APPARATUS AND METHODS FOR LAWFUL INTERCEPTION FOR PROXIMITY SERVICE

Apparatuses and methods are described, which perform control in relation to a connection for proximity service between at least two devices, perform lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and configure at least one radio access network control element to perform the lawful interception in relation to the proximity service.
Fig. 4
LAWFUL INTERCEPTION FOR PROXIMITY SERVICE

FIELD

[0001] The present invention relates to an apparatus, a method and a computer program product for enabling law interception for proximity service.

RELATED BACKGROUND ART

[0002] The following meanings for the abbreviations used in this specification apply:
[0003] ADMF Administration Function
[0004] CC Content of Communication
[0005] CN Core Network
[0006] D2D device-to-device
[0007] DRSF D2D Registration Server Function
[0008] eNB Enhanced NodeB
[0009] EPS Evolved Packet System
[0010] IRI Interception Related Information
[0011] LEMF Law Enforcement Monitoring Facility
[0012] LI Lawful Interception
[0013] M2M machine-to-machine
[0014] MME Mobility Management Entity
[0015] P2P peer-to-peer
[0016] PDN-GW Packet Data Network Gateway
[0017] ProSe Proximity Service
[0018] PWS Public Warning System
[0019] RAN Radio Access Network
[0020] S-GW Serving Gateway
[0021] T2T terminal-to-terminal
[0022] UE user equipment
[0023] Embodiments of the present invention relate to proximity services and lawful interception (LI) for 3GPP Rel-12 and beyond. According to 3GPP TR 22.803, one of ProSe requirements is to support regional or national regulatory requirements (e.g. lawful interception, PWS).

[0024] Presently, the LI functionality is located in the core network. However, ProSe is promoting the network controlled discovery and communication between UEs that are in proximity to be able to use a “direct mode” or “locally-routed” path, which may not involve the core network (CN). Namely, the direct mode path is a direct connection between the two UEs without involving further network elements such as an eNB. The locally-routed path is an indirect connection between the two UEs via an eNB without involving CN.

[0025] Thus, the connection of UEs by proximity service does not involve the core network. Therefore, the intercepted information may not be available to the core network LI entities.

[0026] One option was discussed in document “LS on Proximity Services and Lawful Interception from SA3-LI to SA1,2,3” (3GPP TS 32.433, 3GPP TSG-SA3-LI Meeting #48, Dublin, Ireland, 5-7 Feb. 2013) and document “Solution for direct discovery and communication using E-UTRAN” (S2-130308, SA WG2 Meeting #95, Prague, Czech Republic, 28 Jan.-1 Feb. 2013) to disable ProSe capabilities for UEs under surveillance or move the communication for the UE under surveillance from ProSe communication mode to infrastructure mode. That is, the ProSe communication is disabled for these UEs, so that the communication is performed via the core network, so that LI in the core network is possible. However, as indicated in the document “LS on Proximity Services and Lawful Interception from SA3-LI to SA1,2,3” mentioned above, detectability issues need to be considered for this option as LI should be done in non-detectable manner. In addition, moving ProSe communication to infrastructure mode may degrade the communication performance (e.g. delay and perhaps also throughput), which may not be favorable by the end user and this also means the benefits of ProSe communication may not be achieved as EPC, e.g. P-GW or S-GW is involved in the ProSe communication user plane data transportation.

[0027] Thus, there is a need to improve lawful interception in a case in which UEs use proximity service connections.

SUMMARY

[0028] Embodiments of the present invention address this situation and to enable lawful interception also for devices using a direct connection such a proximity service connection.

[0029] According to a first aspect of the present invention, there is provided an apparatus comprising a processor and a memory for storing instructions to be executed by the processor, wherein the processor is configured to perform control in relation to a connection for proximity service between at least two devices, to perform lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and to configure at least one radio access network control element to perform the lawful interception in relation to the proximity service.

