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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 November 2015 (26.11.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/177398 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/FI2014/050383

(22) International Filing Date:
20 May 2014 (20.05.2014)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventors: **BERGIUS, Hannu**; Vesakuja 1 A 1, FI-36200 Kangasala (FI). **HOLTMANNS, Silke**; Härkäpurontie 15, FI-01800 Klaukkala (FI).

(74) Agent: **ESPATENT OY**; Kaivokatu 10 D, FI-00100 Helsinki (FI).

(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, 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, 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, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

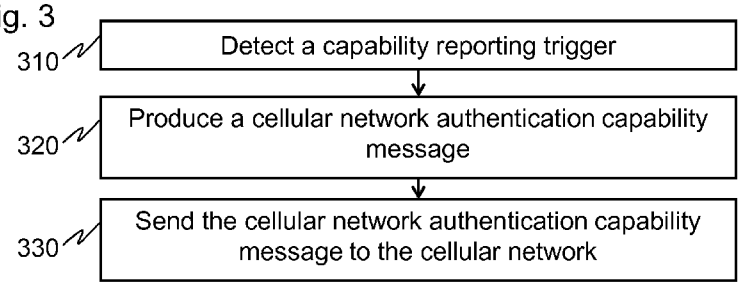
Published:

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

WO 2015/177398 A1

(54) Title: CELLULAR NETWORK AUTHENTICATION CONTROL

Fig. 3



(57) Abstract: A cellular terminal detects any capability reporting trigger and responsively to such determination produces a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and transmits the cellular network authentication capabilities message to the cellular network. The cellular network receives the network authentication capabilities message from a cellular terminal, selects a cellular authentication algorithm based on capabilities indicated by the network authentication capabilities message; and performs cellular authentication with the cellular terminal using the selected cellular authentication algorithm.

CELLULAR NETWORK AUTHENTICATION CONTROL

TECHNICAL FIELD

[0001] The present application generally relates to cellular network authentication control.

BACKGROUND

[0002] This section illustrates useful background information without admission of any technique described herein representative of the state of the art.

[0003] Cellular telecommunications networks or cellular networks are ubiquitous in modern societies. As a necessary condition, they need to be secured to avoid phone bill frauds and to secure communications against illegal interception of private calls and messages. To this end, telecommunications operators of modern cellular networks protect their subscribers with a host of different techniques that typically rely on digital signal processing.

[0004] To enable a cellular terminal to start communications, the terminals need to attach to a network in a network attach process. In the network registration process, a cellular terminal exchanges signals to authenticate itself or more accurately its subscription, typically using a subscriber identity module (SIM). In the network attach or registration process, the cellular terminal obtains from the network and the SIM access information such as a session key with which the cellular terminal can subsequently communicate in the cellular network. The access information typically changes to prevent re-use of the access information by a possible illegal interceptor.

[0005] Encryption is a basic tool that is employed also in other types of digital cellular systems. Already GSM enabled encryption to practically prevent illegal interception. The development of computer technology has subsequently made old encryption techniques more vulnerable, but also helped to enhance the security techniques used in cellular systems. For instance, wide-band CDMA (W-CDMA) was designed for stronger security by enabling also the network to authenticate itself to the cellular terminals. In the W-CDMA, the subscriber identity is provided by a Universal Integrated Circuit Card (UICC) that runs a Universal Subscriber Identity Module (USIM). The USIM produces e.g. a session key based on a shared secret stored on the UICC, challenge and replay attack prevention codes received from the

network and cryptographic algorithm that is enhanced over the one used in GSM. Also the authentication signaling is enhanced in the W-CDMA over GSM e.g. for protection against some man-in-the-middle attacks.

[0006] In parallel with the development of security methods for securing the communications in the cellular systems, there are also growing needs for developing the security structure of cellular terminals. At present, most cellular terminals contain an identity module slot known as a SIM slot in which a user can place and replace an identity module card (e.g. UICC). There is also development towards software based identity modules that are not physically replaceable and in addition enable over-the-air change of subscription from one operator to another. The embedded form factor prevents theft of the identity module from a cellular terminal. The terminals with embedded secure modules are often unattended machines. Such software identity modules may be very useful e.g. for built-in vehicular communication systems so that their emergency reporting capabilities and possible burglar control systems could not be easily deactivated by removing a SIM.

[0007] While necessary for security, the authentication signaling unfortunately delays completion of a network attach procedures. Moreover, the inventors have now identified that in some particular combinations of cellular terminal equipment, network configuration and encryption authentication protocols, a cellular terminal might engage into a perpetually failing loop so that its user could not establish telecommunications connectivity at all.

SUMMARY

[0008] Various aspects of examples of the invention are set out in the claims.

[0009] According to a first example aspect of the present invention, there is provided a method in a cellular terminal comprising:

[0010] detecting any capability reporting trigger and responsively to such determination:

[0011] producing a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

[0012] transmitting the cellular network authentication capabilities message to the cellular network.

[0013] It may be a capability reporting trigger that the cellular terminal is about to send one or more of: an attach request message; a tracking area update request; and a routing area update request.

[0014] The method may comprise receiving from the cellular network a capability request message for authentication capabilities. The receiving of the capability request message may form a capability reporting trigger.

[0015] The cellular terminal may comprise a security entity. The security entity may comprise a secure element. The security entity may comprise a subscriber identity module application. The cellular terminal may comprise user equipment. The user equipment may be configured to perform communications over radio interface with a base station. The security entity may be configured to computation of authentication key management for cellular authentication.

[0016] The user equipment may be selected from a group consisting of: a mobile terminal; a laptop computer; a vehicle; a car; a car key; a portable device; a handheld electronic device; and a single or multifunction device with cellular radio capability. The secure element may be removable or embedded or integrated in an existing processor architecture (e.g. baseband circuitry, main processor, central processing unit, and / or master control unit).

[0017] The security entity may be configured to form content for the capabilities message. The security entity may be configured to receive a request for the content for the capabilities message and to responsively produce the content for the capabilities message. The security entity may be configured to receive an authentication request and to respectively produce the content for the capabilities message.

[0018] The cellular terminal may comprise a processor configured to control operations of the cellular terminal.

[0019] The security entity may be a software-based entity. The security entity may comprise a processor that is configured to operate independently from the processor of the cellular terminal. The security entity may be contained in an integrated circuit. The security entity may be contained in an universal integrated circuit card, UICC or SoC (system on chip), TPM (trusted platform module), TCM (trusted computing module), trusted element or a virtual secure element as part of the baseband chip. The security entity may be contained in an embedded universal integrated circuit card, eUICC.

[0020] The processor of the cellular terminal may be configured to perform authentication related communications in a non-access stratum, NAS, layer.

[0021] The cellular terminal may be configured to receive an update command and to responsively update the security entity. The cellular terminal may be configured to update the security entity to support an earlier unsupported cellular authentication algorithm.

