and the transceiver transmits, from the PIN AF, a first response message comprising an application session establishment response.

[0126] In certain embodiments, the transceiver transmits, to the PIN AF, a second request message comprising a PIN session binding policy request, wherein the second request message
30 comprises a list of authenticated PIN element IDs and corresponding binding policies.

[0127] In some embodiments, the transceiver receives, from the PIN AF, a second response message comprising a PIN session binding policy response.

[0128] In various embodiments, the transceiver receives a data send request from a locally registered PIN element.

[0129] In one embodiment, the transceiver transmits, to the PIN AF, a third request message comprising a data request message an authentication and key management for A-TID of the first network device, a (PEGC) PIN element ID, a target PIN element ID, a source PIN element ID, or some combination thereof.

5 [0130] In certain embodiments, the transceiver receives, from the PIN AF, a third response message comprising a data response message comprising a direct communication key (K_{DC}) and an access token.

[0131] In some embodiments, the transceiver transmits a data send response to the locally registered PIN element, the data send response comprising the K_{DC} and the access token.

10 [0132] In various embodiments, the first network device comprises a (PEGC), a (PEMC), or a combination thereof.

[0133] In one embodiment, a method of a first network device comprises: performing a local authentication and registration of PIN elements with preconfigured credentials; transmitting, to a PIN AF, a first request message comprising an application session establishment request; and
15 transmitting, from the PIN AF, a first response message comprising an application session establishment response.

[0134] In certain embodiments, the method further comprises transmitting, to the PIN AF, a second request message comprising a PIN session binding policy request, wherein the second request message comprises a list of authenticated PIN element IDs and corresponding binding
20 policies.

[0135] In some embodiments, the method further comprises receiving, from the PIN AF, a second response message comprising a PIN session binding policy response.

[0136] In various embodiments, the method further comprises receiving a data send request from a locally registered PIN element.

25 [0137] In one embodiment, the method further comprises transmitting, to the PIN AF, a third request message comprising a data request message an A-TID of the first network device, a (PEGC) PIN element ID, a target PIN element ID, a source PIN element ID, or some combination thereof.

[0138] In certain embodiments, the method further comprises receiving, from the PIN AF,
30 a third response message comprising a data response message comprising a direct communication key (K_{DC}) and an access token.

[0139] In some embodiments, the method further comprises transmitting a data send response to the locally registered PIN element, the data send response comprising the K_{DC} and the access token.

[0140] In various embodiments, the first network device comprises a (PEGC), a (PEMC), or a combination thereof.

[0141] In one embodiment, an apparatus comprises a PIN AF. The apparatus further comprises: a processor; and a transceiver coupled to the processor, wherein: the transceiver receives, from a first network device, a first request message comprising an application session establishment request; the transceiver transmits, to a second network device, a second request message comprising a Naanf_AKMA_ApplicationKey_Get request; the transceiver receives, from the second network device, a first response message comprising a Naanf_AKMA_ApplicationKey_Get response, wherein the first response message comprises a list of managed PIN element IDs and their corresponding binding policies; and the transceiver transmits, to the first network device, a second response message comprising an application session establishment response.

[0142] In certain embodiments, the transceiver receives, from the first network device, a third request message comprising a PIN session binding policy request, and the third request message comprises a list of authenticated PIN element IDs and corresponding binding policies.

[0143] In some embodiments, the processor stores the list of authenticated PIN element IDs and their corresponding binding policies.

[0144] In various embodiments, the processor matches the list of managed PIN element IDs and their corresponding binding policies to the list of authenticated PIN element IDs and their corresponding binding policies.

[0145] In one embodiment, the transceiver transmits, to the first network device, a third response message comprising a PIN session binding policy response.

[0146] In certain embodiments, the transceiver receives, from the first network device, a data request message, and the data request message comprises an A-TID of the first network device, a (PEGC) PIN element ID, a target PIN element ID, a source PIN element ID, or some combination thereof.

[0147] In some embodiments, the processor determines a binding of source PIN elements and target PIN elements.

[0148] In various embodiments, the processor determines a binding of two or more locally registered PIN elements.

[0149] In one embodiment, the processor derives a direct communication key (K_{DC}) and an access token.

[0150] In certain embodiments, the transceiver transmits, to the first network device, a protected pairing request message including the K_{DC} and the access token.

[0151] In some embodiments, the second network device comprises an AKMA anchor function (AAnF).

[0152] In one embodiment, a method of a PIN AF comprises: receiving, from a first network device, a first request message comprising an application session establishment request; transmitting, to a second network device, a second request message comprising a Naanf_AKMA_ApplicationKey_Get request; receiving, from the second network device, a first response message comprising a Naanf_AKMA_ApplicationKey_Get response, wherein the first response message comprises a list of managed PIN element IDs and their corresponding binding policies; and transmitting, to the first network device, a second response message comprising an application session establishment response.

[0153] In certain embodiments, the method further comprises receiving, from the first network device, a third request message comprising a PIN session binding policy request, wherein the third request message comprises a list of authenticated PIN element IDs and corresponding binding policies.

[0154] In some embodiments, the method further comprises storing the list of authenticated PIN element IDs and their corresponding binding policies.

[0155] In various embodiments, the method further comprises matching the list of managed PIN element IDs and their corresponding binding policies to the list of authenticated PIN element IDs and their corresponding binding policies.

[0156] In one embodiment, the method further comprises transmitting, to the first network device, a third response message comprising a PIN session binding policy response.

[0157] In certain embodiments, the method further comprises receiving, from the first network device, a data request message, wherein the data request message comprises an A-TID of the first network device, a (PEGC) PIN element ID, a target PIN element ID, a source PIN element ID, or some combination thereof.

[0158] In some embodiments, the method further comprises determining a binding of source PIN elements and target PIN elements.

[0159] In various embodiments, the method further comprises determining a binding of two or more locally registered PIN elements.

[0160] In one embodiment, the method further comprises deriving a direct communication key (K_{DC}) and an access token.

[0161] In certain embodiments, the method further comprises transmitting, to the first network device, a protected pairing request message including the K_{DC} and the access token.

[0162] In some embodiments, the second network device comprises an AKMA anchor function (AAnF).

[0163] In one embodiment, an apparatus comprises a PIN element. The apparatus further comprises: a transceiver; and a processor coupled to the transceiver, wherein: the transceiver performs a local authentication and registration of the PIN element with preconfigured credentials; and the transceiver sends a request to a first network device for sending data to a second device outside the local network.