[0031] Furthermore, according to an example of an embodiment, there is provided a method comprising: performing control in relation to a connection for proximity service between at least two devices, to receive configuration information for performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and to configure at least one radio access network control element to perform the lawful interception in relation to the proximity service.

[0032] In addition, according to an example of an embodiment, there is provided an apparatus comprising a processor and a memory for storing instructions to be executed by the processor, wherein the processor is configured to provide control in a radio access network, to perform control in relation to a connection for proximity service between at least two devices, to receive configuration information for performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and to report interception information with respect to the at least one device to be intercepted.

[0033] Furthermore, according to an example of an embodiment, there is provided a method comprising providing control in a radio access network, performing control in relation to a connection for proximity service between at least two devices, receiving configuration information for performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and reporting interception information with respect to the at least one device to be intercepted.

[0034] In addition, according to an example of an embodiment, there is provided an apparatus comprising a processor and a memory for storing instructions to be executed by the processor, wherein the processor is configured to provide a connection to a radio access network, to receive interception information intercepted by lawful interception with respect to at least one device to be intercepted, wherein the at least one device is intercepted.
device is one of at least two devices connected by a connection for proximity service in the radio access network.

Moreover, according to an example of an embodiment, there is provided a method comprising providing a connection to a radio access network, and receiving interception information intercepted by lawful interception with respect to at least one device to be intercepted, wherein the at least one device is one of at least two devices connected by a connection for proximity service in the radio access network.

In addition, according to an example of an embodiment, there is provided a system comprising a device-to-device registration server function and at least one radio access network control element, wherein the device-to-device registration server function is configured to perform control in relation to a connection for proximity service between at least two devices, to perform lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and to configure the at least one radio access network control element to perform the lawful interception in relation to the proximity service; and the at least one radio access network control element is configured to perform control in relation to a connection for proximity service between the at least two devices, to receive configuration information from the device-to-device registration server function, and to report interception information with respect to the at least one device to be intercepted.

The above described examples of embodiments may be modified as defined in the dependent claims.

In addition, according to embodiments, there is provided, for example, a computer program product for a computer, comprising software code portions for performing the above defined methods, when said product is run on the computer. The computer program product may comprise a computer-readable medium on which said software code portions are stored. Furthermore, the computer program product may be directly loadable into the internal memory of the computer and/or transmittable via a network by means of at least one of upload, download and push procedures.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, features, details and advantages will become more fully apparent from the following detailed description of embodiments of the present invention which is to be taken in conjunction with the appended drawings, in which:

FIG. 1 shows an example of simplified structures of network elements involved according to an embodiment of the present invention,

FIGS. 2, 3 and 4 show examples of reference configurations for a ProSe lawful interception according to embodiments of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

In the following, description will be made to embodiments of the present invention. It is to be understood, however, that the description is given by way of example only, and that the described embodiments are by no means to be understood as limiting the present invention thereto. Furthermore, words “comprising” and “including” should be understood as not limiting the described embodiments to consist of only those features that have been mentioned and such embodiments may also contain also features, structures, units, modules etc. that have not been specifically mentioned.

In the following, different exemplifying embodiments will be described using, as an example of an access architecture to which the embodiments may be applied, a radio access architecture based on long term evolution advanced (LTE Advanced, LTE-A), without restricting the embodiments to such an architecture, however. It is obvious for a person skilled in the art that the embodiments may also be applied to other kinds of communications networks having a suitable means by adjusting parameters and procedures appropriately. Some examples of other options for suitable systems are the universal mobile telecommunications system (UMTS) radio access network (UTRAN or E-UTRAN), long term evolution (LTE, the same as E-UTRA), wireless local area network (WLAN or WiFi), worldwide interoperability for microwave access (WiMAX), Bluetooth®, personal communications services (PCS), ZigBee®, wideband code division multiple access (WCDMA), systems using ultra-wideband (UWB) technology, sensor networks, mobile ad-hoc networks (MANETs) and Internet Protocol multimedia sub-systems (IMS) and beyond 4th generation (4G) or 5G.