[0022] The capabilities message may be contained within another cellular network authentication message that is produced by the cellular terminal for the cellular network. The capabilities message may be conveyed using a set of bits of an authentication management field, AMF, in an authentication token, AUTN.

[0023] The capabilities message may be contained within an authentication failure message.

[0024] The capabilities message may be contained within an authentication response message.

[0025] The cellular terminal may be configured to support any one or more of a plurality of cryptographic algorithms for the cellular authentication.

[0026] The cryptographic algorithms may be selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK. The TUAK may refer to an algorithm set that complies with 3GPP TS 35.231 v. 12.0.1. The TUAK may be configured to employ AES cryptography. The TUAK may be based on Keccak permutation.

[0027] The authentication capabilities message may comprise an indication for whether the cellular terminal supports any one or more of: MILENAGE; 128 bit TUAK; and 256 bit TUAK.

[0028] According to a second example aspect of the present invention, there is provided a method in a cellular network comprising:

[0029] receiving cellular network authentication capabilities message from a cellular terminal;

[0030] selecting a cellular authentication algorithm based on capabilities indicated by the network authentication capabilities message; and

[0031] performing cellular authentication with the cellular terminal using the selected cellular authentication algorithm.

[0032] The method may comprise maintaining a subscriber database. The subscriber database may be updated based on the network authentication message. The subscriber database may be a home location register.

[0033] The cellular network may be configured to receive the network authentication capabilities message from a non-access stratum, NAS, layer.

[0034] The cellular network may be configured to detect if the cellular terminal's cryptographic capabilities should be updated. The cellular network may be configured to detect that the cellular terminal's cryptographic capabilities should be updated if the cellular terminal is not capable of operating using a cryptographic algorithm that it should support and for which there is an update that is compatible with the cellular terminal. The cellular network may be configured to send to the cellular terminal an update command to cause updating of the security entity. The cellular network may be configured to update the subscriber database on updating of the cryptographic capabilities of the cellular terminal.

[0035] The capabilities message may be contained within another cellular network authentication message that is produced by the cellular terminal for the cellular network. The capabilities message may be conveyed using a set of bits of an authentication management field, AMF, in an authentication token, AUTN.

[0036] The authentication token may comprise 128 bits, 192 bits, 256 bits or 320 bits. The authentication token may consist of 128 bits, 192 bits, 256 bits or 320 bits. In case that the authentication token is more than 256 bits, excess bits may be discarded.

[0037] The authentication token may comprise a sequence number, SQN. The sequence number may consist of 48 bits.

[0038] The authentication token may comprise an anonymity key, AK. The anonymity key may consist of 48 bits.

[0039] The authentication token may comprise an authentication management field, AMF. The authentication management field may consist of 16 bits. The authentication management field may comprise 7 spare bits. The spare bits may be used to indicate cryptography adaptation information. The cryptography adaptation information may comprise lengths of different cryptography parameters.

[0040] The authentication token may comprise a challenge, RAND. The challenge may consist of 128 bits.

[0041] The cellular authentication may employ a cipher key, CK. The cipher

key may consist of 64 bits, 128 bits or 256 bits.

[0042] The cellular authentication may employ an integrity key, IK. The integrity key may consist of 64 bits, 128 bits or 256 bits.

[0043] The cellular authentication may employ a response parameter, RES. The response parameter may consist of 32 bits, 64 bits, 128 bits or 256 bits.

[0044] The capabilities message may be contained within an authentication failure message.

[0045] The capabilities message may be contained within an authentication response message.

[0046] The cellular network may be configured to support any one or more of a plurality of cryptographic algorithms for the cellular authentication.

[0047] The cryptographic algorithms may be selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK. The TUAK may refer to an algorithm set that complies with 3GPP TS 35.231 v. 12.0.1. The TUAK may be configured to employ AES cryptography. The TUAK may be based on Keccak permutation.

[0048] The authentication capabilities message may comprise an indication for whether the cellular terminal supports any one or more of: MILENAGE; 128 bit TUAK; and 256 bit TUAK.

[0049] According to a third example aspect of the present invention, there is provided an apparatus comprising means for performing the method of the first or second example aspect.

[0050] According to a fourth example aspect there is provided an apparatus comprising a processor configured to perform the method of the first or second example aspect.

[0051] According to a fifth example aspect there is provided an apparatus comprising at least one processor and at least one memory including computer program code; the at least one memory and the computer program code configured to, with the at least one processor, cause the apparatus to perform at least the method of the first or second example aspect.

[0052] According to a sixth example aspect there is provided a computer program comprising code for performing the method of the first or second example aspect.

[0053] According to a seventh example aspect there is provided a computer readable memory medium comprising the computer program of the sixth example aspect.

[0054] Any foregoing memory medium may comprise a digital data storage such as a data disc or diskette, optical storage, magnetic storage, holographic storage, opto-magnetic storage, phase-change memory, resistive random access memory, magnetic random access memory, solid-electrolyte memory, ferroelectric random access memory, organic memory or polymer memory. The memory medium may be formed into a device without other substantial functions than storing memory or it may be formed as part of a device with other functions, including but not limited to a memory of a computer, a chip set, and a sub assembly of an electronic device.

[0055] Different non-binding example aspects and embodiments of the present invention have been illustrated in the foregoing. The embodiments in the foregoing are used merely to explain selected aspects or steps that may be utilized in implementations of the present invention. Some embodiments may be presented only with reference to certain example aspects of the invention. It should be appreciated that corresponding embodiments may apply to other example aspects as well.

BRIEF DESCRIPTION OF THE DRAWINGS

[0056] For a more complete understanding of example embodiments of the present invention, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0057] Fig. 1 shows an architectural drawing of a system of an example embodiment;

[0058] Fig. 2 shows a flow chart of a process of an example embodiment;

[0059] Fig. 3 shows a flow chart of a process according to an example embodiment of the invention;

[0060] Fig. 4 shows a block diagram of an apparatus of an example embodiment; and

[0061] Fig. 5 shows a block diagram of an apparatus of an example embodiment.

DETAILED DESCRIPTON OF THE DRAWINGS

[0062] An example embodiment of the present invention and its potential advantages are understood by referring to Figs. 1 through 4 of the drawings. In this document, like reference signs denote like parts or steps.

[0063] Fig. 1 an architectural drawing of a system of an example embodiment. A cellular terminal 100 is drawn with user equipment 110 and a security entity such as a secure element. The security entity may contain a USIM 120. In an example embodiment, the USIM is an application on a software implemented security element. In an example embodiment, the security entity is a software-based entity. In an example embodiment, the security entity comprises a processor that is configured to operate independently from the processor of the cellular terminal. In an example embodiment, the security entity is contained in an integrated circuit. In an example embodiment, the security entity is contained in an universal integrated circuit card, UICC or system on chip (SoC), trusted platform module (TPM), trusted computing module (TCM), trusted element or a virtual secure element as part of the baseband chip or main processor. In an example embodiment, the security entity is contained in an embedded universal integrated circuit card (eUICC).

