



(51) International Patent Classification:
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/CN2017/111028

(22) International Filing Date:
15 November 2017 (15.11.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karaportti 3, Espoo, 02610 (FI).

(71) Applicant (for LC only): **NOKIA TECHNOLOGIES
(BEIJING) CO., LTD.** [CN/CN]; Unit 18, Room 1001,
Level 10, East Tower, World Financial Center, No. 1,
East Third Ring Middle Road, Chaoyang District, Beijing
100020 (CN).

(72) Inventors: **WANG, Zhi**; No. 55, Hongdao Road, Qingdao,
Shandong 266003 (CN). **CAI, Yigang**; 23643 Royal Wor-
lington Drive, Naperville, IL 60564 (US).

(74) Agent: **KING & WOOD MALLESONS**; 20th Floor,
East Tower, World Financial Centre, No. 1 Dongsanhuan
Zhonglu, Chaoyang District, Beijing 100020 (CN).

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

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,

(54) Title: AUTHORIZATION OF APPLICATIONS FOR DIRECT DISCOVERY

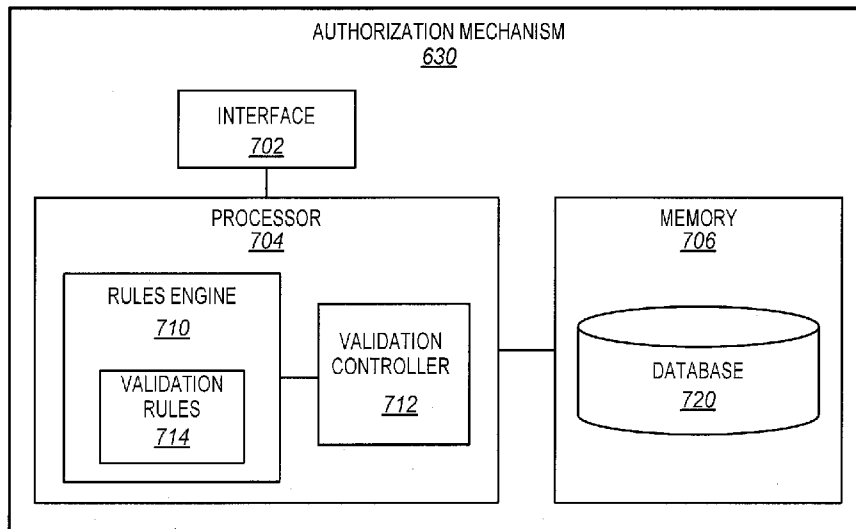


FIG. 7

(57) Abstract: Systems, methods, and software for authorizing an application in User Equipment (UE) for direct discovery. In one embodiment, an authorization mechanism receives information (e.g., application ID) for a discovery request sent by an application in a UE. In response to the discovery request, the authorization mechanism challenges the UE for information regarding security parameters that are mapped to the application ID. Based on the information provided by the UE, the authorization mechanism determines whether the application is authorized for direct discovery.



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

Published:

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

AUTHORIZATION OF APPLICATIONS FOR DIRECT DISCOVERY

Field of the Invention

5 The invention is related to the field of communication systems and, in particular, to direct discovery for proximity services.

Background

10 Mobile communications have primarily involved a mobile station (i.e., User Equipment (UE)) communicating with a base station that is in turn connected to a core network. The control and user plane traffic was routed through the core network. Proximity services or proximity-based services refer to services provided between UEs being in proximity to each other. Proximity services utilize the radio technologies of the UEs so that the UEs in close proximity can exchange communications directly with one another without
15 going through the core network, which is also referred to as device-to-device (D2D) communications.

 The Third Generation Partnership Program (3GPP) has defined Proximity Services (ProSe), which allows for D2D communications as an underlay to a cellular network. In D2D communications, UEs transmit data signals to each other over a direct link using the cellular
20 resources instead of routing the data signals through the core network. Therefore, D2D communications involve directly transmitting traffic between UEs that are in the vicinity of one another instead of routing the traffic over a core network, such as the Evolved Packet Core (EPC). Because there is direct communication between UEs that are in close proximity, D2D communications offload traffic from the EPC network without additional infrastructure.
25 D2D communications may also offer higher data rates, lower transfer delays, and better power efficiency within a UE.

 Proximity services generally include discovery, direct communication, and UE-to-network relay. Discovery is a procedure that identifies UEs that are in proximity with each other. Direct communication is a procedure where UEs in proximity are able to
30 communicate using local radio resources. UE-to-network relay is a procedure where a UE can relay traffic from a remote UE to the network, or from the network to the remote UE. For example, if a UE (referred to as a remote UE) is outside of the coverage area of the base stations for a network, then the UE-to-network relay procedure allows the remote UE to transmit traffic to a relay UE that is in the coverage area of a base station through a direct

communication with the relay UE. The relay UE in turn forwards the traffic from the remote UE to the network by communicating with a base station of the network.

The 3GPP has defined some procedures for authorizing a UE during a discovery procedure. However, present authorization procedures may be insufficient to detect
5 malicious applications that attempt to use proximity services.

Summary

Embodiments described herein provide mechanisms for authorizing an application on a UE that is requesting direct discovery. When an application on a UE sends a discovery
10 request for ProSe, an authorization mechanism as described herein provides enhanced discovery authorization procedures to ensure that the application is authorized for direct discovery. Applications for proximity services are distinguished by Application Identifiers (ID), and a network operator may define one or more security parameters for the Application IDs. The authorization mechanism described herein sends a challenge message to the UE
15 requesting information related to the security parameters for the Application ID provided in the discovery request, and is able to determine whether the application is authorized for direct discovery using the Application ID based on the answer to the challenge message provided by the UE. The discovery authorization procedures described herein are advantageously able to determine when a malicious application is spoofing an Application ID so that discovery
20 requests from this malicious application may be rejected.

One embodiment comprises an authorization mechanism that performs a discovery authorization procedure for ProSe. The authorization mechanism includes a validation controller configured to receive information for a discovery request sent by an application in a
25 UE. The discovery request includes an Application ID for the application. The authorization mechanism further includes a rules engine configured to determine validation rules for the discovery authorization procedure. The validation controller is configured to send a security challenge message to the UE requesting challenge values for security parameters that are mapped to the Application ID, to receive a security answer message from the UE in response to the security challenge message, to extract the challenge values for the security parameters
30 from the security answer message as provided by the UE, and to determine whether the application is authorized for direct discovery using the Application ID based on the challenge values for the security parameters and the validation rules. The validation controller is configured to generate a validation indicator to authorize the discovery request sent by the application when the application is authorized for direct discovery using the Application ID.

In another embodiment, the validation controller is configured to generate a rejection indicator to reject the discovery request sent by the application when the application is not authorized for direct discovery using the Application ID.

5 In another embodiment, the authorization mechanism further includes a database that maps the security parameters to the Application ID. The security parameters mapped to the Application ID include authorized values provisioned for the Application ID.

In another embodiment, the validation controller is configured to identify the authorized values for the security parameters mapped to the Application ID, and to compare the challenge values provided by the UE to the authorized values provisioned for the Application ID to determine whether the application is authorized for direct discovery using the Application ID.

In another embodiment, the validation controller is configured to send the security challenge message to the UE requesting a network address assigned to the UE.

15 In another embodiment, the validation controller is configured to send the security challenge message to the UE requesting a Public Land Mobile Network (PLMN) code.

In another embodiment, the validation controller is configured to send the security challenge message to the UE requesting a location code for the UE.

In another embodiment, the validation controller is configured to send the security challenge message to the UE requesting a passcode used to access the application.

20 In another embodiment, the authorization mechanism is implemented in a ProSe function that receives the discovery request from the UE.

In another embodiment, the authorization mechanism is implemented in a ProSe Application Server that is communicatively coupled to a ProSe function that receives the discovery request from the UE.

25 Another embodiment comprises a method of performing a discovery authorization procedure for ProSe. The method comprises receiving information for a discovery request sent by an application in a UE, where the discovery request includes an Application ID for the application. The method comprises determining validation rules for the discovery authorization procedure, sending a security challenge message from the authorization mechanism to the UE requesting challenge values for security parameters that are mapped to the Application ID, receiving a security answer message from the UE in response to the security challenge message, extracting the challenge values for the security parameters from the security answer message as provided by the UE, and determining whether the application is authorized for direct discovery using the Application ID based on the challenge values for

the security parameters and the validation rules. The method comprises generating a validation indicator to authorize the discovery request sent by the application when the application is authorized for direct discovery using the Application ID.

5 In another embodiment, the method further comprises generating a rejection indicator to reject the discovery request sent by the application when the application is not authorized for direct discovery using the Application ID.

In another embodiment, the method comprises storing a database that maps the security parameters to the Application ID. The security parameters mapped to the Application ID include authorized values provisioned for the Application ID.

10 In another embodiment, the step of determining whether the application is authorized for direct discovery comprises identifying the authorized values for the security parameters mapped to the Application ID, and comparing the challenge values provided by the UE to the authorized values provisioned for the Application ID to determine whether the application is authorized for direct discovery using the Application ID.

15 Another embodiment comprises a non-transitory computer readable medium embodying programmed instructions executed by one or more processors, wherein the instructions direct the processors to implement an authorization mechanism that performs a discovery authorization procedure for ProSe. The authorization mechanism is configured to receive information for a discovery request sent by an application in a UE, where the
20 discovery request includes an Application ID for the application. The authorization mechanism is configured to determine validation rules for the discovery authorization procedure, to send a security challenge message to the UE requesting challenge values for security parameters that are mapped to the Application ID, to receive a security answer message from the UE in response to the security challenge message, to extract the challenge
25 values for the security parameters from the security answer message as provided by the UE, and to determine whether the application is authorized for direct discovery using the Application ID based on the challenge values for the security parameters and the validation rules. The authorization mechanism is configured to generate a validation indicator to authorize the discovery request sent by the application when the application is authorized for
30 direct discovery using the Application ID.

In another embodiment, the authorization mechanism is configured to generate a rejection indicator to reject the discovery request sent by the application when the application is not authorized for direct discovery using the Application ID.

In another embodiment, the authorization mechanism is configured to store a database that maps the security parameters to the Application ID. The security parameters mapped to the Application ID include authorized values provisioned for the Application ID.

5 In another embodiment, the authorization mechanism is configured to identify the authorized values for the security parameters mapped to the Application ID, and to compare the challenge values provided by the UE to the authorized values provisioned for the Application ID to determine whether the application is authorized for direct discovery using the Application ID.

10 In another embodiment, the authorization mechanism is implemented in a ProSe function that receives the discovery request from the UE.

In another embodiment, the authorization mechanism is implemented in a ProSe Application Server that is communicatively coupled to a ProSe function that receives the discovery request from the UE.

15 Another embodiment comprises an authorization mechanism that performs a discovery authorization procedure for ProSe. The authorization mechanism includes a means for receiving information for a discovery request sent by an application in a UE, where the discovery request includes an Application ID for the application. The authorization mechanism includes a means for determining validation rules for the discovery authorization procedure. The authorization mechanism includes a means for sending a security challenge message to the UE requesting challenge values for security parameters that are mapped to the Application ID. The authorization mechanism includes a means for receiving a security answer message from the UE in response to the security challenge message. The authorization mechanism includes a means for extracting the challenge values for the security parameters from the security answer message as provided by the UE. The authorization mechanism includes a means for determining whether the application is authorized for direct discovery using the Application ID based on the challenge values for the security parameters and the validation rules. The authorization mechanism includes a means for generating a validation indicator to authorize the discovery request sent by the application when the application is authorized for direct discovery using the Application ID.

