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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 March 2018 (01.03.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/037149 A1

(51) International Patent Classification:
G06F 21/60 (2013.01) *H04W 76/02* (2009.01)
H04L 29/06 (2006.01) *H04W 76/04* (2009.01)
H04W 12/08 (2009.01)

(21) International Application Number:
PCT/FI2016/050574

(22) International Filing Date:
22 August 2016 (22.08.2016)

(25) Filing Language: English

(26) Publication Language: English

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

(72) Inventors: **MALKAMÄKI, Esa Mikael**; Riippakoivuntie 17 B, 02130 Espoo (FI). **HENTTONEN, Tero**; Kivenlahdenkatu 3 B 22, 02320 Espoo (FI).

(74) Agent: **SEPPO LAINE OY**; Itämerenkatu 3 A, 00180 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, 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,

(54) Title: SECURITY PROCEDURE

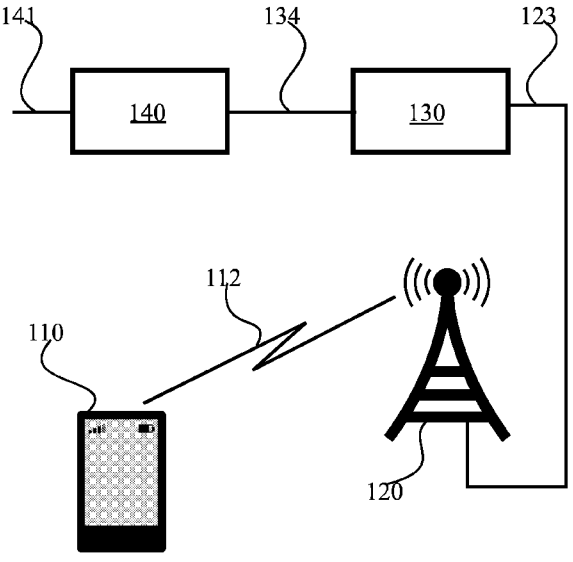

FIGURE 1

(57) Abstract: According to an example aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to establish information to be provided to a base station device, before activation of a first encryption scheme, cause transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and begin, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device

WO 2018/037149 A1

[Continued on next page]

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))*

SECURITY PROCEDURE

FIELD

[0001] The present invention relates to data encryption in a communication system.

BACKGROUND

[0002] In communication networks, which may comprise wireless and/or wired networks, user equipments may have different modes with respect to the network. For example, in cellular wireless networks, a user equipment may find itself in an idle more or a connected mode.

[0003] Idle mode is characterized by a presence of a generic rough location knowledge of the user equipment, which may be referred to as a UE context, and/or an absence of an active communication context between the user equipment and the network. The user equipment may be paged by the network, and the network may be arranged to keep track of the whereabouts of the user equipment. Similarly, the user equipment may invoke a connection establishment process to activate a communication context with the network. An idle mode user equipment may conduct cell re-selection measurements, for example.

[0004] Connected mode, on the other hand, may be characterized by more cell-level knowledge of user location and/or presence of an active communication context between the user equipment and the network. Information communicated over such an active communication context may be encrypted, or ciphered, to protect its security while in transit. An active communication context may comprise a protocol structure with a plurality of layers, such that layers are encapsulated in each other, to enable maintenance of the overall connection at different network stages. For example, a physical layer may connect a wireless terminal to a base station or access point, and convey all higher layers as payload of the physical layer. Such higher layers may comprise, for example a transport layer and an application layer conveying as payload information a user may be presented with.

[0005] In some technologies, when the user equipment, UE, connects to the network for the very first time, it is neither in idle nor in connected mode. The first connection is then used to register the UE via an initial attachment procedure to the network, so that it becomes aware of the rough location of the user equipment even when it doesn't have an active communication context present. After the initial connection, the user equipment is provided information it needs to connect to the network in subsequent connection attempts, and the network is provided information about a user identity for the subsequent connection attempts. Hence, after the initial attachment, the user equipment can operate in idle and connected mode and the network has a stored UE context.

[0006] In connection with a connection establishment procedure, the connection is established and encryption is activated. In order for encryption to work, participating entities must support the same encryption algorithms and modalities, such that data encrypted by a transmitter may be decrypted by a recipient. Decrypting is a term used when referring to reversing, or undoing, an encrypting operation. For example, an encrypting operation obtains a ciphertext from a plaintext, and decryption then obtains the original plaintext from the ciphertext.

[0007] Encryption may be activated by the network by transmitting a security command to the user equipment. An example of a security command is the SecurityModeCommand of long term evolution, LTE.

SUMMARY OF THE INVENTION

[0008] The invention is defined by the features of the independent claims. Some specific embodiments are defined in the dependent claims.

[0009] According to a first aspect of the present invention, there is provided an apparatus comprising a memory configured to store information, at least one processing core configured to receive the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme, obtain an unencrypted form of the information, and use the unencrypted form of

the information to provide service to the user equipment before or after the first encryption scheme is activated.

[0010] Various embodiments of the first aspect may comprise at least one feature from the following bulleted list:

- the apparatus is configured to process a triggering of the activation of the first encryption scheme during a connection establishment procedure
- the apparatus is configured to obtain the unencrypted form of the information via a core network
- apparatus is configured to obtain the unencrypted form of the information at least partly by requesting an unencryption key from a core network
- the first encryption scheme comprises an access stratum AS encryption scheme
- the second encryption scheme comprises a non-access stratum, NAS, encryption scheme relating to the user equipment
- the apparatus is configured to obtain the unencrypted form of the information by providing the encrypted form of the information to a mobility management entity, and by receiving the unencrypted form of the information from the mobility management entity
- the second encryption scheme comprises an encryption scheme pre-negotiated between the core network and the user equipment
- the apparatus is configured to receive an encryption key from a core network, and to decrypt the information to thereby obtain the unencrypted form
- the information comprises at least one of secondary cell measurement results and a secondary cell configuration requested by the user equipment
- the at least one processing core is configured to cause transmission of a security command comprising an instruction to trigger activation of the first encryption scheme between the user equipment and a network
- the apparatus is comprised in a base station device.

[0011] According to a second aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to establish information to be provided to a base station device, before activation of a first encryption

scheme, cause transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and begin, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

[0012] Various embodiments of the second aspect may comprise at least one feature from the following bulleted list:

- information comprises at least one of secondary cell measurement results and a desired secondary cell configuration
- the apparatus is configured to begin using the first encryption scheme responsive to a security command communicated with the base station device, the security command including an instruction to activate the first encryption scheme
- the apparatus is configured to cause the transmission of the information in connection with a connection establishment process
- the apparatus is configured to cause the transmission of the information in a non access stratum container.

[0013] According to a third aspect of the present invention, there is provided an apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to receive an initial UE message from a base station device, perform a cryptographic operation as a response to the initial UE message, and cause transmission of an initial context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

[0014] Various embodiments of the third aspect may comprise at least one feature from the following bulleted list:

- the cryptographic operation comprises decryption of information present in the initial UE message, and the output of the cryptographic operation comprises decrypted information
- the cryptographic operation comprises derivation of an encryption key, and the output of the cryptographic operation comprises the encryption key, the encryption key being distinct from K_{eNB}.

[0015] According to a fourth aspect of the present invention, there is provided a method comprising storing information in an apparatus, receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme, obtaining an unencrypted form of the information, and using the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

[0016] Various embodiments of the fourth aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the first aspect.

[0017] According to a fifth aspect of the present invention, there is provided a method, comprising establishing information to be provided to a base station device, before activation of a first encryption scheme, causing transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and beginning, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

[0018] Various embodiments of the fifth aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the second aspect.

[0019] According to a sixth aspect of the present invention, there is provided a method, comprising receiving an initial UE message from a base station device, performing a cryptographic operation as a response to the initial UE message, and causing transmission of an initial context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

[0020] Various embodiments of the sixth aspect may comprise at least one feature corresponding to a feature from the preceding bulleted list laid out in connection with the third aspect.

[0021] According to a seventh aspect of the present invention, there is provided an apparatus comprising means for storing information in an apparatus, means for receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme, means for

obtaining an unencrypted form of the information, and means for using the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

[0022] According to an eighth aspect of the present invention, there is provided an apparatus comprising means for establishing information to be provided to a base station device, means for causing transmission of the information, before activation of a first encryption scheme, in a form encrypted using a second encryption scheme, to the base station device, and means for beginning, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

[0023] According to a ninth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least store information in an apparatus, receive the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme, obtain an unencrypted form of the information, and use the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

[0024] According to a tenth aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least establish, in an apparatus, information to be provided to a base station device, before activation of a first encryption scheme, cause transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and begin, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

[0025] According to an eleventh aspect of the present invention, there is provided a non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least receive an initial UE message from a base station device, perform a cryptographic operation as a response to the initial UE message, and cause transmission of an initial

context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

[0026] According to a twelfth aspect of the present invention, there is provided a computer program configured to cause a method in accordance with at least one of the fourth, fifth and sixth aspects to be performed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention;

[0028] FIGURE 2 illustrates an example embodiment of early encryption in accordance with principles of the invention.

[0029] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention;

[0030] FIGURE 4 illustrates an example embodiment of early encryption in accordance with principles of the invention;

[0031] FIGURE 5 illustrates an example embodiment of early encryption in accordance with principles of the invention;

[0032] FIGURE 6 is a flow graph of a method in accordance with at least some embodiments of the present invention;

[0033] FIGURE 7 is a flow graph of a method in accordance with at least some embodiments of the present invention;

[0034] FIGURE 8 is an example embodiment in accordance with principles of the present invention;

[0035] FIGURE 9 is an example embodiment in accordance with principles of the present invention, and

[0036] FIGURE 10 is an example embodiment in accordance with principles of the present invention.

EMBODIMENTS

[0037] When a user equipment, UE, moves from RRC IDLE to RRC CONNECTED mode the first messages between UE and eNB during random access procedure are sent unciphered, these including, for example, *RRCConnectionRequest* message over SRB0 in random access Msg3, *RRCConnectionSetup* message from eNB to UE over SRB0 in random access Msg4 and *RRCConnectionSetupComplete* from UE to eNB over SRB1 in random access Msg5. The lack of security is natural for the very first message, for example *RRCConnectionRequest*, since at this initial phase eNB does not know which UE it is communicating with. *RRCConnectionSetup* message is already sent to a single UE and could in principle be encrypted. The same applies to *RRCConnectionSetupComplete* message from UE to eNB, it could also be encrypted. However, in current LTE systems encryption is turned on after *SecurityModeCommand* which is sent to UE after eNB has communicated with MME and received the keys.

[0038] Since the initial messages are unciphered, they cannot contain any critical information that would reveal, for example, either the UE location or other UE-specific information that may be used maliciously. UE may have some useful information that could be used by the eNB already in the first RRC reconfiguration after the initial connection setup, but in the current LTE system, security between UE and eNB has to be setup first and only after that the information can be requested from the UE. And only after receiving the additional information from the UE, eNB can perform another RRC reconfiguration taking that information into account.

[0039] In this invention we propose new security mechanisms such that UE could send relevant information encrypted to eNB in an earlier phase such that the eNB can take the UE information into use already in the first RRC reconfiguration after security mode command, for example.

