(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 4 346 251 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.04.2024 Bulletin 2024/14

(21) Application number: **23199458.3**

(22) Date of filing: **25.09.2023**

(51) International Patent Classification (IPC):
H04W 8/12 $^{(2009.01)}$ ***H04W 12/0431*** $^{(2021.01)}$
H04W 12/06 $^{(2021.01)}$

(52) Cooperative Patent Classification (CPC):
H04W 12/0431; H04W 12/06; H04W 8/12

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA
Designated Validation States:
KH MA MD TN

(30) Priority: **29.09.2022 IN 202241055934**

(71) Applicant: **Nokia Technologies Oy**
02610 Espoo (FI)

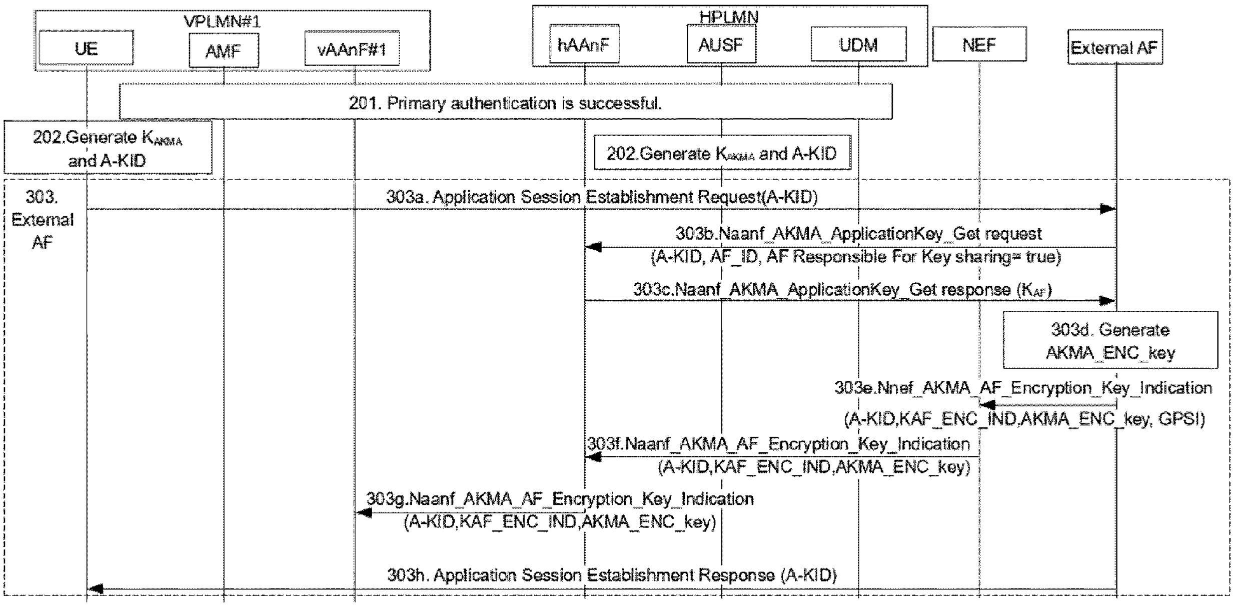
(72) Inventors:
- **KHARE, Saurabh**
  Bangalore (IN)
- **MAVUREDDI DHANASEKARAN, Ranganathan**
  Munich (DE)

(74) Representative: **Nokia EPO representatives**
Nokia Technologies Oy
Karakaari 7
02610 Espoo (FI)

(54) METHOD AND APPARATUS FOR LAWFUL INTERCEPTION FOR AKMA ROAMING ARCHITECTURE

(57) A method, apparatus, and computer program for receiving an application session establishment request comprising an authentication and key management for applications, AKMA, Key Identifier, A-KID; producing an application key request (Naanf AKMA ApplicationKey_Get request) comprising information elements AKMA Key Identifier A-KID; an application function identifier, AF_ID; and an application encryption key indication (Nnef_AKMA_AF_Encryption_Key_Indication); and sending the produced application key request (Naanf AKMA ApplicationKey_Get request) to a home AKMA anchor function, hAAnF, or to a network exposure function, NEF, for enabling lawful interception in the VPLMN.

