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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 December 2014 (11.12.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/196983 A1

(51) International Patent Classification:
G06F 7/04 (2006.01)

(21) International Application Number:
PCT/US2013/044708

(22) International Filing Date:
7 June 2013 (07.06.2013)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventor; and

(71) Applicant *(for US only)*: **NARAYANAN, Ram, Lakshmi** [US/US]; 1063 Morse Avenue, Apt 8-101, Sunnyvale, CA 94089 (US).

(74) Agents: **ALBASSAM, Majid, S.** et al.; Squire Sanders (US) LLP, 8000 Towers Crescent Drive, 14th Floor, Vienna, VA 22182-6212 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

[Continued on next page]

(54) Title: COMMUNICATION ESTABLISHMENT USING IDENTIFIERS FOR D2D ENVIRONMENT

(57) Abstract: Systems, methods, apparatuses, and computer program products for establishing D2D communication using mobile or cellular identifiers are provided. One method may include receiving, by a server in a mobile network, an identity request message for an identity of a user equipment. The method may then include, while the mobile network is online, generating an identity certificate for the user equipment and sending the identity certificate to the user equipment for use when the mobile network is offline.

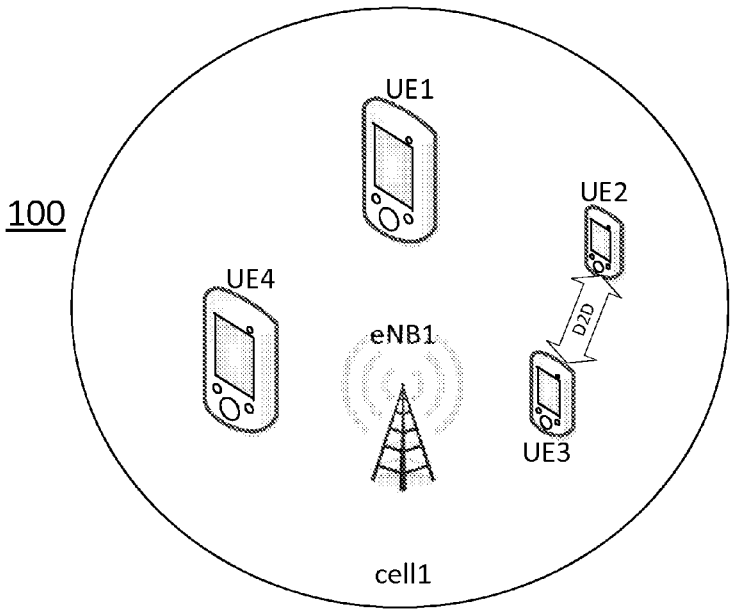

Fig. 1

WO 2014/196983 A1

Published:

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

COMMUNICATION ESTABLISHMENT USING IDENTIFIERS FOR D2D ENVIRONMENT

BACKGROUND:

Field:

[0001] Certain embodiments generally relate to communication systems, and for example, to device-to-device (D2D) communication integrated into a communications network, such as long-term evolution (LTE) or long-term evolution advanced (LTE-A) cellular network specified by the 3rd Generation Partnership Project (3GPP).

Description of the Related Art:

[0002] Two types of communication networks are cellular networks and ad-hoc networks. A cellular network is a radio network made up of one or more cells, where each cell is served by at least one centralized controller, such as a base station (BS), a Node B, or an evolved Node B (eNB). In a cellular network, a user equipment (UE) communicates with another UE via the centralized controller, where the centralized controller relays messages sent by a first UE to a second UE, and visa-versa. In contrast, in an ad-hoc network, a UE directly communicates with another UE, without the need of a centralized controller. Utilizing a cellular network versus an ad-hoc network has its benefits and drawbacks. For example, utilizing a cellular network over an ad-hoc network provides the benefit of easy resource control and interference control. However, utilizing a cellular network over an ad-hoc network also provides the drawback of inefficient resource utilization. For instance, additional resources may be required in a cellular network when the two UEs are close to each other, as compared to an ad-hoc network.

[0003] A hybrid network utilizes both a cellular mode and a D2D

transmission mode. In a hybrid network, a UE can choose to communicate either via a cellular mode or a D2D transmission mode. As an example, a hybrid network may allow UEs to communicate either via a cellular mode (i.e. via a centralized controller) or via an autonomous D2D transmission mode where the UEs can establish a channel without the need for a centralized controller. The UE can make this selection depending on which mode provides better overall performance. Thus, a hybrid network can improve total system performance over a cellular network or an ad-hoc network. However, in order to utilize a hybrid network, issues related to resource sharing and interference situations may need to be addressed.

[0004] In addition, there are some situations in which cellular networks may not be available because they are off-line. For example, in disaster or catastrophic situation, cellular networks may be knocked off-line for various reasons. However, reliable communications networks are likely even more necessary in these disaster situations to help alleviate damage and coordinate emergency response.

SUMMARY:

[0005] One embodiment is directed to a method including receiving, by a server in a mobile network, an identity request message for an identity of a user equipment. The method may further include, while the mobile network is online, generating an identity certificate for the user equipment. The method may then include sending the identity certificate to the user equipment for use when the mobile network is offline.

[0006] Another embodiment is directed to an apparatus. The apparatus includes at least one processor and at least one memory comprising computer program code. The at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus at least to

receive an identity request message for an identity of a user equipment in a mobile network, and, while the mobile network is online, generate an identity certificate for the user equipment. The at least one memory and the computer program code may further be configured, with the at least one processor, to cause the apparatus at least to send the identity certificate to the user equipment for use when the mobile network is offline.

[0007] Another embodiment is directed to a computer program, embodied on a computer readable medium, wherein the computer program is configured to control a processor to perform a process. The process includes receiving an identity request message for an identity of a user equipment in a mobile network. The process may further include, while the mobile network is online, generating an identity certificate for the user equipment. The method may then include sending the identity certificate to the user equipment for use when the mobile network is offline.

[0008] Another embodiment is directed to a method including receiving, by a user equipment in a mobile network, at least one identity certificate from an identity distribution server. The method may also include using the at least one identity certificate to establish device-to-device (D2D) communication with at least one other user equipment when the mobile network is offline.

[0009] Another embodiment is directed to an apparatus. The apparatus includes at least one processor and at least one memory comprising computer program code. The at least one memory and the computer program code are configured, with the at least one processor, to cause the apparatus at least to receive at least one identity certificate from an identity distribution server in a mobile network, and to use the at least one identity certificate to establish device-to-device (D2D) communication with at least one other user equipment when the mobile network is offline.