[0040] Transmitting information in encrypted form from a user equipment to a base station already before activation of communication context encryption, or ciphering, may provide benefits, such as a reduced delay before the base station can act on the received information. By communication context encryption, or context encryption, it is meant encryption employed in encrypting information transmitted in the communication context of a connected state, that is, for example, the communication context that is present as a prerequisite for connected state. It is also sometimes called access stratum, AS, encryption or security. Certain information types are not suitable for transmission in unencrypted format, wherefore at least some embodiments of the invention provide for early transmission of information in encrypted form. In detail, a non-access stratum, NAS, container and security may be used, or a dedicated early encryption key may be derived for use in connection establishment prior to activation of the communication context encryption. Advantageously, for example, the base station may at least receive information from the user equipment and potentially also reconfigure a connection with the user equipment, using the information, already before communication context encryption is active.

[0041] By NAS it is meant a functional layer in a protocol stack, the layer being arranged between a UE and a core network. This layer may be used to manage establishments of communication sessions and/or maintaining continuous connectivity with a UE as it moves, for example. In an LTE system, once a UE has performed an initial attach procedure with the network, it has a UE context stored within the mobility management entity, MME.

[0042] FIGURE 1 illustrates an example system in accordance with at least some embodiments of the present invention. The system comprises a user equipment, UE, 110, which may comprise a smartphone, mobile phone, tablet computer, laptop computer, desktop computer or indeed another kind of suitable device. UE 110 is in wireless communication with a base station 120, via wireless link 112. Base station is a term employed frequently when discussing radio nodes in cellular communication systems, however in the context of the present document it should be appreciated that also non-cellular systems are envisaged to benefit from embodiments of the present invention, and are not to be excluded by this terminological choice. Access point is a term often employed when discussing non-cellular radio nodes.

[0043] Base station 120, wireless link 112 and UE 110 are arranged to operate in accordance with a communication standard, to thereby obtain interoperability. For example, wideband code division multiple access, WCDMA, and long term evolution, LTE, and 5G are cellular communication standards. On the other hand, wireless local area network, WLAN, and worldwide interoperability for microwave access, WiMAX, are examples of non-cellular communication standards. While described herein as a wireless communication system, other embodiments of the invention may be implemented as wired communication systems. Wired communication standards include Ethernet, for example. In case of a wired communication system link 112 is not wireless but wired.

[0044] Base station 120 is coupled, via connection 123, with node 130. Node 130 may be comprised as node in a core network or a radio access network, for example. Node 130 may comprise a mobility management entity, MME, or switch, for example. Connection 123 may comprise a wired connection, wireless connection or a partly wireless connection. Connection 123 may be used to convey payload traffic between node 130 and base station 120. Node 130 is coupled with gateway 140 via connection 134, and gateway 140 is, in turn, coupled with further networks via connection 141. Connections 134 and 141 may comprise wire-line connections, for example. Wire-line connections may comprise Ethernet and/or fibre-optic connections, for example.

[0045] Via base station 120, node 130 and gateway 140, UE 110 may communicate with correspondent entities, which may be servers on the Internet, telephone endpoints in domestic or foreign locations or, for example, banking services in an corporate extranet.

[0046] When transitioning from an idle state to a connected state, UE 110 may trigger establishment of at least one physical channel over link 112. In detail, UE 110 may trigger a connection establishment process including, such as, for example, a random access procedure. For example, UE 110 may transmit a random access preamble to base station 120, which may reply with a random access response. UE 110 may then transmit a connection request to base station 120, an example of a connection request being a RRCConnectionRequest message in accordance with the LTE system.

[0047] Once base station 120 has responded to a connection request message, for example by transmitting a connection setup message, and received a connection setup complete message from the UE 110, base station 120 may consult node 130, or another node, to obtain context information relating to UE 110. Node 130 may comprise an MME,

for example. The context information may comprise an encryption key to be used in communication context encryption. An example of a connection setup complete message is a RRCConnectionSetupComplete message in accordance with an LTE system, and an example of a context encryption key is K_{eNB}. Other technologies have similar messages and keys.

[0048] A security command may be transmitted to UE 110 from base station 120 to cause the context encryption to be activated. A security command may comprise at least one of the following: information on a ciphering algorithm to use, information on an integrity algorithm to use and a message authentication code - integrity, MAC-I, field. A MAC-I field may be used to ensure message integrity, for example. After the security command is received and acted on in UE 110, encryption of information in the communication context may be accomplished using the context encryption. Alternatively, a security command may be known as a security instruction.

[0049] From the point of view of base station 120, context encryption is activated when the security command is sent and from the point of view of UE 110, context encryption is activated when the security command is received and processed. Base station 120 may thus trigger the activation of the context encryption, although in some embodiments a triggering message may be transmitted by UE 110.

[0050] On the other hand, UE 110 may have information that may be useful to provide to base station 120 already before context encryption is active. Such information may comprise secondary cell measurement results and/or a secondary cell configuration desired by UE 110, for example. In case such information is of a kind that requires encryption, encrypting the information would be beneficial, but since context encryption is not yet active, another encryption may be used. Such information may be used by base station 120 to provide service to the user equipment, in other words, the information may be intended for use in base station 120, and not merely provided to base station 120 for forwarding for use in further nodes. Base station 120 may provide service by using the information, for example to configure an aspect of UE 110. The another encryption, used before context encryption is available, will be referred to herein as early encryption as it may be employed in connection with a connection establishment process before context encryption is used. Early encryption may be used also at other times.

[0051] FIGURE 2 illustrates an example embodiment of early encryption in accordance with principles of the invention. On the vertical axes are disposed, from the left to the right, UE 110, base station 120 and node 130. Node 130 may comprise a MME in this embodiment, for example. Time advances from the top toward the bottom. The overall process of FIGURE 2, like those of FIGURE 4 and FIGURE 5, is a transition from idle state to connected, or active, state.

[0052] In phase 210, base station 120 may page UE 110. This phase is optional, as the invention is equally applicable to mobile-originated communications. Phase 220 comprises, for example, a random access process to obtain radio resources for communication between UE 110 and base station 120. Phase 220 may comprise, for example, RRC connection request and setup messages exchanged between UE 110 and base station 120, which form part of a RRC connection establishment procedure.

[0053] Phase 230 comprises a message transmitted from UE 110 to base station 120, the message comprising information intended for use in base station 120, the information being in the message in encrypted form. The message itself may be a RRC connection setup complete message, for example, but in various embodiments the message may go under different names. The message of phase 230 is transmitted before context encryption is yet active between UE 110 and base station 120. The information, in encrypted form, may be in a NAS container, for example. The use of NAS encryption provides the early encryption in embodiments in accordance with FIGURE 2. Early encryption is distinct from context encryption.

[0054] In phase 240, base station 120 communicates with node 130 in connection with the connection establishment procedure. In phase 240, base station 120 provides the NAS container it has received in phase 230 to node 130. Node 130 decrypts the NAS container in phase 250, and returns the information, in unencrypted form, to base station 120 in phase 260. Further, in phase 260 node 130 may instruct base station 120 concerning the connection establishment, for example by providing an encryption key for use in the context encryption.

[0055] Once in receipt of information provided in phase 260, base station may apply the information that was provided under the early encryption in phase 230. Phase 270 comprises transmission of a security command from base station 120 to UE 110, the security command being described herein above. Phases 280 to 2110 are provided as

technological context and are described in light of an LTE system, however in different communication technologies these phases may proceed in differing manners. In detail, phase 280 may comprise a connection reconfiguration, which may comprise an addition of a secondary cell in accordance with the information communicated to base station 120 using the early encryption. Phase 280 and phase 270 may be transmitted in a same transport block. Phase 290 may comprise a security command response, for example a security mode complete message, and phase 2100 may comprise a connection reconfiguration complete message, responsive to completion of a reconfiguration instructed in phase 280. Phase 2110 may comprise an initial context setup response, in response to messaging of phase 260. In general, base station 120 may be configured to reconfigure a connection with UE 110, using the information provided under the early encryption, for example before the context encryption is active.

[0056] Phase 2120 comprises communication of data between UE 110 and the network, the information being secured using the context encryption which is active at this point.

[0057] FIGURE 3 illustrates an example apparatus capable of supporting at least some embodiments of the present invention. Illustrated is device 300, which may comprise, for example, a mobile communication device such as UE 110 or, in applicable parts, base station 120 of FIGURE 1. Comprised in device 300 is processor 310, which may comprise, for example, a single- or multi-core processor wherein a single-core processor comprises one processing core and a multi-core processor comprises more than one processing core. Processor 310 may comprise more than one processor. A processing core may comprise, for example, a Cortex-A8 processing core manufactured by ARM Holdings or a Steamroller processing core produced by Advanced Micro Devices Corporation. Processor 310 may comprise at least one Qualcomm Snapdragon and/or Intel Atom processor. Processor 310 may comprise at least one application-specific integrated circuit, ASIC. Processor 310 may comprise at least one field-programmable gate array, FPGA. Processor 310 may be means for performing method steps in device 300. Processor 310 may be configured, at least in part by computer instructions, to perform actions.

[0058] Device 300 may comprise memory 320. Memory 320 may comprise random-access memory and/or permanent memory. Memory 320 may comprise at least one RAM chip. Memory 320 may comprise solid-state, magnetic, optical and/or holographic

memory, for example. Memory 320 may be at least in part accessible to processor 310. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be means for storing information. Memory 320 may comprise computer instructions that processor 310 is configured to execute. When computer instructions configured to cause processor 310 to perform certain actions are stored in memory 320, and device 300 overall is configured to run under the direction of processor 310 using computer instructions from memory 320, processor 310 and/or its at least one processing core may be considered to be configured to perform said certain actions. Memory 320 may be at least in part comprised in processor 310. Memory 320 may be at least in part external to device 300 but accessible to device 300.

[0059] Device 300 may comprise a transmitter 330. Device 300 may comprise a receiver 340. Transmitter 330 and receiver 340 may be configured to transmit and receive, respectively, information in accordance with at least one cellular or non-cellular standard. Transmitter 330 may comprise more than one transmitter. Receiver 340 may comprise more than one receiver. Transmitter 330 and/or receiver 340 may be configured to operate in accordance with global system for mobile communication, GSM, wideband code division multiple access, WCDMA, long term evolution, LTE, IS-95, wireless local area network, WLAN, Ethernet and/or worldwide interoperability for microwave access, WiMAX, standards, for example.

[0060] Device 300 may comprise a near-field communication, NFC, transceiver 350. NFC transceiver 350 may support at least one NFC technology, such as NFC, Bluetooth, Wibree or similar technologies.

[0061] Device 300 may comprise user interface, UI, 360. UI 360 may comprise at least one of a display, a keyboard, a touchscreen, a vibrator arranged to signal to a user by causing device 300 to vibrate, a speaker and a microphone. A user may be able to operate device 300 via UI 360, for example to accept incoming telephone calls, to originate telephone calls or video calls, to browse the Internet, to manage digital files stored in memory 320 or on a cloud accessible via transmitter 330 and receiver 340, or via NFC transceiver 350, and/or to play games.

[0062] Device 300 may comprise or be arranged to accept a user identity module 370. User identity module 370 may comprise, for example, a subscriber identity module, SIM, card installable in device 300. A user identity module 370 may comprise information

identifying a subscription of a user of device 300. A user identity module 370 may comprise cryptographic information usable to verify the identity of a user of device 300 and/or to facilitate encryption of communicated information and billing of the user of device 300 for communication effected via device 300.