[0064] The system further comprises a cellular telecommunication network 200 that comprises an E-UTRAN or eNB 210, a mobility management entity MME 220, a home subscriber server, HSS 230 (e.g. home location register HLR, authentication center AuC), a serving gateway 240, a serving gateway support node, SGSN 250, a Universal Terrestrial Radio Access Network, UTRAN 260 and a GSM EDGE Radio Access Network, GERAN 270.

[0065] Fig. 2 shows a flow chart of a process of an example embodiment. In step 21, the cellular terminal sends a non-access stratum (NAS) attach request or network registration request to the MME 220 via the eNB 210. The MME 220 requests 22 authentication data (e.g. an authentication quintet) from the HSS 230 and responsively receives 23 an authentication data response with the requested authentication data. The MME 220 then sends 24 an NAS authentication request to the terminal 100 that replies 25 with an NAS authentication response if the terminal 100 is capable of decoding the NAS authentication request and to produce the NAS authentication response. To this end, the terminal 100 has to support the authentication algorithm used by the MME and possess a shared secret that is

known by the HSS 230 and the terminal 100. If the terminal 100 fails to decode the NAS authentication request, the terminal 100 replies 25' with a NAS authentication failure.

[0066] After successful decoding of the NAS authentication request and the responsive NAS authentication response, the MME sends 26 to the terminal 100 a NAS security mode completion message and the terminal 100 replies 27 with a corresponding NAS security mode complete message. In another example embodiment, either or both the NAS security mode completion and NAS security mode complete reply is / are omitted or substituted by one or more other signals or messages.

[0067] The various messages of Fig. 2 and their processing can be implemented in a large variety of different ways.

[0068] In an example embodiment, the process of Fig. 2 starts from another request that requires authentication procedure triggering such as a tracking area update request or a routing area request to the cellular network 200 instead of the network registration request.

[0069] In an example embodiment, the authentication request message 24 comprises an indication of a selected cryptographic algorithm from a group of a plurality of cryptographic algorithms. In an example embodiment, the cryptographic algorithms are selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK. The TUAK may refer to an algorithm set that complies with 3GPP TS 35.231 v. 12.0.1. The TUAK may be configured to employ AES cryptography. The TUAK may be based on Keccak permutation.

[0070] Fig. 3 shows a flow chart of a process according to an example embodiment of the invention. The process comprises:

[0071] detecting 310 any capability reporting trigger and responsively to such determination:

[0072] producing 320 a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

[0073] transmitting 330 the cellular network authentication capabilities message to the cellular network.

[0074] In an example embodiment, it is a capability reporting trigger that the cellular terminal is about to send one or more of: an attach request message; a tracking area update request; and a routing area update request.

[0075] In an example embodiment, the process comprises receiving from the cellular network a capability request message for authentication capabilities. The receiving of the capability request message may form a capability reporting trigger.

[0076] In an example embodiment, the security entity is configured to form content for the capabilities message. In an example embodiment, the security entity is configured to receive a request for the content for the capabilities message and to responsively produce the content for the capabilities message. In an example embodiment, the security entity is configured to receive an authentication request and to respectively produce the content for the capabilities message.

[0077] In an example embodiment, the processor of the cellular terminal is configured to perform authentication related communications in a non-access stratum, NAS, layer.

[0078] In an example embodiment, the cellular terminal is configured to receive an update command and to responsively update the security entity. In an example embodiment, the cellular terminal is configured to update the security entity to support an earlier unsupported cellular authentication algorithm.

[0079] In an example embodiment, the capabilities message is contained within another cellular network authentication message that is produced by the cellular terminal for the cellular network. In an example embodiment, the capabilities message is conveyed using a set of bits of an authentication management field, AMF, in an authentication token, AUTN.

[0080] In an example embodiment, the capabilities message is contained within an authentication failure message.

[0081] In an example embodiment, the capabilities message is contained within an authentication response message.

[0082] In an example embodiment, the selected cryptographic algorithm employs a cipher key, CK. The cipher key may consist of 64 bits, 128 bits or 256 bits.

[0083] In an example embodiment, the selected cryptographic algorithm employs an integrity key, IK. The integrity key may consist of 64 bits, 128 bits or 256 bits.

[0084] In an example embodiment, the selected cryptographic algorithm employs a response parameter, RES. The response parameter may consist of 32 bits, 64 bits, 128 bits or 256 bits.

[0085] In an example embodiment, the authentication request message 24 is an extended authentication request message. In an example embodiment, the extended authentication request comprises a message type indication that is configured to cause legacy terminals to neglect the extended authentication request message.

[0086] In an example embodiment, the extended authentication request comprises a field configured to accommodate a 256 bit authentication token, AUTN.

[0087] In an example embodiment, the authentication request message 24 is an updated authentication request. In an example embodiment, the updated authentication request comprises an identifier for indicating which cryptographic algorithm is being used for the authentication. In an example embodiment, the identifier is a new field in addition to those in the normal authentication request. In an example embodiment, the normal authentication request complies with 3GPP TS 24.301 or 3GPP TS 24.008. In an example embodiment, the identifier is contained in one or more bits of the authentication management field, AMF.

[0088] In an example embodiment, the authentication request message 24 comprises a protocol discriminator. In an example embodiment, the authentication request message comprises a security header type. In an example embodiment, the authentication request message comprises a non-access stratum key set identifier. In an example embodiment, the authentication request message comprises a spare half octet. In an example embodiment, the authentication request message comprises a challenge, RAND (e.g. evolved packet system, EPS, challenge). In an example embodiment, the authentication request message comprises an authentication token, AUTN. In an example embodiment, the authentication token comprises an authentication management field, AMF. The authentication management field may comprise a parameter indicating the bit-length of TUAK to be used.

[0089] In an example embodiment, the message type of the updated authentication request matches with that of the normal authentication request message. In an example embodiment, the updated authentication request comprises a 256 bit authentication token field. The updated authentication request may

comprise a 256 bit authentication token field only if a 256 bit authentication token is being used. Otherwise, the updated authentication request may comprise a 128 bit authentication token field.

[0090] In an example embodiment, the authentication token comprises 128 bits, 192 bits, 256 bits or 320 bits. In an example embodiment, the authentication token consists of 128 bits, 192 bits, 256 bits or 320 bits. In case that the authentication token is more than 256 bits, excess bits may be discarded.

[0091] In an example embodiment, the authentication token comprises a sequence number, SQN. In an example embodiment, the sequence number consists of 48 bits.

[0092] In an example embodiment, the authentication token comprises an anonymity key, AK. In an example embodiment, the anonymity key consists of 48 bits.

[0093] In an example embodiment, the authentication token comprises an authentication management field, AMF. In an example embodiment, the authentication management field consists of 16 bits. In an example embodiment, the authentication management field comprises 7 spare bits. In an example embodiment, the spare bits are used to indicate cryptography adaptation information. In an example embodiment, the cryptography adaptation information comprises lengths of different cryptography parameters.