[00010] Another embodiment is directed to a computer program, embodied on a computer readable medium, wherein the computer program is configured to control a processor to perform a process. The process includes receiving at least one identity certificate from an identity distribution server in a mobile network. The process may also include using the at least one identity certificate to establish device-to-device (D2D) communication with at least one other user equipment when the mobile network is offline.

BRIEF DESCRIPTION OF THE DRAWINGS:

[00011] For proper understanding of the invention, reference should be made to the accompanying drawings, wherein:

[00012] Fig. 1 illustrates an example of a system, according to one embodiment;

[00013] Fig. 2 illustrates an example of a signaling diagram, according to an embodiment;

[00014] Fig. 3a illustrates an example of an apparatus, according to one embodiment;

[00015] Fig. 3b illustrates an example of an apparatus, according to another embodiment;

[00016] Fig. 4a illustrates an example of a flow diagram of a method, according to one embodiment; and

[00017] Fig. 4b illustrates an example of a flow diagram of a method, according to another embodiment.

DETAILED DESCRIPTION:

[00018] It will be readily understood that the components of the invention,

as generally described and illustrated in the figures herein, may be arranged and designed in a wide variety of different configurations. Thus, the following detailed description of the embodiments of systems, methods, apparatuses, and computer program products for establishing communication using mobile or cellular identifiers for a D2D environment, as represented in the attached figures, is not intended to limit the scope of the invention, but is merely representative of selected embodiments of the invention.

[00019] The features, structures, or characteristics of the invention described throughout this specification may be combined in any suitable manner in one or more embodiments. For example, the usage of the phrases "certain embodiments," "some embodiments," or other similar language, throughout this specification refers to the fact that a particular feature, structure, or characteristic described in connection with the embodiment may be included in at least one embodiment of the present invention. Thus, appearances of the phrases "in certain embodiments," "in some embodiments," "in other embodiments," or other similar language, throughout this specification do not necessarily all refer to the same group of embodiments, and the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. Additionally, if desired, the different functions discussed below may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the described functions may be optional or may be combined. As such, the following description should be considered as merely illustrative of the principles, teachings and embodiments of this invention, and not in limitation thereof.

[00020] Disasters are exceptional events that are can be either man made, such as terrorist attacks, or natural disasters, such as earthquakes, hurricanes, tornadoes, wildfires and floods, etc. Disasters create emergency situations, and can cause physical damage as well as social disorder. In these

emergency situations, basic provisions and services, such as food, water, shelter, protection and medical help are needed. The effort required to provide these basic services to the victims generally must be coordinated quickly via a reliable communication network.

[00021] Prior disaster events provide certain lessons that may be applied to future events. For example, generally, most of the casualties occur within 48 hours after the disaster event. Cellular network towers, communication, and power lines that were present before the disaster may not be operational. As a result, victims or users affected in the disaster area usually are not able to communicate with their families via the usual wired or wireless (e.g., cellular) communication networks. Disaster relief operations take place with help of medical personnel, fire and police departments, and, as a result of the issues noted above, they may have issues establishing reliable communications, which may be established very late.

[00022] After a disaster event, proper restoration of infrastructure can take weeks to months. In such situations, when there is no network coverage, victims in the disaster region try to help each other and may form groups among themselves to, for example, reach a safe place until proper communication and rescue operations are in place. Mobile phones and other wireless or communications devices that victims are carrying may not be useful in reaching emergency personnel or other victims within the disaster region itself. For example, people may attempt to call each other using their devices, but when communications systems are not available or damaged, they will not be able to reach anyone. In the absence of the cellular network(s), it is not possible to make calls using phone numbers, as the association between users and phone numbers are maintained inside the cellular network infrastructure. Similarly, identities such as Skype™ ID, Google™ ID will be valid only when they are in contact with the network, and those identities may also not be available after a disaster event.

[00023] As part of LTE-Advanced standardization, Device-to-Device (D2D) communication is currently being standardized in 3GPP. D2D standardization is still in the early phase of defining use case(s), but it will be important to include use cases that are applicable to emergency networks. Network assisted public safety communication is currently being worked out as part of D2D requirements, and existing requirements are not adequate to support disaster relief network services that demand infrastructure-less support. As mentioned above, D2D can allow for a hybrid combination of infrastructure-mode and ad hoc communication.

[00024] Certain embodiments of the invention provide a scheme in which the cellular network infrastructure can assist in distribution of the required identities and associated mappings prior to disaster events. These identities may then be later used for ad-hoc mode (e.g., emergency) type communication. The same identities can be used by many applications to build networks in D2D ad-hoc mode environment. Embodiments can be useful for disaster and emergency situations, as described herein, but are not limited to such situations. In fact, embodiments can equally be applied in other situations where the centralized cellular network is not available.

[00025] People are used to being able to easily establish communication, such as making phone calls, text messages, etc. In the event of a disaster, people are even in more need of establishing communication and it cannot be expected that victims will use other modes or applications to communicate, and, in fact, there are no applications on phones that are disaster specific.

[00026] There are a number of identities that are familiar to phone users. For example, a phone number is an identity used by phones, including cellular phones or UEs, to establish calls. An internet protocol (IP) address (e.g., assigned by dynamic host configuration protocol (DHCP) or Static) is an identity assigned to each device or endpoint in a network and is used to

communicate data services between them. IP addresses, however, may not be permanent and users generally do not remember them. An email address is an example of a permanent identity, but is not real time (e.g., a user must periodically log-on in order to receive e-mail messages). All these example identities have scope, and a lifetime associated with them. The scope of these identifies are restricted to a realm, zone, or particular architecture. As a result, these identities are not usable when the network infrastructure is not available for some reason.

[00027] Phone numbers may be the most common and well known identity associated with communication. Most people remember at least some important phone numbers, and almost all mobile phones have the ability to locally store a contact list including phone numbers. Phone numbers are applicable to both fixed and mobile phone service. In a cellular network, for example, the subscriber identity module (SIM) of the mobile phone may store its International Mobile Subscriber Identity (IMSI), keys and other useful information to establish the identities of the users. As suggested by its name, the IMSI is a unique number identifying the subscriber within the network.

[00028] The mapping of the phone number to the IMSI is stored inside the cellular network, for example by the Home Subscriber System (HSS). When a UE makes a call or establishes any communication via network, the network internally maps the IMSI to a Mobile Subscriber Integrated Services Digital Network-Number (MSISDN), and establishes two party communications. If such scenario needs to happen in direct device-to-device communication (D2D) ad hoc mode each phone needs to maintain its identity correctly. The MSISDN is a number uniquely identifying a subscription in a mobile/cellular network. In other words, the MSISDN is the telephone number to the SIM in a mobile/cellular phone.