It should be appreciated that communication systems and apparatuses thereof will be integrated towards an infrastructure (more and more) based on undedicated and programmable hardware providing needed functionalities. A network element may be a computing equivalent device that gathers programmable resources based on virtualization technologies.

In the following, a general embodiment of the present invention is described by referring to FIG. 1. In particular, FIG. 1 shows several elements involved in the procedures according to embodiments of the present invention. Examples are for an apparatus in which procedures according to embodiments of the invention can be applied are a DRSF and an eNB. The DRSF is responsible for registration, authentication and identifying of TD2D users and management of TD2D sessions including the mobility management and radio resource management, which may be a standalone element (unit, module) or be implemented in another network element (unit, module) as such as MME or eNB, for example. The apparatuses may also be parts of the corresponding network elements (e.g., DRSF and eNB). The DRSF may be located in a server, host or corresponding unit or element.

In the example of FIG. 1, it is assumed that the DRSF is located in the MME. Moreover, an S-GW/PDN-GW as an example for an apparatus providing a gateway function for the radio access network is connected to the eNB and the DRSF.

The DRSF, or the corresponding apparatus, comprises a processor and a memory for storing instructions to be executed by the processor, and may also comprise a connection unit, which is configured to provide connection to a network. Likewise, the eNB, or the corresponding apparatus, comprises a processor and a memory for storing instructions to be executed by the processor, and may also comprise a connection unit, which is configured to provide connection to a network, for example a radio access network (RAN), via which devices such as UEs 3 and 4 may be connected. The S-GW/PDN-GW, or the corresponding apparatus, comprises a processor and a memory for storing instructions to be executed by the processor,
and may also comprise a connection unit 53, which is configured to provide connection to other network elements.

0049 It should be understood that the memories as described above may be internal or external or it may be provided as a service via network. Further, the memory may include volatile and/or non-volatile memory. The memory may store computer program code and/or operating systems, information, data, content or the like for the processor to perform operations according to embodiments. The memory may comprise one or more memory units, each of them may be a random access memory, hard drive, etc. The memory units may be at least partly removable and/or detachably operationally coupled to the apparatus. The memory may be of any type suitable for the current technical environment and it may be implemented using any suitable data storage technology, such as semiconductor-based technology, flash memory, magnetic and/or optical memory devices.

0050 In the example of FIG. 1 it is assumed that the UEs 3 and 4 have a connection for proximity service, which may either be an indirect connection via the eNB 2 without involving the core network or a direct connection without involving the eNB 2.

0051 The processor (one or more units, modules, entities, microprocessors, such as single-chip computer element(s), or chipsets(s)) 11 of the DRSF 1 is configured to perform control in relation to a connection for proximity service between at least two devices (e.g., the UEs 3 and 4), to perform lawful interception in relation to the proximity service with respect to at least one device to be intercepted (e.g., the UE 3 or 4) of the at least two devices, and to configure at least one radio access network control element (e.g., eNB 2) to perform the lawful interception in relation to the proximity service.

0052 The processor (one or more units, modules, entities, microprocessors, such as single-chip computer element(s), or chipsets(s)) 21 of the eNB 2 is configured to provide control in a radio access network, perform control in relation to a connection for proximity service between at least two devices (e.g., the UEs 3 and 4), to receive configuration information for performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and to report interception information with respect to the at least one device to be intercepted.

0053 The processor (one or more units, modules, entities, microprocessors, such as single-chip computer element(s), or chipsets(s)) 51 of the S-GW/PDN-GW 5 is configured to provide a connection to a radio access network, to receive interception information intercepted by lawful interception with respect to at least one device (e.g., UE 3 or UE 4) to be intercepted, wherein the at least one device is one of at least two devices connected by a connection for proximity service in the radio access network.

0054 Thus, in case of the DRSF, the processor 11 of the DRSF 1 may instruct the eNB 2 to carry out lawful interception with respect to one or both of the UEs 3 and 4, and the DRSF may report the interception information to a corresponding entity such as a LEMF.

