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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 February 2017 (23.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/029282 A1

(51) International Patent Classification:
H04W 8/20 (2009.01) *H04W 12/06* (2009.01)
H04W 12/04 (2009.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/EP2016/069409

(22) International Filing Date:
16 August 2016 (16.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/205,774 17 August 2015 (17.08.2015) US

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

(72) Inventor: **HORN, Guenther**; Prälat-Zistl-Str. 12, 80331 Munich (DE).

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

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

Published:

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

WO 2017/029282 A1

(54) Title: SECURITY PROCEDURES FOR THE CELLULAR INTERNET OF THINGS

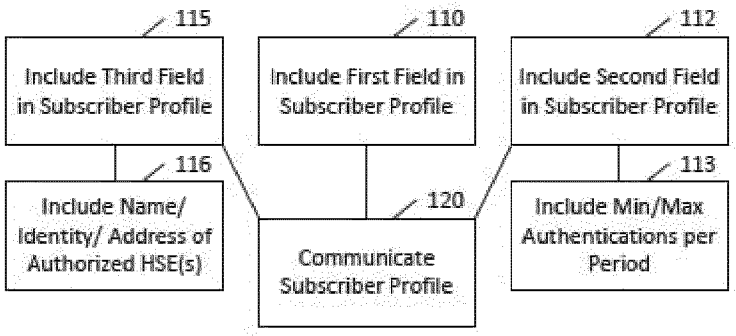

Figure 1

(57) Abstract: Various communication systems may benefit from appropriate security measures. For example, the cellular internet of things may benefit from suitable security procedures. A method can include including a first field in a subscriber profile. The first field can be configured to determine a minimum strength for at least one cryptographic algorithm to be used between a user equipment associated with this subscription and a support node. The method can also include transmitting the subscriber profile between a subscriber database and the support node.

DESCRIPTION

TITLE:

Security Procedures for the Cellular Internet of Things

CROSS-REFERENCE TO RELATED APPLICATION:

[0001] This application is related to and claims the benefit and priority of U.S. Provisional Patent Application No. 62/205,774, filed August 17, 2015, which is hereby incorporated herein by reference.

BACKGROUND:

Field:

[0002] Various communication systems may benefit from appropriate security measures. For example, the cellular internet of things may benefit from suitable security procedures.

Description of the Related Art:

[0003] The Cellular Internet of Things (CIoT) is an area of the third generation partnership project (3GPP) and is related to various 3GPP working groups, in particular global system for mobile communication (GSM) enhanced data rates for GSM evolution (EDGE) radio access network (GERAN), RAN2, SA2, and SA3, including security.

[0004] The 3GPP work on security for the CIoT is split into two streams: one that relates to improving on general packet radio service (GPRS) security, and another that relates to providing end-to-middle (e2m) security for CIoT between the device and a CIoT server in the home network. The CIoT server in the home network can be referred to as a home public land mobile network (HPLMN) security endpoint (HSE).

[0005] The current state of the discussion for e2m security for CIoT is captured in a draft technical report (TR), namely 3GPP TR 33.863 v0.2.0 “Study on battery efficient security for very low throughput Machine Type Communication Devices; (Release 13),” available at http://www.3gpp.org/DynaReport/33863.htm, the entirety of which is hereby incorporated herein by reference.

[0006] Battery efficient security can involve several issues. A first issue relates to crypto policy in the GPRS access network. 3GPP TR 33.863 v0.2.0 contains provisions that require the upgrade of GGSNs and SGSNs, including the upgrade of the current GPRS infrastructures.

[0007] In particular, 3GPP TR 33.863 v0.2.0 describes a pre-condition that “The SGSN/MME has indicated the supported security configuration of the GERAN/E-UTRAN to the H-PLMN

i.e. the used confidentiality algorithm and integrity protection algorithm (e.g. for GERAN: GEA4 in use, e.g for LTE 128-EEA2 and 128-EIA2 in use)." Such an indication is not conventionally available on the interface between SGSN and HLR.