[00029] IP addresses are dynamically assigned and are generally not remembered by any applications inside cellular/mobile phones (e.g., UE). Using an ad hoc network is helpful to build a network only with nodes, but they do not have common identity. Most of the Ad hoc routing protocols deal with connection, and route convergence. Existing IP and/or phone services cannot run on top of it due to a lack of centralized control.

[00030] Application based identities, such as email addresses, are useful when IP connectivity is established as they demand services to establish communications. Similarly, popular Peer-to-Peer (P2P) applications such as Google Hangout™, Skype™, Tango™, FaceTime™, etc. all requires centralized infrastructure.

[00031] Fig. 1 illustrates an example of a communication system 100, according to one embodiment. In this embodiment, system 100 includes one cell, cell 1. System 100 also includes one eNB, eNB1. However, as one of ordinary skill would readily appreciate, system 100 can include any number of cells and/or eNBs. In this example, eNB1 is located in cell 1 and can serve UEs within its serving area. System 100 also includes UE1, UE2, UE3, and UE4, which are each located in cell 1. In this example, UE2 and UE3 are in D2D communication, while UE1 and UE4 are served by the cellular network infrastructure via eNB1. As a result, according to this example, communication system 100 may be considered a hybrid network that can utilize both a cellular mode and a D2D transmission mode.

[00032] In a disaster scenario, victims may not be able to use existing identities discussed above (e.g., phone numbers, IP addresses, email addresses) and associated services to establish communication. For example, when victim (e.g., UE1) tries to reach other victim (e.g., UE2) they tend to use the regular dialler applications on the phone, and, when the network infrastructure is not available, will not be able to establish a

connection. Naming identities, such as phone numbers, IP addresses (IPv4 and IPv6), email addresses, websites, etc., which are associated with a central infrastructure are likely not usable and not available.

[00033] In view of the above, systems are needed that allow users to communicate to other users normally without any infrastructure, such as what may occur in a disaster situation. In the absence of such a mechanism, it would be difficult to establish any D2D communication in an ad hoc environment.

[00034] Therefore, according to an embodiment, identities are prepared and distributed to UEs in order to later enable offline emergency communications. This procedure can be performed when the UEs are getting normal service, during service activation itself, or at regular intervals. Then, when network infrastructure is knocked offline (e.g. due to a disaster event), the previously distributed identities can be used for ad-hoc network topology creation. As a result, the identities can be utilized to serve disaster type applications such as voice call.

[00035] Fig. 2 illustrates an example of a signaling diagram for securely transferring identities (e.g., MSISDN and its associated credentials) to a mobile/cellular phone (e.g., UE). Subsequently, using these transferred identities, infrastructure-less communication can be established for direct D2D communication. At least two approaches may be used to distribute credentials, namely the PUSH and PULL mechanisms, as illustrated in Fig. 2. Fig. 2 illustrates some examples of network elements in wireless access network technologies that may be used to achieve the functionality of embodiments of the invention. However, the functionality that is illustrated in Fig. 2 could be implemented (or combined) with other network elements.

[00036] In the following, examples of the possible message exchange(s) for identity certificate distribution are described in connection with the

embodiment of Fig. 2. First, an embodiment according to a PULL mechanism is described. As illustrated in Fig. 2, at 1, UE-1 is powered ON and completes the network attach. While in this example, the network attach is performed via a visitor location register (VLR) (as in 2G networks), it could also be performed, for example, by a mobility management entity (MME) in case of 4G, or any other appropriate entity depending on the type of network. Embodiments of the invention are applicable to all types of wireless access networks and their associated entities.

[00037] Continuing with Fig. 2, at 2, UE-1 sends a REQUEST_IDENTITY_CERTIFICATE message towards the identity distribution server. There are a number of ways that this identity distribution server could be placed in the existing network infrastructure. For example, it could be part of the pre-configuration performed by the operator, or it could be part of the device management framework. A main purpose of this server is to securely distribute identities of the phone, such as MSISDN and associated credentials.

[00038] Then, at 3, the identity distribution server passes the UE credentials that it receives (such as IMSI, temporary mobile subscriber identity (TMSI), etc.) to the HSS/VLR sub-systems and request Authentication Centre (AuC), to verify the UE and generate secure signature information. At 4, after a successful response from HSS sub-system, the identity distribution server prepares the UE identity certificate. It collects all the information that is required to generate the identities and prepares them as certificates. For example, the identity distribution server may collect the required information for public certificates, which contains issuers name, date, and validity, and also the MSISDN identity.

[00039] According to one embodiment, the certificate may be valid for a 30 day period (or less). In an embodiment, the UE may renew the certificate

at regular intervals. A shorter validity period avoids overuse and eliminates the need for certificate revocation list maintenance. This helps assure that the identity was issued by an operator.

[00040] Then, at 5, the prepared certificate is passed back to the HSS (AuC) which is requested to sign and generate the public certificate. The signed certificate with identity credentials is passed back, at 6, to the identity distribution server. At 7, the RESPONSE_IDENTITY_CERTIFICATE is sent by the identity server to UE-1. The RESPONSE_IDENTITY_CERTIFICATE contains MSISDN information as part of the public certificate.

[00041] Next, an embodiment according to a PUSH mechanism is described. In this embodiment, the identity certificate is generated and the network does automatic push of the information. As illustrated in Fig. 2, at 8, UE-2 is powered ON and completes the network attach. After successful completion of network attach, at 9, wireless access network infrastructure equipment (such as VLR or MME or other suitable server such as device management or patch management server) may initiate a request to push the identify certificate via a GENERATE_IDENTITY message. At 10, the identity distribution server prepares the UE identity certificate in a similar manner to that discussed above in connection with step 4. At 11, the prepared certificate is passed back to the HSS (AuC) which is requested to sign and generate the public certificate. Then, at 12, the signed certificate with identity credentials is passed back, at 6, to the identity distribution server. At 13, the RESPONSE_IDENTITY_CERTIFICATE is sent by the identity server to UE-2.

[00042] According to certain embodiments, after receiving the identity certificate, UE-1 and/or UE-2 can store the identity certificate securely in its SIM or in protected storage. The chosen storage message can be specific to

the operator. As mentioned above, the lifetime of the certificate can be made short and, in order to avoid generating the keys each time, the network could send an updated certificate by updated date change. Also, in one embodiment, usage of certificate may only be valid in the absence of centralized network infrastructure. Applications that are using these certificates should be trusted by operator (such as dialer application inside the phone).