30 The above summary provides a basic understanding of some aspects of the specification. This summary is not an extensive overview of the specification. It is intended to neither identify key or critical elements of the specification nor delineate any scope of the particular embodiments of the specification, or any scope of the claims. Its sole purpose is to

present some concepts of the specification in a simplified form as a prelude to the more detailed description that is presented later.

Description of the Drawings

5 Some embodiments of the invention are now described, by way of example only, and with reference to the accompanying drawings. The same reference number represents the same element or the same type of element on all drawings.

FIG. 1 illustrates an architecture for ProSe features.

FIG. 2 illustrates a service pre-configuration procedure for a UE.

10 FIG. 3 illustrates a service authorization procedure for a UE.

FIG. 4 illustrates a discovery request procedure for an announcing UE.

FIG. 5 illustrates a discovery request procedure for a monitoring UE.

FIG. 6 illustrates an architecture for proximity services in an illustrative embodiment.

15 FIG. 7 is a block diagram of an authorization mechanism in an illustrative embodiment.

FIG. 8 illustrates a database in an illustrative embodiment.

FIG. 9 is a flow chart illustrating a method of performing a discovery authorization procedure in an illustrative embodiment.

20 FIG. 10 is a flow chart illustrating a method of determining whether an application is authorized for direct discovery in an illustrative embodiment.

FIG. 11 is a flow diagram when an authorization mechanism is implemented in a ProSe function in an illustrative embodiment.

FIG. 12 is a flow diagram when an authorization mechanism is implemented in a ProSe Application Server in an illustrative embodiment.

25

Description of Embodiments

The figures and the following description illustrate specific exemplary embodiments. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the embodiments and are included within the scope of the embodiments. Furthermore, any
30 examples described herein are intended to aid in understanding the principles of the embodiments, and are to be construed as being without limitation to such specifically recited examples and conditions. As a result, the inventive concept(s) is not limited to the specific embodiments or examples described below, but by the claims and their equivalents.

FIG. 1 illustrates an architecture 100 for ProSe features. Architecture 100 illustrates a non-roaming scenario in a Public Land Mobile Network (PLMN) as described in 3GPP TS 23.303 (version 15.0.0), which is incorporated by reference as if fully included herein.

Architecture 100 includes an Evolved Packet Core (EPC) network 110 that communicates with UEs 120-121 over a Radio Access Network (RAN), which is illustrated as an Evolved-UMTS Terrestrial Radio Access Network (E-UTRAN) 112. Although not shown in FIG. 1, E-UTRAN 112 includes a plurality of base stations (e.g., eNodeB) that provide wireless connections between UEs 120-121 (and other UEs) and EPC network 110. EPC network 110 includes a Mobility Management Entity (MME) 114, an S-GW 115, and a P-GW 116. Architecture 100 also includes a Home Subscriber Server (HSS) 117 and a Secure User Plane Location Platform (SLP) 118. HSS 117 stores subscription information for UEs 120-121 in the form of subscriber profiles. SLP 118 maintains location information for UEs 120-121.

Architecture 100 further includes a Proximity Service (ProSe) function 130 and a ProSe Application Server (AS) 132. ProSe Application Server 132 supports storage of EPC ProSe User IDs and ProSe function IDs, and mapping of Application Layer User IDs and EPC ProSe User IDs. ProSe function 130 is a logical function that is used for network-related actions required for ProSe. ProSe function 130 plays different roles for each of the features of ProSe. There may be one ProSe function 130 in each PLMN that supports proximity services. ProSe function 130 includes three main sub-functions that perform different roles depending on the ProSe feature. One sub-function is a Direct Provisioning Function (DPF) that is used to provision a UE with parameters in order use direct discovery and direct communication. The DPF provisions the UEs with PLMN-specific parameters that allow the UEs to use proximity services in this specific PLMN. Another sub-function is a Direct Discovery Name Management Function, which is used for open direct discovery to allocate and process Applications IDs and Application Codes used in direct discovery. This sub-function maintains a table that lists the mapping between the Application ID and Application Code. In addition, this sub-function generates filters for monitoring UEs. Another sub-function is an EPC-level discovery ProSe function, which authorizes and configures UEs for EPC-level ProSe discovery and EPC-assisted WLAN direct discovery and communication. The reference point (PC4a) between HSS 117 and ProSe function 130 is used to provide subscription information in order to authorize access for direct discovery and direct communication on a per-PLMN basis.

UEs 120-121 may be considered as ProSe-enabled, meaning that they support ProSe requirements and associated procedures. A ProSe-enabled UE may refer to a non-Public Safety UE or a Public Safety UE. UEs 120-121 include an application 122-123, respectively, that is used to access/provide proximity services. UEs 120-121 support the following
5 functions: exchange of ProSe control information between the UE and ProSe function 130 over the PC3 reference point, procedures for open and restricted direct discovery of other UEs over the PC5 reference point, procedures for one-to-one or one-to-many direct communication over the PC5 reference point, and procedures to act as a UE-to-network relay.

Proximity services as discussed herein include the following functions: discovery,
10 direct communication (D2D), and UE-to-network relay. Discovery is a process that identifies a UE in proximity of other UEs. One type of discovery is direct discovery, which is a process employed by a UE to discover other UEs in its vicinity by using only the capabilities of the two UEs. For example, one UE may use local radio resources to discover the presence of other UEs in its vicinity. Another type of discovery is referred to as EPC-level discovery,
15 which is a process by which EPC network 110 determines the proximity of two UEs and informs them of their proximity. For example, a server in EPC network 110 may monitor the location of UEs, and inform the UEs of their proximity.

Direct communication is a communication between two or more UEs in proximity by means of user data plane transmissions using radio technology (e.g., E-UTRA) via a channel
20 not traversing any network node (other than possibly a base station of a RAN). Direct communication allows the UEs to use local radio resources to communicate directly with each other without routing traffic through a core network, such as EPC network 110. For example, UEs may directly communicate through the radio resources available to both UEs from a RAN, such as from a base station. UEs may also directly communicate through the
25 radio resources of the UEs themselves, such as over the PC5 reference point. Either way, the traffic exchanged between the UEs is not routed through the core network, but is routed directly between the UEs over a wireless interface.

UE-to-network relay is a function where one UE provides functionality to support connectivity to “unicast” services for one or more remote UEs. A remote UE refers to a UE
30 that is not served by a RAN (e.g., E-UTRAN), and communicates with a Packet Data Network (PDN) through a UE-to-network relay. For instance, if a remote UE is out-of-coverage of a RAN, then the remote UE may still access the PDN through another UE (relay UE) that is in-coverage of the RAN. A relay UE is a device that is enabled for UE-to-network relay. UE-to-network relay allows for one-to-one or one-to-many

communications from the network to a remote UE via a relay UE which is in-coverage, or from a remote UE to the network via a relay UE that is in-coverage.

FIG. 2 illustrates a service pre-configuration procedure for a UE 120. The Home PLMN (HPLMN) pre-configures UE 120 with the authorization information for a list of PLMNs where UE 120 is authorized to perform direct discovery, direct communication, or both. If there is no associated UE context, ProSe function 130 obtains the subscription information for direct discovery and/or direct communication from HSS 117.

In order to access a proximity service, a UE 120-121 (i.e., a non-public safety UE) has to first be authorized and configured for the service. FIG. 3 illustrates a service authorization procedure for UE 120. UE 120 receives service authorization for direct discovery, direct communication, or both with a given validity time from ProSe function 130 of its HPLMN. UE 120 performs this service authorization procedure before starting the setup of direct discovery or direct communication if UE 120 has no valid authorization information, when a UE is already engaged in a direct discovery or direct communication but changes its registered PLMN, or when a prior authorization expires. To identify ProSe function 130 of its HPLMN, UE 120 may interact with a Domain Name Service (DNS) function (not shown) to discover ProSe function 130, or information for ProSe function 130 may be pre-provisioned in UE 120. UE 120 transmits an authorization request for direct discovery, direct communication, or both to ProSe function 130 in its HPLMN. In response to the authorization request, ProSe function 130 transmits a request for subscription information (e.g., a subscriber profile) associated with UE 120 to HSS 117, assuming that ProSe function 130 does not already have this information for UE 120. HSS 117 identifies subscription information for UE 120 that is related to proximity services (e.g., direct discovery and/or direct communication), and transmits a response to ProSe function 130 with the subscription information. ProSe function 130 then sends an authorization response to UE 120 with authorization information for a proximity service, which is stored by UE 120. UE 120 may perform direct discovery and/or direct communications using a PLMN that is authorized by ProSe function 130.

After authorization and provisioning, UEs 120-121 may send a discovery request to EPC network 110, which is processed by ProSe function 130. Two types of discovery are defined for direct discovery: open and restricted. In open discovery, no explicit permission is needed from a UE being discovered. In restricted discovery, explicit permission is needed from a UE being discovered. The 3GPP has also defined two possible direct discovery modes: Model A and Model B. Model A ("I am here"), defines two roles for UEs that are

participating in direct discovery. One role is an announcing UE, which announces certain information that could be used by UEs in proximity that have permission to discover. The other role is a monitoring UE, which monitors certain information of interest in proximity of announcing UEs. In this model, the announcing UE broadcasts discovery messages at
5 pre-defined discovery intervals, and the monitoring UEs that are interested in these messages read them and process them.

Model B (“Who is there?”/“Are you there?”) is used when restricted discovery type is used, and defines two roles for UEs that are participating in direct discovery. One role is a discoverer UE, which transmits a request containing certain information about what it is
10 interested to discover. The other role is a discoveree UE, which can respond with some information related to the discoverer’s request.

FIG. 4 illustrates a discovery request procedure for an announcing UE 120 (non-roaming, open discovery). UE 120 is configured with a data structure of the Application IDs corresponding to its HPLMN. If UE 120 is authorized to announce in its HPLMN, then
15 UE 120 sends a discovery request to ProSe function 130. The discovery request includes a ProSe Application ID, UE Identity, announce command, Application ID, Discovery Entry ID, [Requested Timer], [Application Level Container], and [PC5_tech]. The ProSe Application ID indicates what the UE is interested to announce. The UE Identity is set to its International Mobile Subscriber Identity (IMSI). The Application ID represents a unique identifier of the
20 UE application that has triggered the transmission of the discovery request. The Discovery Entry ID indicates whether this is a new request. The Requested Timer is an optional parameter, and indicates the length of validity timer associated with the ProSe Application Code that the UE expects to receive from ProSe function 130. PC5_tech is an optional parameter that indicates the PC5 radio technology (e.g., E-UTRA, WLAN) that UE 120
25 wishes to use for announcements. ProSe function 130 checks for the authorization of the application represented by the Application ID. If there is no associated UE context, then ProSe function 130 checks with HSS 117 regarding the authorization of UE 120 for discovery, and creates a new context for UE 120 that contains the subscription parameters for UE 120.