[0063] Processor 310 may be furnished with a transmitter arranged to output information from processor 310, via electrical leads internal to device 300, to other devices comprised in device 300. Such a transmitter may comprise a serial bus transmitter arranged to, for example, output information via at least one electrical lead to memory 320 for storage therein. Alternatively to a serial bus, the transmitter may comprise a parallel bus transmitter. Likewise processor 310 may comprise a receiver arranged to receive information in processor 310, via electrical leads internal to device 300, from other devices comprised in device 300. Such a receiver may comprise a serial bus receiver arranged to, for example, receive information via at least one electrical lead from receiver 340 for processing in processor 310. Alternatively to a serial bus, the receiver may comprise a parallel bus receiver.

[0064] Device 300 may comprise further devices not illustrated in FIGURE 3. For example, where device 300 comprises a smartphone, it may comprise at least one digital camera. Some devices 300 may comprise a back-facing camera and a front-facing camera, wherein the back-facing camera may be intended for digital photography and the front-facing camera for video telephony. Device 300 may comprise a fingerprint sensor arranged to authenticate, at least in part, a user of device 300. In some embodiments, device 300 lacks at least one device described above. For example, some devices 300 may lack a NFC transceiver 350 and/or user identity module 370.

[0065] Processor 310, memory 320, transmitter 330, receiver 340, NFC transceiver 350, UI 360 and/or user identity module 370 may be interconnected by electrical leads internal to device 300 in a multitude of different ways. For example, each of the aforementioned devices may be separately connected to a master bus internal to device 300, to allow for the devices to exchange information. However, as the skilled person will appreciate, this is only one example and depending on the embodiment various ways of interconnecting at least two of the aforementioned devices may be selected without departing from the scope of the present invention.

[0066] FIGURE 4 illustrates an example embodiment of early encryption in accordance with principles of the invention. On the vertical axes are disposed, as in FIGURE 2, UE 110, base station 120 and node 130.

[0067] Phases 410 to 420 correspond to phases 210 and 220 of FIGURE 2, respectively.

[0068] Phase 430 comprises a message transmitted from UE 110 to base station 120, the message comprising information intended for use in base station 120, the information being in the message in encrypted form. The message itself may be a RRC connection setup complete message, for example, but in various embodiments the message may go under different names. The message of phase 430 is transmitted before context encryption is yet active between UE 110 and base station 120. The information, in encrypted form, may be encrypted using an early encryption key. The early encryption key may be generated, for example in connection with an initial attachment of UE 110 with the network. The early encryption key may be generated using a Diffie-Hellman exchange, for example. The use of the early encryption key provides the early encryption in embodiments in accordance with FIGURE 4 The early encryption key may be established in a NAS layer procedure, for example. Alternatively to a NAS procedure, a default integrity/ciphering algorithm could be defined and the keys could be defined without negotiating between UE and MME.

[0069] Figures 4 and 5 illustrate embodiments where new, temporary, security would be defined between the UE and the base station, which in LTE is an eNB. The new early encryption key could be derived, in LTE technology, from K_{ASME} in UE and in MME and MME would provide the key to eNB when requested by eNB. eNB would request the early encryption key when it would receive early-encrypted UE information. Early encryption key request could be added to some existing message(s) over S1, such as, for example, INITIAL UE MESSAGE, or a new message could be created for it. And the early encryption key could be provided to eNB in some existing message, such as, for example, INITIAL CONTEXT SETUP REQUEST where also K_{eNB} is provided, or a new message could be defined. eNB could then decipher the early-encrypted UE information with the early encryption key or a key derived from the early encryption key received from MME. In addition to early (de)ciphering key, eNB and UE could derive also an early integrity protection key from the early encryption key. The early integrity key could be used to

integrity protect the messages sent by the UE. The advantage of these alternatives is that information received from the UE need not be sent to MME for deciphering and returned back to the eNB for use. In general, a security scheme may comprise an integrity protection scheme and/or an encryption scheme. An encryption scheme, in turn, may comprise early encryption or context encryption, for example.

[0070] In phase 440, base station 120 communicates with node 130 in connection with the connection establishment procedure. In phase 440, base station 120 requests the early encryption key to be provided to base station 120. Node 130 retrieves, generates or re-generates the early encryption key in phase 450, and provides it to base station 120 in phase 460. Further, in phase 460 node 130 may instruct base station 120 concerning the connection establishment, for example by providing an encryption key for use in the context encryption. In other words, phase 460 may comprise node 130 providing two encryption keys to base station 120, namely the key for context encryption and the key for early encryption.

[0071] Base station 120 may use the early encryption key to decrypt, in phase 470, the information provided by UE 110 in phase 430, to thereby obtain the information in unencrypted form.

[0072] Once in receipt of the information provided in phase 430, in unencrypted form, base station 120 may apply the information that was provided under the early encryption in phase 430. Phase 480 comprises transmission of a security command from base station 120 to UE 110, the security command being described herein above. Phases 490 to 4120 are provided as technological context and are described in light of an LTE system, however in different communication technologies these phases may proceed in differing manners. In detail, phase 490 may comprise a connection reconfiguration, which may comprise an addition of a secondary cell in accordance with the information communicated to base station 120 using the early encryption. Phase 490 and phase 480 may be transmitted in a same transport block. Phase 4100 may comprise a security command response, for example a security mode complete message, and phase 4110 may comprise a connection reconfiguration complete message, responsive to completion of a reconfiguration instructed in phase 490. Phase 4120 may comprise an initial context setup response, in response to messaging of phase 460, for example. In general, base station 120

may be configured to reconfigure a connection with UE 110, using the information provided under the early encryption, for example before the context encryption is active.

[0073] Phase 4130 comprises communication of data between UE 110 and the network, the information being secured using the context encryption which is active at this point.

[0074] FIGURE 5 illustrates an example embodiment of early encryption in accordance with principles of the invention. The embodiment of FIGURE 5 resembles that of FIGURE 4 in that an early encryption key is used. Phases 510 and 520 correspond to phases 410 and 420 of FIGURE 4, respectively.

[0075] Phase 530 comprises a message transmitted from UE 110 to base station 120, the message comprising an indication that information intended for use in base station 120 is available in UE 110. The message comprising the indication does not comprise the information itself. The information may be of the type that requires ciphering to transmit, while being useful to base station 120 already before context encryption is active. The message of phase 530 may be a RRC connection setup complete message, for example, but in various embodiments the message may go under different names. The message of phase 530 is transmitted before context encryption is yet active between UE 110 and base station 120.

[0076] Responsive to the indication of phase 530, base station 120 may request the indicated information to be provided from UE 110 to base station 120. Such a request is illustrated in FIGURE 5 as phase 532. For example, the information may comprise secondary cell measurement information, or a desired secondary cell configuration. Phases 540 and 532 may take place at more or less the same time, or one before or after the other. As the information will be provided from UE 110 using early encryption, where base station 120 requests for the information, base station 120 also requests for the early encryption key from node 130. Such requesting may be comprised in phase 540.

[0077] The information, in encrypted form, may be encrypted using the early encryption key. The early encryption key may be generated, for example in connection with an initial attachment of UE 110 with the network. The early encryption key may be generated using a Diffie-Hellman exchange, for example. The use of the early encryption key provides the early encryption in embodiments in accordance with FIGURE 5

[0078] In phase 540, base station 120 communicates with node 130 in connection with the connection establishment procedure. In phase 540, base station 120 requests the early encryption key to be provided to base station 120. Node 130 retrieves, generates or re-generates the early encryption key in phase 550, and provides it to base station 120 in phase 560. Further, in phase 560 node 130 may instruct base station 120 concerning the connection establishment, for example by providing an encryption key for use in the context encryption. In other words, phase 560 may comprise node 130 providing two encryption keys to base station 120, namely the key for context encryption and the key for early encryption.

[0079] UE 110 may provide the information, in encrypted form, to base station 120 in phase 535, as a response to the requesting of phase 532. Base station 120 may use the early encryption key to decrypt, in phase 570, the information provided by UE 110 in phase 535, to thereby obtain the information in unencrypted form.

[0080] Once in receipt of the information provided in phase 535, in unencrypted form, base station may apply the information that was provided under the early encryption in phase 535. Phase 580 comprises transmission of a security command from base station 120 to UE 110, the security command being described herein above. Phases 590 to 5120 are provided as technological context and are described in light of an LTE system, however in different communication technologies these phases may proceed in differing manners. In detail, phase 590 may comprise a connection reconfiguration, which may comprise an addition of a secondary cell in accordance with the information communicated to base station 120 using the early encryption.. Phase 5100 may comprise a security command response, for example a security mode complete message, and phase 5110 may comprise a connection reconfiguration complete message, responsive to completion of a reconfiguration instructed in phase 590. Phase 5120 may comprise an initial context setup response, in response to messaging of phase 560, for example. In general, base station 120 may be configured to reconfigure a connection with UE 110, using the information provided under the early encryption, for example before the context encryption is active.

[0081] Phase 5130 comprises communication of data between UE 110 and the network, the information being secured using the context encryption which is active at this point.

[0082] An advantage of FIGURE 4 and FIGURE 5 embodiments is that the information, which is sensitive enough to require encryption, is not communicated between the base station and node 130. An advantage of the FIGURE 5 embodiment is that the message of phase 530 does not increase in size, as the information is not automatically included therein, and base station 120 is merely enabled to request the information if it is useful in the prevailing circumstances. The described security scheme may be useful also with suspend/resume, namely, when the UE connection is resumed, all secondary cells, including the entirety of the secondary cell group, SCG, are released. Hence, when the UE requests a resumption of a previously suspended connection, it may indicate that it may utilize also carrier aggregation in accordance with a new primary cell configuration, which may benefit from the present invention. The described security mechanism may also be usable with 5G or other cellular technologies with idle-to-connected transitions where security needs to be activated prior to UE sending any measurement information to eNB.

[0083] FIGURE 6 is a flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in base station 120, for example, or in a control device configured to control the functioning thereof, when implanted therein.

[0084] Phase 610 comprises storing information in an apparatus. Phase 620 comprises receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme. Phase 630 comprises obtaining an unencrypted form of the information. Finally, phase 640 comprises using the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

[0085] FIGURE 7 is a flow graph of a method in accordance with at least some embodiments of the present invention. The phases of the illustrated method may be performed in UE 110, for example, or in a control device configured to control the functioning thereof, when implanted therein.

[0086] Phase 710 comprises establishing information to be provided to a base station device. Phase 720 comprises, before activation of a first encryption scheme, causing transmission of the information, in a form encrypted using a second encryption scheme, to the base station device. Finally, phase 730 comprises beginning using the first encryption

scheme in communication between the apparatus and the base station device, after causing the transmission of the information.

[0087] Further example embodiments with example message names and contents are shown in FIGUREs 8, 9 and 10. They are examples of embodiments in FIGUREs 2, 4 and 5, respectively. We propose to use a pre-defined encryption when sending UE-specific information to eNB, along with explicit or implicit indication to eNB of whether the key information or decrypted message needs to be retrieved via MME.

[0088] In particular, one possibility, illustrated in FIGURE 8, would be to use existing NAS encryption keys, negotiated at ATTACH time, also to encrypt the information sent by UE, in addition to a normal NAS message. Then the UE Information should be sent to MME, which would decrypt it and return the unciphered message to eNB before, during or after the normal context setup procedure.

[0089] Alternatively, FIGUREs 9 and 10, the UE information could be encrypted using a new temporary idle-to-connected, "ItoC" mode encryption scheme such that the keys are negotiated between UE and MME at ATTACH time. Then, eNB would request the keys from MME when receiving UE Information and there would not be need to send UE Information to MME and return it back to eNB.