[00043] Once the identity certificate(s) are distributed, the UEs may use those certificates to aid in D2D communication in an ad-hoc network scenario. For instance, during an emergency situation such as disaster, the UE could use the identities, such as MSISDN, stored inside the certificate as its own identity. This identity can then be supplied as part of a routing update to determine the neighboring UEs. Before making calls, the UEs in the disaster region need to know about each other and can establish any ad hoc communication to discover their topology.

[00044] There are around 40+ routing protocols in use. Along with routing updates, each UE may send its own identifiers, which can be used to populate a routing table in each node. Each UE will contain route information, such as IPv4/IPv6 address and its neighbour UE reachable information, along with their MSISDN identity. By pushing user identifiers to its lower layer, UEs can run the phone call routing service over Ad hoc network. As a result, UE-1 can talk to UE-2 just like with a phone call.

[00045] When a UE is in ad-hoc mode (or D2D infrastructure less mode), the default dialler application takes inputs from the user, and forwards it to any interfaces (normally, when user dials using the phone dialler application, it interacts with the cellular CS network). Now, users could dial in using their phone numbers to contact each other in disaster region.

[00046] Based on the type of ad-hoc routing protocols, presence

information can be easily derived from each node's routing table (containing identities), and then updated in the contact list of phones. Disaster regions contain many differentiating parameters or factors, including terrain, type of location, size of location, number of people living before disaster, etc. Embodiments have taken into account extensive simulations of human mobility models in disaster regions, and how embodiments of the invention can assist them to survive and move to a disaster free zone more quickly.

[00047] Fig. 3a illustrates an example of an apparatus 10 according to an embodiment. In one embodiment, apparatus 10 may be a network entity, such as an identity distribution server, VLR, MME, HSS, and/or AuC illustrated in Fig. 2 above. It should be noted that one of ordinary skill in the art would understand that apparatus 10 may include components or features not shown in Fig. 3a. Only those components or features necessary for illustration of the invention are depicted in Fig. 3a.

[00048] As illustrated in Fig. 3a, apparatus 10 includes a processor 22 for processing information and executing instructions or operations. Processor 22 may be any type of general or specific purpose processor. While a single processor 22 is shown in Fig. 3a, multiple processors may be utilized according to other embodiments. In fact, processor 22 may include one or more of general-purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs), field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), and processors based on a multi-core processor architecture, as examples.

[00049] Apparatus 10 further includes a memory 14, which may be coupled to processor 22, for storing information and instructions that may be executed by processor 22. Memory 14 may be one or more memories and of any type suitable to the local application environment, and may be implemented using any suitable volatile or nonvolatile data storage

technology such as a semiconductor-based memory device, a magnetic memory device and system, an optical memory device and system, fixed memory, and removable memory. For example, memory 14 can be comprised of any combination of random access memory (RAM), read only memory (ROM), static storage such as a magnetic or optical disk, or any other type of non-transitory machine or computer readable media. The instructions stored in memory 14 may include program instructions or computer program code that, when executed by processor 22, enable the apparatus 10 to perform tasks as described herein.

[00050] Apparatus 10 may also include one or more antennas 25 for transmitting and receiving signals and/or data to and from apparatus 10. Apparatus 10 may further include a transceiver 28 configured to transmit and receive information. For instance, transceiver 28 may be configured to modulate information on to a carrier waveform for transmission by the antenna(s) 25 and demodulate information received via the antenna(s) 25 for further processing by other elements of apparatus 10. In other embodiments, transceiver 28 may be capable of transmitting and receiving signals or data directly.

[00051] Processor 22 may perform functions associated with the operation of apparatus 10 including, without limitation, precoding of antenna gain/phase parameters, encoding and decoding of individual bits forming a communication message, formatting of information, and overall control of the apparatus 10, including processes related to management of communication resources.

[00052] In an embodiment, memory 14 stores software modules that provide functionality when executed by processor 22. The modules may include, for example, an operating system that provides operating system functionality for apparatus 10. The memory may also store one or more

functional modules, such as an application or program, to provide additional functionality for apparatus 10. The components of apparatus 10 may be implemented in hardware, or as any suitable combination of hardware and software.

[00053] In one embodiment, apparatus 10 may be an identity distribution server. In this embodiment, apparatus 10 may be controlled by memory 14 and processor 22 to receive an identity request message for an identity of a UE in a mobile network. While the mobile network is online, apparatus 10 may be controlled by memory 14 and processor 22 to generate an identity certificate for the UE, and to send the identity certificate to the UE for use when the mobile network is offline.

[00054] According to an embodiment, apparatus 10 may be controlled by memory 14 and processor 22 to receive the identity request message from the UE. In another embodiment, apparatus 10 may be controlled by memory 14 and processor 22 to receive the identity request message from a network node, such as a VLR, a MME, a device management server, or a patch management server. In one embodiment, apparatus 10 may be controlled by memory 14 and processor 22 to verify the identity of the UE with a HSS sub-system. According to an embodiment, apparatus 10 may also be controlled by memory 14 and processor 22 to forward the identity certificate to the HSS sub-system for signing and for generating a public certificate. In one embodiment, the identity certificate is valid for a period of 30 days or less.

[00055] Fig. 3b illustrates an example of an apparatus 20 according to another embodiment. In an embodiment, apparatus 20 may be a UE. It should be noted that one of ordinary skill in the art would understand that apparatus 20 may include components or features not shown in Fig. 3b. Only those components or features necessary for illustration of the invention are depicted in Fig. 3b.

[00056] As illustrated in Fig. 3b, apparatus 20 includes a processor 32 for processing information and executing instructions or operations. Processor 32 may be any type of general or specific purpose processor. While a single processor 32 is shown in Fig. 3b, multiple processors may be utilized according to other embodiments. In fact, processor 32 may include one or more of general-purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs), field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), and processors based on a multi-core processor architecture, as examples.

[00057] Apparatus 20 further includes a memory 34, which may be coupled to processor 32, for storing information and instructions that may be executed by processor 32. Memory 34 may be one or more memories and of any type suitable to the local application environment, and may be implemented using any suitable volatile or nonvolatile data storage technology such as a semiconductor-based memory device, a magnetic memory device and system, an optical memory device and system, fixed memory, and removable memory. For example, memory 34 can be comprised of any combination of random access memory (RAM), read only memory (ROM), static storage such as a magnetic or optical disk, or any other type of non-transitory machine or computer readable media. The instructions stored in memory 34 may include program instructions or computer program code that, when executed by processor 32, enable the apparatus 20 to perform tasks as described herein.