[0094] In an example embodiment, the authentication token comprises a challenge, RAND. In an example embodiment, the challenge consists of 128 bits.

[0095] In an example embodiment, the decoding the authentication request message 24 to a decoded authentication request is performed according to the selected cryptographic algorithm and based on a shared secret known by the cellular terminal and a network operator of the cellular terminal.

[0096] In an example embodiment, the process comprises, based on the decoded authentication request, the shared secret and the selected cryptographic algorithm, producing and encrypting the authentication response message 25.

[0097] In an example embodiment, the authentication response message 25 comprises a message type indication. In an example embodiment, the message type indication identifies the authentication response message as an extended authentication response message. In an example embodiment, the message type indication matches with that of a normal authentication response message. In an

example embodiment, the message type indication of the normal authentication response message complies with 3GPP TS 24.301.

[0098] In an example embodiment, the extended authentication response message comprises a variable length authentication response parameter, RES. In an example embodiment, the authentication response parameter has a length selected from a group consisting of any one or more of: 32 bits, 64 bits, 128 bits or 256 bits.

[0099] In an example embodiment, the authentication response message 25 is provided with a new information element in comparison the normal authentication response message. In an example embodiment, the new information element is configured to accommodate a 128 bit or a 256 bit authentication response parameter.

[00100] In an example embodiment, the authentication response message 25 comprises an extended authentication response parameter field that is configured to accommodate a 128 bit or a 256 bit authentication response parameter.

[00101] In an example embodiment, the authentication response message 25 comprises a cryptography algorithm indication.

[00102] Fig. 4 shows an example block diagram of an apparatus 400 according to an example embodiment. The apparatus 400 comprises a memory 420 that comprises a volatile memory 430 and a non-volatile memory 440 that is configured to store computer programs or software comprising computer program code 450. The apparatus 400 further comprises at least one processor 410 for controlling the operation of the apparatus 400 using the computer program code 450 and an input/output system 460 for communicating with other entities or apparatuses. Accordingly, the input/output system 460 comprises one or more communication units or modules providing communication interfaces towards other entities and/or apparatuses. In an example embodiment, the processor 410 is configured to run the program code 450 in the volatile memory 430. In an example embodiment, the apparatus 400 is configured to operate as the MME 220.

[00103] The processor 410 comprises, for example, any one or more of: a master control unit (MCU); a microprocessor; a digital signal processor (DSP); an application specific integrated circuit (ASIC); a field programmable gate array; and a microcontroller.

[00104] Fig. 5 shows an example block diagram of an apparatus 500

according to an example embodiment. The apparatus 500 comprises a memory 520 that comprises a volatile memory 530 and a non-volatile memory 540 that is configured to store computer programs or software comprising computer program code 550. The apparatus 500 further comprises at least one processor 510 for controlling the operation of the apparatus 500 using the computer program code 550. The apparatus 500 further comprises an input/output system 560 for communicating with other entities or apparatuses. Accordingly, the input/output system 560 comprises one or more communication units or modules providing communication interfaces towards other entities and/or apparatuses. The apparatus 500 further comprises a secure element (SE) 570 secure element that contains one or more network access applications such as SIM(s) or USIM(s). In an example embodiment, the SE 570 is an application that is hosted by a secure element which is implemented as software. In another example embodiment, the secure element 570 comprises a universal integrated circuit card, UICC. In an example embodiment, the processor 510 is configured to run the program code 550 in the volatile memory 530. In an example embodiment, the apparatus 500 is configured to operate as the cellular terminal 100.

[00105] The processor 510 comprises, for example, any one or more of: a master control unit (MCU); a microprocessor; a digital signal processor (DSP); an application specific integrated circuit (ASIC); a field programmable gate array; and a microcontroller.

[00106] Without in any way limiting the scope, interpretation, or application of the claims appearing below, a technical effect of one or more of the example embodiments disclosed herein is that cellular networks may be allowed to develop by their authentication features to a greater extent using existing equipment or in other words, that the life span of existing equipment may be increased and / or the security of cellular networks may be enhanced. Another technical effect of one or more of the example embodiments disclosed herein is that reliability issues may be avoided or mitigated with relation to cellular authentication procedures. Another technical effect of one or more of the example embodiments disclosed herein is that the capability information may be transferred with little changes in the existing cellular networks. For example, the AUTN may consist of SQN, AK, AMF and MAC. The sequence number SQN (separate instance) may be stored in the HLR/HSS for all subscribers. In such a case, adding bits to SQN might have large or even critical

impacts to the HLR/HSS. AMF field, on the contrary, may be better suited a field for carrying authentication capability information. AMF may also be better suited for this function than the AK field or the MAC field the change of which might cause severe and / or wide impact on operator network as a whole.

[00107] Embodiments of the present invention may be implemented in software, hardware, application logic or a combination of software, hardware and application logic. In an example embodiment, the application logic, software or an instruction set is maintained on any one of various conventional computer-readable media. In the context of this document, a “computer-readable medium” may be any non-transitory media or means that can contain, store, communicate, propagate or transport the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer, with one example of a computer described and depicted in Fig. 4 or 5. A computer-readable medium may comprise a computer-readable storage medium that may be any media or means that can contain or store the instructions for use by or in connection with an instruction execution system, apparatus, or device, such as a computer.

[00108] If desired, the different functions discussed herein may be performed in a different order and/or concurrently with each other. Furthermore, if desired, one or more of the before-described functions may be optional or may be combined.

[00109] Although various aspects of the invention are set out in the independent claims, other aspects of the invention comprise other combinations of features from the described embodiments and/or the dependent claims with the features of the independent claims, and not solely the combinations explicitly set out in the claims.

[00110] It is also noted herein that while the foregoing describes example embodiments of the invention, these descriptions should not be viewed in a limiting sense. Rather, there are several variations and modifications which may be made without departing from the scope of the present invention as defined in the appended claims.

WHAT IS CLAIMED IS

1. A method in a cellular terminal comprising:

detecting any capability reporting trigger and responsively to such determination:

producing a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

transmitting the cellular network authentication capabilities message to the cellular network.

2. The method of claim 1, wherein it is a capability reporting trigger that the cellular terminal is about to send one or more of: an attach request message; a tracking area update request; and a routing area update request.

3. The method of claim 1 or 2, comprising receiving from the cellular network a capability request message for authentication capabilities.

4. The method of any of preceding claims, wherein the receiving of the capability request message forms a capability reporting trigger.

5. The method of any of preceding claims, wherein the cellular terminal comprises a security entity.

6. The method of claim 5, wherein the security entity comprises a secure element.

7. The method of claim 6, wherein the secure element is removable or embedded or integrated in an existing processor architecture.

8. The method of any of claims 5 to 7, wherein the security entity comprises a subscriber identity module application.

9. The method of any of claims 5 to 8, wherein the cellular terminal comprises user equipment.

10. The method of claim 9, wherein the user equipment is configured to perform communications over radio interface with a base station.