Fig. 3


VPLMN#1
UE
AMF
vAAnF#1
HPLMN
hAAnF
AUSF
UDM
NEF
External AF
201. Primary authentication is successful.
202.Generate KAKMA and A-KID
202.Generate KAKMA and A-KID
303. External AF
303a. Application Session Establishment Request(A-KID)
303b.Naanf_AKMA_ApplicationKey_Get request
(A-KID, AF_ID, AF Responsible For Key sharing= true)
303c.Naanf_AKMA_ApplicationKey_Get response (KAF)
303d. Generate AKMA_ENC_key
303e.Nnef_AKMA_AF_Encryption_Key_Indication
(A-KID,KAF_ENC_IND,AKMA_ENC_key, GPSI)
303f.Naanf_AKMA_AF_Encryption_Key_Indication
(A-KID,KAF_ENC_IND,AKMA_ENC_key)
303g.Naanf_AKMA_AF_Encryption_Key_Indication
(A-KID,KAF_ENC_IND,AKMA_ENC_key)
303h. Application Session Establishment Response (A-KID)

Processed by Luminess, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] Various example embodiments relate to lawful interception for AKMA roaming architecture.

BACKGROUND

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

[0003] Authentication and Key management for Applications based on 3GPP credentials, AKMA, is being standardized. For example, clause 4.2 of 3GPP TS 33.535 V17.6.0 specifies that the following network elements are parts of AKMA architecture: an AKMA anchor function, AAnF, an application function, AF, a network exposure function, NEF, an authentication server function, AUSF, and a unified data management, UDM. Clause 4.3 of 3GPP TS 33.535 V17.6.0 specifies that the following service-based interfaces, SBIs, are involved in the AKMA architecture: a service-based interface exhibited by the NEF, Nnef, a service-based interface exhibited by the UDM, Nudm, and a service-based interface exhibited by the AAnF, Naanf. The AKMA architecture has been used as a solution to protect communication between user equipment, UE, and the AF, in the scenarios of proximity-based services, ProSe, and message service for massive internet of things, MioT, over the 5G System, MSGin5G. Roaming aspects have not been adequately addressed in the current release of 3GPP 17. In particular, it is desirable to standardize a new roaming architecture for the AKMA. It is further desirable that the new AKMA roaming architecture provides support for lawful interception.

[0004] An authentication proxy is missing in the AKMA. The authentication proxy in the AKMA could help to improve cost effectiveness and relieve the application servers, AS, of some security tasks.

SUMMARY

[0005] The scope of protection sought for various embodiments of the invention is set out by the independent claims. The embodiments and features, if any, described in this specification that do not fall under the scope of the independent claims are to be interpreted as examples useful for understanding various embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] 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:

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

Fig. 2 shows a simplified signaling diagram of some features of example embodiments related to using an internal application function, AF of a home public land mobile network, HPLMN, and a remote AF;

Fig. 3 shows a simplified signaling diagram of some features of example embodiments related to an external AF; and

Fig. 4 shows a block diagram of an apparatus of an example embodiment.

DETAILED DESCRIPTON OF THE DRAWINGS

[0007] 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.

[0008] Fig. 1 shows an architectural drawing of a system of an example embodiment. In Fig. 1, user equipment, UE, 110 with a mobile subscription 112 is roaming in a visited network that is a visited public land mobile network, VPLMN 120. The home and visited networks depend on the subscription used by the UE and vary for different subscriptions. The VPLMN 120 comprises normal structures and functionalities to support 3GPP 5G operations. It is useful for understanding some embodiments of present disclosure to note following parts of the VPLMN: an access and mobility management function 122; a visited PLMN AKMA anchor function, vAAnF, 124; and an internal application function, AF, 126 of the VPLMN. Fig.1 further comprises a home public land mobile network, HPLMN 130 of the subscription 112 in use by the user equipment 110. Among others, the HPLMN 130 comprises an internal Application Function, AF, 132; a unified data management 134; a home PLMN akma anchor function, hAAnF, 136; and an authentication server function, AUSF,138. The system 100 further comprises a network exposure function, NEF, 140; and an external AF 150.

[0009] In a 5G core network, 5GC, there may remain some operational and security issues in the roaming architecture for the AKMA. In this document, various embodiments are disclosed for providing for lawful interception, LI.

a) when the UE 110 is in the VPLMN 120 and the internal AF 132 of the HPLMN is used by the UE 110; or

b) when the UE 110 is in the VPLMN 120 and the external AF 150 is used by the UE 110.

[0010] In case a), the HPLMN 130 should enable decrypting the user services for LI purposes, e.g., by issuing on an authorized LI request an AKMA encryption key to a function assigned for this purpose, such as a User Plane Function, UPF (not shown). To this end, an encryption key and further information may be needed, such as replay attack protectors (nonces) applied, counters, and/or indication of a cipher algorithm used. In an example embodiment, application encryption key material term comprises the AKMA encryption key or the information required for the hAAnF or the vAAnF to produce the AKMA encryption key and any further information required to decrypt the encrypted data. In case of simplicity, the AKMA encryption key refers herein to the information with which the AKMA encryption can be decrypted.