[0008] Moreover, when e2m security is guaranteed for the user plane then it may not be important whether the user plane is additionally encrypted over the access between UE and SGSN. Additionally, strong signaling protection between the UE and SGSN may not be needed, as the termination point of e2m security, the HSE, can control whether the desired e2m security association was established or not. This control by the HSE can preclude the man-in-the-middle attacks which are possible in 2G.

[0009] Secondly, the indication described 3GPP TR 33.863 v0.2.0 may not help the SGSN to learn which crypto algorithms have to be applied for this UE from the home network's point of view.

[0010] Furthermore, if the visited network hosting the SGSN or the MME cannot be trusted, then there is no apparent reason why the home network would trust this indication from the SGSN. Furthermore, for LTE this indication may not make sense, as strong cryptographic algorithms are in place in LTE.

[0011] A second issue relates to authentication and key usage policy in the visited network. 3GPP contribution S3-151367, which can be found at ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_79_Nanjing/Docs/, states that an HLR/HSS-driven authentication policy is needed because the H-PLMN is better informed than the V-PLMN, as to the best authentication policy which will maximize the battery capacity of the UE. Moreover, the same document states that the HLR/HSS should provide an expiration time for the authentication vectors and specifically states, "When the expiration time is reached, the SGSN/MME should either use the stored, unused and not expired AV or request new AV to the HLR/HSS." S3-151367 is hereby incorporated herein by reference. However, there is no conventional way of communicating such a policy to the SGSN or MME.

[0012] A third issue relates to usage of e2m security. 3GPP TR 33.863 v0.2.0 describes a mechanism for establishing e2m security between UE and HSE. For this purpose, cryptographic keys are established with the support of the HLR or HSS. However, not all UEs may require e2m security. For example, only certain CIoT UEs may need e2m security.

[0013] Furthermore, S3-151367 mentions an authentication management field (AMF) to be used in deriving keys for e2m security. The AMF is a 16-bit field in an authentication vector that is generated in the Authentication Centre (AuC). However, there is no conventional way for the AuC to know whether the bit in the AMF related to e2m security for CIoT has to be set. Additionally, neither 3GPP TR 33.863 v0.2.0 nor S3-151367 indicates how the HLR or HSS

could know whether keys for establishing e2m security are required for a particular subscription.

[0014] A fourth issue relates to key derivation for HSE. 3GPP TR 33.863 v0.2.0 describes a mechanism for establishing e2m security between UE and HSE. In this mechanism, keys called "E2E CK/IK" are derived in a deterministic fashion from the UMTS AKA keys or EPS AKA keys CK and IK. This approach is based on there being one e2m security termination point HSE. However, the UE may want to communicate with two or more such termination points, such as HSE1 and HSE2. Conventionally there is no mechanism that derives multiple keys "E2E CK/IK", one for each such termination point.

SUMMARY:

[0015] According to a first embodiment, a method can include including a first field in a subscriber profile. The first field can be configured to determine a minimum strength for at least one cryptographic algorithm to be used between a user equipment associated with this subscription and a serving node. The method can also include transmitting the subscriber profile between a subscriber database and the support node.

[0016] In a variant, the support node can be a serving general packet radio service support node.

[0017] In a variant, the subscriber database can be a home location register.

[0018] In a variant, the transmitting can include transmitting the subscriber profile from the subscriber database to the support node or transmitting the subscriber profile from the support node to the subscriber database.

[0019] In a variant, the subscriber profile can include at least one of a general packet radio service subscriber profile, a third generation subscriber profile, or a fourth generation subscriber profile.

[0020] In a variant, the first field can include a list of permitted algorithms or a list of forbidden algorithms.

[0021] In a variant, the method can further include including a second field in the subscriber profile. The second field can be configured to determine an authentication policy required for a subscriber corresponding to the subscriber profile.

[0022] In a variant, the method can further include including, in the second field, a minimum and maximum allowed numbers of authentication in a certain period.

[0023] In a variant, the second field can further be configured to indicate whether derivation of new keys K_{eNB} from an existing K_{ASME} is permitted.

[0024] In a variant, the method can further include including a third field in the subscriber

profile. The third field can be configured to indicate to a network element whether the network element needs to provide support for establishing end-to-middle security.