11. The method of claim 9 or 10, wherein the user equipment is selected from a group consisting of: a mobile terminal; a laptop computer; a vehicle; a car; a car key; a portable device; a handheld electronic device; and a single or multifunction device with cellular radio capability.

12. The method of any of claims 5 to 11, wherein the security entity is configured to computation of authentication key management for cellular authentication.

13. The method of any of claims 5 to 12, wherein the security entity is configured to form content for the capabilities message.

14. The method of claim 13, wherein the security entity is configured to receive a request for the content for the capabilities message and to responsively produce the content for the capabilities message.

15. The method of claim 13 or 14, wherein the security entity is configured to receive an authentication request and to respectively produce the content for the capabilities message.

16. The method of any of claims 5 to 15, wherein the security entity is a software-based entity.

17. The method of any of claims 5 to 16, wherein the security entity comprises a processor that is configured to operate independently from the processor of the cellular terminal.

18. The method of any of claims 5 to 17, wherein the security entity is contained in an integrated circuit.

19. ;The method of any of claims 5 to 18, wherein the security entity is contained in an embedded universal integrated circuit card; a universal integrated circuit card;

system on chip; trusted platform module; trusted computing module; trusted element; or a virtual secure element as part of the baseband chip.

20. The method of any of preceding claims, wherein the cellular terminal comprises a processor configured to control operations of the cellular terminal.

21. The method of claim 20, wherein the processor of the cellular terminal is configured to perform authentication related communications in a non-access stratum layer.

22. The method of any of claims 5 to 21, wherein the cellular terminal is configured to receive an update command and to responsively update the security entity.

23. The method of claim 22, wherein the cellular terminal is configured to update the security entity to support an earlier unsupported cellular authentication algorithm.

24. The method of any of preceding claims, wherein the capabilities message is contained within another cellular network authentication message that is produced by the cellular terminal for the cellular network.

25. The method of any of preceding claims, wherein the capabilities message is conveyed using a set of bits of an authentication management field in an authentication token.

26. The method of any of preceding claims, wherein the capabilities message is contained within an authentication failure message.

27. The method of any of preceding claims, wherein the capabilities message is contained within an authentication response message.

28. The method of any of preceding claims, wherein the cellular terminal is configured to support any one or more of a plurality of cryptographic algorithms for the cellular authentication.

29. The method of any of preceding claims, wherein the cryptographic algorithms is selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK.

30. The method of any of preceding claims, wherein the authentication capabilities message comprises an indication for whether the cellular terminal supports any one or more of: MILENAGE; 128 bit TUAK; and 256 bit TUAK.

31. A method in a cellular network comprising:

receiving cellular network authentication capabilities message from a cellular terminal;

selecting a cellular authentication algorithm based on capabilities indicated by the network authentication capabilities message; and

performing cellular authentication with the cellular terminal using the selected cellular authentication algorithm.

32. The method of claim 31, comprising maintaining a subscriber database.

33. The method of claim 31 or 32, wherein the subscriber database is updated based on the network authentication message.

34. The method of any of claims 31 to 33, wherein the subscriber database is a home location register.

35. The method of any of claims 31 to 34, wherein the cellular network is configured to receive the network authentication capabilities message from a non-access stratum layer.

36. The method of any of claims 31 to 35, wherein the cellular network is configured to detect if the cellular terminal's cryptographic capabilities should be updated.

37. The method of any of claims 31 to 36, wherein the cellular network is configured to detect that the cellular terminal's cryptographic capabilities should be updated if the cellular terminal is not capable of operating using a cryptographic

algorithm that it should support and for which there is an update that is compatible with the cellular terminal.

38. The method of any of claims 31 to 37, wherein the cellular network is configured to send to the cellular terminal an update command to cause updating of the security entity.

39. The method of any of claims 31 to 38, wherein the cellular network is configured to update the subscriber database on updating of the cryptographic capabilities of the cellular terminal.

40. The method of any of claims 31 to 39, wherein the capabilities message is contained within another cellular network authentication message that is produced by the cellular terminal for the cellular network.

41. The method of any of claims 31 to 40, wherein the capabilities message is conveyed using a set of bits of an authentication management field in an authentication token.

42. The method of claim 41, wherein the authentication token comprises 128 bits, 192 bits, 256 bits or 320 bits.

43. The method of any of claims 41 to 42, wherein the authentication token consists of 128 bits, 192 bits, 256 bits or 320 bits.

44. The method of claim 43, wherein in the case that the authentication token is more than 256 bits, excess bits are discarded.

45. The method of any of claims 41 to 44, wherein the authentication token comprises a sequence number.

46. The method of claim 45, wherein the sequence number consists of 48 bits.

47. The method of any of claims 41 to 46, wherein the authentication token comprises an anonymity key.

48. The method of claim 47, wherein the anonymity key consists of 48 bits.

49. The method of any of claims 41 to 48, wherein the authentication token comprises an authentication management field.

50. The method of claim 49, wherein the authentication management field consists of 16 bits.

51. The method of claim 49 or 50, wherein the authentication management field comprises 7 spare bits.

52. The method of claim 51, wherein the spare bits are used to indicate cryptography adaptation information.

53. The method of claim 52, wherein the cryptography adaptation information comprises lengths of different cryptography parameters.

54. The method of any of claims 41 to 53, wherein the authentication token comprises a challenge.

55. The method of any of claims 41 to 54, wherein the challenge consists of 128 bits.

56. The method of any of claims 31 to 55, wherein the cellular authentication employs a cipher key.

57. The method of claim 56, wherein the cipher key consists of 64 bits, 128 bits or 256 bits.

58. The method of any of claims 31 to 57, wherein the cellular authentication employs an integrity key, IK.

59. The method of claim 58, wherein the integrity key consists of 64 bits, 128 bits or 256 bits.

60. The method of any of claims 31 to 59, wherein the cellular authentication employs a response parameter.

61. The method of claim 60, wherein the response parameter consists of 32 bits, 64 bits, 128 bits or 256 bits.

62. The method of any of claims 31 to 61, wherein the capabilities message is contained within an authentication failure message.

63. The method of any of claims 31 to 62, wherein the capabilities message is contained within an authentication response message.

64. The method of any of claims 31 to 63, wherein the cellular network is configured to support any one or more of a plurality of cryptographic algorithms for the cellular authentication.

65. The method of claim 64, wherein the cryptographic algorithms are selected from a group consisting of MILENAGE; 128 bit TUAK; and 256 bit TUAK.

66. The method of any of claims 31 to 65, wherein the authentication capabilities message comprises an indication for whether the cellular terminal supports any one or more of: MILENAGE; 128 bit TUAK; and 256 bit TUAK.

67. A process comprising the method of any of claims 1 to 30 and the method of any of claims 31 to 66.

68. An apparatus comprising:

means for detecting any capability reporting trigger and responsively to such determination:

producing a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

transmitting the cellular network authentication capabilities message to the cellular network.