[0164] In certain embodiments, the transceiver receives a pairing request message from the first network device, the pairing request message comprises a direct communication key (K_{DC}), an access token, at least one target PIN element identifier, a PIN element address associated with at least one second network device, or some combination thereof.

[0165] In some embodiments, the processor computes an authentication value using a hash function, the access token, and the at least one target PIN element identifier.

[0166] In various embodiments, the transceiver transmits an authentication request to the at least one second network device, and the authentication request comprises an authentication value.

[0167] In one embodiment, the transceiver receives an authentication request comprising an authentication value from a network device with the at least one PIN element identifier from the pairing request message.

[0168] In certain embodiments, the processor computes an authentication value using a hash function, the access token, and the at least one PIN element identifier, and compares the authentication value with the authentication value received from the network device with the at least one PIN element identifier from the pairing request message.

[0169] In some embodiments, the processor sets up the secure connection by deriving a security key (K_{DC}).

[0170] In one embodiment, a method of a PIN element comprises: performing a local authentication and registration of the PIN element with preconfigured credentials; and sending a request to a first network device for sending data to a second device outside the local network.

[0171] In certain embodiments, the method further comprises receiving a pairing request message from the first network device, the pairing request message comprises a direct communication key (K_{DC}), an access token, at least one target PIN element identifier, a PIN element address associated with at least one second network device, or some combination thereof.

[0172] In some embodiments, the method further comprises computing an authentication value using a hash function, the access token, and the at least one target PIN element identifier.

[0173] In various embodiments, the method further comprises transmitting an authentication request to the at least one second network device, and the authentication request comprises an authentication value.

5 [0174] In one embodiment, the method further comprises receiving an authentication request comprising an authentication value from a network device with the at least one PIN element identifier from the pairing request message.

[0175] In certain embodiments, the method further comprises computing an authentication value using a hash function, the access token, and the at least one PIN element identifier, and comparing the authentication value with the authentication value received from the network device
10 with the at least one PIN element identifier from the pairing request message.

[0176] In some embodiments, the method further comprises setting up the secure connection by deriving a security key (K_{DC}).

[0177] Embodiments may be practiced in other specific forms. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope
15 of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

CLAIMS

1. An apparatus comprising:
a processor; and
a memory coupled to the processor, the memory comprising instructions
5 executable by the processor to cause the apparatus to:
perform a local authentication and registration of personal internet of
things network (PIN) elements with preconfigured credentials;
transmit, to a PIN application function (AF), a first request message
comprising an application session establishment request; and
10 transmit, from the PIN AF, a first response message comprising an
application session establishment response.
2. The apparatus of claim 1, wherein the instructions are further executable by the processor
to cause the apparatus to transmit, to the PIN AF, a second request message comprising a
PIN session binding policy request, wherein the second request message comprises a list
15 of authenticated PIN element IDs and corresponding binding policies.
3. The apparatus of claim 2, wherein the instructions are further executable by the processor
to cause the apparatus to receive, from the PIN AF, a second response message
comprising a PIN session binding policy response.
4. The apparatus of claim 1, wherein the instructions are further executable by the processor
20 to cause the apparatus to receive a data send request from a locally registered PIN
element.
5. The apparatus of claim 4, wherein the instructions are further executable by the processor
to cause the apparatus to transmit, to the PIN AF, a third request message comprising a
data request message an authentication and key management for applications (AKMA)
25 temporary user equipment (UE) ID (A-TID) of the apparatus, a PIN element with
gateway capabilities (PEGC) PIN element ID, a target PIN element ID, a source PIN
element ID, or a combination thereof.

6. The apparatus of claim 5, wherein the instructions are further executable by the processor to cause the apparatus to receive, from the PIN AF, a third response message comprising a data response message comprising a direct communication key (K_{DC}) and an access token.
- 5 7. The apparatus of claim 6, wherein the instructions are further executable by the processor to cause the apparatus to transmit a data send response to the locally registered PIN element, the data send response comprising the K_{DC} and the access token.
8. The apparatus of claim 1, wherein the apparatus comprises a PIN element with gateway capabilities (PEGC), a PIN element with management capabilities (PEMC), or a
10 combination thereof.
9. An apparatus comprising:
a processor; and
a memory coupled to the processor, the memory comprising instructions
executable by the processor to cause the apparatus to:
15 receive, from a first network device, a first request message comprising an
application session establishment request;
transmit, to a second network device, a second request message
comprising a Naanf_AKMA_ApplicationKey_Get request;
receive, from the second network device, a first response message
20 comprising a Naanf_AKMA_ApplicationKey_Get response,
wherein the first response message comprises a list of managed
personal internet of things network (PIN) element identifiers (IDs)
and their corresponding binding policies; and
transmit, to the first network device, a second response message
25 comprising an application session establishment response.
10. The apparatus of claim 9, wherein the instructions are further executable by the processor to cause the apparatus to receive, from the first network device, a third request message comprising a PIN session binding policy request, and the third request message comprises a list of authenticated PIN element IDs and corresponding binding policies.

11. The apparatus of claim 10, wherein the instructions are further executable by the processor to cause the apparatus to store the list of authenticated PIN element IDs and their corresponding binding policies.
12. The apparatus of claim 11, wherein the instructions are further executable by the processor to cause the apparatus to match the list of managed PIN element IDs and their corresponding binding policies to the list of authenticated PIN element IDs and their corresponding binding policies.
13. An apparatus comprising:
a processor; and
a memory coupled to the processor, the memory comprising instructions executable by the processor to cause the apparatus to:
perform a local authentication and registration of a personal internet of things network (PIN) element with preconfigured credentials; and
send a request to a first network device for sending data to a second device outside a local network.
14. The apparatus of claim 13, wherein the instructions are further executable by the processor to cause the apparatus to receive a pairing request message from the first network device, the pairing request message comprises a direct communication key (K_{DC}), an access token, at least one target PIN element identifier, a PIN element address associated with at least one second network device, or a combination thereof.
15. The apparatus of claim 14, wherein the instructions are further executable by the processor to cause the apparatus to compute an authentication value using a hash function, the access token, and the at least one target PIN element identifier.