[0090] Using NAS security for sending UE info intended for the eNB is depicted in FIGURE 8. In the figure, SCell measurement results or desired/indicated/requested SCell configuration (sCellInfo) is used as an example of possible UE info that is intended for eNB. A new NAS message could be specified for this purpose, for example 'NAS UE info to eNB' message which would contain a container for the control info intended for eNB. In this embodiment, the new NAS message with the container is sent over S1 to MME which would decipher the contents of the container and return the decrypted UE info to eNB as part of the next S1 message, for example INITIAL CONTEXT SETUP REQUEST message. Alternatively, a new S1 messages could be defined for this purpose. In the figure, the new NAS message is sent over the air as part of RRCConnectionSetupComplete message. Alternatively, a new RRC message could be defined. The advantage of this alternative is that no new security keys are needed. The existing NAS keys would be reused.

[0091] FIGUREs 9 and 10 illustrate alternatives where new, temporary, security would be defined between the UE and eNB. The new idle-to-connected "ItoC" key, or early encryption key, could be derived from K_{ASME} in UE and/or in MME and MME could provide the key to eNB when requested by eNB. eNB would request the ItoC key when it

would receive encrypted UE info. ItoC key request could be added to some existing message(s) over S1, for example INITIAL UE MESSAGE, or a new message could be created for it. And the new ItoC key, K_{ItoC}, could be provided to eNB in some existing message, such as, for example, INITIAL CONTEXT SETUP REQUEST where also K_{eNB} is provided, or a new message could be defined. eNB could then decipher the UE info with a key derived from K_{ItoC}. The advantage of these alternatives is that UE info is not sent to MME.

[0092] In FIGURE 9, the UE information is provided within RRCConnectionSetupComplete message.

[0093] FIGURE 10 illustrates an alternative where the UE information is requested by eNB, for example by UEInformationRequest message, and sent within, for example, UEInformationResponse message using the new ItoC early encryption. In this alternative UEInformationRequest and UEInformationResponse messages are sent before normal security activation, that is, before SecurityModeCommand, which is not allowed in prior versions of specifications. The request itself may be transmitted without ciphering since eNB does not, yet, have the new key.

[0094] An advantage of this alternative is that RRCConnectionSetupComplete message does not grow much, only growing by the indication of new UE information. Compared to legacy UE information transfer, the transfer could be started already before normal security activation by using the new ItoC security.

[0095] The new ItoC security could be temporary and it would only be used until normal security between UE and eNB is activated.

[0096] To create the ItoC key, either a new NAS level procedure between UE and MME should be defined, similar to NAS security mode command, or for this purpose a default integrity/ciphering algorithm could be defined and the keys could be defined without negotiating between UE and MME and/or eNB.

[0097] The new, early, security mechanism could be used also with 5G or other cellular technologies with idle-to-connected transition where security needs to be activated prior to UE sending any measurement information to eNB .

[0098] It is to be understood that the embodiments of the invention disclosed are not limited to the particular structures, process steps, or materials disclosed herein, but are extended to equivalents thereof as would be recognized by those ordinarily skilled in the relevant arts. It should also be understood that terminology employed herein is used for the purpose of describing particular embodiments only and is not intended to be limiting.

[0099] Reference throughout this specification to one embodiment or an embodiment means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Where reference is made to a numerical value using a term such as, for example, about or substantially, the exact numerical value is also disclosed.

[00100] As used herein, a plurality of items, structural elements, compositional elements, and/or materials may be presented in a common list for convenience. However, these lists should be construed as though each member of the list is individually identified as a separate and unique member. Thus, no individual member of such list should be construed as a de facto equivalent of any other member of the same list solely based on their presentation in a common group without indications to the contrary. In addition, various embodiments and example of the present invention may be referred to herein along with alternatives for the various components thereof. It is understood that such embodiments, examples, and alternatives are not to be construed as de facto equivalents of one another, but are to be considered as separate and autonomous representations of the present invention.

[00101] Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the preceding description, numerous specific details are provided, such as examples of lengths, widths, shapes, etc., to provide a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[00102] While the forgoing examples are illustrative of the principles of the present invention in one or more particular applications, it will be apparent to those of ordinary skill in the art that numerous modifications in form, usage and details of implementation can be made without the exercise of inventive faculty, and without departing from the principles and concepts of the invention. Accordingly, it is not intended that the invention be limited, except as by the claims set forth below.

[00103] The verbs “to comprise” and “to include” are used in this document as open limitations that neither exclude nor require the existence of also un-recited features. The features recited in depending claims are mutually freely combinable unless otherwise explicitly stated. Furthermore, it is to be understood that the use of "a" or "an", that is, a singular form, throughout this document does not exclude a plurality.

INDUSTRIAL APPLICABILITY

[00104] At least some embodiments of the present invention find industrial application in enhancing data security and/or reducing delays in initiating connectivity.

ACRONYMS LIST

5G	fifth generation
LTE	long term evolution
MME	mobility management entity
NAS	non access stratum
RACH	random access channel
RRC	radio resource control
SCG	secondary cell group
UE	user equipment
WCDMA	wideband code division multiple access
WiMAX	worldwide interoperability for microwave access
WLAN	wireless local area network

REFERENCE SIGNS LIST

110	UE (user equipment)
120	base station
130	node
140	gateway

112	wireless link
123, 134, 141	connections
210 – 2120	phases of the method of FIGURE 2
300 – 370	structure of the device of FIGURE 3
410 – 4130	phases of the method of FIGURE 4
510 – 5130	phases of the method of FIGURE 5
610 – 640	phases of the method of FIGURE 6
710 – 730	phases of the method of FIGURE 7

CLAIMS:

1. An apparatus comprising:
   - a memory configured to store information;
   - at least one processing core configured to:
     - receive the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme;
     - obtain an unencrypted form of the information, and
     - use the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

2. The apparatus according to claim 1, wherein the apparatus is configured to process a triggering of the activation of the first encryption scheme during a connection establishment procedure.

3. The apparatus according to claim 1 or 2, wherein the apparatus is configured to obtain the unencrypted form of the information via a core network.

4. The apparatus according to claim 1 or 2, wherein the apparatus is configured to obtain the unencrypted form of the information at least partly by requesting an unencryption key from a core network.

5. The apparatus according to any of claims 1 - 4, wherein the first encryption scheme comprises an access stratum AS encryption scheme.

6. The apparatus according to any of claims 1, 2 or 3, wherein the second encryption scheme comprises a non-access stratum, NAS, encryption scheme relating to the user equipment.

7 The apparatus according to any of claims 1, 2, 3, 5 and 6, wherein the apparatus is configured to obtain the unencrypted form of the information by providing the encrypted

form of the information to a mobility management entity, and by receiving the unencrypted form of the information from the mobility management entity.

8. The apparatus according to claim 1 or 2, wherein the second encryption scheme comprises an encryption scheme pre-negotiated between the core network and the user equipment.

9. The apparatus according to claim 1 or 8, wherein the apparatus is configured to receive an encryption key from a core network, and to decrypt the information to thereby obtain the unencrypted form.

10. The apparatus according to any of claims 1 - 9, wherein the information comprises at least one of secondary cell measurement results and a secondary cell configuration requested by the user equipment.

11. The apparatus according to any of claims 1 - 10, wherein the at least one processing core is configured to cause transmission of a security command comprising an instruction to trigger activation of the first encryption scheme between the user equipment and a network.

12. The apparatus according to any preceding claim, wherein the apparatus is comprised in a base station device.

13. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to:

- establish information to be provided to a base station device;
- before activation of a first encryption scheme, cause transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and
- begin, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

14. The apparatus according to claim 13, wherein the information comprises at least one of secondary cell measurement results and a desired secondary cell configuration.

15. The apparatus according to claim 13 or 14, wherein the apparatus is configured to begin using the first encryption scheme responsive to a security command communicated with the base station device, the security command including an instruction to activate the first encryption scheme.

16. The apparatus according to any of claims 13 – 15, wherein the apparatus is configured to cause the transmission of the information in connection with a connection establishment process.

17. The apparatus according to any of claims 13 – 16, wherein the apparatus is configured to cause the transmission of the information in a non access stratum container.

18. An apparatus comprising at least one processing core, at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processing core, cause the apparatus at least to:

- receive an initial UE message from a base station device;
- perform a cryptographic operation as a response to the initial UE message, and
- cause transmission of an initial context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

19. An apparatus according to claim 18, wherein the cryptographic operation comprises decryption of information present in the initial UE message, and the output of the cryptographic operation comprises decrypted information.

20. An apparatus according to claim 18, wherein the cryptographic operation comprises derivation of an encryption key, and the output of the cryptographic operation comprises the encryption key, the encryption key being distinct from K_{eNB}.

21. A method comprising:

- storing information in an apparatus;
- receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme;
- obtaining an unencrypted form of the information, and
- using the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

22. The method according to claim 21, further comprising processing a triggering of the activation of the first encryption scheme during a connection establishment procedure.

23. The method according to claim 21 or 22, wherein the unencrypted form of the information is obtained via a core network.

24. The method according to claim 21 or 22, wherein the unencrypted form of the information is obtained at least partly by requesting an unencryption key from a core network.

25. The method according to any of claims 21 - 24, wherein the first encryption scheme comprises an access stratum AS encryption scheme.

26. The method according to any of claims 21, 22 or 23, wherein the second encryption scheme comprises a non-access stratum, NAS, encryption scheme relating to the user equipment.

27 The method according to any of claims 21, 22, 23, 25 and 26, wherein the unencrypted form of the information is obtained by providing the encrypted form of the information to a mobility management entity, and by receiving the unencrypted form of the information from the mobility management entity.

28. The method according to claim 21 or 22, wherein the second encryption scheme comprises an encryption scheme pre-negotiated between the core network and the user equipment.

29. The method according to claim 21 or 28, further comprising receiving an encryption key from a core network, and decrypting the information to thereby obtain the unencrypted form.

30. The method according to any of claims 21 - 29, wherein the information comprises at least one of secondary cell measurement results and a secondary cell configuration requested by the user equipment.

31. The method according to any of claims 21 - 30, further comprising causing transmission of a security command comprising an instruction to trigger activation of the first encryption scheme between the user equipment and a network.

32. The method according to any of claims 21 - 31, wherein the method is performed in a base station device.

33. A method, comprising:

- establishing information to be provided to a base station device;
- before activation of a first encryption scheme, causing transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and
- beginning, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

34. The method according to claim 33, wherein the information comprises at least one of secondary cell measurement results and a desired secondary cell configuration.

35. The method according to claim 33 or 34, wherein use of the first encryption scheme is begun responsive to a security command communicated with the base station device, the security command including an instruction to activate the first encryption scheme.

36. The method according to any of claims 33 – 35, wherein the information is caused to be transmitted in connection with a connection establishment process.