69. The apparatus of claim 68, comprising means for performing the method of any of claims 2 to 30.

70. An apparatus, comprising:

a processor configured to:

detect any capability reporting trigger and responsively to such determination:

produce a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

transmit the cellular network authentication capabilities message to the cellular network.

71. The apparatus of claim 70, further comprising a memory that contains executable instructions that if executed by the processor cause the apparatus to perform the method of any of claims 1 to 30.

72. An apparatus, comprising:

at least one processor; and

at least one memory including computer program code

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

detecting any capability reporting trigger and responsively to such determination:

producing a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

transmitting the cellular network authentication capabilities message to the cellular network.

73. The apparatus of claim 72, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus to perform the method of any of claims 2 to 30.

74. A computer program, comprising:

code for detecting any capability reporting trigger and responsively to such determination:

producing a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

transmitting the cellular network authentication capabilities message to the cellular network;

when the computer program is run on a processor.

75. The computer program of claim 74, further comprising code for causing performing of the method of any of claims 2 to 30.

76. A computer readable non-transitory memory medium comprising the computer program of claim 74 .

77. An apparatus comprising:

means for detecting any capability reporting trigger and responsively to such determination:

producing a cellular network authentication capabilities message indicative of cellular network authentication capabilities available for the terminal; and

transmitting the cellular network authentication capabilities message to the cellular network.

78. The apparatus of claim 68, comprising means for performing the method of any of claims 2 to 30.

79. An apparatus, comprising:

a processor configured to:

receive cellular network authentication capabilities message from a cellular terminal;

select a cellular authentication algorithm based on capabilities indicated by the network authentication capabilities message; and

perform cellular authentication with the cellular terminal using the selected cellular authentication algorithm.

80. The apparatus of claim 79, further comprising a memory that contains executable instructions that if executed by the processor cause the apparatus to perform the method of any of claims 31 to 66.

81. An apparatus, comprising:

at least one processor; and

at least one memory including computer program code

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

receiving cellular network authentication capabilities message from a cellular terminal;

selecting a cellular authentication algorithm based on capabilities indicated by the network authentication capabilities message; and

performing cellular authentication with the cellular terminal using the selected cellular authentication algorithm.

82. The apparatus of claim 81, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the apparatus to perform the method of any of claims 32 to 66.

83. A system comprising the apparatus of any of claims 68 to 73 and the apparatus of any of claims 77 to 82.

84. A computer program, comprising:

code for receiving cellular network authentication capabilities message from a cellular terminal;

code for selecting a cellular authentication algorithm based on capabilities indicated by the network authentication capabilities message; and

code for performing cellular authentication with the cellular terminal using the selected cellular authentication algorithm;

when the computer program is run on a processor.

85. The computer program of claim 84, further comprising code for causing performing of the method of any of claims 32 to 66.