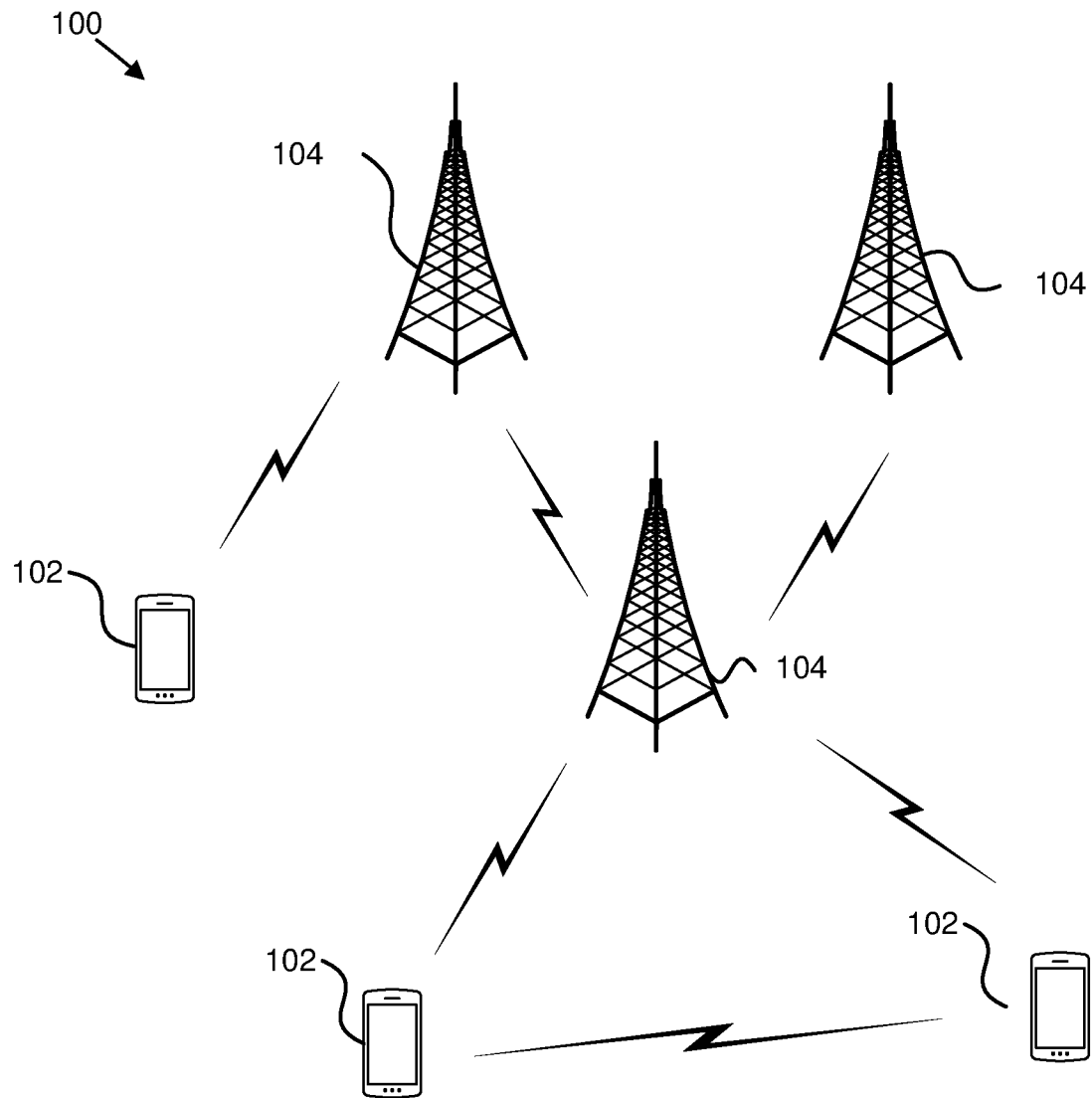


FIG. 1

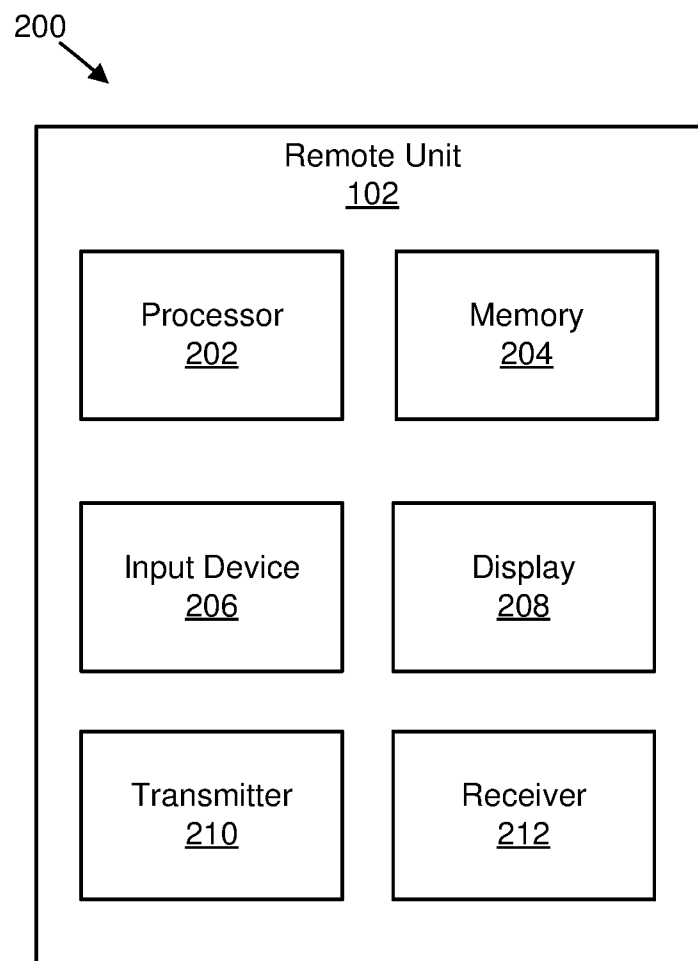


FIG. 2

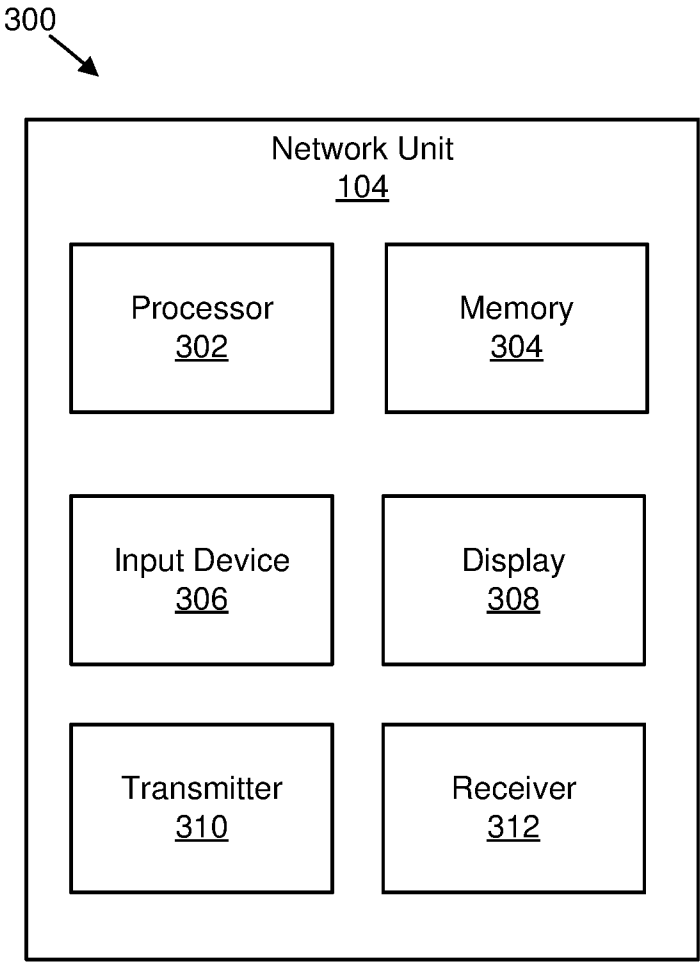


FIG. 3

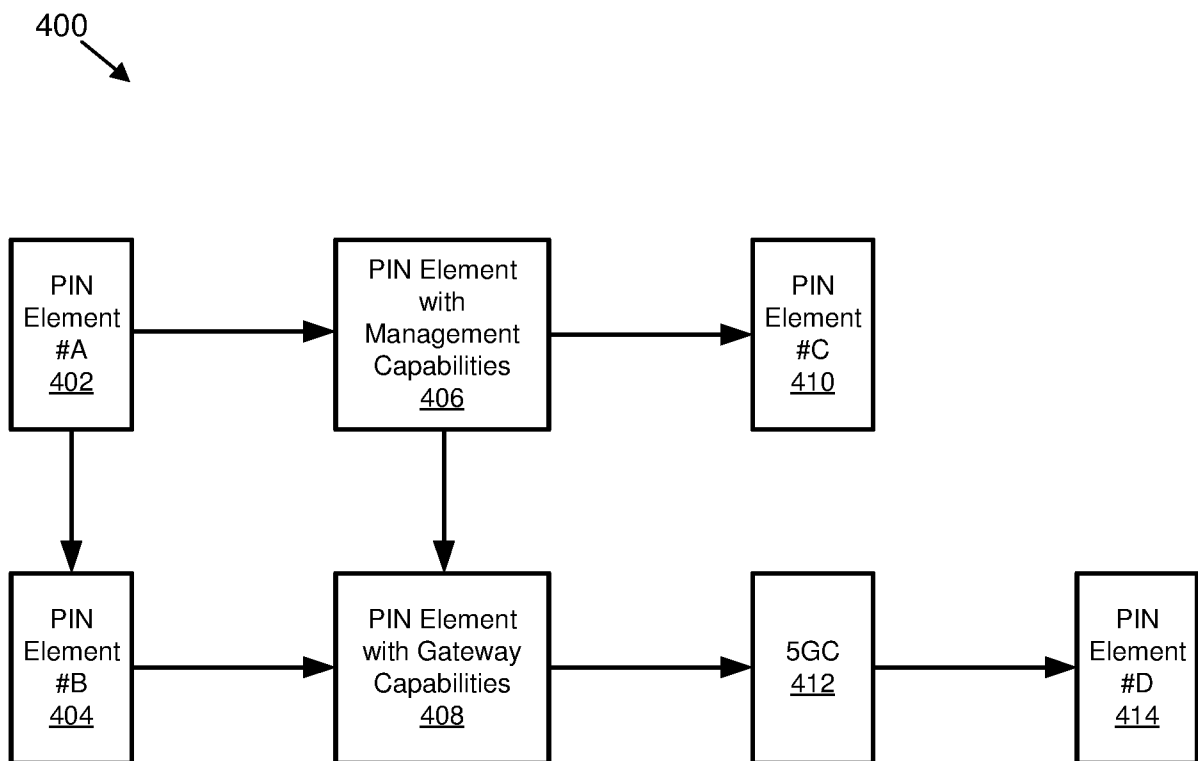


FIG. 4

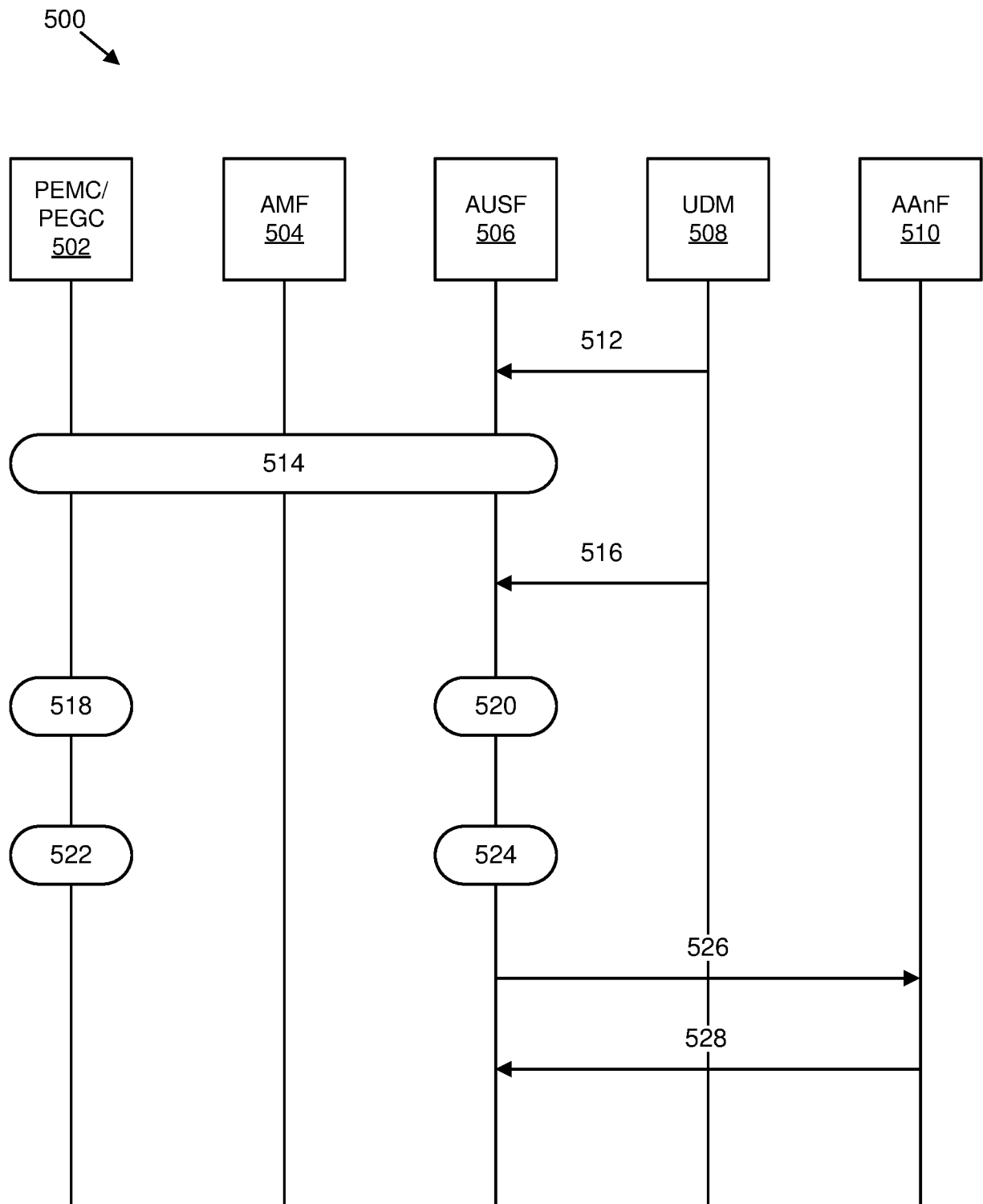


FIG. 5

600 ↘

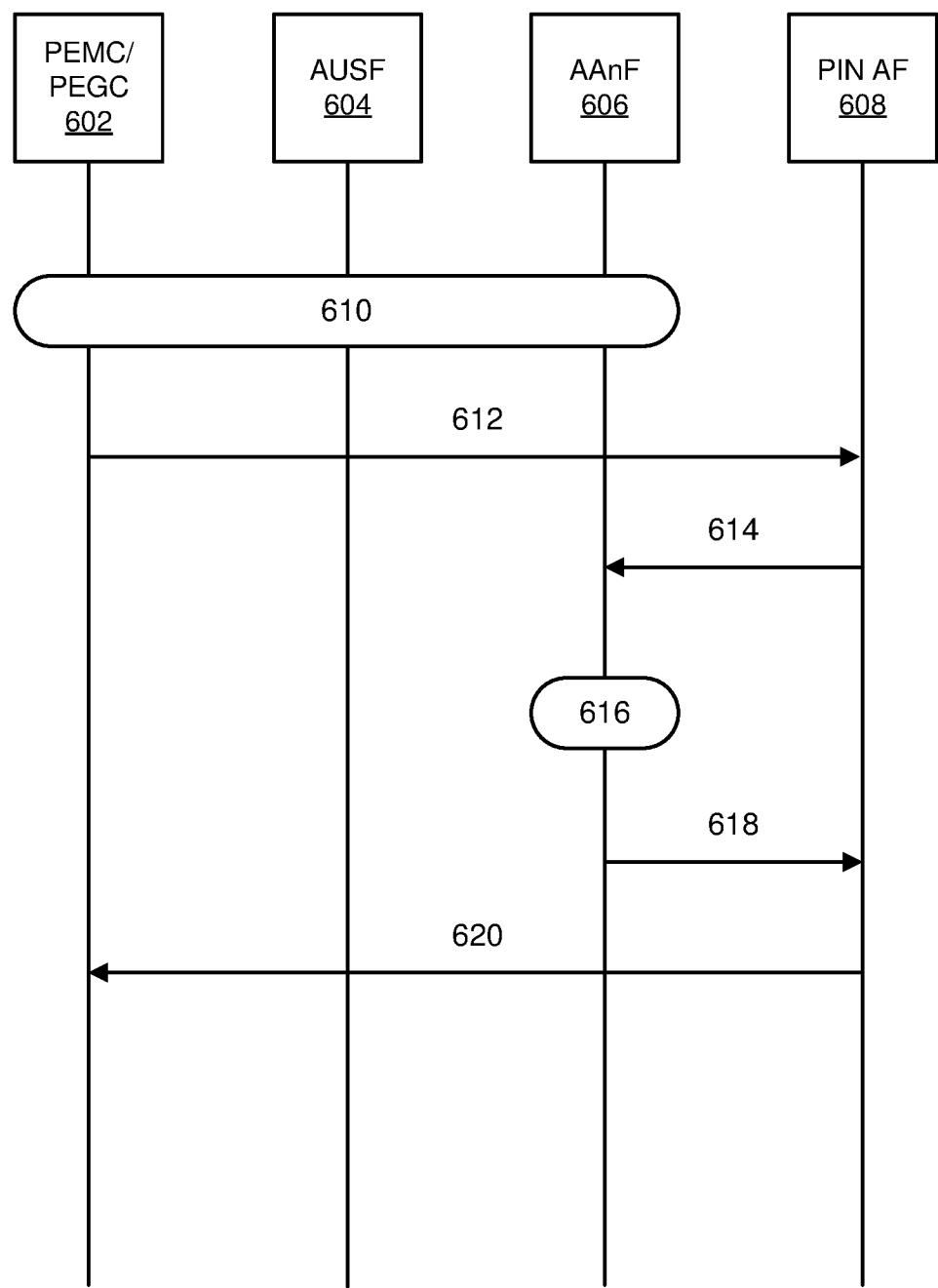


FIG. 6

700 ↘

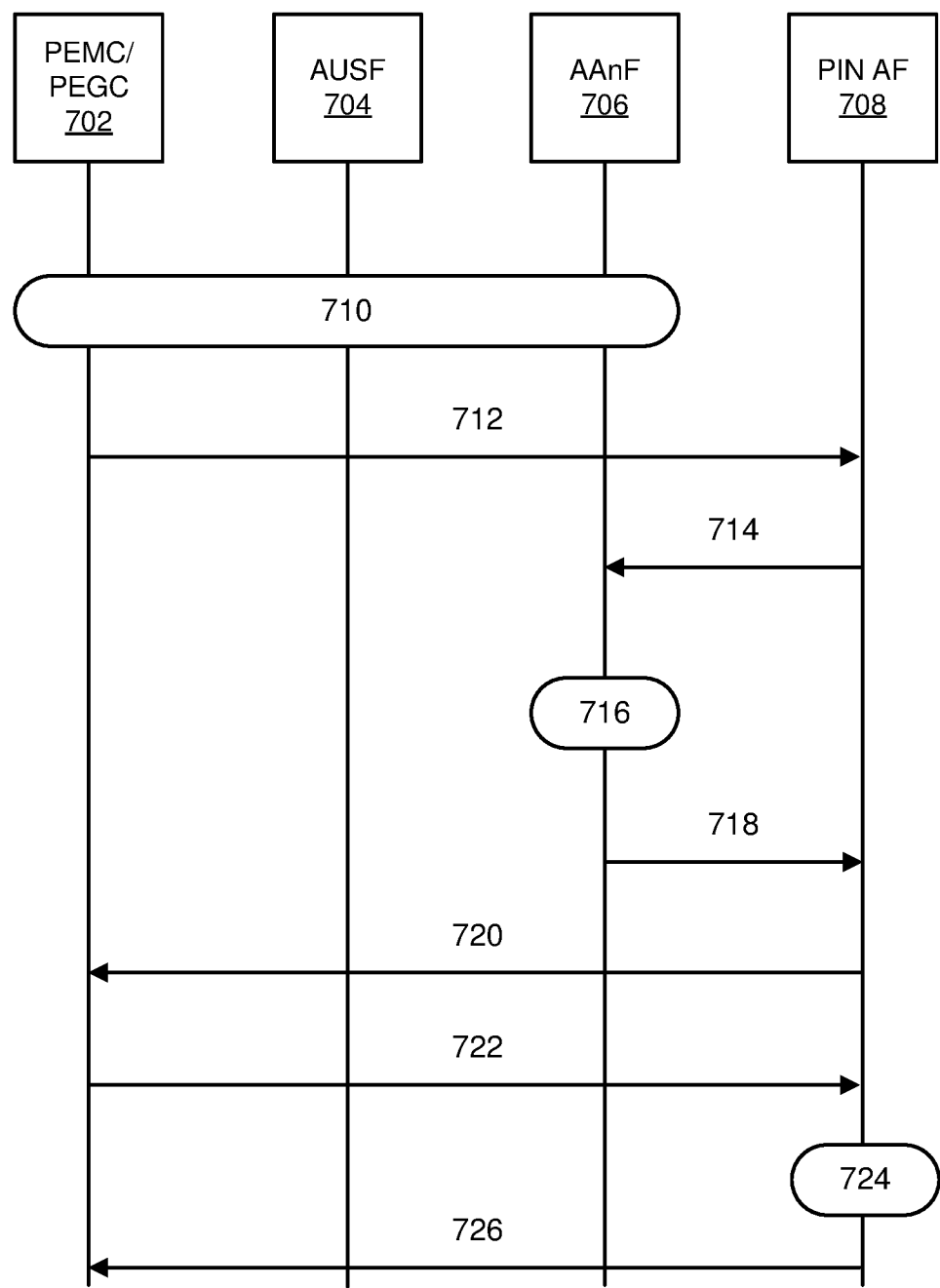


FIG. 7

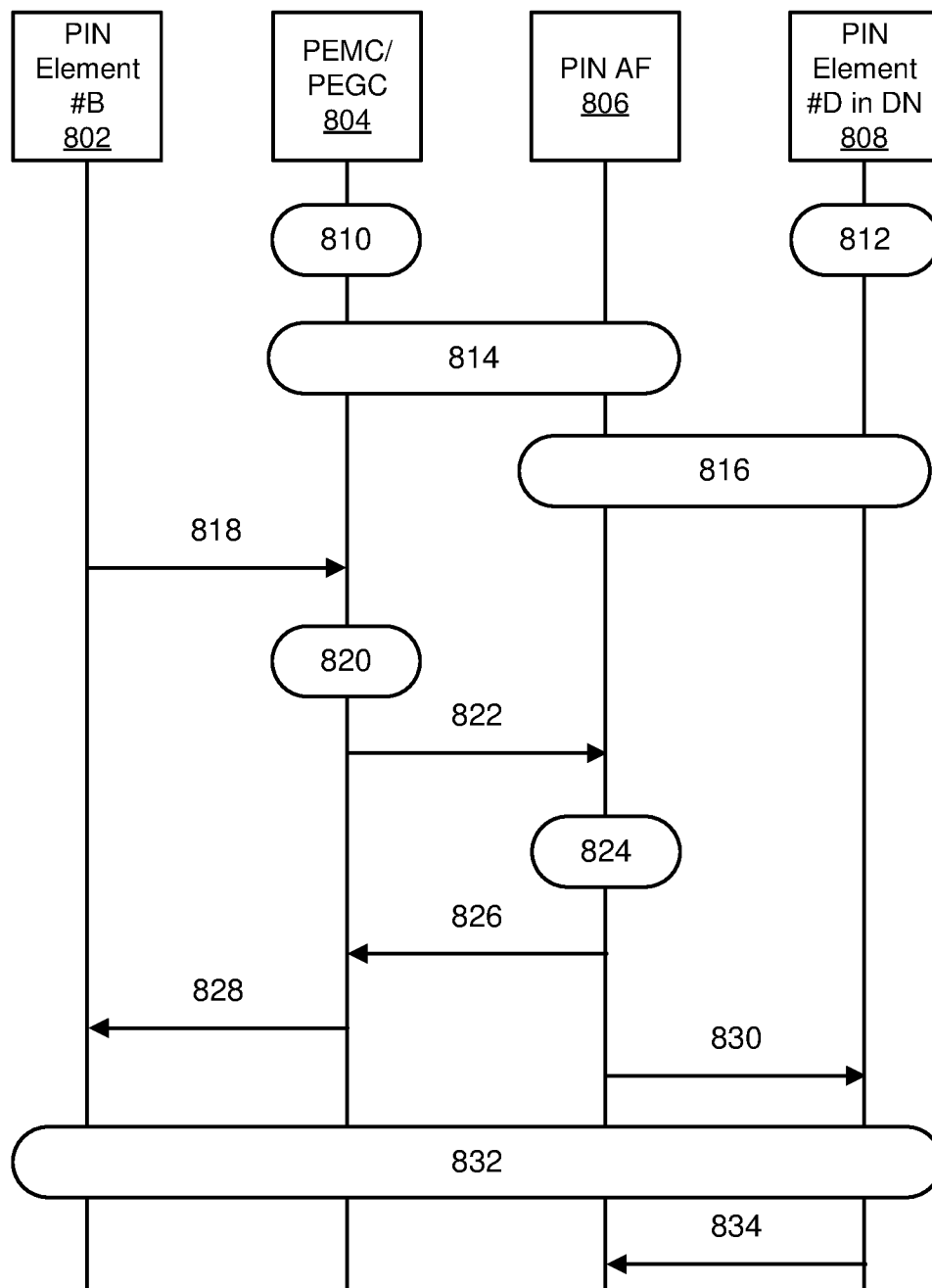
800
↓

FIG. 8