[0025] In a variant, the network element can be a home location register or a home subscriber server.

[0026] In a variant, the method can also include including, in the third field names, identities, addresses, or any combination thereof, of at least one home public land mobile network security endpoint authorized to communicate with the user equipment.

[0027] According to a second embodiment, an apparatus can include means for performing the method according to the first embodiment in any of its variants.

[0028] According to a third embodiment, an apparatus can include at least one processor and at least one memory and computer program code. The at least one memory and the computer program code can be configured to, with the at least one processor, cause the apparatus at least to perform the method according to the first embodiment in any of its variants.

[0029] According to a fourth embodiment, a computer program product may encode instructions for performing a process including the method according to the first embodiment in any of its variants.

[0030] According to a fifth embodiment, a non-transitory computer readable medium may encode instructions that, when executed in hardware, perform a process including the method according to the first embodiment in any of its variants.

BRIEF DESCRIPTION OF THE DRAWINGS:

[0031] For proper understanding of the invention, reference should be made to the accompanying drawings, wherein:

[0032] Figure 1 illustrates a method according to certain embodiments.

[0033] Figure 2 illustrates a system according to certain embodiments.

DETAILED DESCRIPTION:

[0034] Battery efficient security can involve several issues, as outlined above. Some of these issues may be related in that certain embodiments may address them through extensions to the subscriber profile for CIoT purposes. Another issue relates to deriving different keys for different servers, but may be resolved in combination with or separately from the other issues.

[0035] Certain embodiments may address the issue of crypto policy in a GPRS access network. For example, certain embodiments may include a field in the GPRS subscriber

profile. This field can determine the minimum strength(s) for the cryptographic algorithm(s) to be used between the UE with this subscription and the SGSN. For 3G and 4G subscriptions, this field may not be needed. The field can determine a general minimum strength for all cryptographic algorithms, or respective minimum strengths for each corresponding cryptographic algorithm. Other ways of indicating minimum strength, such as by groups, are also permitted.

[0036] Certain embodiments may allow the home network to flexibly inform the serving node in the visited network of the required crypto policy for the radio access.

[0037] The field in the subscriber profile may, for example, contain lists of permitted algorithms or lists of forbidden algorithms. These can respectively referred to as white lists and black lists. These lists can be encoded in the form of an efficient encoding, using either the algorithm codes from the radio access networks, or different codes. The different codes may be specific to this use in the subscriber profile.

[0038] Certain embodiments, therefore, may be able to provide e2m security without having to upgrade the interface between the SGSN and the HLR, as subscriber profiles may be supportable without additional upgrades. Furthermore, an SGSN not recognizing the field can ignore the field. Thus, certain embodiments may provide for backwards compatibility.

[0039] Additionally, certain embodiments may address the issue of authentication and key usage policy in the visited network. For example, certain embodiments may include another field in the GPRS, 3G, or 4G subscriber profiles. The additional field can determine the authentication policy required for the subscriber.

[0040] Certain embodiments can address the issue of authentication and key usage policy as an add-on to addressing the issue of crypto policy in a GPRS access network. Thus, both issues may be addressed by extending a subscriber profile for CIoT purposes

[0041] The field in the subscriber profile could state the minimum and maximum allowed numbers of authentication in a certain period. The minimum is relevant for security, the maximum is relevant for battery-saving as authentications can drain the battery of very low cost CIoT devices.

[0042] In addition, for LTE, the field can give an indication whether the HSE is allowed to derive new keys K_{eNB} from an existing K_{ASME}, as described in 3GPP TS 33.401, clause 7.2.9.2.

[0043] Certain embodiments can further address the issue of usage of e2m security. In certain embodiments, yet another field can be included in the GPRS, 3G, or 4G subscriber profiles. The field can indicate to the HLR or HSS whether the HLR or HSS needs to provide support for establishing e2m security. This field can be used as an add-on to one or both of

the previously described fields.

[0044] The field in the GPRS, 3G or 4G subscriber profiles could contain just one bit. This bit could be sent from the HLR or HSS front ends to the AuC to indicate whether to set a particular bit in the Authentication Management Field (AMF). This field does not need to be sent to the serving node and can be kept internal to the HLR or HSS. In certain embodiments, this field could be managed by management entity for CIoT subscribers.