86. A computer readable non-transitory memory medium comprising the computer program of claim 85.

Fig. 1

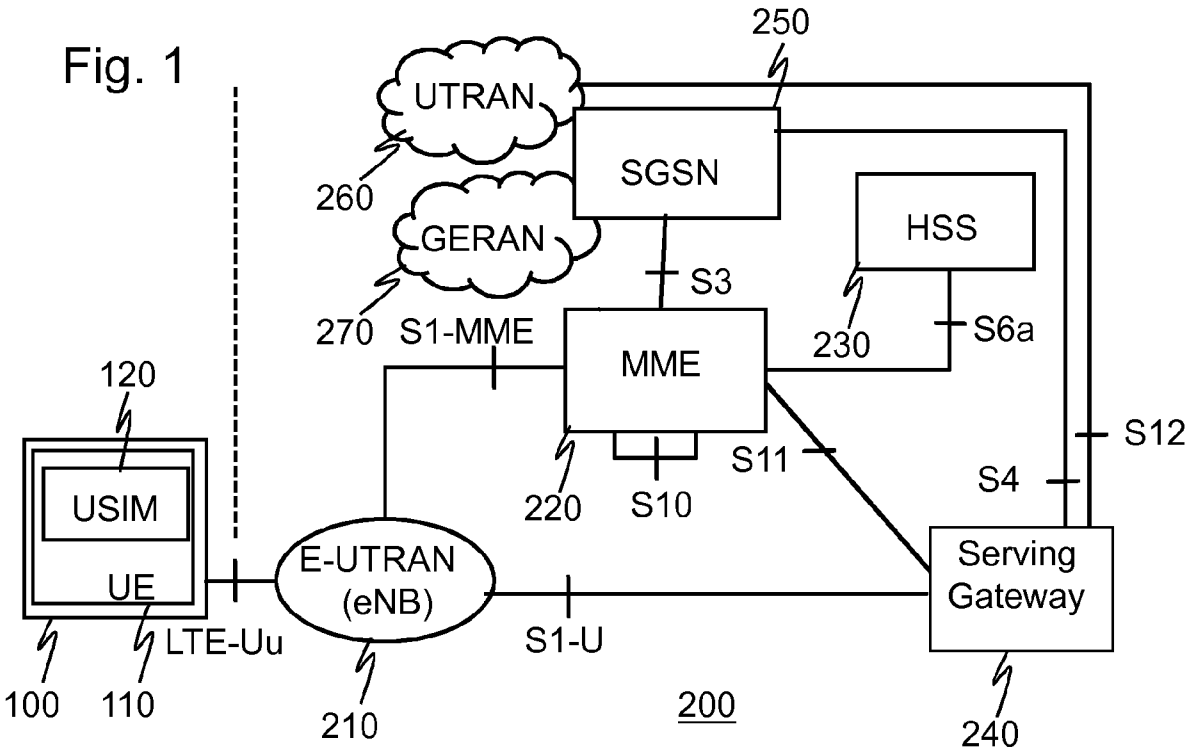


Fig. 2

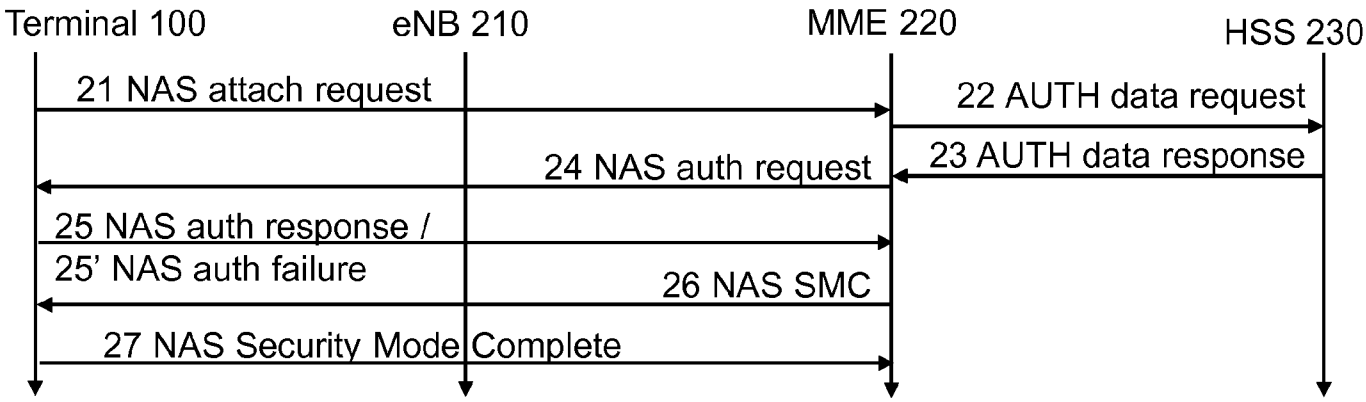
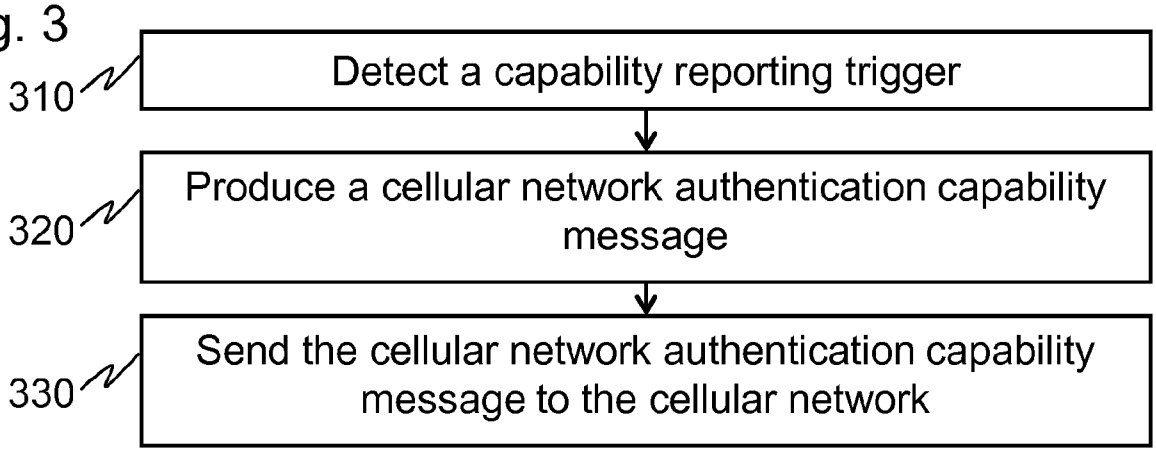
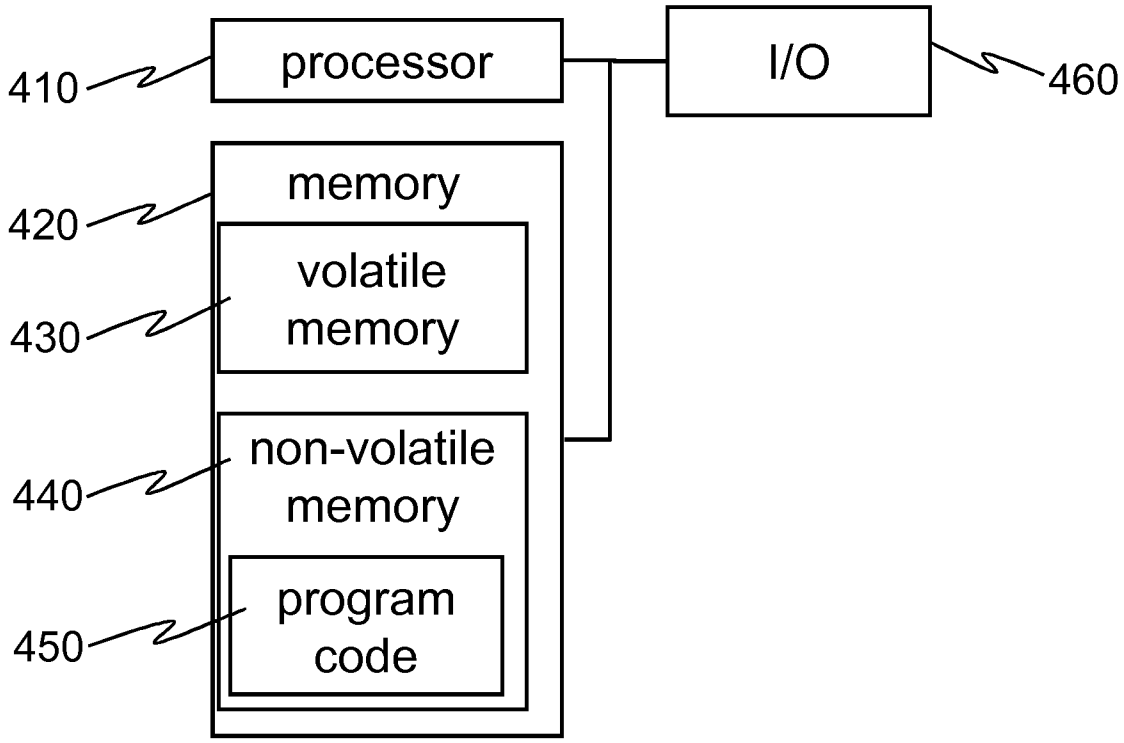