[00058] Apparatus 20 may also include one or more antennas 35 for transmitting and receiving signals and/or data to and from apparatus 20. Apparatus 20 may further include a transceiver 38 configured to transmit and receive information. For instance, transceiver 38 may be configured to modulate information on to a carrier waveform for transmission by the antenna(s) 35 and demodulate information received via the antenna(s) 35 for

further processing by other elements of apparatus 20. In other embodiments, transceiver 38 may be capable of transmitting and receiving signals or data directly.

[00059] Processor 32 may perform functions associated with the operation of apparatus 20 including, without limitation, precoding of antenna gain/phase parameters, encoding and decoding of individual bits forming a communication message, formatting of information, and overall control of the apparatus 20, including processes related to management of communication resources.

[00060] In an embodiment, memory 34 stores software modules that provide functionality when executed by processor 32. The modules may include, for example, an operating system that provides operating system functionality for apparatus 20. The memory may also store one or more functional modules, such as an application or program, to provide additional functionality for apparatus 20. The components of apparatus 20 may be implemented in hardware, or as any suitable combination of hardware and software.

[00061] As mentioned above, according to one embodiment, apparatus 20 may be a UE. In this embodiment, apparatus 20 may be controlled by memory 34 and processor 32 to receive at least one identity certificate from an identity distribution server in a mobile network, and to use the at least one identity certificate to establish device-to-device (D2D) communication with at least one other user equipment when the mobile network is offline. 24. In one embodiment, apparatus 20 may be further controlled by memory 34 and processor 32 to transmit a routing update comprising the at least one identity certificate to determine neighboring UEs. 25. Apparatus 20 may be controlled by memory 34 and processor 32 to store the at least one identity in its SIM or in protected storage. According to one embodiment, the at least

one identity certificate may be valid only when the mobile network is offline.

[00062] Fig. 4a illustrates an example of a flow chart of a method for preparing and distributing identities that can be used for offline D2D communication, according to one embodiment. In one example, the method of Fig. 4a may be performed by a server, such as an identity distribution server, in a mobile network. The method may include, at 400, receiving an identity request message for an identity of a UE. The method may then include, at 410, generating an identity certificate for the UE while the mobile network is online. The method may also include, at 420, verifying the identity of the user equipment with a HSS sub-system. The method can also include, at 430, forwarding the identity certificate to the home subscription server sub-system for signing and for generating a public certificate. The method may then include, at 440, sending the identity certificate to the user equipment for use when the mobile network is offline.

[00063] Fig. 4b illustrates an example of a flow chart of a method for using identity certificate information for D2D communication when the mobile network is offline, according to one embodiment. In one example, the method of Fig. 4b may be performed by a UE. The method may include, at 450, receiving at least one identity certificate from an identity distribution server. At 460, the method may include storing the at least one identity in a subscriber identity module or in protected storage. The method may also include, at 470, using the at least one identity certificate to establish D2D communication with at least one other user equipment when the mobile network is offline. For instance, the using of the at least one identity certificate may include transmitting a routing update comprising the at least one identity certificate to determine neighboring user equipment.

[00064] In some embodiments, the functionality of any of the methods described herein, such as those illustrated in Figs. 4a and 4b discussed

above, may be implemented by software and/or computer program code stored in memory or other computer readable or tangible media, and executed by a processor. In other embodiments, the functionality may be performed by hardware, for example through the use of an application specific integrated circuit (ASIC), a programmable gate array (PGA), a field programmable gate array (FPGA), or any other combination of hardware and software.

[00065] In view of the above, embodiments provide a mechanism to use identities in a decentralized and controlled manner such that they can be utilized, for example, for D2D or emergency service communication. For example, in some embodiments, cellular identities can be available for offline service in emergency situation. An embodiment includes a mechanism wherein the identity certificates of each user are securely transferred for future use (e.g., in case of emergency situations). In other words, embodiments provide mechanisms to enable usage of mobile broadband networks to support offline type of service. Accordingly, some embodiments provide a mechanism wherein user-known identities are pushed to routing layer (X-Layer approach) and enables use of applications seamlessly in D2D ad-hoc mode. Embodiments are compatible with all types of cellular or mobile technology, such as LTE, LTE-A, etc. Therefore, embodiments can be standardized to enable D2D ad-hoc (infrastructure less) mode communication

[00066] One having ordinary skill in the art will readily understand that the invention as discussed above may be practiced with steps in a different order, and/or with hardware elements in configurations which are different than those which are disclosed. Therefore, although the invention has been described based upon these preferred embodiments, it would be apparent to those of skill in the art that certain modifications, variations, and alternative constructions would be apparent, while remaining within the spirit and scope

of the invention. In order to determine the metes and bounds of the invention, therefore, reference should be made to the appended claims.

WE CLAIM:

1. A method, comprising:

receiving, by a server in a mobile network, an identity request message for an identity of a user equipment;

while the mobile network is online, generating an identity certificate for the user equipment; and

sending the identity certificate to the user equipment for use when the mobile network is offline.

2. The method according to claim 1, wherein the receiving comprises receiving the identity request message from the user equipment.

3. The method according to claim 1, wherein the receiving comprises receiving the identity request message from a network node.

4. The method according to claim 3, wherein the network node comprises at least one of a visitor location register, a mobility management entity, a device management server, or a patch management server.

5. The method according to claims 1 or 2, wherein the server comprises an identity distribution server.

6. The method according to claims 1, 2, or 3, further comprising: verifying the identity of the user equipment with a home subscription server sub-system.

7. The method according to claim 6, wherein the generating further comprises forwarding the identity certificate to the home subscription server sub-system for signing and for generating a public certificate.

8. The method according to claim 1, wherein the identity certificate is valid for a period of 30 days or less.

9. An apparatus, comprising:

at least one processor; and

at least one memory comprising computer program code,

the at least one memory and the computer program code configured, with the at least one processor, to cause the apparatus at least to

receive an identity request message for an identity of a user equipment in a mobile network;

while the mobile network is online, generate an identity certificate for the user equipment; and

send the identity certificate to the user equipment for use when the mobile network is offline.

10. The apparatus according to claim 9, wherein the at least one memory and the computer program code are further configured, with the at least one processor, to cause the apparatus at least to receive the identity request message from the user equipment.

11. The apparatus according to claim 9, wherein the at least one memory and the computer program code are further configured, with the at least one processor, to cause the apparatus at least to receive the identity request message from a network node.

12. The apparatus according to claim 11, wherein the network node comprises at least one of a visitor location register, a mobility management entity, a device management server, or a patch management server.

13. The apparatus according to claims 9 or 10, wherein the apparatus

comprises an identity distribution server.