If UE 120 indicated that it desired application-controlled extension by the inclusion of
30 the Application Level Container, then ProSe function 130 sends an Authorization Request (ProSe Application ID, Request Type, Application Level Container, Allowed number of suffixes) to ProSe Application Server 132. The Request Type is set to “open discovery with application-controlled extension /announce”. The Allowed Number of Suffixes indicates how many ProSe Restricted Code Suffixes the ProSe Application Server 132 can assign for

UE 120. ProSe function 130 locates the ProSe Application Server 132 based on the Application ID. ProSe Application Server 132 returns an Authorization Response (Response Type, ProSe Application Code Suffix pool) to ProSe function 130 with the Response Type set to “open discovery with application-controlled extension /announce ack”. The ProSe
5 Application Code Suffix pool contains the Suffix(es) allocated by ProSe Application Server 132.

If the discovery request is authorized, then ProSe function 130 checks whether UE 120 is authorized to use the ProSe Application ID (e.g., UE 120 is authorized to announce) contained in the discovery request. If UE 120 is authorized to use the ProSe Application ID,
10 then ProSe function 130 responds to UE 120 with a discovery response. The discovery response includes a ProSe Application Code, validity timer, Discovery Entry ID, and [PC5_tech]. The ProSe Application Code is provided by ProSe function 130, and corresponds to the ProSe Application ID that was contained in the discovery request (i.e., is composed from a PLMN ID and a temporary ID for the Application ID). The validity timer
15 indicates for how long this ProSe Application Code is valid. ProSe function 130 takes into account the Requested Timer parameter, if provided by UE 120, when allocating the validity timer. UE 120 will be authorized to announce this ProSe Application Code for the duration of the validity timer and if it remains in the HPLMN. When the validity timer expires or UE 120 changes its registered PLMN, then UE 120 requests a new ProSe Application Code. The
20 optional PC5_tech parameter indicates the PC5 radio technology(ies) that is/are authorized to be used for the assigned ProSe Application Code. After UE 120 receives the discovery response, it is configured to announce on PC5 using a discovery message and the ProSe Application Code.

FIG. 5 illustrates a discovery request procedure for a monitoring UE 121
25 (non-roaming, open discovery). UE 121 is configured with a data structure of the ProSe Application IDs corresponding to its PLMNs. If UE 121 is authorized to monitor in at least one PLMN, then UE 121 sends a discovery request to ProSe function 130. The discovery request from a monitoring UE may include similar information as described above, except the command is set to “Monitor”. The ProSe Application ID(s) indicate what UE 121 is
30 interested in monitoring, and they consist of a subset of the data structure of the PLMN. The Application ID represents a unique identifier of the application that has triggered the transmission of the discovery request message. ProSe function 130 checks for the authorization of the application represented by the Application ID. If there is no associated UE context, then ProSe function 130 checks with HSS 117 regarding the authorization of UE

121 for discovery, and creates a new context for UE 121 that contains the subscription parameters for UE 120.

If UE 121 indicated that it desired application-controlled extension by the inclusion of the Application Level Container, then ProSe function 130 sends an Authorization Request (ProSe Application ID, Request Type, Application Level Container) to ProSe Application Server 132 indicated by the Application ID. The Request Type is set to “open discovery with application-controlled extension /monitor”. ProSe Application Server 132 returns an Authorization Response (Response Type, mask(s) for the ProSe Application Code Suffix(es) corresponding to ProSe Application ID) to ProSe function 130 with the Response Type set to “open discovery with application-controlled extension /monitor ack”.

If the discovery request is authorised, then ProSe function 130 responds to UE 121 with a discovery response. The discovery response includes a Discovery Filter(s), Discovery Entry ID, and [PC5_tech]. The Time to Live (TTL(s)) in the Discovery Filter(s) indicate how long the Discovery Filter(s) are valid. If application-controlled extension is used, the ProSe Application Code in the Discovery Filter is replaced by the ProSe Application Code Prefix. Besides the ProSe Application Code(s), the Discovery Filter may also contain the mask(s) for the ProSe Application Code Suffix, which is/are obtained from ProSe Application Server 132. UE 121 may add additional mask(s) and values for the Suffix part. After UE 121 receives the discovery response, it is configured to monitor on PC5 for Application Codes using the Discovery Filter(s) in the radio resources that are authorized and configured by the PLMN(s) to be used for ProSe. If the TTL corresponding to a Discovery Filter expires (because UE 121 has not refreshed the corresponding discovery request within the duration of the TTL), then ProSe function 130 removes the entry related to that Discovery Filter from the UE context.

Other discovery procedures, such as for restricted discovery, roaming, Model B, etc., are described in 3GPP TS 23.303.

As is evident in the above discovery procedures, ProSe function 130 performs some type of authorization of a UE by querying HSS 117. HSS 117 responds with subscription parameters for the UE, and ProSe function 130 determines whether this application is authorized for discovery. However, one problem is that a UE or other device can spoof an Application ID in a discovery request. The subscriber profile in HSS 117 may not indicate all ProSe applications residing in a UE that is authorized for ProSe. Thus, even if a UE is authorized for ProSe according to the subscriber profile, one or more applications may be maliciously used by this UE. The authorization procedure using HSS 117 is insufficient to protect against spoofed Application IDs.

To solve this and other related issues, an authorization mechanism is employed to detect spoofed Application IDs for proximity services, such as ProSe. When the term “ProSe” is used herein, it may refer to proximity service as described by the 3GPP or other proximity services. FIG. 6 illustrates an architecture 600 for proximity services in an illustrative embodiment. Architecture 600 may have similar elements and reference points as architecture 100 shown in FIG. 1. Architecture 600 may be implemented for 4G (e.g., LTE) or next-generation networks (e.g., 5G).

Architecture 600 includes a PLMN 610 for a non-roaming scenario, although more PLMNs may be included for roaming or inter-PLMN architectures. PLMN 610 is the home PLMN (HPLMN) of a UE 620, and includes a ProSe function 612, a ProSe Application Server (AS) 614, and an HSS 616 that are communicatively coupled to one another. Although not shown in FIG. 6, PLMN 610 may include a core network, and a RAN that includes one or more base stations (e.g., eNodeB). UE 620 is a non-public safety UE enabled for proximity services, and includes a proximity service (e.g., ProSe) application 622 that is configured to request direct discovery and/or direct communication.

PLMN 610 also includes an authorization mechanism 630. Authorization mechanism 630 comprises a system, apparatus, device, network element, etc., that is configured to authorize an application on a UE for direct discovery. Authorization mechanism 630 provides enhanced or additional discovery authorization procedures in response to a discovery request to ensure that the application, which initiated the discovery request, is authorized for direct discovery. As described above, a traditional ProSe function performs some discovery authorization procedures in response to a discovery request by querying an HSS. However, these discovery authorization procedures may not be sufficient when an application maliciously spoofs an Application ID for an application. Thus, authorization mechanism 630 provides enhanced or additional discovery authorization procedures by challenging a UE, which is described in further detail below.

Authorization mechanism 630 is shown generally in FIG. 6 as an element of PLMN 610. As authorization mechanism 630 is part of a system within PLMN 610, it may be a stand-alone element in PLMN 610 that is able to communicate with UE 620, ProSe function 612, ProSe Application Server 614, and/or HSS 616. Alternatively, authorization mechanism 630 may be implemented in ProSe function 612. In another alternative, authorization mechanism 630 may be implemented in ProSe Application Server 614.

FIG. 7 is a block diagram of an authorization mechanism 630 in an illustrative embodiment. Authorization mechanism 630 includes an interface component 702, one or

more processors 704, and a memory 706. Interface component 702 is a hardware component configured to communicate with a variety of elements. For example, interface component 702 may be configured to communicate with UE 620, ProSe function 612, ProSe Application Server 614, and/or HSS 616. Processor 704 represents the internal circuitry, logic, hardware, etc., that provides the functions of authorization mechanism 630. Memory 706 is a computer readable storage medium (e.g., ROM or flash memory) for data, instructions, applications, etc., and is accessible by processor 704. Authorization mechanism 630 may include various other components not specifically illustrated in FIG. 7.

Processor 704 implements a rules engine 710 and a validation controller 712. Rules engine 710 is configured to generate, identify, or determine validation rules 714 that are used to determine whether an application is authorized for direct discovery. Validation controller 712 is configured to determine whether an application is authorized for direct discovery based on validation rules 714. Processor 704 may implement other components for authorizing an application for direct discovery.

In this embodiment, memory 706 is configured to store a database 720 provisioned with security parameters that are mapped to Application IDs. Database 720 may comprise a local database for authorization mechanism 630, or may comprise a network database that is accessible by authorization mechanism 630, such as through interface component 702. FIG. 8 illustrates database 720 in an illustrative embodiment. Database 720 stores records 801-803 for Application IDs 811-813, although records for more Application IDs may also be stored. Each record 801-803 maps an Application ID 811-813 to a set of one or more security parameters 820. A security parameter comprises a characteristic or property that verifies or authenticates a UE or an application. Security parameters 820 include one or more values (e.g., codes, labels, quantities, etc.) that are authorized for its associated Application ID 811-813. For example, record 801 is provisioned for Application ID 811, where Application ID 811 is mapped to security parameters 820. Security parameters 820 include a UE Identity, network address(es), PLMN code(s), location code(s), passcode(s), UE category type, and discovery type, although other security parameters may be included. Each security parameter includes one or more authorized values that are provisioned for Application ID 811. For example, the UE Identity parameter includes one or more values indicating approved UE Identities (or ranges) for Application ID 811, such as one or more IMSIs. The network address parameter includes one or more values indicating approved network address(es) for Application ID 811, such as one or more transport layer (e.g., IP) addresses. The PLMN code parameter includes one or more values indicating approved PLMN code(s) for Application ID

811. The location code parameter includes one or more values indicating approved location code(s) for Application ID 811. The passcode parameter includes one or more values indicating approved passcode(s) or password(s) for Application ID 811 used to access an application. The UE category type parameter includes one or more values indicating approved UE category types for Application ID 811, such as CAT1-CAT8, LTE Cat-M1 (eMTC), Cat-NB1 (NB-IoT), etc. The discovery type parameter includes one or more values indicating approved discovery types for Application ID 811, such as Model A (open or restricted), announce role for Model A, monitor role for Model A, Model B, Model B discovery type/mode, etc. Additional security parameters and associated values may be provisioned as desired.

In FIG. 6, UE 620 may perform a service pre-configuration procedure as shown in FIG. 2, and a service authorization procedure as shown in FIG. 3. At this point, application 622 in UE 620 may want to initiate a discovery request procedure. Thus, application 622 sends a discovery request to ProSe function 612 (see FIGS. 4-5). The discovery request may include similar information as described above, such as a ProSe Application ID, UE Identity, command, Application ID, Discovery Entry ID, [Requested Timer], [Application Level Container], and [PC5_tech]. Authorization mechanism 630 then performs a discovery authorization procedure as described in further detail in FIG. 9.

FIG. 9 is a flow chart illustrating a method 900 of performing a discovery authorization procedure in an illustrative embodiment. The steps of method 900 will be described with reference to authorization mechanism 630 in FIG. 7, but those skilled in the art will appreciate that method 900 may be performed in other devices. The steps of the flow charts described herein are not all inclusive and may include other steps not shown, and the steps may be performed in an alternative order.