0055 Alternatively, the DRSF may only be involved in configuring eNB for L1, so that the report from the eNB 2 goes to MME (for IRI) and S/PDN-GW 5 (for CC) directly without involving of DRSF.

0056 In case of an indirect connection of the two UEs 3 and 4, the interception information can easily be obtained by the eNB 2. However, in case of a direct connection, it would at least be difficult to obtain communication content information. Therefore, according to an embodiment, the eNB 2 may change the direct connection between the two UEs 3 and 4 to an indirect connection, so that the connection extends via the eNB 2.

0057 Hence, according to embodiments of the present invention, lawful interception is enabled also in the RAN, and therefore also possible for proximity service connections.

0058 In the following, a more detailed embodiment of the present invention is described as a clarifying example.

0059 As mentioned above, according to embodiments of the invention, L1 functionalities are extended from CN to RAN so that proximity services (including D2D discovery and D2D communication either directly between at least two devices or locally routed through eNB) can be kept for L1 targeted UE. In particular, L1 functional architecture is extended to cover ProSe related key EPS nodes (i.e. DRSF and eNB) in order to allow the intercept related information (IRI/events and as well the content of communication (CC) for ProSe) to be available. The possible reference configuration for ProSe interception is illustrated in FIGS. 2 and 3 as an implementation example, which are described later. To support ProSe interception, the following enhancements are proposed:

0060 Upon L1 configuration (e.g., activation, deactivation and interrogation of L1) received by MME or S/PDN-GW, the DRSF is informed for the L1 configuration of the targeted UE in which the information of target identifier and L1 related information (e.g. whether CC should be provided) is included. The target identifier may be indicated explicitly in the form e.g. S-TMSI or D2D ID or implicitly by the signaling transport bearer identifier.

0061 For provision of IRI for ProSe, the following ProSe related events may be introduced: UE requested proximity services including D2D discovery and D2D communication, D2D bearer activation/modification/deactivation, successful D2D discovery etc. They may be introduced by the new events which may be applicable to DRSF/eNB or be extended from current available events. For instance, for UEs in connected state, D2D bearer activation/modification/deactivation events may be provided by enhancing the current bearer activation/modification/deactivation events with additional D2D bearer related information. To achieve successful D2D discovery information, DRSF/eNB may be an applicable L1 entity if D2D discovery procedure requires the network involvement for e.g. identifying the UE. However, if D2D discovery is fully based on pre-configured parameters without network involvement, UE may be configured to report such event in background manner so that each discovery behaviour of the targeted UE can be intercepted.

0062 For provision of CC for ProSe, the activation of L1 CC may trigger the mode switching from direct D2D mode to the locally routed data path mode so that the eNB may be able to duplicate the data packets transmitted between D2D UEs. That is, in this case the eNB is configured to change the direct connection of the DSD UEs to an indirect connection via the eNB.

0063 The activation of L1 CC may also trigger the change of user plane security keys which are adopted in direct D2D mode (i.e., the direct connection between the D2D UEs) and locally routed data path mode (i.e., the indirect connection between the D2D UEs via the eNB) respectively in case security keys for direct mode and locally routed optimized path mode are different.
In addition, the activation/deactivation of LI CC may also trigger the establishment/release of the user plane transport bearer from eNB to S-PDN-GW for provision of CC, which can be regarded as a new trigger for user plane transport bearer management over S1-U interface.

Alternatively, as another option, the establishment/release of the user plane transport bearer from eNB to S-PDN-GW may be triggered when ProSe communication starts/ends. Thus, the established transport bearer may be used by the eNB to transmit the duplicated data packets to S-PDN-GW for providing the intercepted CC.

One possible reference configuration for ProSe interception is shown in FIGS. 2 and 3, in which DRSF is assumed to be located in MME.

As shown in FIGS. 2 and 3, a LEMF is provided which receives intercepted information, such as IRI and CC, and which instructs network elements to perform Lawful Interception. A ADMF is connected, by means of a mediation function, via an interface H11 to the LEMF. A delivery function 2 is connected, by means of a mediation function, via an interface H2 to the LEMF. The delivery function 2 may be connected with the ADMF via an interface X1_2.