[0045] The field could contain the names, or identities, or addresses, of the HSE or HSEs authorized to communicate with the UE. Any combination of names, identities, and/or addresses can be provided in the field.

[0046] Certain embodiments may address the issue of key derivation for HSE. For example, there may be two termination points, HSE1 and HSE2, for e2m security. HSE1 and HSE2 may be running two different IoT applications. There may be separate application level security to separate applications. Alternatively, HSE1 and HSE2 may not reside in the home network, but may be hosted by third parties. Thus, for this additional or alternative reason it may be useful for HSE1 and HSE2 to have separate security with different cryptographic keys. Otherwise, a compromise of one HSE1 may also compromise the second one, and HSE1 could spy on HSE2.

[0047] New keys E2E-HSE can be used instead of the keys "E2E CK/IK" described in TR 33.863 v0.2.0. The purpose of the key derivation, such as e2m security for CIoT, can be input to the key derivation together with the name or identity or address of the HSE. In this or any other way, it can be arranged that HSE1 cannot know the key of HSE2, and vice versa.

[0048] In order to derive the new keys E2E-HSE, any Key Derivation Function (KDF) can be used. For example, the KDF defined in 3GPP TS 33.220, Annex B, and used in 3GPP TS 33.401, Annex A, could be used. The name of the HSE, as well as the keys CK and IK resulting from a run of UMTS AKA or EPS AKA when authenticating the UE, can be provided as input to the key derivation.

[0049] So, an example of a formula for obtaining the desired keys can be as follows: E2E-HSE = KDF (CK, IK; HSE-id, e2m-CIoT). where KDF is the Key Derivation Function from TS 33.220, the input key is equal to the concatenation CK || IK of CK and IK, HSE-id is the name of the HSE, and "e2m-CIoT" indicates that the key is for use with e2m-security in CIoT.

[0050] In accordance with certain embodiments, more than one HSE can be used by one UE simultaneously without the risk of lowering security. For example, security may be preserved even when both HSEs are not within a home network.

[0051] Figure 1 illustrates a method according to certain embodiments. As shown in Figure 1, a method can include, at 110, including a first field in a subscriber profile. The first field can

be configured to determine a minimum strength for at least one cryptographic algorithm to be used between a user equipment associated with this subscription and a support node. The method can also include, at 120, transmitting the subscriber profile between a subscriber database and the support node. The subscriber profile may be communicated between other networks in addition to, or instead of, the subscriber database and the support node.

[0052] The support node can, for example, be a serving general packet radio service support node. The subscriber database can be a home location register or other database.

[0053] The transmitting at 120 can include transmitting the subscriber profile from the subscriber database to the support node or transmitting the subscriber profile from the support node to the subscriber database. This transmission may be directly between the support node and the subscriber database or via one or more other nodes.

[0054] The subscriber profile can be a general packet radio service subscriber profile, a third generation subscriber profile, a fourth generation subscriber profile, or any combination thereof. Other kinds of subscriber profiles are also permitted.

[0055] The first field can include a list of permitted algorithms, a list of forbidden algorithms, or both kinds of lists.

[0056] The method can further include, at 112, including a second field in the subscriber profile. The second field can be configured to determine an authentication policy required for a subscriber corresponding to the subscriber profile.

[0057] The method can additionally include, at 113, including, in the second field, a minimum and maximum allowed numbers of authentication in a certain period. Other aspects of an authentication policy can likewise be indicated in the second field. For example, the second field can further be configured to indicate whether derivation of new keys K_{eNB} from an existing K_{ASME} is permitted.

[0058] The method can also include, at 115, including a third field in the subscriber profile. The third field can be configured to indicate to a network element whether the network element needs to provide support for establishing end-to-middle security. The network element can be a home location register or a home subscriber server.

[0059] The method can further include, at 116, including, in the third field names, identities, addresses, or any combination thereof, of at least one home public land mobile network security endpoint authorized to communicate with the user equipment.