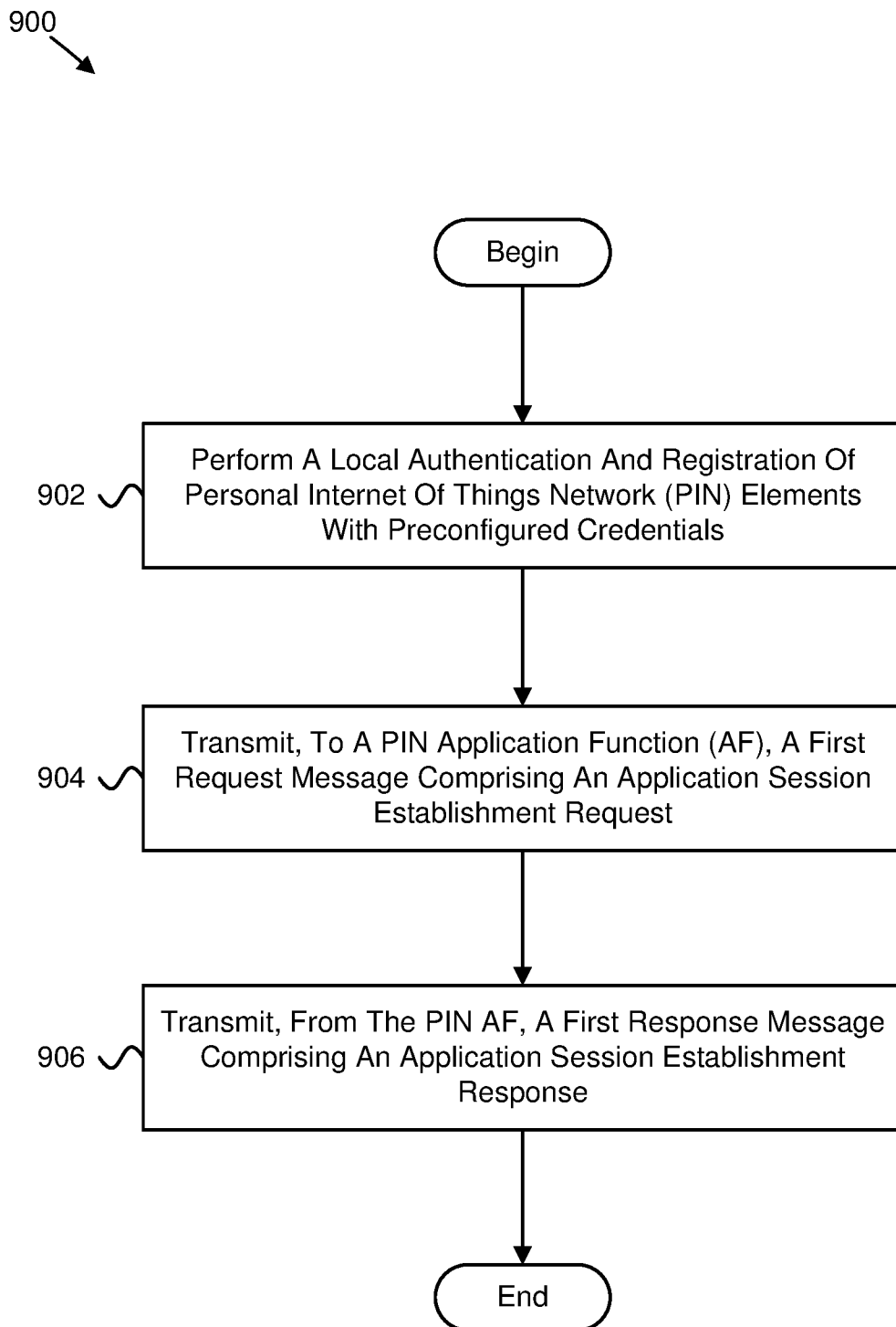


FIG. 9

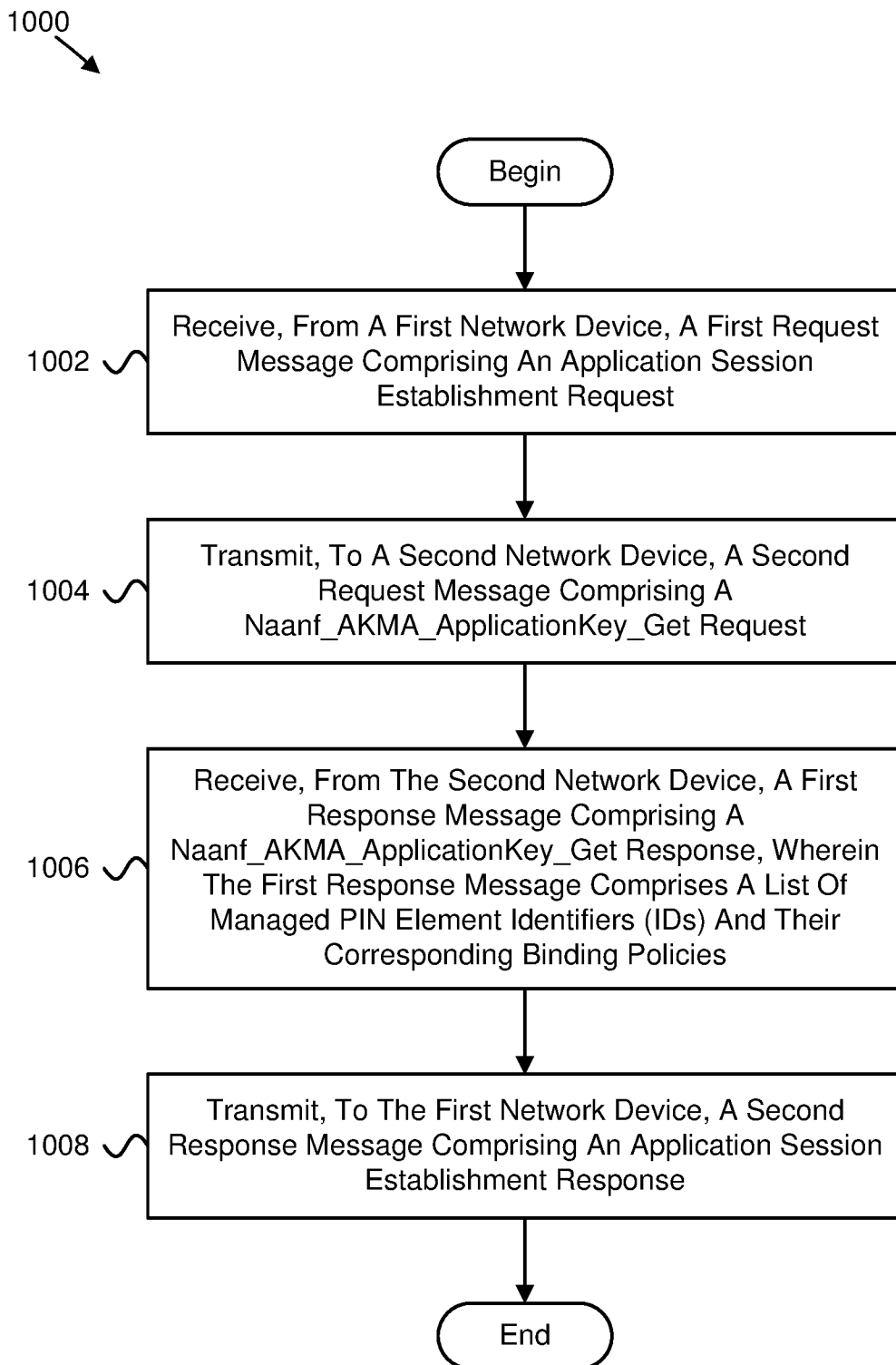


FIG. 10

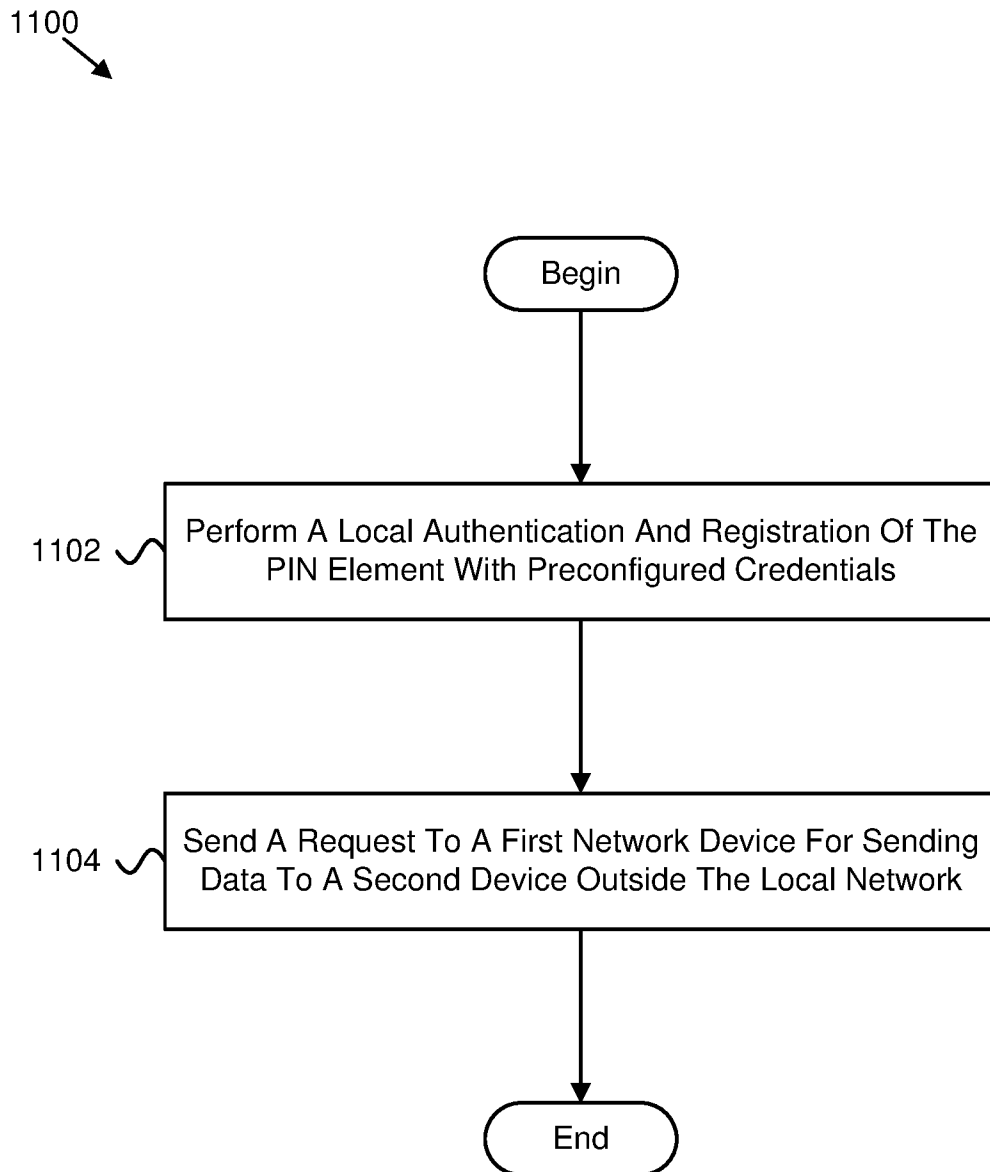


FIG. 11

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2023/052314

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W76/11 H04L12/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 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, WPI Data, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Personal