In the example according to FIG. 2, the MME, which includes the DRSF (e.g., DRSF 1 shown in FIG. 1) is connected to the ADMF and the delivery function 2 via interfaces X1_1 and X2, respectively. Since the DRSF is assumed to be located in the MME, the interface between DRSF and eNB (e.g., ENB 2 shown in FIG. 1) is S1 control plane (S1-C) interface.

In more detail, the example of FIG. 2 shows the case in which Lawful Interception is only performed by providing IRI, so that the eNB is involved in reporting IRI, which in this case may include the ProSe related events described above. Hence, reporting is performed in this case via the S1-C interface to the MME which also accommodate the DRSF functions.

In the example of FIG. 3, a further delivery function, namely delivery function 3 is connected by means of a mediation function, via interface H3 to the LEMF. The delivery function 3 may be connected to the ADMF via interface X1_3.

In the example of FIG. 3, the S-GW/PDN-GW (e.g., S-GW/PDN-GW 5 shown in FIG. 1) is connected to the ADMF, the delivery function 2 and the delivery function via interfaces X1_1, X2 and X3, respectively. The S-GW/PDN-GW is connected to the DRSF (which is included in the MME) via interface S11, and with an eNB (e.g., eNB 2 shown in FIG. 2) via interface S1-U.

Thus, FIG. 3 shows an example of the case in which Lawful Interception is also carried out by reporting CC. In this case, the eNB reports IRI to the MME with DRSF co-located via the S1-C interface similar as shown in FIG. 2, but also via the S1-U interface to the core network, i.e., to the S-GW/PDN-GW.

Hence, the proposed enhancement according to embodiments of the present invention may be implemented by introducing new procedures or information elements over S1 and S11 interfaces.

An advantage of the solution according to embodiments of the present invention is that LI can be supported for both discovery and communication, without switching back to infrastructure path mode which may lose the benefits of ProSe communication. Meanwhile, with such proposal, it is possible to make the user unaware of the LI happening for the ProSe.

It is noted that the embodiments and the present invention in general is not limited to the specific examples given above.

For example, with respect to FIGS. 2 and 3 it was described that the DRSF is located in the MME. However, the invention is not limited to such network architecture. The DRSF may be a standalone network element and the proposed enhancement may be an implementation over the interface between MME and DRSF and the interface between DRSF and eNB.

Such an example is shown in FIG. 4, which is similar to FIG. 2 except that the DRSF is a standalone network element (or is located in another suitable network element other than the MME or eNB). In this case, the DRSF configures the eNB to report IRI, for example, and the eNB reports IRI via the interface S1-C directly to the MME, without involving the DRSF.

In this case, a general example for the MME may be an apparatus which may have a similar structure as the DRSF or the S-GW/PDN-GW shown in FIG. 1. That is, such an apparatus comprises a processor and a memory for storing instructions to be executed by the processor. The processor is configured to provide a connection to a radio access network, to perform a mobility management function, to receive interception information intercepted by lawful interception with respect to at least one device to be intercepted, wherein at least one device is one of at least two devices connected by a connection for proximity service in the radio access network. The processor may further be configured to receive interception information (e.g., IRI) from a device-to-device registration server function (e.g., the DRSF 1 shown in FIG. 1), wherein the interception information may comprise events related to the connection for proximity service.

Further alternatively, it is also possible that, when the DRSF is a standalone network element, the eNB reports IRI via the DRSF, i.e., not directly to the MME.

Thus, there are three alternatives: i) DRDF co-located with MME and IRI reported to MME&DRSF by eNB, ii) DRSF is standalone element, IRI reported to MME via DRSF iii) DRSF is standalone element, IRI reported to MME without involving of DRSF.

A further alternative is that the DRSF is co-located in eNB. In this case, reporting of IRI to MME via eNB or DRSF is possible.