37. A method, comprising:

- receiving an initial UE message from a base station device;
- performing a cryptographic operation as a response to the initial UE message, and
- causing transmission of an initial context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

38. An apparatus comprising:

- means for storing information in an apparatus;
- means for receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme;
- means for obtaining an unencrypted form of the information, and
- means for using the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

39. An apparatus comprising:

- means for establishing information to be provided to a base station device;
- means for causing transmission of the information, before activation of a first encryption scheme, in a form encrypted using a second encryption scheme, to the base station device, and
- means for beginning, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

40. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- store information in an apparatus;
- receive the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme;
- obtain an unencrypted form of the information, and

- use the unencrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

41. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- establish, in an apparatus, information to be provided to a base station device;
- before activation of a first encryption scheme, cause transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and
- begin, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

42. A non-transitory computer readable medium having stored thereon a set of computer readable instructions that, when executed by at least one processor, cause an apparatus to at least:

- receive an initial UE message from a base station device;
- perform a cryptographic operation as a response to the initial UE message, and
- cause transmission of an initial context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

43. A computer program configured to cause a method in accordance with at least one of claims 21 - 37 to be performed.

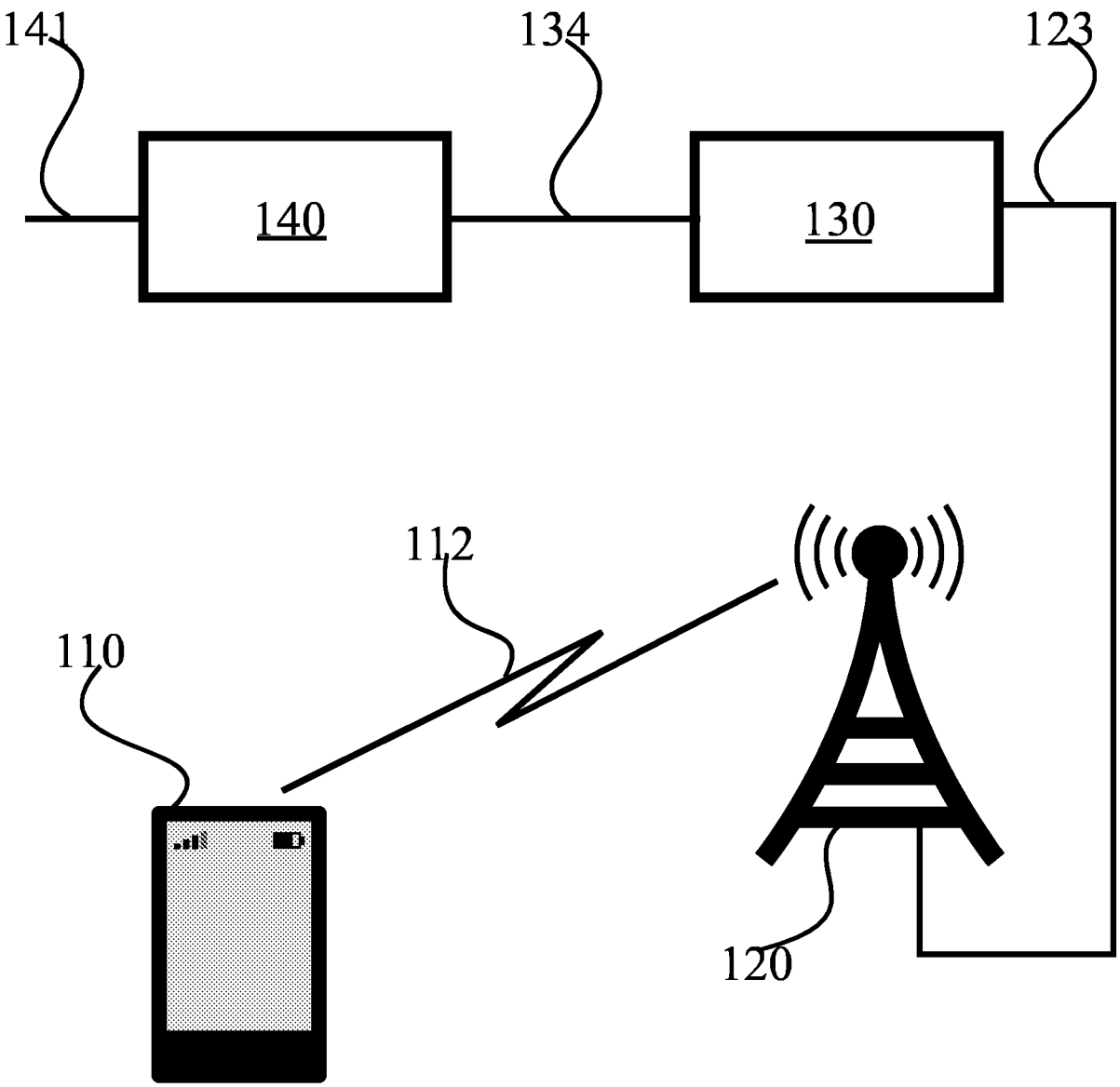

FIGURE 1

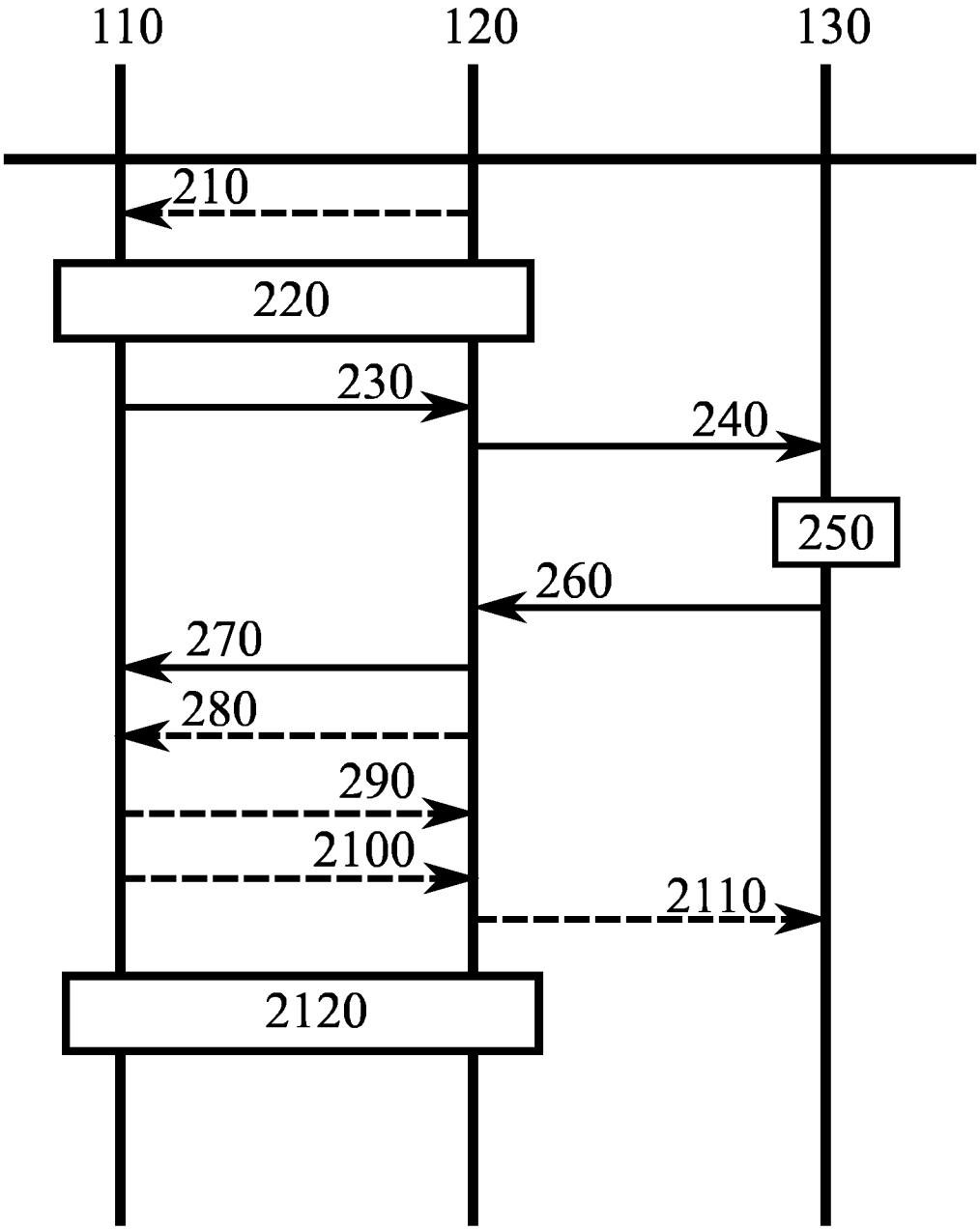

FIGURE 2

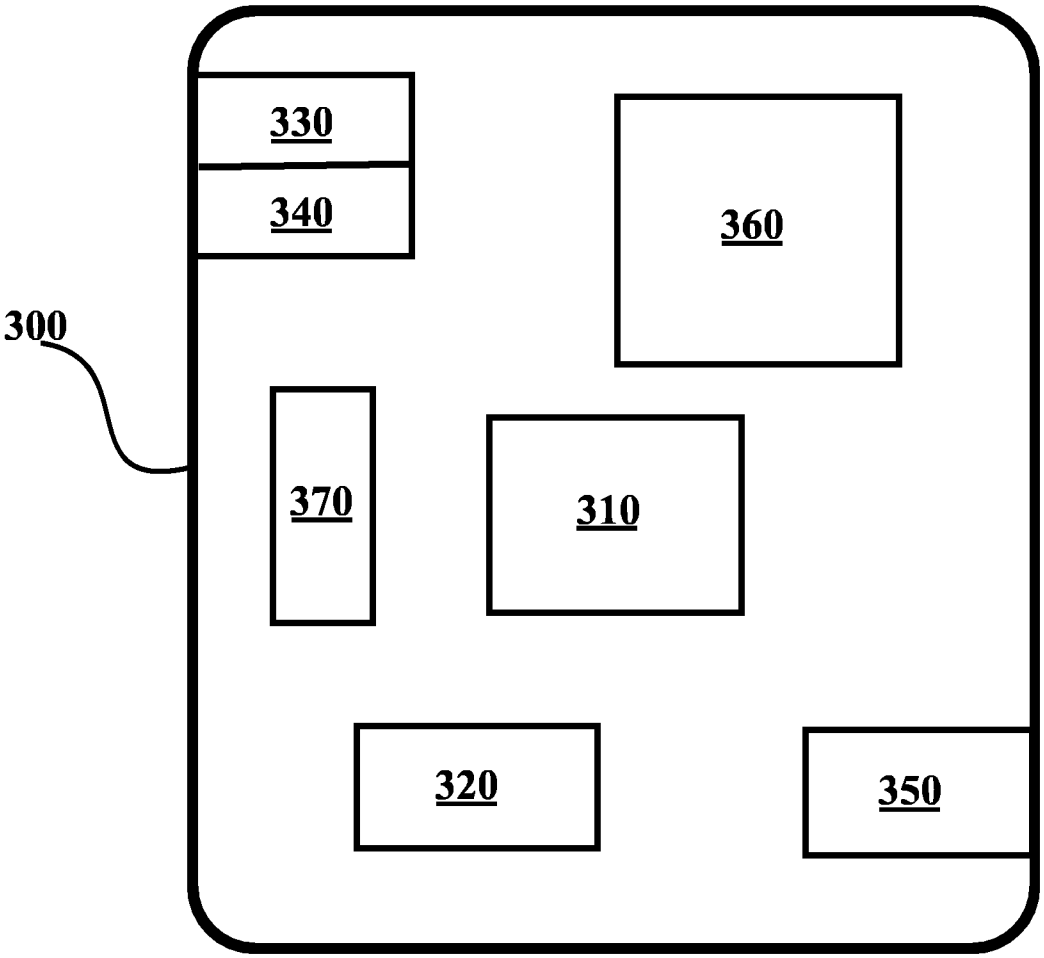

FIGURE 3

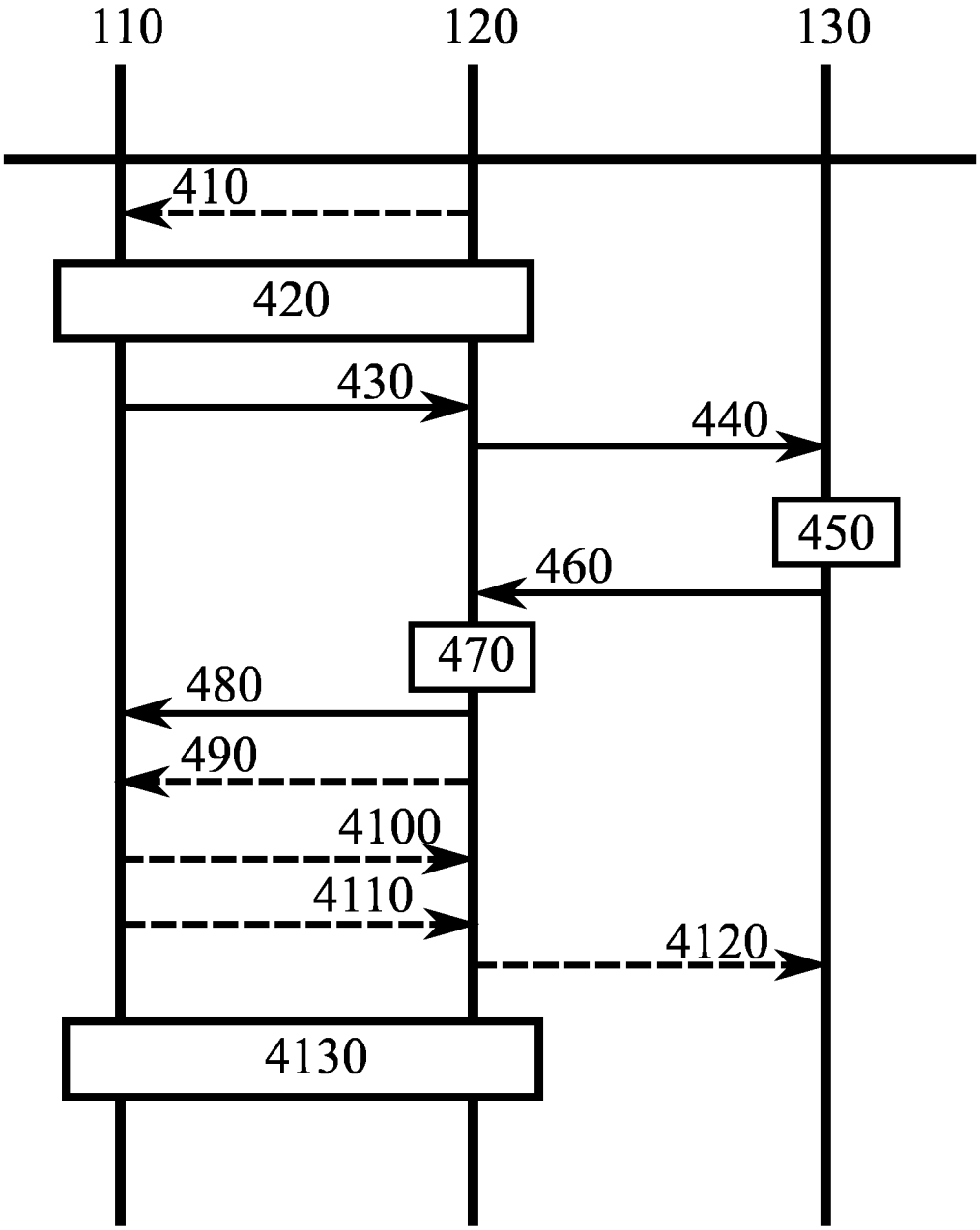
110
120
130
410
420
430
440
450
460
470
480
490
4100
4110
4120
4130

FIGURE 4

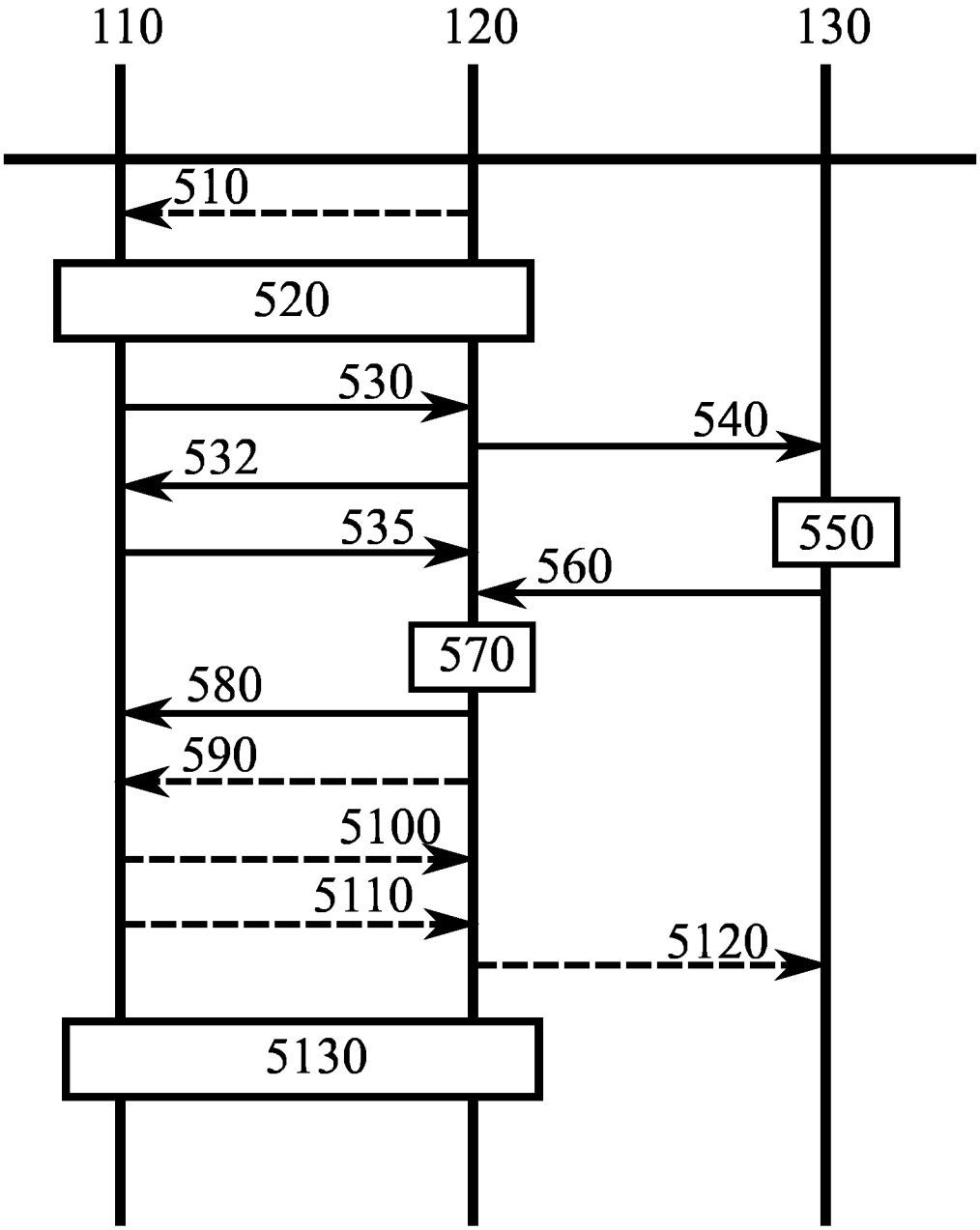
110
120
130
510
520
530
540
532
535
550
560
570
580
590
5100
5110
5120
5130

FIGURE 5

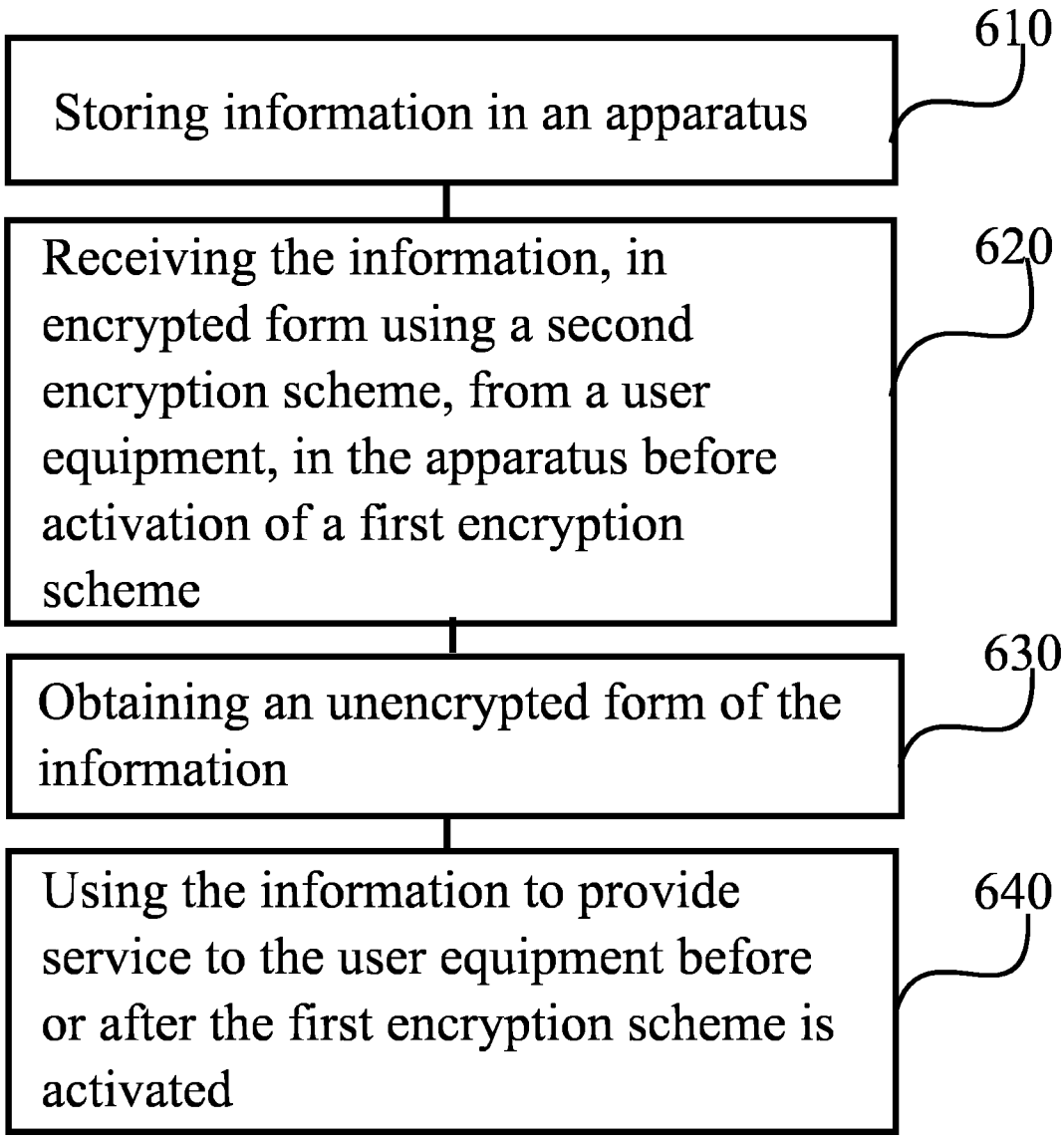
610
Storing information in an apparatus
620
Receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus before activation of a first encryption scheme
630
Obtaining an unencrypted form of the information
640
Using the information to provide service to the user equipment before or after the first encryption scheme is activated