Internet of Things (PIoT) networks (Release 18)", 3GPP DRAFT; S1-211309, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , 9 June 2021 (2021-06-09), XP052027777, Retrieved from the Internet: URL:https://ftp.3gpp.org/tsg_sa/WG1_Serv/TSGS1_94e_ElectronicMeeting/Docs/S1-211309.zip S1-211309-22859-110_rm.docx [retrieved on 2021-06-09] page 24, paragraph Section 5.5 - page 28 the whole document ----- -/-	1, 4, 8

☒ 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

24 May 2023

Date of mailing of the international search report

24/07/2023

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

Adkhis, Franck

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2023/052314

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 2021/368341 A1 (LIAO CHING-YU [US]) 25 November 2021 (2021-11-25) abstract paragraph [0003] paragraph [0125] - paragraph [0134]; figure 10 claims 1-20 -----	1-8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2023/052314

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims;; it is covered by claims Nos.:

1-8

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-8

Apparatus to securely register personal internet of things network (PIN) elements and establish a session with a PIN application function.

2. claims: 9-12

Apparatus to receive a list of managed personal internet of things network (PIN) element identifiers (IDs), their corresponding binding policies and to establish an application session with a network device.

3. claims: 13-15

Apparatus to request a first network device for sending data to a second device outside a local network.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2023/052314

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2021368341	A1	25-11-2021	NONE