14. The apparatus according to claims 9, 10, or 11, wherein the at least one memory and the computer program code are further configured, with the at least one processor, to cause the apparatus at least to verify the identity of the user equipment with a home subscription server sub-system.

15. The apparatus according to claim 14, wherein the at least one memory and the computer program code are further configured, with the at least one processor, to cause the apparatus at least to forward the identity certificate to the home subscription server sub-system for signing and for generating a public certificate.

16. The apparatus according to claim 9, wherein the identity certificate is valid for a period of 30 days or less.

17. A computer program, embodied on a computer readable medium, wherein the computer program is configured to control a processor to perform a process, comprising:

receiving an identity request message for an identity of a user equipment in a mobile network;

while the mobile network is online, generating an identity certificate for the user equipment; and

sending the identity certificate to the user equipment for use when the mobile network is offline.

18. A method, comprising:

receiving, by a user equipment in a mobile network, at least one identity certificate from an identity distribution server; and

using the at least one identity certificate to establish device-to-device

(D2D) communication with at least one other user equipment when the mobile network is offline.

19. The method according to claim 18, wherein the using further comprises transmitting a routing update comprising the at least one identity certificate to determine neighboring user equipment.

20. The method according to claims 18 or 19, further comprising: storing the at least one identity in a subscriber identity module or in protected storage.

21. The method according to claim 18, wherein the identity certificate is valid for a period of 30 days or less.

22. The method according to claims 18 or 19, wherein the at least one identity certificate is valid only when the mobile network is offline.

23. An apparatus, comprising:

at least one processor; and

at least one memory comprising computer program code,

the at least one memory and the computer program code configured, with the at least one processor, to cause the apparatus at least to

receive at least one identity certificate from an identity distribution server in a mobile network; and

use the at least one identity certificate to establish device-to-device (D2D) communication with at least one other user equipment when the mobile network is offline.

24. The apparatus according to claim 23, wherein the at least one memory and the computer program code are further configured, with the at least one processor, to cause the apparatus at least to transmit a routing update

comprising the at least one identity certificate to determine neighboring user equipment.

25. The apparatus according to claims 23 or 24, wherein the at least one memory and the computer program code are further configured, with the at least one processor, to cause the apparatus at least to store the at least one identity in a subscriber identity module or in protected storage.

26. The apparatus according to claim 23, wherein the identity certificate is valid for a period of 30 days or less.

27. The apparatus according to claims 23 or 24, wherein the at least one identity certificate is valid only when the mobile network is offline.

28. The apparatus according to claim 23, wherein the apparatus comprises a user equipment.

29. A computer program, embodied on a computer readable medium, wherein the computer program is configured to control a processor to perform a process, comprising:

receiving at least one identity certificate from an identity distribution server in a mobile network; and

using the at least one identity certificate to establish device-to-device (D2D) communication with at least one other user equipment when the mobile network is offline.