Moreover, the embodiments described above were described by referring to device-to-device (D2D) communications. However, the invention is not limited to this concept, and can equally be applied to machine-to-machine (M2M) communications, terminal-to-terminal (T2T) communications, peer-to-peer (P2P) communications, or the like.

According to another example of an embodiment, an apparatus is provided which comprises

means for performing control in relation to a connection for proximity service between at least two devices,

means for performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and

means for configuring at least one radio access network control element to perform the lawful interception in relation to the proximity service.
In addition, according to a further example of an embodiment, an apparatus is provided which comprises

- means for providing control in a radio access network,
- means for performing control in relation to a connection for proximity service between at least two devices,
- means for receiving configuration information for performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and
- means for reporting interception information with respect to the at least one device to be intercepted.

According to still further example of an embodiment, an apparatus is provided which comprises

- means for providing a connection to a radio access network, and
- means for receiving interception information intercepted by lawful interception with respect to at least one device to be intercepted, wherein the at least one device is one of at least two devices connected by a connection for proximity service in the radio access network.

It is to be understood that any of the above modifications can be applied singly or in combination to the respective aspects and/or embodiments to which they refer, unless they are explicitly stated as excluding alternatives.

It should be appreciated that

- an access technology via which a signal is transferred to and from a network element may be any suitable present or future technology, such as WLAN (Wireless Local Access Network), WiMAX (Worldwide Interoperability for Microwave Access), LTE, LTE-A, Bluetooth, Infrared, and the like may be used; Additionally, embodiments may also apply wired technologies, e.g., IP based access technologies like cable networks or fixed lines—a user device (also called UE, user equipment, user terminal, terminal device, etc.) illustrates one type of an apparatus to which resources on the air interface may be allocated and assigned, and thus any feature described herein with a user device may be implemented with a corresponding apparatus, such as a relay node. An example of such a relay node is a Layer 3 relay (self-backhauling relay) towards the base station or eNB. The user device typically refers to a portable computing device that includes wireless mobile communication devices operating with or without a subscriber identification module (SIM), including, but not limited to, the following types of devices: a mobile station (mobile phone), smartphone, personal digital assistant (PDA), handset, device using a wireless modem (alarm or measurement device, etc.), laptop and/or touch screen computer, tablet, game console, notebook, and multimedia device. It should be appreciated that a user device may also be a nearly exclusive uplink only device, of which an example is a camera or video camera loading images or video clips to a network. It should be appreciated that a device may be regarded as an apparatus or an assembly of more than one apparatus, whether functionally in cooperation with each other or functionally independently of each other but in a same device housing.

Embodiments suitable to be implemented as software code or portions of it and being run using a processor are software code independent and can be specified using any known or future developed programming language, such as a high-level programming language, such as objective-C, C, C++, C#, Java, etc., or a low-level programming language, such as a machine language, or an assembler, implementation of embodiments, is hardware independent and may be implemented using any known or future developed hardware technology or any hybrids of these, such as a microprocessor or CPU (Central Processing Unit), MOS (Metal Oxide Semiconductor), CMOS (Complementary MOS), BIMOS (Bipolar MOS), BiCMOS (Bipolar CMOS), ECL (Emitter Coupled Logic), and/or TTL (Transistor-Transistor Logic).

Embodiments may be implemented as individual devices, apparatuses, units or means or in a distributed fashion, for example, one or more processors may be used or shared in the processing, or one or more processing sections or processing portions may be used and shared in the processing, wherein one physical processor or more than one physical processor may be used for implementing one or more processing portions dedicated to specific processing as described.

An apparatus may be implemented by a semiconductor chip, a chipset, or a (hardware) module comprising such chip or chipset;

Embodiments may also be implemented as any combination of hardware and software, such as ASIC (Application Specific IC (Integrated Circuit)) components, FPGA (Field-programmable Gate Arrays) or CPLD (Complex Programmable Logic Device) components or DSP (Digital Signal Processor) components.