Validation controller 712 receives information for the discovery request sent by application 622 in UE 620 to ProSe function 612 (step 902), such as through interface component 702. If authorization mechanism 630 is implemented in ProSe function 612, then validation controller 712 may receive the actual discovery request that was sent by application 622. If authorization mechanism 630 is a stand-alone element or is implemented in ProSe Application Server 614, then validation controller 712 may receive the information for the discovery request from ProSe function 612, such as in an authorization request. The information for the discovery request at least includes an Application ID for application 622.

Rules engine 710 determines validation rules 714 for the discovery authorization procedure (step 904). Validation rules 714 comprise any rules that validate an application on

a UE that initiates a discovery request. Validation rules 714 may include a network address check. This rule may compare a dynamic network address (e.g., IP address) assigned to a UE with a range of network addresses that are approved (whitelist) or not approved (black list) for an Application ID. Validation rules 714 may include a PLMN code check, which verifies whether direct discovery by the application is allowed in the PLMN (which a UE is attached). Validation rules 714 may include an application passcode check, which verifies whether a passcode (or password) provided by an application/UE matches an approved passcode for the application. Validation rules 714 may include a network (PLMN) sensitivity check. This rule verifies whether an Application ID from an announcing UE belongs to a secure network (home or foreign), as some networks may be restricted from direct discovery for an application. Validation rules 714 may include a network traffic volume check. This rule determines whether traffic volume associated with an Application ID (i.e., either or both of a specific transmitter and transceiver entity address) exceeds a threshold, as a malicious application may generate significant traffic volume. If the threshold is exceeded, then a discovery request may be denied for the application. If traffic volume is below the threshold, then the discovery request may be authorized. Validation rules 714 may include a UE category type check, which verifies whether a UE category type, such as CAT1-CAT8, LTE Cat-M1 (eMTC), Cat-NB1 (NB-IoT), etc., is allowed for an application. Validation rules 714 may include a ProSe discovery type check, which verifies whether an application is authorized for a particular discovery type, such as Model A (open or restricted), announce role for Model A, monitor role for Model A, Model B, Model B discovery type/mode, etc. Validation rules 714 may include a UE location check, which verifies whether a location code for a UE matches an approved location code for an Application ID. Validation rules 714 may include a time check, which verifies whether a discovery request is allowed based on a Time of Day, Day of Week, etc. Other validation rules 714 may be defined as desired.

For the discovery authorization procedure, validation controller 712 sends a security challenge message to UE 620 requesting challenge values for one or more security parameters that are mapped to the Application ID (step 906), such as through interface component 702. UE 620 may store information that may be used for security purposes, and the security challenge message may request that UE 620 responds with this information. The security challenge message is a separate message that is sent to UE 620 after application 622 sends the discovery request to ProSe function 612. The security challenge message may request challenge values for one or more of the security parameters mapped to an Application ID as shown in FIG. 8. For example, the security challenge message may request challenge

values for a network address that is statically or dynamically assigned to UE 620, a PLMN code for the HPLMN for UE 620 or a visited/local PLMN where UE 620 is attached, a location code for UE 620, a passcode used to access application 622, a UE category type for UE 620, etc.

5 If validation controller 712 does not receive a security answer message from UE 620, then validation controller 712 generates a rejection indicator to reject the discovery request sent by application 622 (step 908). If validation controller 712 receives a security answer message from UE 620, such as through interface component 702, then validation controller 712 extracts the challenge values for the security parameters from the security answer
10 message as provided by UE 620 (step 910). Validation controller 712 may also acquire values for some of the security parameters from the discovery request, from HSS 616, or other network entities. Validation controller 712 then determines whether application 622 is authorized for direct discovery using the Application ID based on the challenge values (and optionally other values) for the security parameters and validation rules 714 (step 912). One
15 way of determining whether application 622 is authorized (e.g., step 912 of method 900) is provided in FIG. 10.

FIG. 10 is a flow chart illustrating a method 1000 of determining whether application 622 is authorized for direct discovery in an illustrative embodiment. Validation controller 712 accesses database 720 to identify the authorized values for the security parameters
20 mapped to the Application ID (step 1002). Validation controller 712 then compares the challenge values provided by UE 620 to the authorized values for the Application ID to determine whether application 622 is authorized for direct discovery using the Application ID (step 1004). For instance, when none of the challenge values provided by UE 620 match the authorized values for the Application ID, validation controller 712 determines that
25 application 622 is not authorized for direct discovery using the Application ID (step 1006). When one or more of the challenge values provided by UE 620 match the authorized values for the Application ID, validation controller 712 may determine that application 622 is authorized for direct discovery using the Application ID (step 1008). The number of matches between the challenge values and authorized values required to authorize application 622
30 may depend on a network policy provisioned by the network operator.

As an example of method 1000, one of validation rules 714 may be a network address check, where validation controller 712 compares a network address provided by UE 620 in the security answer message with one or more approved network addresses for the Application ID. If the network address provided by UE 620 in the security answer message

does not match an approved network address for the Application ID, then validation controller 712 may determine that application 622 is not authorized for direct discovery using the Application ID. If the network address provided by UE 620 in the security answer message matches an approved network address for the Application ID, then validation controller 712 may determine that application 622 is authorized for direct discovery using the Application ID, depending on other validation rules 714 (if applicable).

Another one of validation rules 714 may be a passcode check, where validation controller 712 compares a passcode provided by UE 620 in the security answer message with one or more approved passcodes for the Application ID. If the passcode provided by UE 620 in the security answer message does not match an approved passcode for the Application ID, then validation controller 712 may determine that application 622 is not authorized for direct discovery using the Application ID. If the passcode provided by UE 620 in the security answer message matches an approved passcode for the Application ID, then validation controller 712 may determine that application 622 is authorized for direct discovery using the Application ID, depending on other validation rules 714 (if applicable).

Another one of validation rules 714 may be a location code check, where validation controller 712 compares a location code provided by UE 620 in the security answer message with one or more approved location codes for the Application ID. If the location code provided by UE 620 in the security answer message does not match an approved location code for the Application ID, then validation controller 712 may determine that application 622 is not authorized for direct discovery using the Application ID. For instance, if an Application ID is associated with a Brazil country code but UE 620 provides a location code in the United States, then validation controller 712 determines that application 622 is not authorized for direct discovery using the Application ID. If the location code provided by UE 620 in the security answer message matches an approved location code for the Application ID, then validation controller 712 may determine that application 622 is authorized for direct discovery using the Application ID, depending on other validation rules 714 (if applicable).

When application 622 is not authorized for direct discovery using the Application ID, validation controller 712 generates a rejection indicator to reject the discovery request sent by application 622 (step 908). Validation controller 712 may provide the rejection indicator to ProSe function 612, such as through interface component 702, which may then reject the discovery request by sending a discovery response with information indicating that the discovery request has been rejected. If application 622 is authorized for direct discovery using the Application ID, then validation controller 712 generates a validation indicator to

authorize the discovery request sent by application 622 (step 914). Validation controller 712 may provide the validation indicator to ProSe function 612, such as through interface component 702. When application 622 is authorized by validation controller 712, ProSe function 612 may continue with the discovery request procedure, and send a discovery response to UE 620 as indicated in FIGS. 4-5, or may perform further authorization procedures (e.g., query HSS 616). The discovery response may include an Application Code (for announcing), Discovery Filter(s) for monitoring, or other information that allows UE 620/application 622 to perform direct discovery using the Application ID.

Authorization mechanism 630 provides an additional level of validation of an Application ID in response to a discovery request. One technical benefit is that it is more difficult for an application to spoof an Application ID and be granted permission for a discovery procedure by a ProSe function. Thus, proximity services in a network will be utilized by authorized applications, while malicious applications will be blocked.

As described above, authorization mechanism 630 may be implemented in ProSe function 612. FIG. 11 is a flow diagram when authorization mechanism 630 is implemented in ProSe function 612 in an illustrative embodiment. UE 620 (through application 622) sends a discovery request to ProSe function 612. The discovery request includes the ProSe Application ID, UE Identity, command type (announcing, monitoring, etc.), Discovery Entry ID, Application ID, etc. ProSe function 612 (through authorization mechanism 630) then initiates a discovery authorization procedure. ProSe function 612 sends a security challenge message to UE 620 requesting challenge values for one or more security parameters. ProSe function 612 receives a security answer message from UE 620, and extracts the challenge values for the security parameters from the security answer message as provided by UE 620. ProSe function 612 then determines whether application 622 is authorized for direct discovery using the Application ID based on the challenge values (and optionally other values) for the security parameters and validation rules 714. If application 622 is not authorized for direct discovery using the Application ID, then ProSe function 612 rejects the discovery request sent by application 622. If application 622 is authorized for direct discovery using the Application ID, then ProSe function 612 sends a discovery response to UE 620 with information for direct discovery (e.g., Application Code, Discovery Filter, etc.). ProSe Function 612 may also include one or more security parameters (and approved values) associated with the approved Application ID, in the ProSe Application Code Suffix pool (and may be reflected in the Application Code/Mask) of the discovery response.

FIG. 12 is a flow diagram when authorization mechanism 630 is implemented in ProSe Application Server 614 in an illustrative embodiment. UE 620 (through application 622) sends a discovery request to ProSe function 612. The discovery request includes the ProSe Application ID, UE Identity, command type (announcing, monitoring, etc.), Discovery Entry ID, Application ID, etc. Based on network policy, ProSe function 612 requests that ProSe Application Server 614 validate the Application ID in response to the discovery request. Thus, ProSe function 612 sends an authorization request to ProSe Application Server 614. ProSe function 612 includes the Application ID for application 622 and associated parameters in the Application Level Container to ProSe Application Server 614. ProSe Application Server 614 (through authorization mechanism 630) then initiates a discovery authorization procedure. ProSe Application Server 614 sends a security challenge message to ProSe function 612, which forwards the security challenge message to UE 620 requesting challenge values for one or more security parameters. ProSe Application Server 614 may alternatively send the security challenge message directly to UE 620. ProSe function 612 receives a security answer message from UE 620, and forwards the security answer message to ProSe Application Server 614. ProSe Application Server 614 extracts the challenge values for the security parameters from the security answer message as provided by UE 620. ProSe Application Server 614 then determines whether application 622 is authorized for direct discovery using the Application ID based on the challenge values (and optionally other values) for the security parameters and validation rules 714. If application 622 is not authorized for direct discovery using the Application ID, then ProSe Application Server 614 sends an authorization response to ProSe function 612 with a rejection indicator to reject the discovery request sent by application 622. If application 622 is authorized for direct discovery using the Application ID, then ProSe Application Server 614 sends an authorization response to ProSe function 612 with a validation indicator to authorize the discovery request sent by application 622. ProSe function 612 then sends a discovery response to UE 620 based on the validation/rejection indicator. ProSe Function 612 may also include one or more security parameters (and approved values) associated with the approved Application ID, in the ProSe Application Code Suffix pool (and may be reflected in the Application Code/Mask) of the discovery response.

Any of the various elements or modules shown in the figures or described herein may be implemented as hardware, software, firmware, or some combination of these. For example, an element may be implemented as dedicated hardware. Dedicated hardware elements may be referred to as “processors”, “controllers”, or some similar terminology.