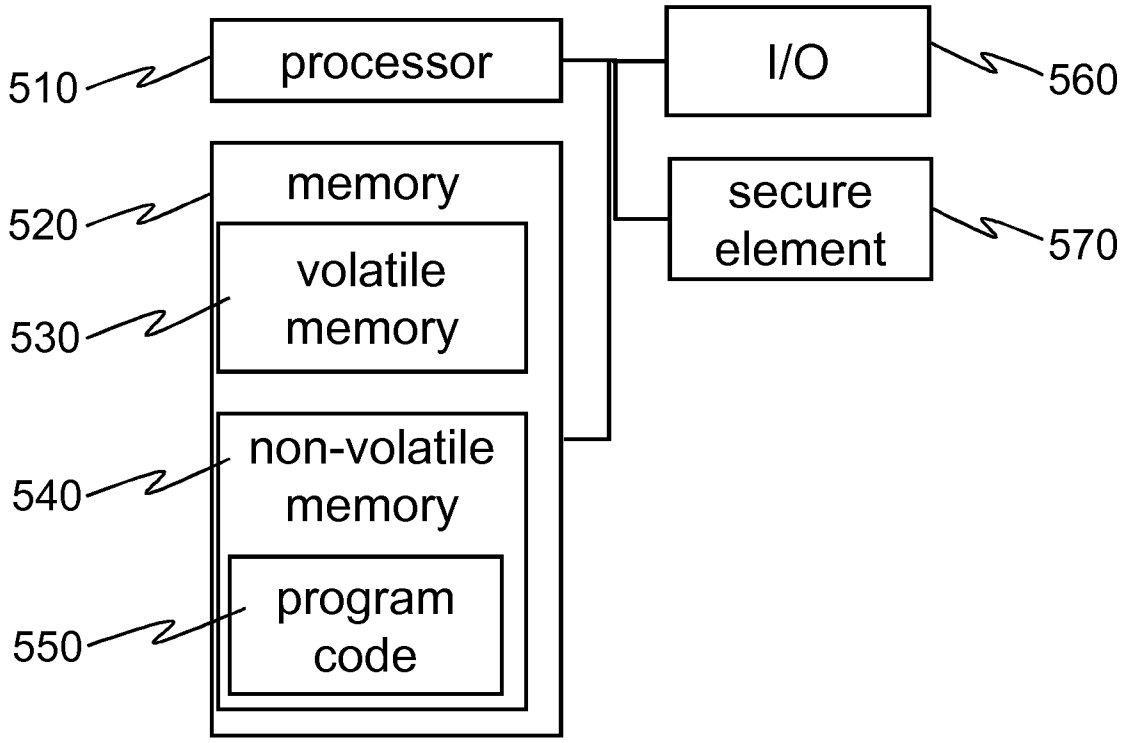
Fig. 3



400 Fig. 4



500 Fig. 5



INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2014/050383

A. **CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

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: H04W, H04L, G06F

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

FI, SE, NO, DK

Electronic data base consulted during the international search (name of data base, and, where practicable, search terms used)

EPO-Internal, WPI, XP3GPP, XPAIP, XPESP, XPESP2, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPOAC, XPRD, XPTK, COMPDX, INSPEC, NPL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010027314 A1 (ERICSSON TELEFON AB L M [SE]) 11 March 2010 (11.03.2010) Figs. 4-5B, 6-11; paragraphs [0001], [0006], [0008], [0020]-[0029], [0040]-[0048], [0064], [0067], [0070]-[0072], [0075]-[0090], [0095]-[0096]	1-36, 38-86
A	EP 2139175 A1 (HUAWEI TECH CO LTD [CN]) 30 December 2009 (30.12.2009) Figs. 1-4; paragraphs [0003], [0013], [0023], [0027], [0048], [0056], [0072], [0087]	1-86
A	US 2008141031 A1 (OBA YOSHIHIRO [US] et al.) 12 June 2008 (12.06.2008) Figs. 1-3C; paragraphs [0083]-[0090], [0106]-[0115]	1-86

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
13 January 2015 (13.01.2015)	29 January 2015 (29.01.2015)

Name and mailing address of the ISA/FI
Finnish Patent and Registration Office
P.O. Box 1160, FI-00101 HELSINKI, Finland
Facsimile No. +358 9 6939 5328

Authorized officer
Yrjö Raivio
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2014/050383

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006026671 A1 (POTTER DARRAN [GB] et al.) 02 February 2006 (02.02.2006) Fig. 1B; paragraphs [0030]-[0035], [0045]-[0052]	3-4
A	WO 2005032201 A1 (ERICSSON TELEFON AB L M [SE]) 07 April 2005 (07.04.2005) Figs. 1-3, 7; page 4, line 1 – page 5, line 30; page 7, line 25 – page 13, line 2; page 16, lines 1 – 15; page 22, line 13 – page 26, line 21	36, 38-39, 44
A	3GPP TS 33.102 v. 12.0.0 (2014-03), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 12), March 2014 [online], [retrieved on 2014-12-09]. Retrieved from the Internet: <URL: http://www.3gpp.org/DynaReport/33.102.htm>. section 6.3; Annex F	24-30, 40-43, 62-66
A	3GPP TS 35.231 v. 12.0.1 (2013-12), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the TUAK Algorithm Set: A Second Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm Specification (Release 12), December 2013 [online], [retrieved on 2014-12-01]. Retrieved from the Internet: <URL: http://www.3gpp.org/DynaReport/35231.htm>. Cited in the application. The whole document, in particular section 5.1.	45-61

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2014/050383

CLASSIFICATION OF SUBJECT MATTER

IPC
H04W 12/06 (2009.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2014/050383

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
WO 2010027314 A1	11/03/2010	CA 2736172 A1	11/03/2010
		EP 2340656 A1	06/07/2011
		JP 2012502548 A	26/01/2012
		JP 2014112969 A	19/06/2014
		NZ 592061 A	31/01/2014
		US 2010064135 A1	11/03/2010
EP 2139175 A1	30/12/2009	EP 2139175 B1	26/12/2012
		CN 101378591 A	04/03/2009
		CN 101378591 B	27/10/2010
		EP 2549701 A1	23/01/2013
		EP 2549701 B1	26/03/2014
		ES 2401039 T3	16/04/2013
		JP 2010533390 A	21/10/2010
		JP 4976548 B2	18/07/2012
		RU 2009146555 A	20/06/2011
		RU 2435319 C2	27/11/2011
		US 2010095123 A1	15/04/2010
		US 8656169 B2	18/02/2014
		US 2014120879 A1	01/05/2014
		US 8812848 B2	19/08/2014
		US 2014295800 A1	02/10/2014
		WO 2009030155 A1	12/03/2009
US 2008141031 A1	12/06/2008	US 8583923 B2	12/11/2013
		CA 2671833 A1	19/06/2008
		CA 2671833 C	27/05/2014
		CN 101379801 A	04/03/2009
		EP 2156641 A2	24/02/2010
		EP 2156641 B1	03/04/2013
		EP 2557829 A2	13/02/2013
		JP 2010502040 A	21/01/2010
		JP 5068810 B2	07/11/2012
		JP 2012199929 A	18/10/2012
		JP 5430709 B2	05/03/2014
		KR 20080087883 A	01/10/2008
		KR 101007955 B1	14/01/2011
		WO 2008072646 A2	19/06/2008
US 2006026671 A1	02/02/2006	US 7194763 B2	20/03/2007
		CA 2575819 A1	23/02/2006
		EP 1779293 A2	02/05/2007
		US 2007118883 A1	24/05/2007

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2014/050383

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
		US 8555340 B2	08/10/2013
		WO 2006020329 A2	23/02/2006
		WO 2006020329 B1	28/12/2006
WO 2005032201 A1	07/04/2005	AT 514294 T	15/07/2011
		AT 552709 T	15/04/2012
		CN 1857024 A	01/11/2006
		CN 1857024 B	28/09/2011
		DK 1671511 T3	03/10/2011
		EP 1671511 A1	21/06/2006
		EP 1671511 B1	22/06/2011
		EP 2357858 A1	17/08/2011
		EP 2357858 B1	04/04/2012
		ES 2367692 T3	07/11/2011
		ES 2384634 T3	10/07/2012
		HK 1095689 A1	10/08/2012
		JP 2007507157 A	22/03/2007
		JP 4688808 B2	25/05/2011
		PT 2357858 E	06/07/2012
		US 2005111666 A1	26/05/2005
		US 7660417 B2	09/02/2010