Embodiments may also be implemented as computer program products, comprising a computer usable medium having a computer readable program code embodied therein, the computer readable program code adapted to execute a process as described in embodiments, wherein the computer usable medium may be a non-transitory medium. Computer program products, also called programs or computer programs, including software routines, applets and macros, may be stored in any apparatus-readable data storage medium and they comprise program instructions to perform one or more particular tasks. A computer program product may comprise one or more computer-executable components which, when the program is run, are configured to carry out embodiments. The one or more computer-executable components may be at least one software code or portions of it.

It is noted that the embodiments and examples described above are provided for illustrative purposes only and are in no way intended that the present invention is restricted thereto. Rather, it is the intention that all variations and modifications be included which fall within the spirit and scope of the appended claims.

1. An apparatus comprising
   a processor and
   a memory for storing instructions to be executed by the processor, wherein the processor is configured to perform control in relation to a connection for proximity service between at least two devices, to perform lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and...
to configure at least one radio access network control element to perform the lawful interception in relation to the proximity service.

2. The apparatus according to claim 1, wherein the interception information to be reported comprises communication content information, and the connection for proximity service between the at least two devices is an indirect connection via the at least one radio access network control element, and

the processor is configured to instruct the at least one radio access network control element to provide the communication content information.

3. The apparatus according to any claim 1, wherein the interception information to be reported comprise connection information and the connection for proximity service between the at least two devices is a direct connection between the at least two devices, and

the processor is configured to instruct the at least one radio access network control element to change the connection for proximity service to an indirect connection via the at least one radio access network control element and to provide the communication content information.

4. The apparatus according to claim 7, wherein the processor is configured to trigger a change of user plane security keys which are adopted in the direct connection and indirect connection respectively, in case security keys for direct connection and indirect connection are different.

5. The apparatus according to claim 9, wherein the processor is configured to receive a trigger for establishing a user plane transport bearer from the apparatus to a core network for providing communication content information upon starting providing of the communication content information, and/or deactivating the user plane transport bearer from the apparatus to the core network upon ending providing of the communication content information.

16. The apparatus according to claim 9, wherein the processor is configured to receive a trigger for establishing a user plane transport bearer from the apparatus to a core network for providing communication content information upon starting providing of the communication content information, and/or deactivating the user plane transport bearer from the apparatus to the core network upon ending providing of the communication content information.

17. The apparatus according to claim 9, wherein the processor is configured to receive a trigger for establishing a user plane transport bearer from the apparatus to a core network for providing communication content information when a communication via the connection for proximity service between the at least two devices starts, and/or deactivating the user plane transport bearer from the apparatus to the core network when the communication via the connection for proximity service between the at least two devices ends.

18. (canceled)

19. An apparatus comprising a processor and a memory for storing instructions to be executed by the processor, wherein the processor is configured to provide a connection to a radio access network, and to receive interception information intercepted by lawful interception with respect to at least one device to be intercepted, wherein the at least one device is one of at least two devices connected by a connection for proximity service in the radio access network.

20. (canceled)

21. (canceled)

22. The apparatus according to claim 19, wherein the processor is configured to trigger establishing a user plane transport bearer from a radio access network control element intercepting the at least one device for providing communication content information upon starting providing of the communication content information, and/or deactivating the user plane transport bearer from the radio access network control element upon ending providing of the communication content information.

23. The apparatus according to claim 19, wherein the processor is configured to trigger establishing a user plane transport bearer from a radio access network control element intercepting the at least one device for providing communication content information when a communication via the connection for proximity service between the at least two devices starts, and/or deactivating the user plane transport bearer from the radio access network control element when the communication via the connection for proximity service between the at least two devices ends.

24. (canceled)

25. (canceled)

26. A method comprising performing control in relation to a connection for proximity service between at least two devices, and performing lawful interception in relation to the proximity service with respect to at least one device to be intercepted of the at least two devices, and
configuring at least one radio access network control element to perform the lawful interception in relation to the proximity service.