When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term “processor” or “controller” should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, a network processor, application specific integrated circuit (ASIC) or other circuitry, field programmable gate array (FPGA), read only memory (ROM) for storing software, random access memory (RAM), non-volatile storage, logic, or some other physical hardware component or module.

Also, an element may be implemented as instructions executable by a processor or a computer to perform the functions of the element. Some examples of instructions are software, program code, and firmware. The instructions are operational when executed by the processor to direct the processor to perform the functions of the element. The instructions may be stored on storage devices that are readable by the processor. Some examples of the storage devices are digital or solid-state memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media.

Although specific embodiments were described herein, the scope of the disclosure is not limited to those specific embodiments. The scope of the disclosure is defined by the following claims and any equivalents thereof.

WHAT IS CLAIMED IS:

1. A system comprising:

an authorization mechanism that performs a discovery authorization procedure for proximity services (ProSe), the authorization mechanism comprising:

a validation controller configured to receive information for a discovery request sent by an application in User Equipment (UE), wherein the discovery request includes an application identifier (ID) for the application; and

a rules engine configured to determine validation rules for the discovery authorization procedure;

the validation controller is configured to send a security challenge message to the UE requesting challenge values for security parameters that are mapped to the application ID, to receive a security answer message from the UE in response to the security challenge message, to extract the challenge values for the security parameters from the security answer message as provided by the UE, and to determine whether the application is authorized for direct discovery using the application ID based on the challenge values for the security parameters and the validation rules;

the validation controller is configured to generate a validation indicator to authorize the discovery request sent by the application when the application is authorized for direct discovery using the application ID.

2. The system of claim 1 wherein:

the validation controller is configured to generate a rejection indicator to reject the discovery request sent by the application when the application is not authorized for direct discovery using the application ID.

3. The system of claim 1 wherein the authorization mechanism further comprises:

a database that maps the security parameters to the application ID;

wherein the security parameters mapped to the application ID include authorized values provisioned for the application ID.

4. The system of claim 3 wherein:

the validation controller is configured to identify the authorized values for the security parameters mapped to the application ID, and to compare the challenge values provided by

the UE to the authorized values provisioned for the application ID to determine whether the application is authorized for direct discovery using the application ID.

5. The system of claim 1 wherein:

5 the validation controller is configured to send the security challenge message to the UE requesting a network address assigned to the UE.

6. The system of claim 1 wherein:

10 the validation controller is configured to send the security challenge message to the UE requesting a Public Land Mobile Network (PLMN) code.

7. The system of claim 1 wherein:

15 the validation controller is configured to send the security challenge message to the UE requesting a location code for the UE.

8. The system of claim 1 wherein:

 the validation controller is configured to send the security challenge message to the UE requesting a passcode used to access the application.

20 9. The system of claim 1 wherein:

 the authorization mechanism is implemented in a ProSe function that receives the discovery request from the UE.

10. The system of claim 1 wherein:

25 the authorization mechanism is implemented in a ProSe Application Server that is communicatively coupled to a ProSe function that receives the discovery request from the UE.

30 11. A method of performing a discovery authorization procedure for proximity services (ProSe), the method comprising:

 receiving, in an authorization mechanism, information for a discovery request sent by an application in User Equipment (UE), wherein the discovery request includes an application identifier (ID) for the application;

determining, at the authorization mechanism, validation rules for the discovery authorization procedure;

sending a security challenge message from the authorization mechanism to the UE requesting challenge values for security parameters that are mapped to the application ID;

5 receiving a security answer message at the authorization mechanism from the UE in response to the security challenge message;

extracting, at the authorization mechanism, the challenge values for the security parameters from the security answer message as provided by the UE;

10 determining whether the application is authorized for direct discovery using the application ID based on the challenge values for the security parameters and the validation rules; and

generating a validation indicator to authorize the discovery request sent by the application when the application is authorized for direct discovery using the application ID.

15 12. The method of claim 11 further comprising:

generating a rejection indicator to reject the discovery request sent by the application when the application is not authorized for direct discovery using the application ID.

13. The method of claim 11 further comprising:

20 storing a database that maps the security parameters to the application ID;
wherein the security parameters mapped to the application ID include authorized values provisioned for the application ID.

14. The method of claim 13 wherein determining whether the application is authorized for
25 direct discovery comprises:

identifying the authorized values for the security parameters mapped to the application ID; and

30 comparing the challenge values provided by the UE to the authorized values provisioned for the application ID to determine whether the application is authorized for direct discovery using the application ID.

15. A non-transitory computer readable medium embodying programmed instructions executed by one or more processors, wherein the instructions direct the processors to implement:

an authorization mechanism that performs a discovery authorization procedure for proximity services (ProSe);

the authorization mechanism is configured to receive information for a discovery request sent by an application in User Equipment (UE), wherein the discovery request
5 includes an application identifier (ID) for the application;

the authorization mechanism is configured to determine validation rules for the discovery authorization procedure;

the authorization mechanism is configured to send a security challenge message to the UE requesting challenge values for security parameters that are mapped to the application ID,
10 to receive a security answer message from the UE in response to the security challenge message, to extract the challenge values for the security parameters from the security answer message as provided by the UE, and to determine whether the application is authorized for direct discovery using the application ID based on the challenge values for the security parameters and the validation rules; and

15 the authorization mechanism is configured to generate a validation indicator to authorize the discovery request sent by the application when the application is authorized for direct discovery using the application ID.

16. The computer readable medium of claim 15 wherein:

20 the authorization mechanism is configured to generate a rejection indicator to reject the discovery request sent by the application when the application is not authorized for direct discovery using the application ID.

17. The computer readable medium of claim 15 wherein:

25 the authorization mechanism is configured to store a database that maps the security parameters to the application ID; and

the security parameters mapped to the application ID include authorized values provisioned for the application ID.

30 18. The computer readable medium of claim 17 wherein:

the authorization mechanism is configured to identify the authorized values for the security parameters mapped to the application ID, and to compare the challenge values provided by the UE to the authorized values provisioned for the application ID to determine

whether the application is authorized for direct discovery using the application ID.

19. The computer readable medium of claim 15 wherein:

5 the authorization mechanism is implemented in a ProSe function that receives the discovery request from the UE.

20. The computer readable medium of claim 15 wherein:

10 the authorization mechanism is implemented in a ProSe Application Server that is communicatively coupled to a ProSe function that receives the discovery request from the UE.