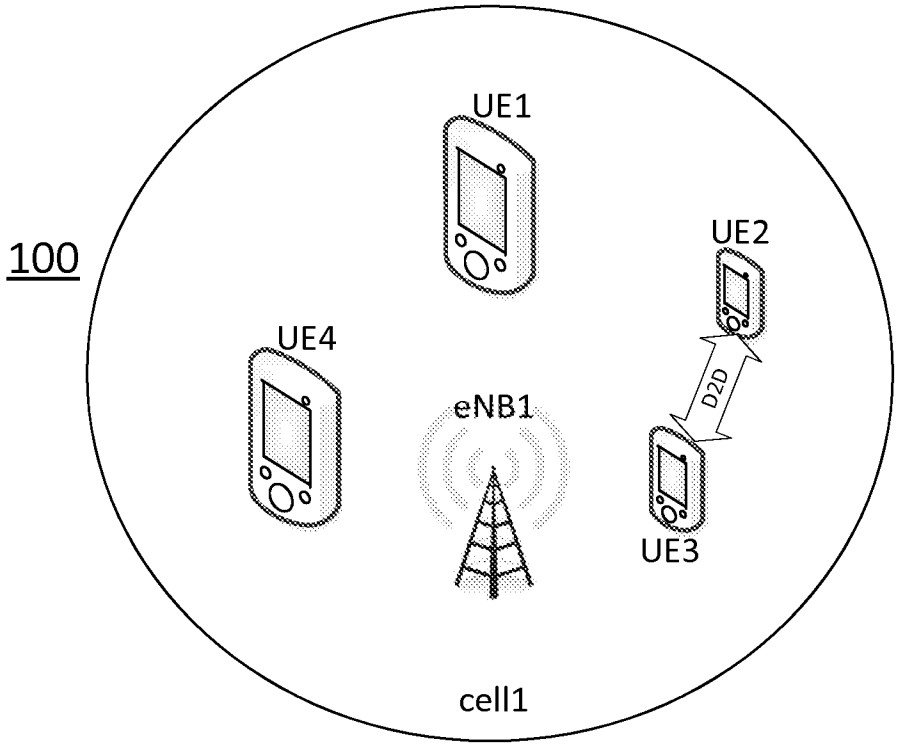

Fig. 1

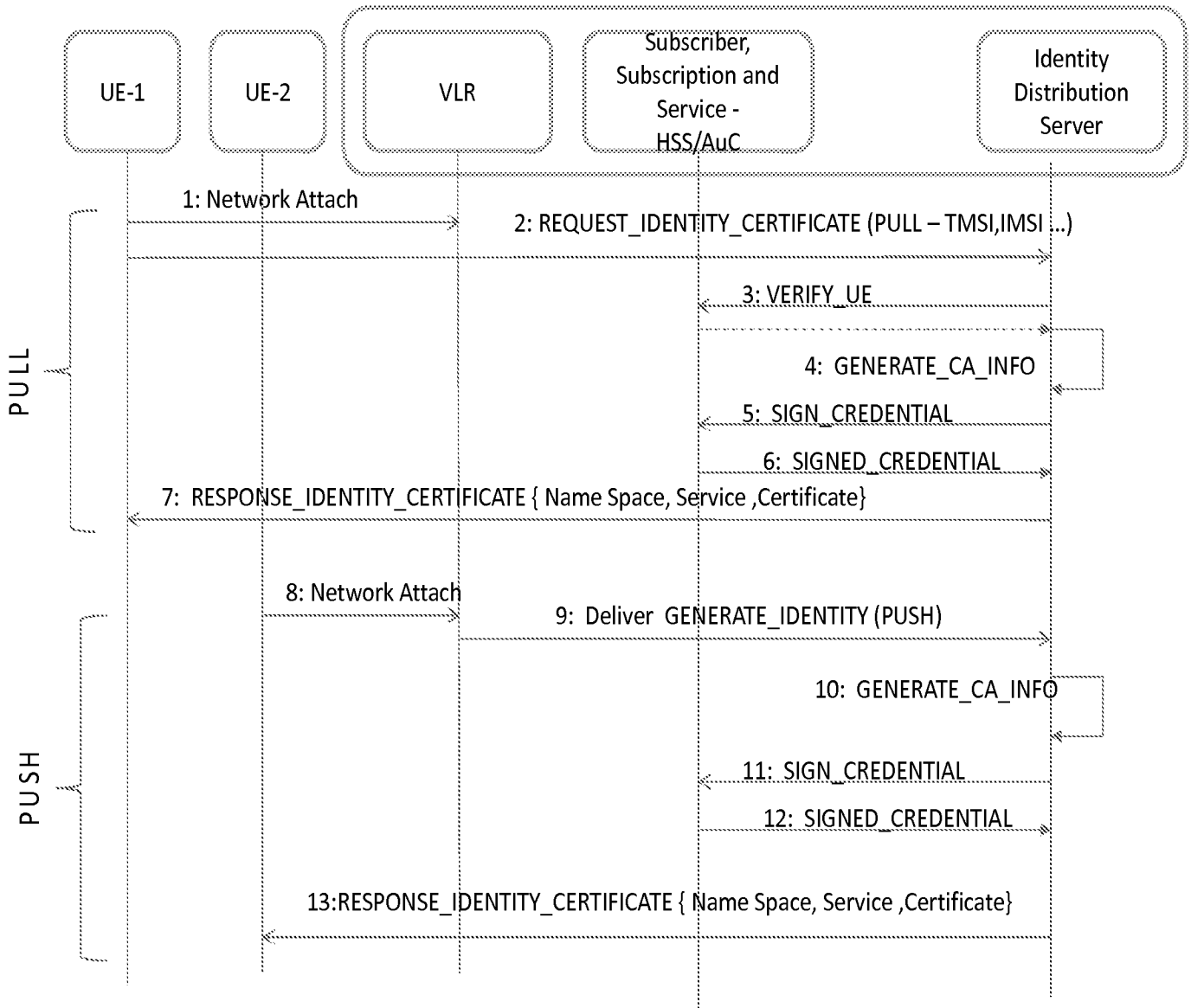
UE-1
UE-2
VLR
Subscriber, Subscription and Service - HSS/AuC
Identity Distribution Server
1: Network Attach
2: REQUEST_IDENTITY_CERTIFICATE (PULL – TMSI,IMSI ...)
3: VERIFY_UE
PULL
4: GENERATE_CA_INFO
5: SIGN_CREDENTIAL
6: SIGNED_CREDENTIAL
7: RESPONSE_IDENTITY_CERTIFICATE { Name Space, Service ,Certificate}
8: Network Attach
9: Deliver GENERATE_IDENTITY (PUSH)
10: GENERATE_CA_INFO
PUSH
11: SIGN_CREDENTIAL
12: SIGNED_CREDENTIAL
13:RESPONSE_IDENTITY_CERTIFICATE { Name Space, Service ,Certificate}

Fig. 2

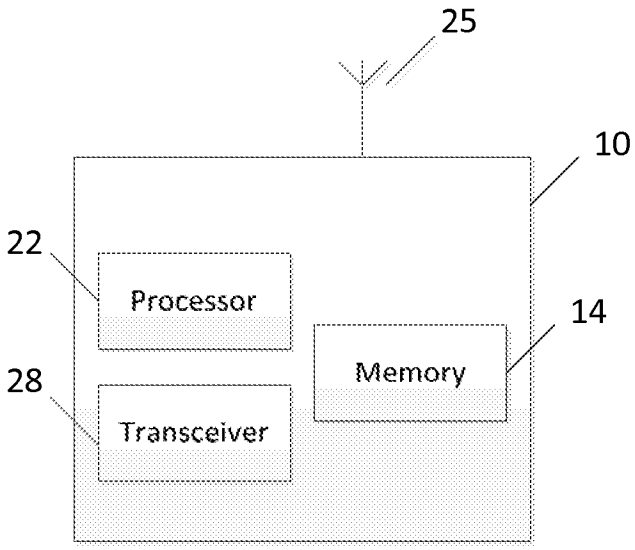
25
10
22
Processor
14
Memory
28
Transceiver

Fig. 3a

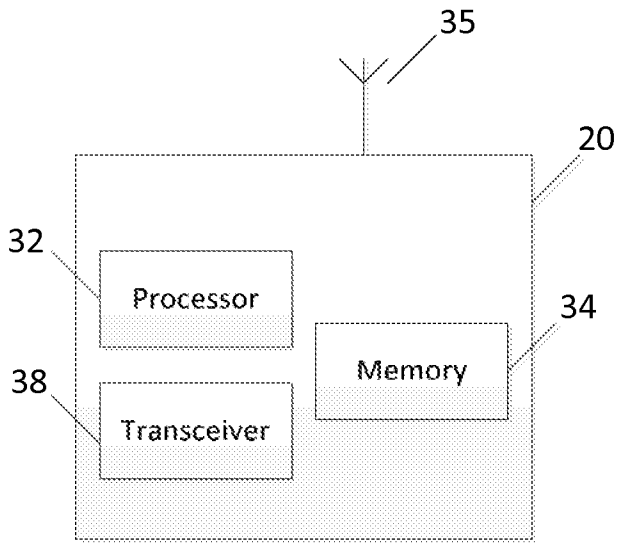
35
20
32
Processor
34
Memory
38
Transceiver