FIGURE 6

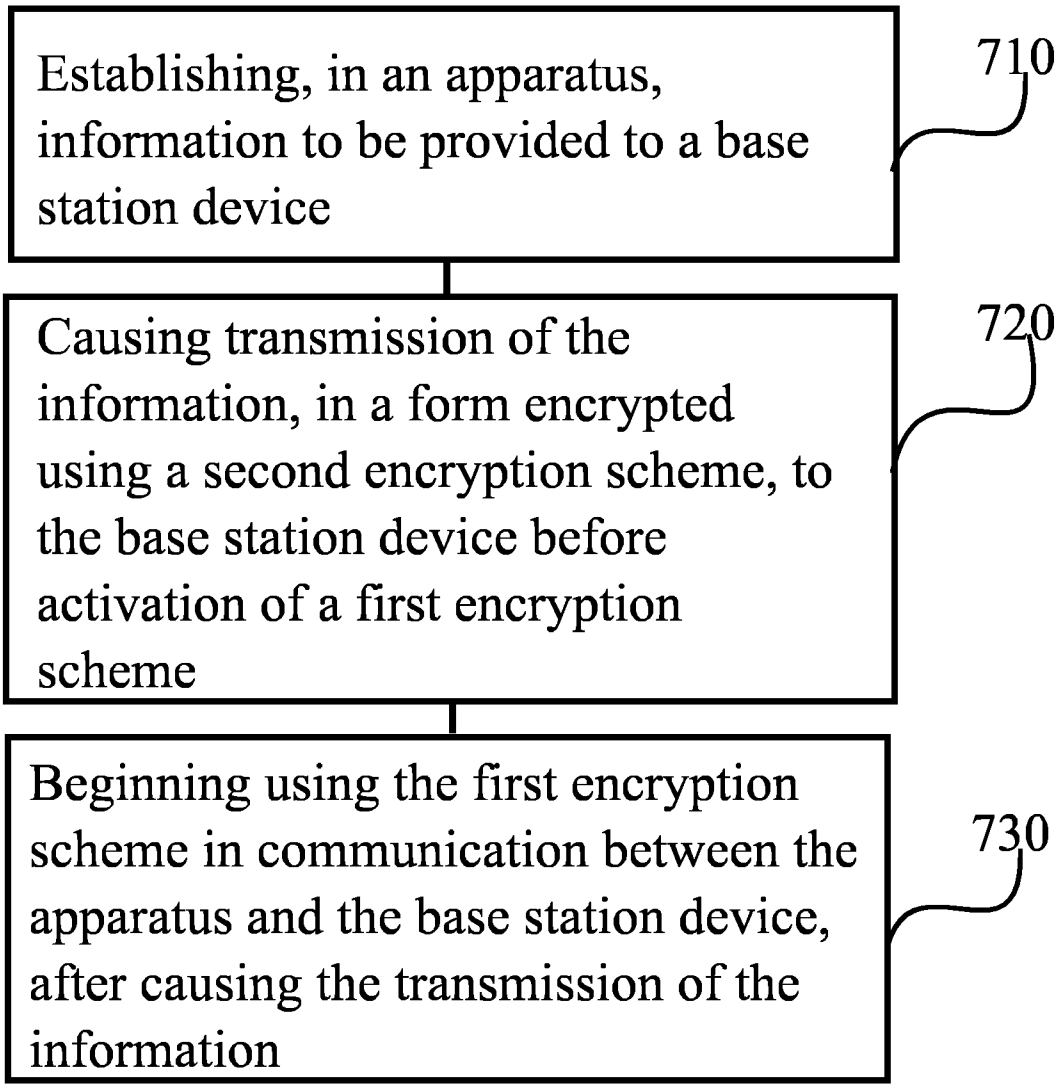
Establishing, in an apparatus, information to be provided to a base station device
710
Causing transmission of the information, in a form encrypted using a second encryption scheme, to the base station device before activation of a first encryption scheme
720
Beginning using the first encryption scheme in communication between the apparatus and the base station device, after causing the transmission of the information
730

FIGURE 7

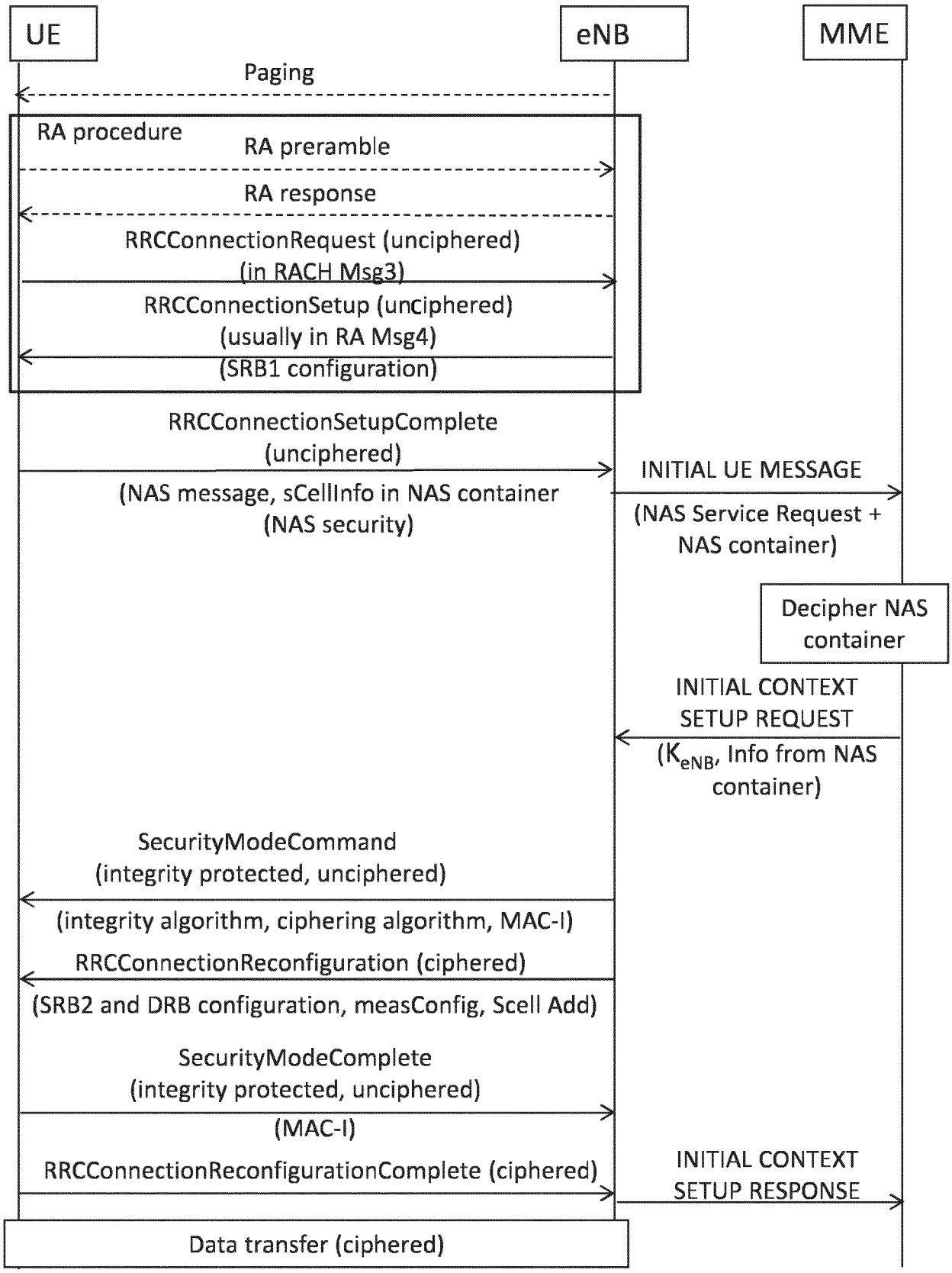
UE
eNB
MME
Paging
RA procedure
RA preramble
RA response
RRCConnectionRequest (unciphered)
(in RACH Msg3)
RRCConnectionSetup (unciphered)
(usually in RA Msg4)
(SRB1 configuration)
RRCConnectionSetupComplete
(unciphered)
(NAS message, sCellInfo in NAS container
(NAS security)
INITIAL UE MESSAGE
(NAS Service Request +
NAS container)
Decipher NAS
container
INITIAL CONTEXT
SETUP REQUEST
(K_{eNB}, Info from NAS
container)
SecurityModeCommand
(integrity protected, unciphered)
(integrity algorithm, ciphering algorithm, MAC-I)
RRCConnectionReconfiguration (ciphered)
(SRB2 and DRB configuration, measConfig, Scell Add)
SecurityModeComplete
(integrity protected, unciphered)
(MAC-I)
RRCConnectionReconfigurationComplete (ciphered)
INITIAL CONTEXT
SETUP RESPONSE
Data transfer (ciphered)