FIG. 1

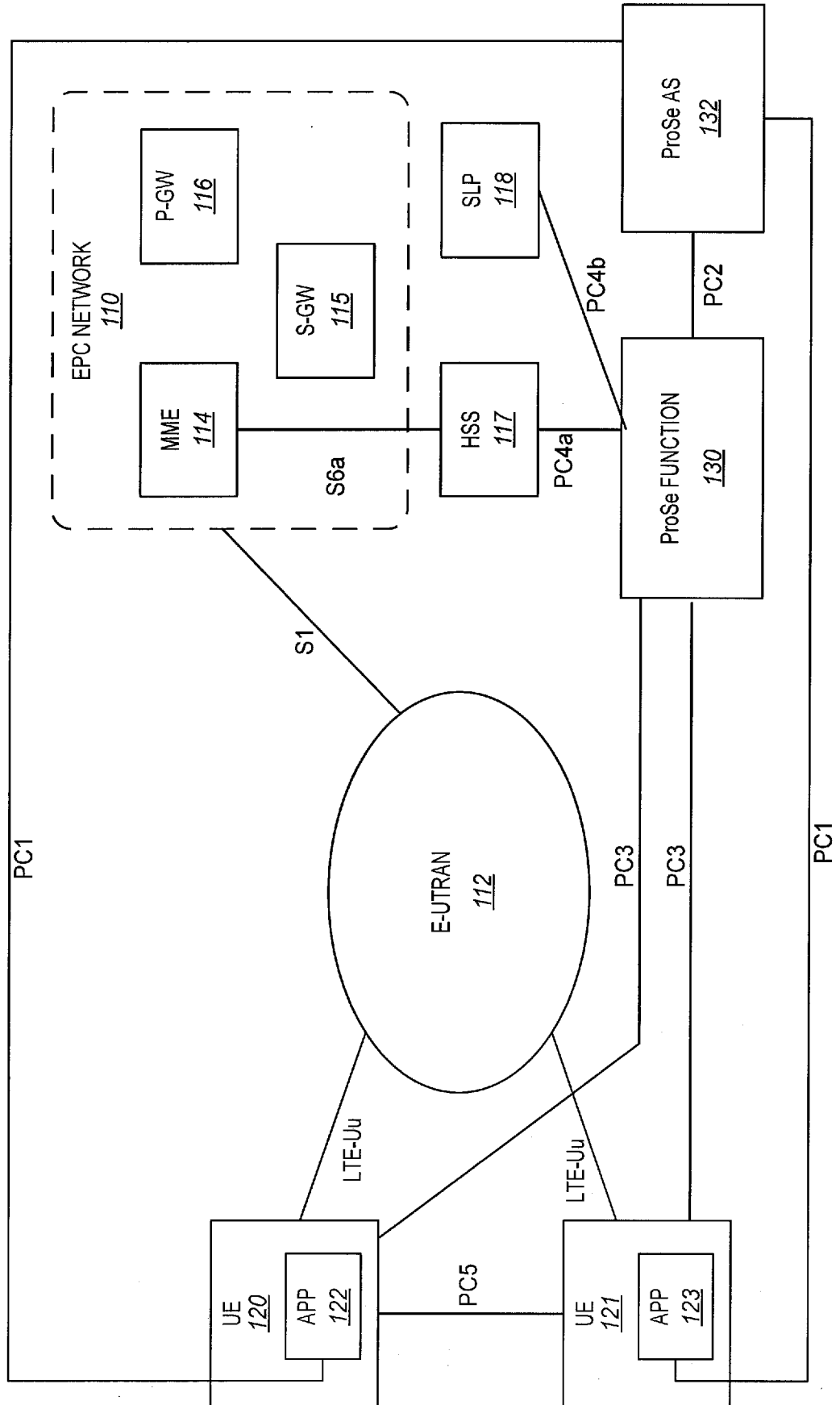


FIG. 2

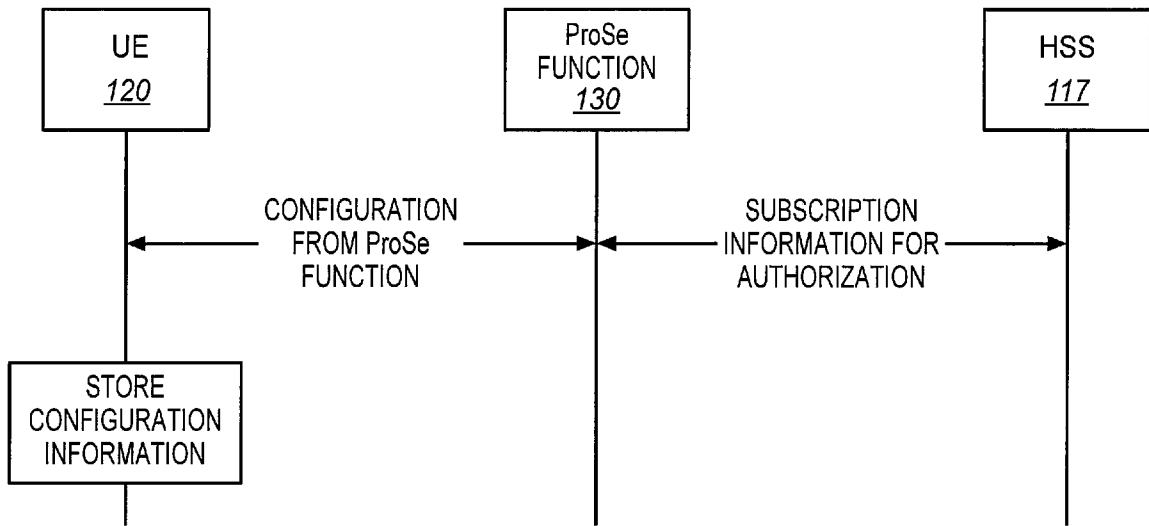


FIG. 3

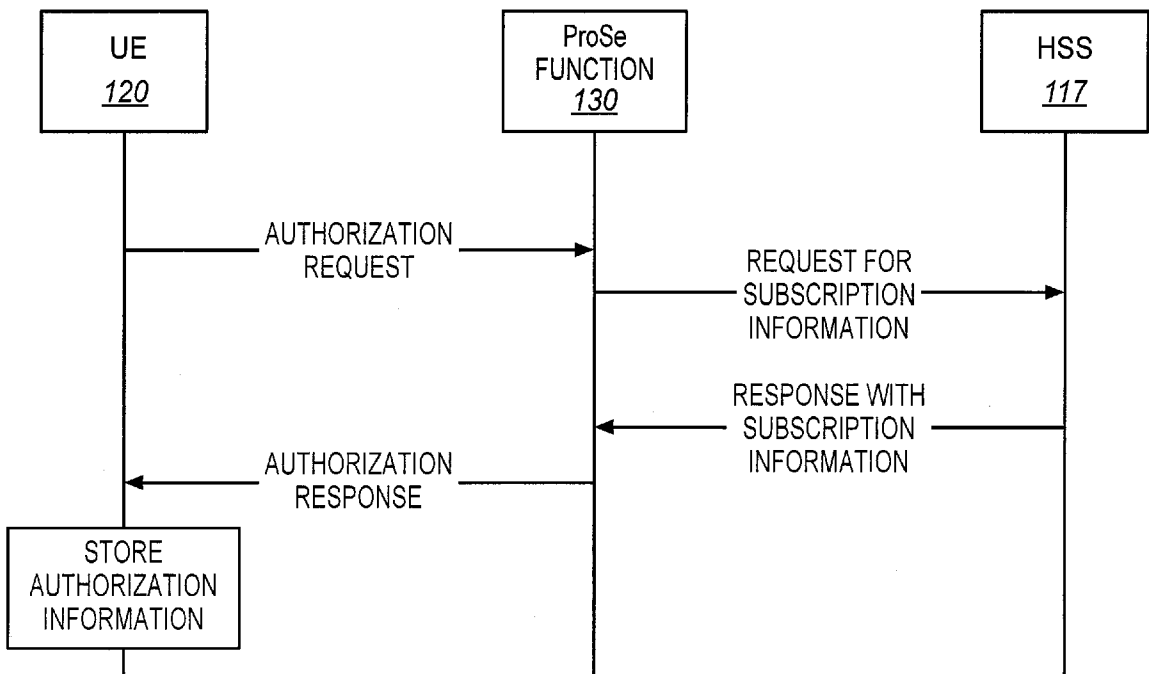


FIG. 4

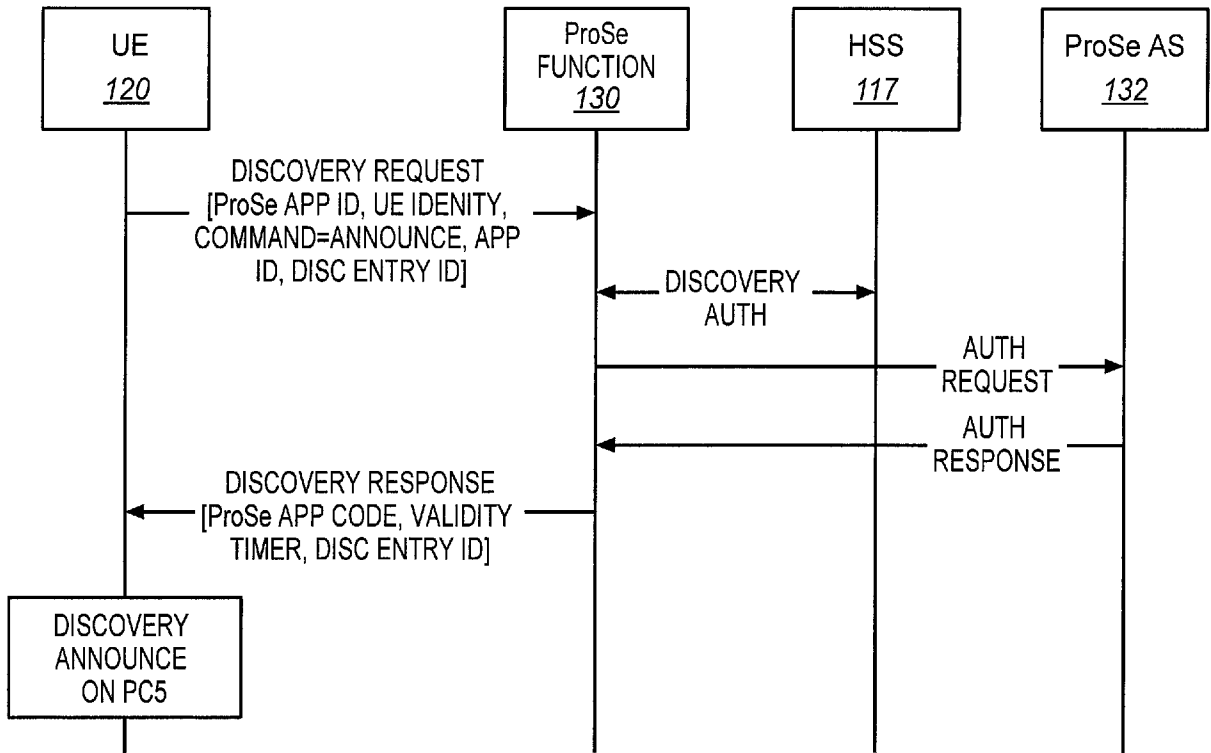


FIG. 5

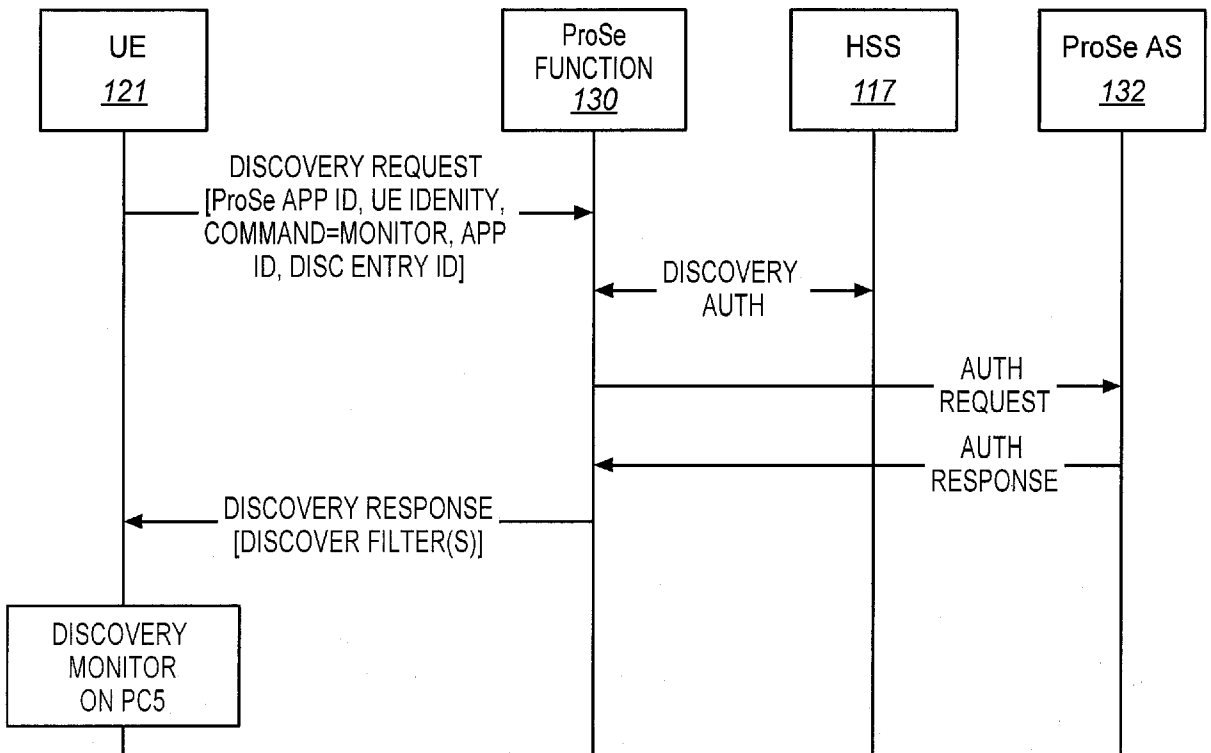


FIG. 6

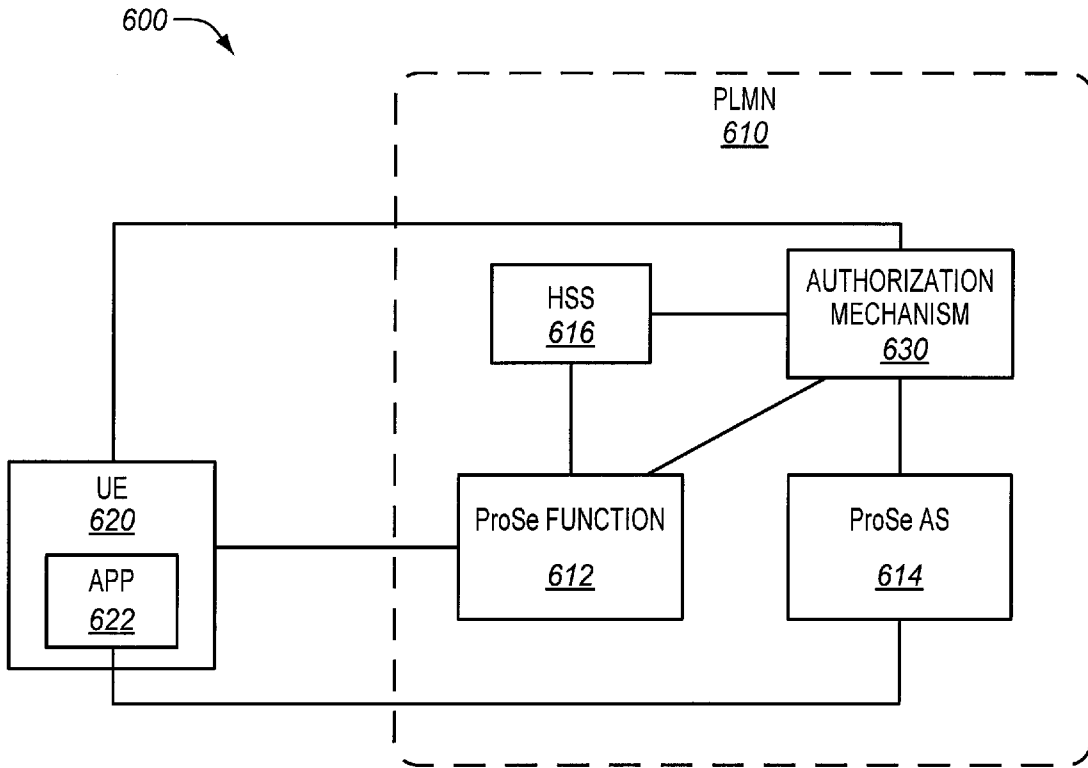


FIG. 7

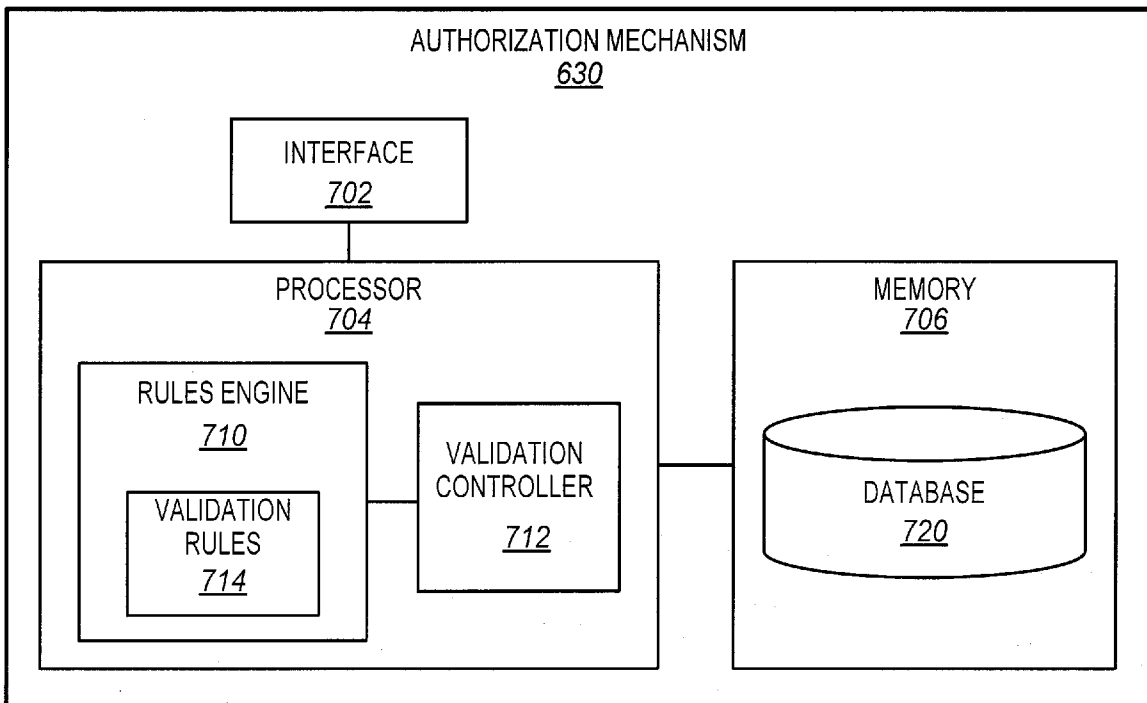


FIG. 8

720

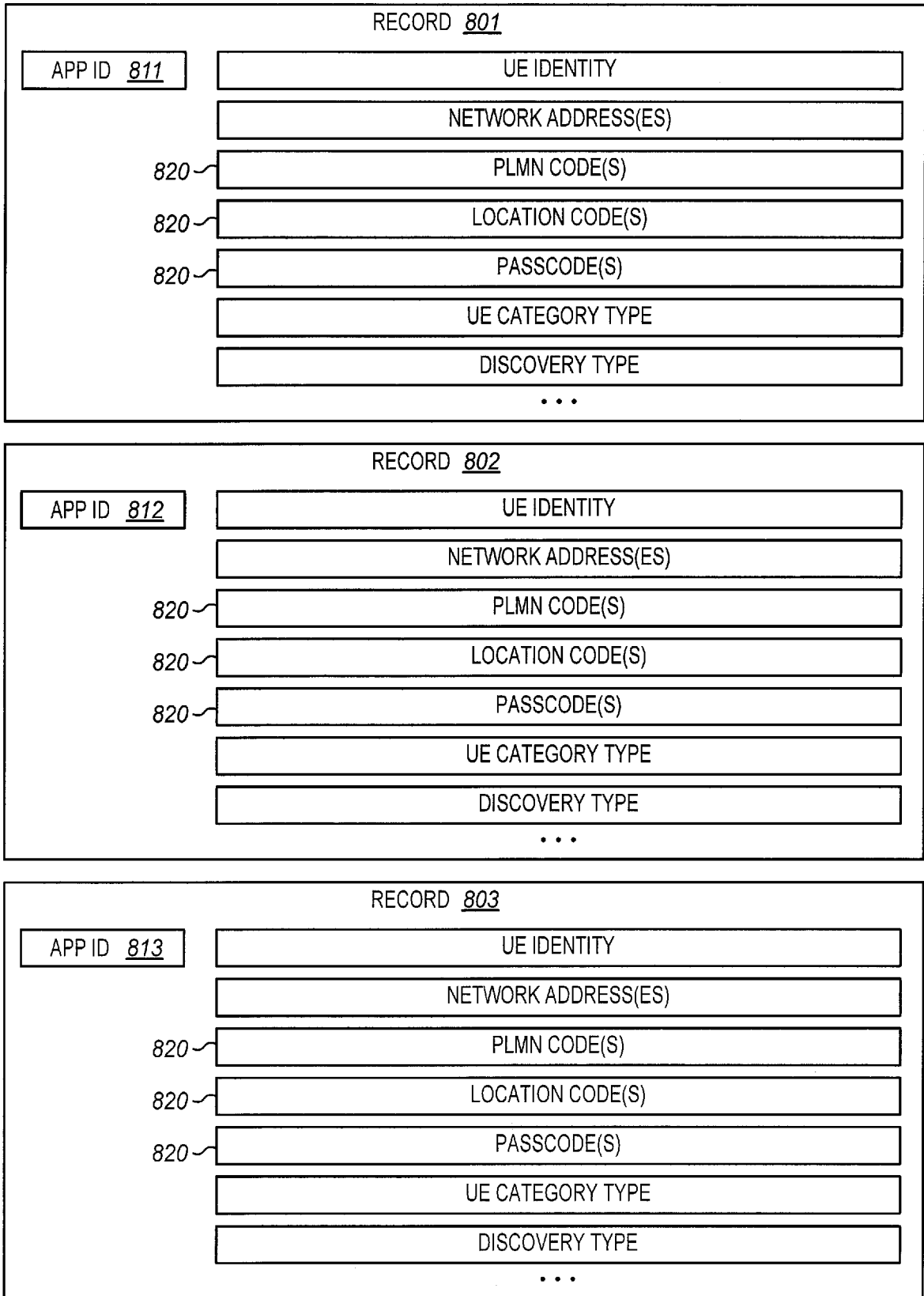


FIG. 9

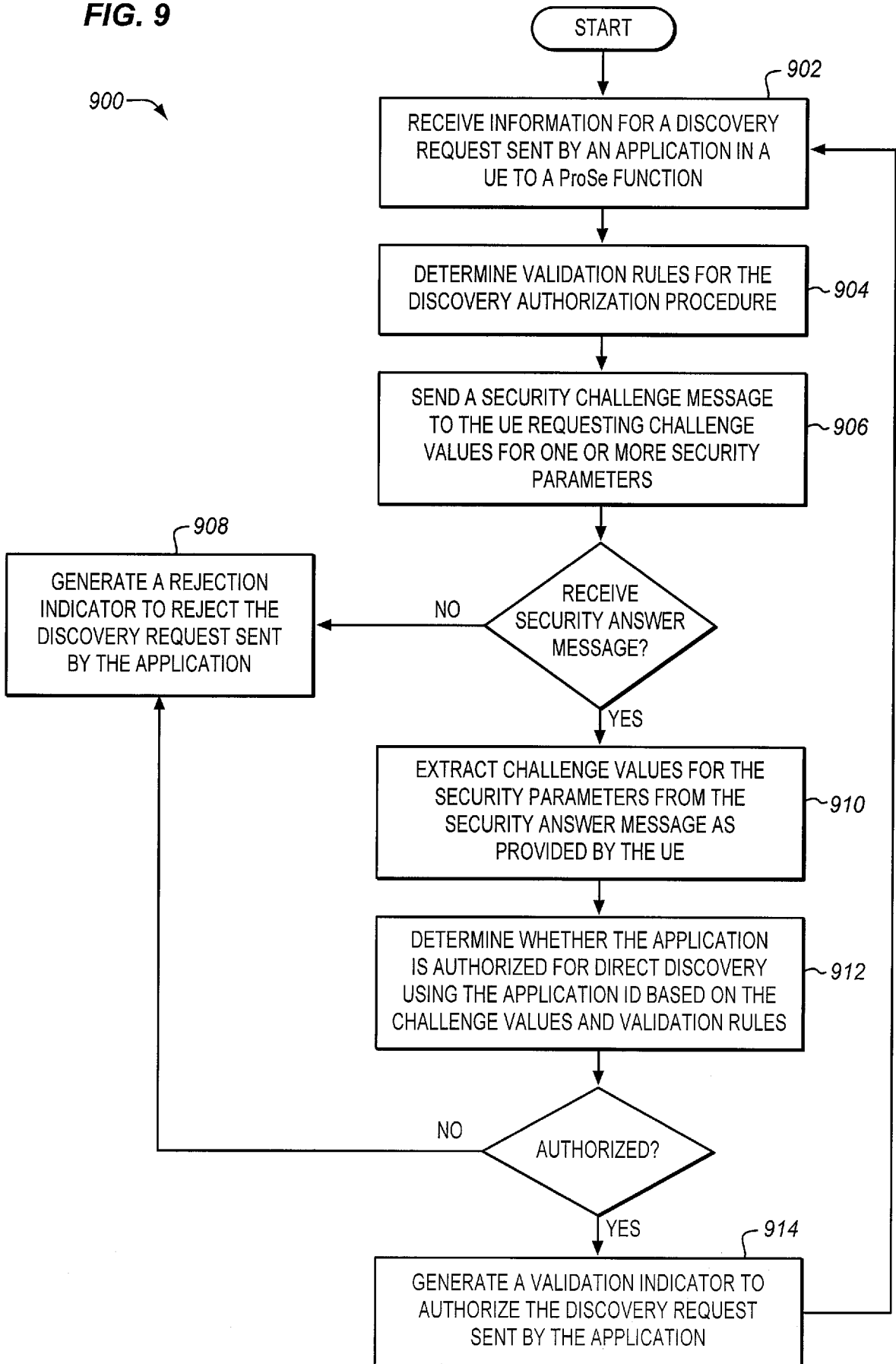


FIG. 10

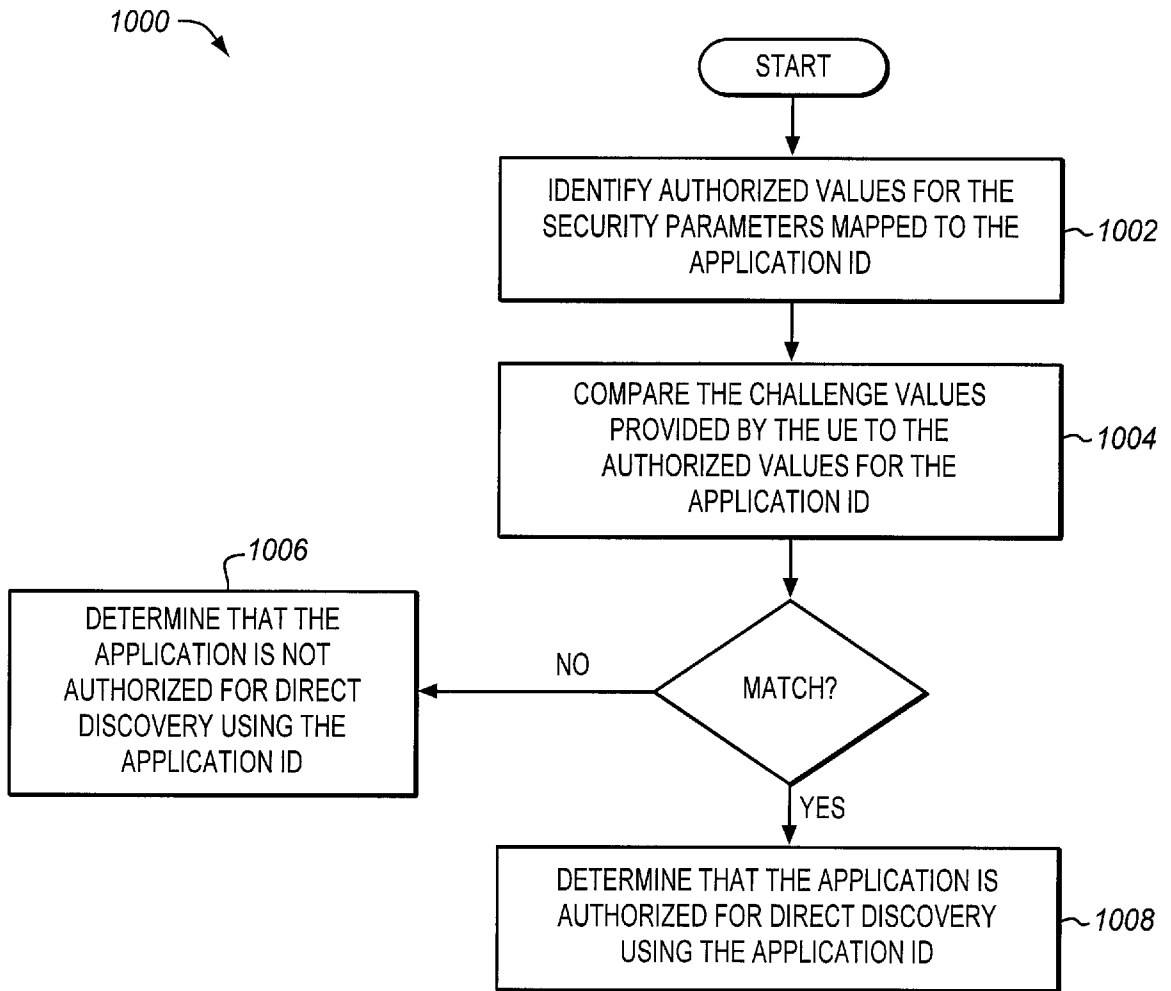


FIG. 11

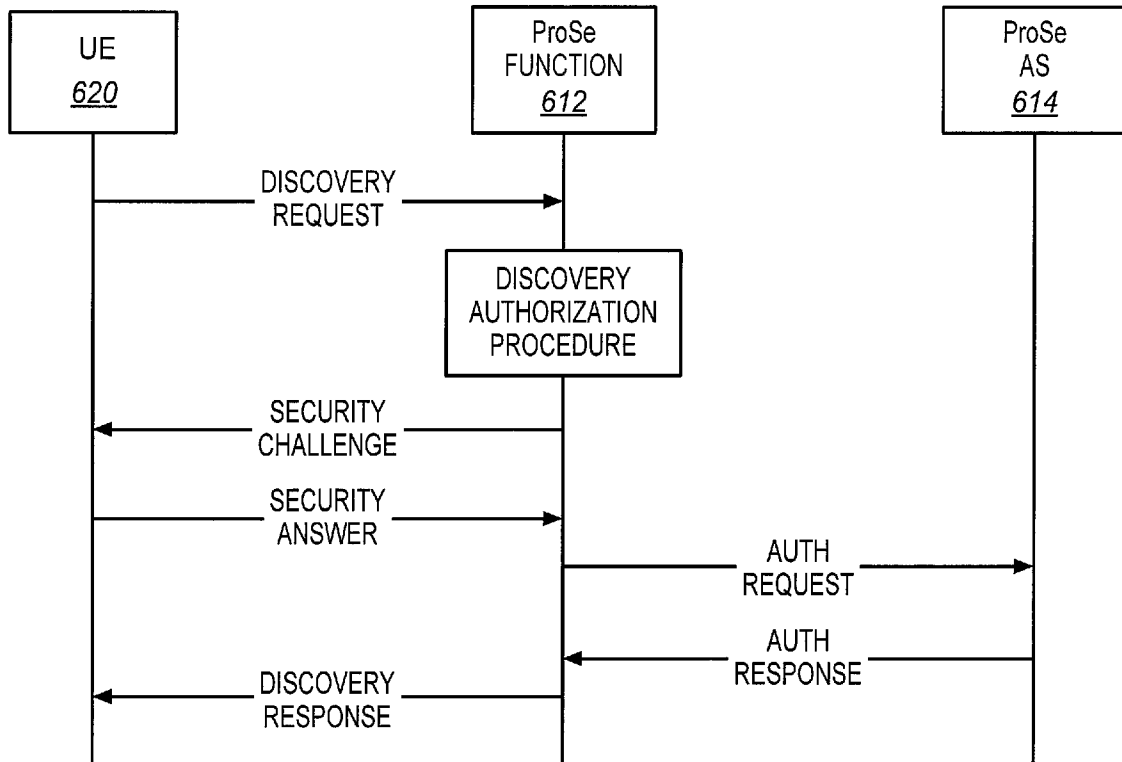
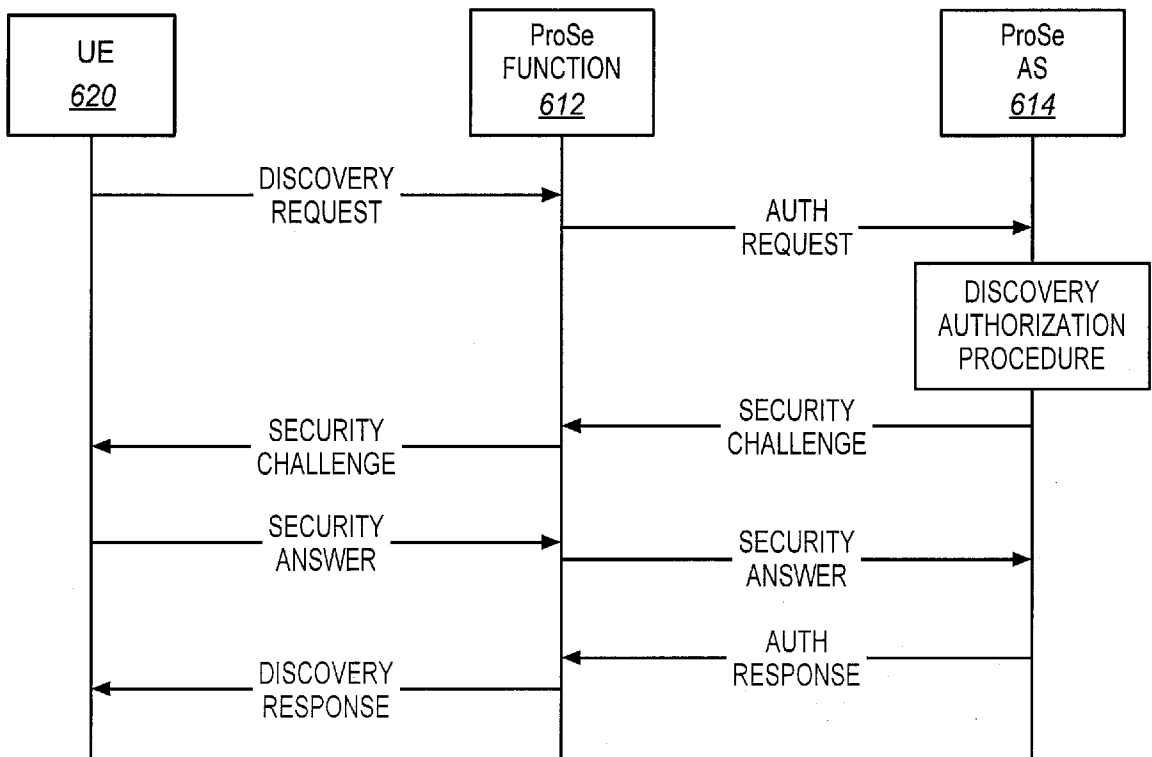


FIG. 12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/111028

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2009.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04Q

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)