[0060] Although the fields are designated as first, second, and third fields, for convenient and clear reference, the fields may be present in the subscriber database in any order with respect to each other and with respect to other fields in the database. Thus, the first field does not have to be the first field of the entire subscriber database, nor present first in time,

nor even in a first position relative to the other fields, if the other fields are present. In certain embodiments, two or more of the fields may be concatenated together, and may still be considered first, second, and third fields. Thus, while individual and distinct fields are one option, such an option is not required in all embodiments.

[0061] Figure 2 illustrates a system according to certain embodiments of the invention. In one embodiment, a system may include multiple devices, such as, for example, at least one UE 210, at least one access node 220, which may be an SGSN or MME, or other network element terminating access security, and at least one network element 230, which may be an HSE, HLR, or any of the other core network elements, either in a home network or a visited network, described herein.

[0062] Each of these devices may include at least one processor, respectively indicated as 214, 224, and 234. At least one memory can be provided in each device, and indicated as 215, 225, and 235, respectively. The memory may include computer program instructions or computer code contained therein. The processors 214, 224, and 234 and memories 215, 225, and 235, or a subset thereof, can be configured to provide means corresponding to the various blocks of Figure 1.

[0063] As shown in Figure 2, transceivers 216, 226, and 236 can be provided, and each device may also include an antenna, respectively illustrated as 217, 227, and 237. Other configurations of these devices, for example, may be provided. For example, network element 230 may be configured for wired communication, instead of or in addition to wireless communication, and in such a case antenna 237 can illustrate any form of communication hardware, without requiring a conventional antenna.

[0064] Transceivers 216, 226, and 236 can each, independently, be a transmitter, a receiver, or both a transmitter and a receiver, or a unit or device that is configured both for transmission and reception.

[0065] Processors 214, 224, and 234 can be embodied by any computational or data processing device, such as a central processing unit (CPU), application specific integrated circuit (ASIC), or comparable device. The processors can be implemented as a single controller, or a plurality of controllers or processors.

[0066] Memories 215, 225, and 235 can independently be any suitable storage device, such as a non-transitory computer-readable medium. A hard disk drive (HDD), random access memory (RAM), flash memory, or other suitable memory can be used. The memories can be combined on a single integrated circuit as the processor, or may be separate from the one or more processors. Furthermore, the computer program instructions stored in the memory and which may be processed by the processors can be any suitable form of computer program

code, for example, a compiled or interpreted computer program written in any suitable programming language.

[0067] The memory and the computer program instructions can be configured, with the processor for the particular device, to cause a hardware apparatus such as UE 210, access node 220, and network element 230, to perform any of the processes described herein (see, for example, Figure 1). Therefore, in certain embodiments, a non-transitory computer-readable medium can be encoded with computer instructions that, when executed in hardware, perform a process such as one of the processes described herein. Alternatively, certain embodiments of the invention can be performed entirely in hardware.

[0068] Furthermore, although Figure 2 illustrates a system including a UE, access node, and network element, embodiments of the invention may be applicable to other configurations, and configurations involving additional elements. For example, not shown, additional UEs and access network elements may be present, and additional core network elements may be present, as mentioned and discussed above.

[0069] 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.

[0070] List of Abbreviations

[0071] AuC = Authentication Centre

[0072] CIoT = Cellular Internet of Things

[0073] E2E = end-to-end

[0074] e2m = end-to-middle

[0075] HLR = Home Location Register

[0076] HSE = HPLMN Security Endpoint

[0077] HSS = Home Subscriber Server

[0078] KDF = Key Derivation Function

[0079] MME = Mobility Management entity

[0080] SGSN = Serving GPRS Support Node

WE CLAIM:

1. A method, comprising:

including a first field in a subscriber profile, wherein the first field is configured to determine a minimum strength for at least one cryptographic algorithm to be used between a user equipment associated with the subscriber profile and a serving node; and

transmitting the subscriber profile between a subscriber database and the support node.

2. The method of claim 1, wherein the support node is a serving general packet radio service support node.

3. The method of claim 1, wherein the subscriber database comprises a home location register.

4. The method of claim 1, wherein the transmitting comprises transmitting the subscriber profile from the subscriber database to the support node or transmitting the subscriber profile from the support node to the subscriber database.