FIGURE 8

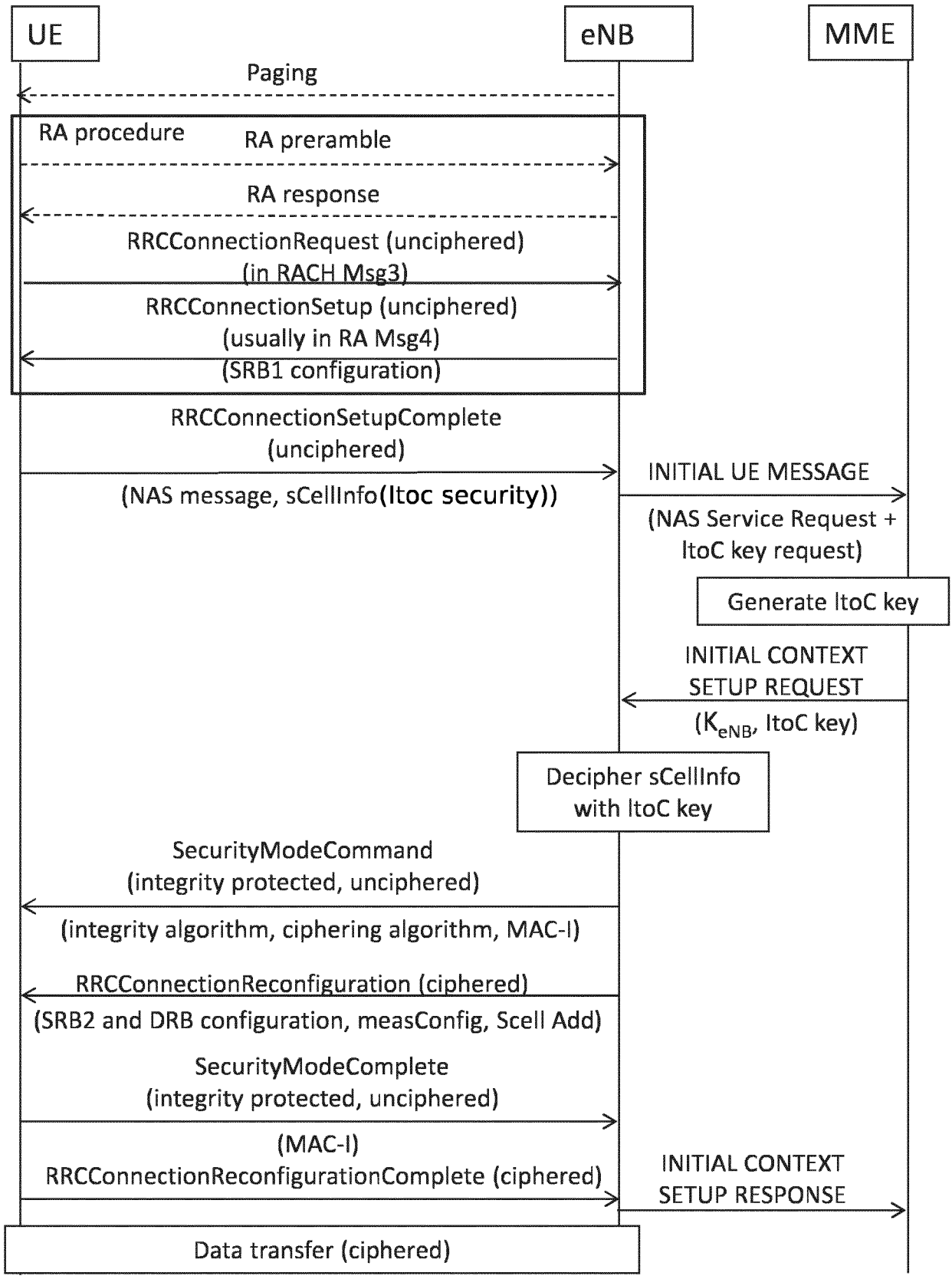
UE
eNB
MME
Paging
RA procedure
RA preramble
RA response
RRCConnectionRequest (unciphered)
(in RACH Msg3)
RRCConnectionSetup (unciphered)
(usually in RA Msg4)
(SRB1 configuration)
RRCConnectionSetupComplete
(unciphered)
(NAS message, sCellInfo(Itoc security))
INITIAL UE MESSAGE
(NAS Service Request +
ItoC key request)
Generate ItoC key
INITIAL CONTEXT
SETUP REQUEST
(K_eNB, ItoC key)
Decipher sCellInfo
with ItoC key
SecurityModeCommand
(integrity protected, unciphered)
(integrity algorithm, ciphering algorithm, MAC-I)
RRCConnectionReconfiguration (ciphered)
(SRB2 and DRB configuration, measConfig, Scell Add)
SecurityModeComplete
(integrity protected, unciphered)
(MAC-I)
RRCConnectionReconfigurationComplete (ciphered)
INITIAL CONTEXT
SETUP RESPONSE
Data transfer (ciphered)

FIGURE 9

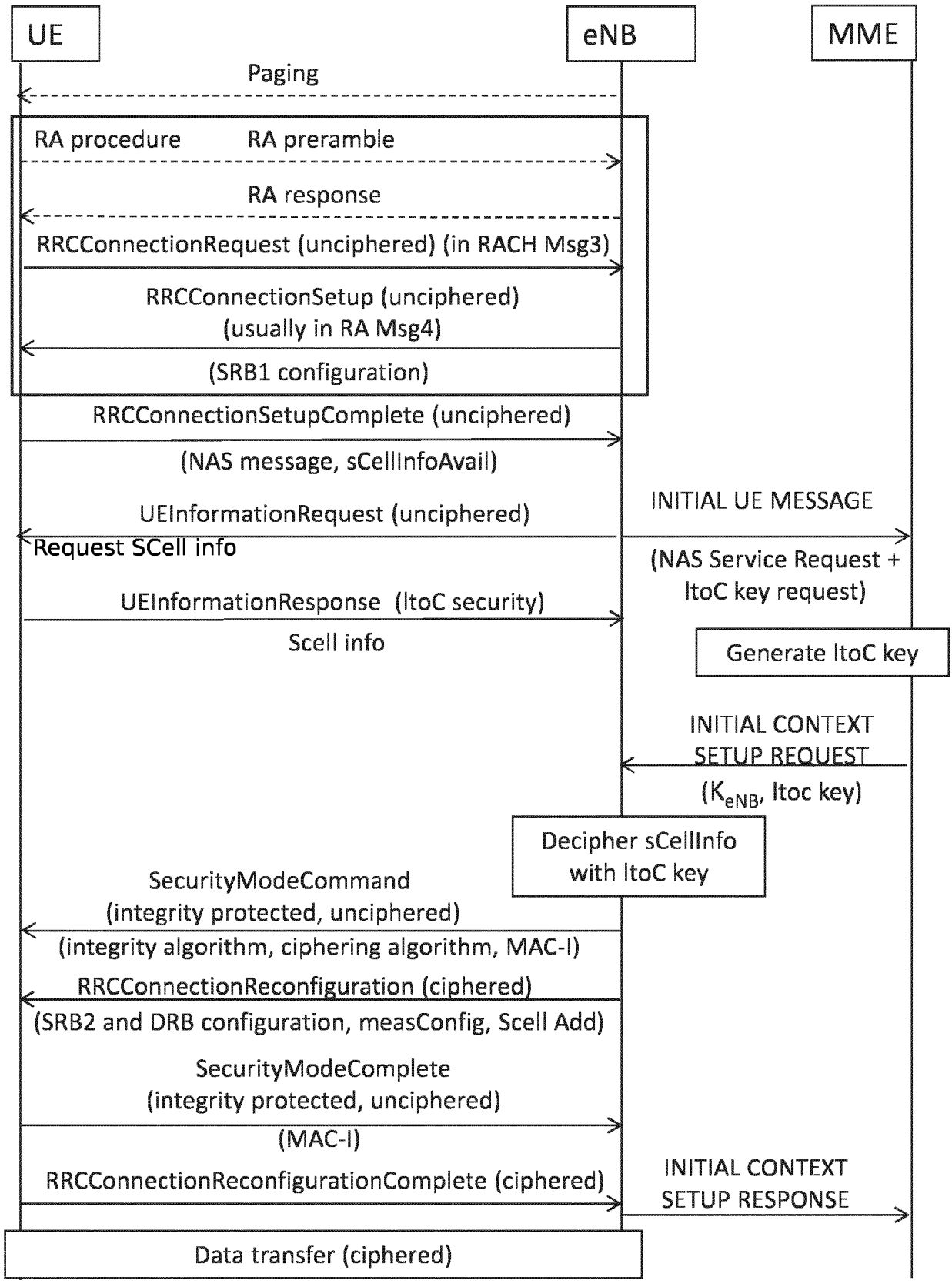
UE
eNB
MME
Paging
RA procedure
RA preramble
RA response
RRCConnectionRequest (unciphered) (in RACH Msg3)
RRCConnectionSetup (unciphered)
(usually in RA Msg4)
(SRB1 configuration)
RRCConnectionSetupComplete (unciphered)
(NAS message, sCellInfoAvail)
INITIAL UE MESSAGE
UEInformationRequest (unciphered)
Request SCell info
(NAS Service Request +
ItoC key request)
UEInformationResponse (ItoC security)
Scell info
Generate ItoC key
INITIAL CONTEXT
SETUP REQUEST
(K_{eNB}, Itoc key)
Decipher sCellInfo
with ItoC key
SecurityModeCommand
(integrity protected, unciphered)
(integrity algorithm, ciphering algorithm, MAC-I)
RRCConnectionReconfiguration (ciphered)
(SRB2 and DRB configuration, measConfig, Scell Add)
SecurityModeComplete
(integrity protected, unciphered)
(MAC-I)
RRCConnectionReconfigurationComplete (ciphered)
INITIAL CONTEXT
SETUP RESPONSE
Data transfer (ciphered)

FIGURE 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050574

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: G06F, H04L, H04W

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, WPIAP, XP3GPP, XPAIP, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPIOP, XPIPCOM, XPJPEG, XPMISC, XPOAC, XPRD, XPTK, COMPDX, INSPEC, PUBCOMP, PUBSUBS, TDB, NPL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"LTE Security II: NAS and AS Security". NMC Consulting Group, 14 October 2014. [Retrieved on 2017-01-19]. Retrieved from the Internet: <URL:http://www.netmanias.com/en/post/techdocs/5903/lte-security/lte-security-ii-nas-and-as-security> Figs. 1, 2, 8, 9, 12; the fourth and fifth paragraphs of section I; the first, second and third paragraphs of section 2.2; section 3.2	1-17, 21-36, 38-41, 43
X	"LTE Security I: LTE Security Concept and LTE Authentication". NMC Consulting Group, 31 July 2013. [Retrieved on 2017-01-19]. Retrieved from the Internet: <URL:http://www.netmanias.com/en/post/techdocs/5902/lte-security/lte-security-i-concept-and-authentication> Fig. 2; section 2.2	1-17, 21-36, 38-41, 43

☒ 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
24 January 2017 (24.01.2017)	26 January 2017 (26.01.2017)

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
Vesa-Matti Louekoski
Telephone No. +358 9 6939 500

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050574

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"S1AP View of LTE Attach & EPS Bearer Setup for two PDNs". EventHelix.com Inc, 2014. [Retrieved on 2017-01-19]. Retrieved from the Internet: <http://www.eventhelix.com/lte/attach/s1ap-lte-attach-eps-bearer-setup.pdf> Pages 1 and 3	18-20, 37, 42, 43
A	US 2015118993 A1 (RUNE JOHAN [SE] et al.) 30 April 2015 (30.04.2015) Abstract	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050574

CLASSIFICATION OF SUBJECT MATTER

IPC
G06F 21/60 (2013.01)
H04L 29/06 (2006.01)
H04W 12/08 (2009.01)
H04W 76/02 (2009.01)
H04W 76/04 (2009.01)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI2016/050574

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Extra Sheet

Invention I:

Claims 1-12, 21-32, 38, 40 and 43 (in part) are directed to apparatuses, a method, a non-transitory computer readable medium and a computer program for storing information in an apparatus, receiving the information, in encrypted form using a second encryption scheme, from a user equipment, in the apparatus, before activation of a first encryption scheme, obtaining an unencrypted form of the information, and using the encrypted form of the information to provide service to the user equipment before or after the first encryption scheme is activated.

Claims 13-17, 33-36, 39, 41 and 43 (in part) are directed to apparatuses, a method, a non-transitory computer readable medium and a computer program for establishing information to be provided to a base station device, before activation of a first encryption scheme, causing transmission of the information, in a form encrypted using a second encryption scheme, to the base station device, and beginning, after causing the transmission of the information, using the first encryption scheme in communication between the apparatus and the base station device.

Invention II : Claims 18-20, 37, 42 and 43 (in part) is directed an apparatus, a method, a non-transitory computer readable medium and a computer program for receiving an initial UE message from a base station device, performing a cryptographic operation as a response to the initial UE message, and causing transmission of an initial context setup request message as a response to the initial UE message, the initial context setup request message comprising an output of the cryptographic operation.

INTERNATIONAL SEARCH REPORT
Information on Patent Family Members

International application No.
PCT/FI2016/050574

Patent document cited in search report	Publication date	Patent family members(s)	Publication date
US 2015118993 A1	30/04/2015	CN 104205903 A	10/12/2014
		EP 2826270 A1	21/01/2015
		WO 2013135287 A1	19/09/2013