CNPAT, CNKI, WPI, EPODOC, 3GPP: D2D, ProSe, authorization, UE, application, ID, validation, security challenge, response, compare

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016219437 A1 (SAMSUNG ELECTRONICS CO., LTD.) 28 July 2016 (2016-07-28) description, paragraphs[0032]-[0043], figures 3A, 3B	1-20
A	US 2016330619 A1 (SAMSUNG ELECTRONICS CO., LTD.) 10 November 2016 (2016-11-10) the whole document	1-20
A	CN 104244444 A (CHINA ACADEMY OF TELECOMM TECHNOLOGY) 24 December 2014 (2014-12-24) the whole document	1-20
A	CN 104066200 A (BEIJING SAMSUNG COMMUNICATION TECHNOLOGY ET AL.) 24 September 2014 (2014-09-24) the whole document	1-20
A	ZTE. "D2D authorization on multiple PLMN scenario" 3GPP TSG-RAN3 Meeting #84 R3-141220, 23 May 2014 (2014-05-23), the whole document	1-20

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

25 June 2018

Date of mailing of the international search report

27 July 2018

Name and mailing address of the ISA/CN

STATE INTELLECTUAL PROPERTY OFFICE OF THE
P.R.CHINA
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Authorized officer

YAN,Sai

Facsimile No. (86-10)62019451

Telephone No. 86-(10)-53961605

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2017/111028

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2016219437	A1	28 July 2016	KR	20150042686	A	21 April 2015
				WO	2015053602	A1	16 April 2015
US	2016330619	A1	10 November 2016	WO	2015105402	A1	16 July 2015
				KR	20150084224	A	22 July 2015
CN	104244444	A	24 December 2014	None			
CN	104066200	A	24 September 2014	KR	20160013005	A	03 February 2016
				WO	2014148859	A1	25 September 2014
				EP	2954712	A1	16 December 2015
				US	2016029423	A1	28 January 2016