27.-30. (canceled)

31. The method according to any one of the claim 26, wherein
the interception information to be reported comprises commu-
nication content information, and the connection for prox-
imity service between the at least two devices is an indirect
connection via the at least one radio access network control
element, and the method further comprises
instructing the at least one radio access network control
element to provide the communication content informa-
tion.

32. The method according to claim 26, wherein the inter-
ception information to be reported comprise connection con-
tent information and the connection for proximity service bet-
ween the at least two devices is a direct connection between
the at least two devices, and
the method further comprises
instructing the at least one radio access network control
element to change the connection for proximity service to an
indirect connection via the at least one radio access network
control element and to provide the communication content informa-
tion.

33. The method according to claim 32, further comprising
triggering a change of user plane security keys which are
adopted in the direct connection and indirect connection re-
spectively, in case security keys for direct connection and
indirect connection are different.

34. The method according to claim 26, wherein the method
is implemented in a device-to-device registration server func-
tion or a mobility management entity or in the radio access
network control element.

35. A method comprising
providing control in a radio access network,
performing control in relation to a connection for proxim-
ity service between at least two devices,
receiving configuration information for performing lawful
interception in relation to the proximity service with respect to
at least one device to be intercepted of the at
least two devices, and
reporting interception information with respect to the at
least one device to be intercepted.

36.-38. (canceled)

39. The method according to claim 35, wherein
the interception information to be reported comprises commu-
nication content information, and the connection for prox-
imity service between the at least two devices is an indirect
connection via a radio access network control
element carrying out the method, and
the method further comprises
reporting the communication content information.

40. The method according to claim 35, wherein the inter-
ception information to be reported comprise connection con-
tent information and the connection for proximity service
between the at least two devices is a direct connection between
the at least two devices, and
the method further comprises
changing the connection for proximity service to an indi-
rect connection via a radio access network control ele-
ment carrying out the method and to report the commu-
nication content information.

41. The method according to claim 40, further comprising
triggering a change of user plane security keys which are
adopted in the direct connection and indirect connection re-
spectively, in case security keys for direct connection and
indirect connection are different.

42. The method according to claim 35, further comprising
receiving a trigger for establishing a user plane transport
bearer from a radio access network control element car-
ying out the method to a core network for providing
communication content information upon starting pro-
viding of the communication content information, and/
or deactivating the user plane transport bearer from the
radio access network control element to the core net-
work upon ending providing of the communication con-
tent information.

43. The method according to claim 35, further comprising
receiving a trigger for establishing a user plane transport
bearer from a radio access network control element car-
ying out the method to a core network for providing
communication content information when a communi-
vation via the connection for proximity service between the
at least two devices starts, and/or deactivating the
user plane transport bearer from the radio access net-
work control element to the core network when the
communication via the connection for proximity service
between the at least two devices ends.

44. (canceled)

45. (canceled)

46. A method comprising
providing a connection to a radio access network, and
receiving interception information intercepted by lawful
interception with respect to at least one device to be
intercepted, wherein the at least one device is one of at
least two devices connected by a connection for prox-
imity service in the radio access network.

47. (canceled)

48. (canceled)

49. The method according to claim 46, further comprising
triggering establishing a user plane transport bearer from a
radio access network control element intercepting the
at least one device to a gateway element performing the
method for providing communication content informa-
tion upon starting providing of the communication content informa-
tion, and/or deactivating the user plane transport bearer from the
radio access network control element to the gateway element upon ending providing
of the communication content information.

50. The method according to claim 46, further comprising
triggering establishing a user plane transport bearer from a
radio access network control element intercepting the
at least one device to a gateway element performing the
method for providing communication content informa-
tion when a communication via the connection for prox-
imity service between the at least two devices starts,
and/or deactivating the user plane transport bearer from the
radio access network control element to the gateway element when the communication via the connection for proximity service between the at least two devices ends.

51. (canceled)

52. A computer program product comprising code means
for performing a method according to claim 26 when run on
a processing means or module.

53. (canceled)