5. The method of claim 1, wherein the subscriber profile comprises at least one of a general packet radio service subscriber profile, a third generation subscriber profile, or a fourth generation subscriber profile.

6. The method of claim 1, wherein the first field comprises a list of permitted algorithms or a list of forbidden algorithms.

7. The method of claim 1, further comprising:

including a second field in the subscriber profile, wherein the second field is configured to determine an authentication policy required for a subscriber corresponding to the subscriber profile.

8. The method of claim 7, further comprising:

including, in the second field, a minimum and maximum allowed numbers of authentication in a certain period.

9. The method of claim 7, wherein the second field is further configured to indicate

whether derivation of new keys K_{eNB} from an existing K_{ASME} is permitted.

10. The method of claim 1, further comprising:

including a third field in the subscriber profile, wherein the third field is configured to indicate to a network element whether the network element needs to provide support for establishing end-to-middle security.

11. The method of claim 10, wherein the network element comprises a home location register or a home subscriber server.

12. The method of claim 10, further comprising:

including, in the third field, names, identities, addresses, or any combination thereof, of at least one home public land mobile network security endpoint authorized to communicate with the user equipment.

13. An apparatus, comprising:

means for performing the method according to any of claims 1-12.

14. An apparatus, comprising:

at least one processor; and

at least one memory including computer program code,

wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus at least to perform the method according to any of claims 1-12.

15. A computer program product encoding instructions for performing a process, the process comprising the method according to any of claims 1-12.

16. A non-transitory computer readable medium encoding instructions that, when executed in hardware, perform a process including the method according to any of claims 1-12.

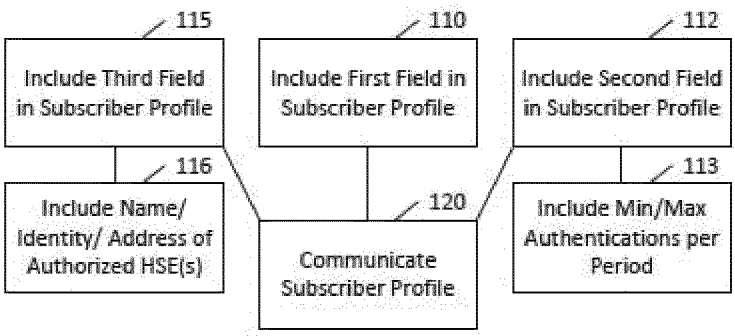
115
Include Third Field in Subscriber Profile
110
Include First Field in Subscriber Profile
112
Include Second Field in Subscriber Profile
116
Include Name/ Identity/ Address of Authorized HSE(s)
120
Communicate Subscriber Profile
113
Include Min/Max Authentications per Period