Fig. 3b

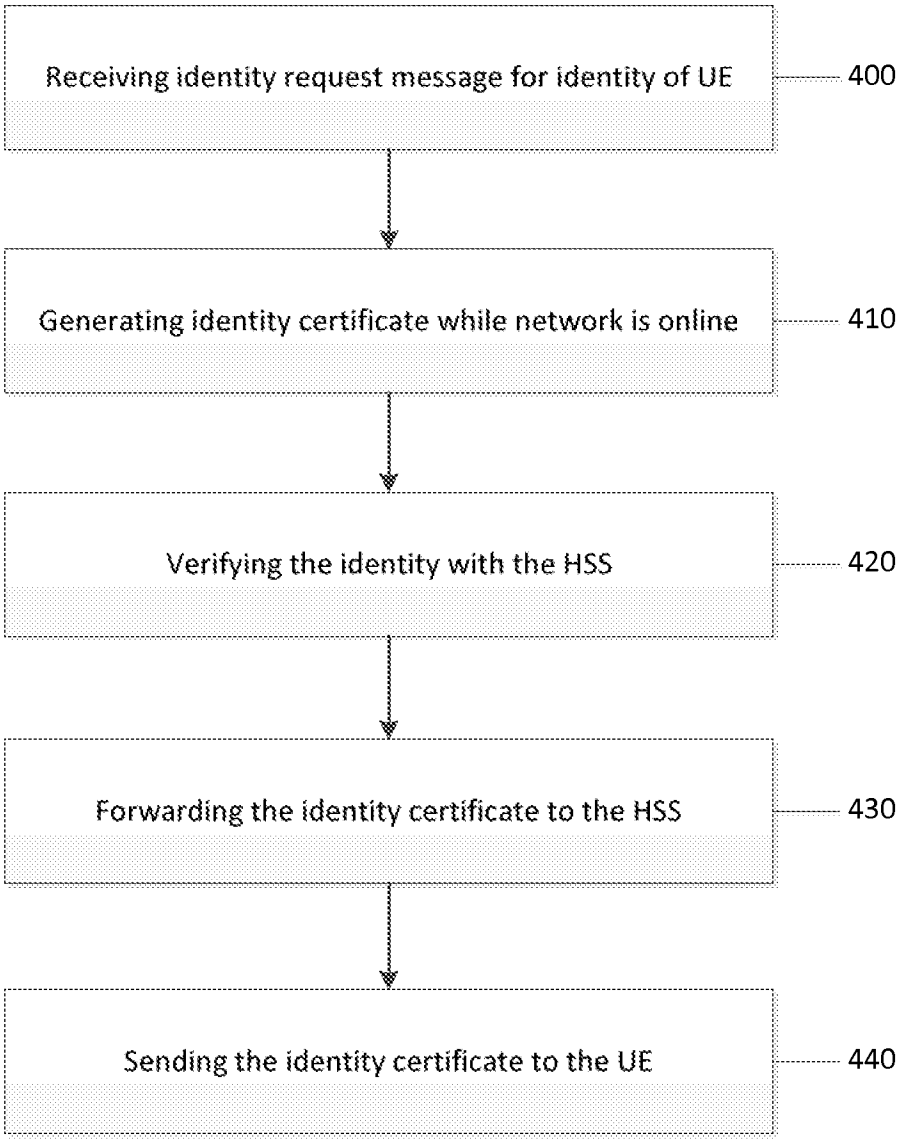
Receiving identity request message for identity of UE
400
Generating identity certificate while network is online
410
Verifying the identity with the HSS
420
Forwarding the identity certificate to the HSS
430
Sending the identity certificate to the UE
440

Fig. 4a

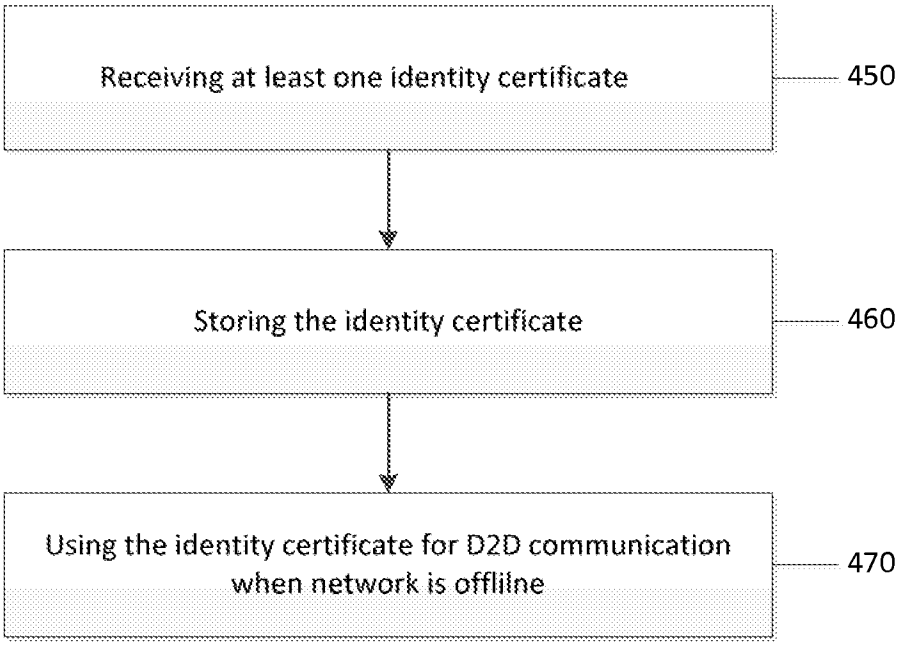
Receiving at least one identity certificate
450
Storing the identity certificate
460
Using the identity certificate for D2D communication when network is offlilne
470

Fig. 4b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US13/44708

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/04 (2013.01)
USPC - 726/10
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)
IPC(8) Classification(s): G06F 7/04, 15/16; H04L 9/32 (2013.01)
USPC Classification(s): 726/10, 5; 709/227; 713/173

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)
MicroPatent (US-G, US-A, EP-A, EP-B, WO, JP-bib, DE-C,B, DE-A, DE-T, DE-U, GB-A, FR-A); ProQuest; IEEE/IEEEXplore; Google/Google Scholar; IP.com; Search Terms Used: mobile, cellular, cell, wireless, station, emergency, disaster, outage, offline, certificate, token, expire, valid, dedicated, specific, alternative

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/0261792 A1 (OERTON, K., et al.) October 27, 2011; figures 1-4; paragraphs [0031], [0033], [0035], [0036], [0043], [0051]-[0053], [0056], [0089]	1-4, 5/1, 5/2, 6/1, 6/2, 6/3, 9-12, 13/9, 13/10, 14/9, 14/10, 14/11, 17, 18, 20/18, 23, 25/23, 28, 29
--		----------
Y		7/6/1, 7/6/2, 7/6/3, 8, 15/14/9, 15/14/10, 15/14/11, 16, 19, 20/19, 21, 22/18, 22/19, 24, 25/24, 26, 27/23, 27/24
Y	US 2002/0080752 A1 (JOHANSSON, F., et al.) June 27, 2002; paragraphs [0189], [0192], [0196], [0198]	7, 15, 19, 20/19, 24, 25/24
Y	US 2002/0165824 A1 (MICALI, S.) November 7, 2002; paragraphs [0017], [0089]	8, 16, 21, 26
Y	US 6247127 B1 (VANDERGEEST, R.) June 12, 2001; figure 2; column 4, lines 36-45	22/18, 22/19, 27/23, 27/24

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 December 2013 (06.12.2013)	16 DEC 2013
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)