Figure 1

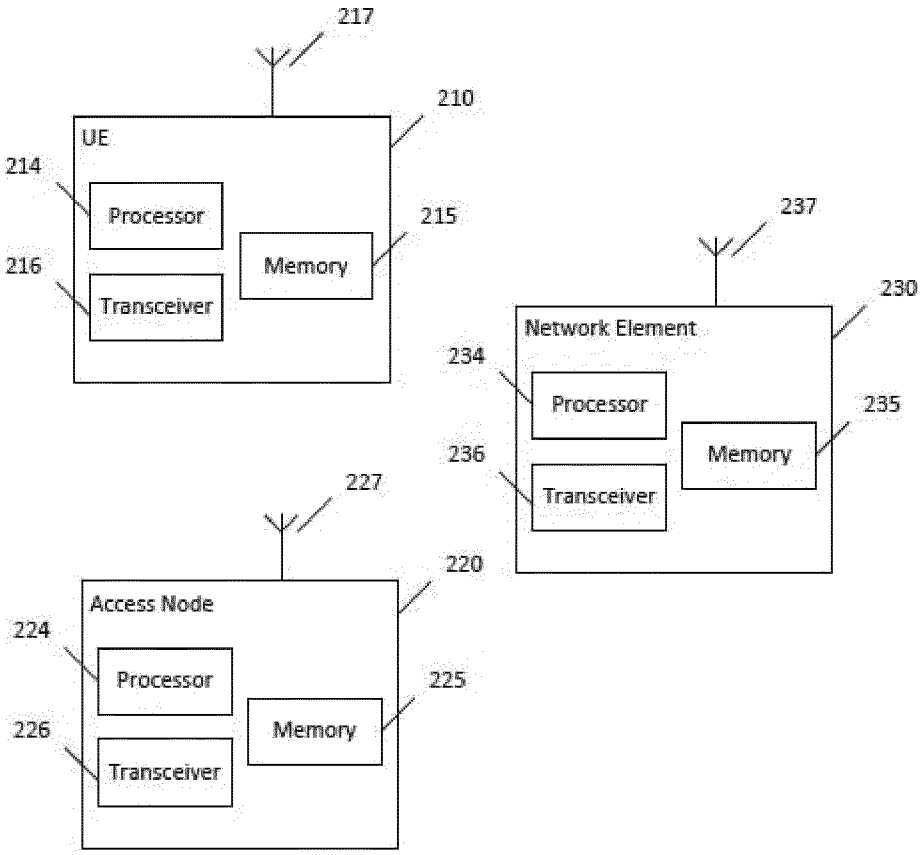
217
210
UE
214
Processor
215
Memory
216
Transceiver
237
230
Network Element
234
Processor
235
Memory
236
Transceiver
227
220
Access Node
224
Processor
225
Memory
226
Transceiver

Figure 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/069409

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W8/20 H04W12/04 H04W12/06 H04L29/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2005/135625 A1 (TANIZAWA YOSHIMICHI [JP] ET AL) 23 June 2005 (2005-06-23) abstract paragraph [0040] - paragraph [0070] figures 3, 4, 6	1,6, 13-16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 October 2016	28/10/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Poppe, Fabrice

3

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3RD GENERATION PARTNERSHIP PROJECT; TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS: "Study on EGPRS Access Security Enhancements with relation to cellular IoT (Release 13)", 3GPP TR 33.860 V0.2.0, 13 May 2015 (2015-05-13), XP050966408, [retrieved on 2015-05-13] 4 Cellular IoT 5.1 Key Issue #1: Entity authentication and key agreement 5.2 Key Issue #2: Eavesdropping 6.1 Solution #1: Integrity protection of signalling and algorithm negotiation -----	1-16
A	3RD GENERATION PARTNERSHIP PROJECT; TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS: "Study on battery efficient security for very low throughput Machine Type Communication Devices (Release 13)", 3GPP TR 33.863 V0.2.0, 13 May 2015 (2015-05-13), XP050966406, [retrieved on 2015-05-13] cited in the application 4.5 Battery usage challenges 6.1 Solution #1: "UE to HPLMN" security solutions based on UMTS/EPS AKA enhancements -----	1-16
A	VODAFONE: "pCR to FS_BEST_MTC_Sec: Adding UE to GGSN security s", 3GPP SA WG3, S3-151367 , 13 April 2015 (2015-04-13), XP050963040, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_79_Nanjing/Docs/ [retrieved on 2015-04-13] cited in the application the whole document -----	1-16
X,P	NOKIA NETWORKS: "pCR to TR 33.863 (CIoT BEST) on end-to-middle security solution based on AKA", 3GPP TSG SA WG3 (Security) Meeting #80, S3-152081 , 28 August 2015 (2015-08-28), XP051043195, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_80_Tallinn/Docs/ [retrieved on 2015-08-28] the whole document -----	1-16

-/--

3

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	3RD GENERATION PARTNERSHIP PROJECT; TECHNICAL SPECIFICATION GROUP SERVICES AND SYSTEM ASPECTS: "Study on battery efficient security for very low throughput Machine Type Communication Devices (Release 13)", 3GPP TR 33.863 V0.3.0, 14 September 2015 (2015-09-14), XP050995987, [retrieved on 2015-09-14] 6.2 Solution #2: "End-to-middle security based on AKA" -----	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2016/069409

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005135625 A1	23-06-2005	JP 4000111 B2	31-10-2007
		JP 2005184463 A	07-07-2005
		US 2005135625 A1	23-06-2005