[0011] In case b), the HPLMN 130 has no internal access to the AKMA encryption key. Instead, in an example embodiment, the external AF 150 indicates how the AKMA encryption key is formed so that the HPLMN 130 may be able to obtain the AKMA encryption key. In an example embodiment, the external AF 150 sends the application encryption material to the NEF 140 and the NEF 140 either obtains the AKMA encryption key or passes the application encryption material to the HPLMN 130 or to the VPLMN 120.

[0012] There are three main cases for the AKMA encryption key: 1) using an AKMA Application Key, K_{AF}; 2) using a derivative of the K_{AF}; and 3) using a special key that is independent of the K_{AF}.

[0013] In deriving the AKMA encryption key from the K_{AF}, the AKMA encryption key can be derived, e.g., by a key derivation function or by encrypting at least the K_{AF} or a portion thereof and optionally some further information, such as a sequence counter, timestamp, or a nonce. For example, the derived AKMA encryption key can be formed with a key derivation function from concatenated or otherwise combined K_{AF} and the nonce. The key derivation function may be advantageous in its processing cost.

[0014] The third case may arise particularly when an independently operating data center or computer cloud implements the external AF. In such a case, the neither the HPLMN nor the VPLMN can provide for the LI unless the external AF provides for such capabilities. In an example embodiment where the AKMA encryption key is based on the K_{AF}, the external AF sends an indication via the NEF to the hAAnF. If this indication is set, the hAAnF will push the AKMA encryption key to the vAAnF or to the VPLMN. Otherwise, if this indication is not set, i.e., external AF is using the special key, the hAAnF informs the VPLMN that the AKMA encryption key is not available to the HPLMN. On the other hand, if the external AF needs to send the AKMA encryption key to the vAAnF, then it is passed to the NEF and routed therefrom via the hAAnF to vAAnF. In an example embodiment, instead of the external AF sending the AKMA encryption key, the AAnF fetches the AKMA encryption key from the external AF and provides same to the vAAnF of the VPLMN. It is further possible that the special key is not issued by the external AF when requested by the HPLMN. In that case, the HPLMN may simply indicate to the VPLMN that the AKMA encryption key is not available.

[0015] Fig. 2 shows a simplified signaling diagram of some features of example embodiments related to using the internal AF of the HPLMN and the external AF. In Fig. 2, some particularly interesting information elements are indicated. However, it should be appreciated that in some example embodiments, not all the drawn information elements are transferred. Fig. 2 illustrates:

201: Successfully performing a primary authentication by the UE through the VPLMN with the HPLMN. Hence, the UE gains mobile connectivity.

202: Generating an AKMA anchor key, K_{AKMA}, and an AKMA key identifier, A-KID, by the UE and by the AUSF of the HPLMN. In the HPLMN, the AUSF informs the hAAnF of the K_{AKMA} and the A-KID.

203: This is a process of an example embodiment wherein the internal AF of the HPLMN is used.

203a: The UE sends an application session establishment request with the A-KID to the internal AF.

203b: The internal AF then sends an application key request (Naanf AKMA ApplicationKey_Get request) to the hAAnF. In an example embodiment, the application key request comprises the A-KID, the AF_ID, and a key sharing responsibility indication AF_responsible for Key_sharing set to Boolean value True.

203c: The hAAnF responds with an application key response message (Naanf AKMA ApplicationKey_Get response). In an example embodiment, the application key response message comprises the K_{AF}.

203d: The internal AF pushes the AKMA encryption key to the vAAnF with an application encryption indication (KAF_ENC_IND), and

203e: The internal AF also sends an application session establishment response message to the UE. The application encryption indication (KAF_ENC_IND) of the previous step indicates by a first value (e.g., 1) that the K_{AF} is used as an AKMA encryption key; by a second value (e.g., 2), that a derivative of the K_{AF} is used as the AKMA encryption key; and by a third value (e.g., 3) that a special key independent of the K_{AF} is used as the AKMA encryption key.

204: This is a process of an example embodiment wherein the external AF of the HPLMN is used.

204a: The UE sends an application session establishment request with the A-KID to the external AF, as in 203a to the internal AF.

204b: The external AF produces and sends an application key request (Naanf AKMA ApplicationKey_Get request) comprising the A-KID; the AF_ID; and the application encryption indication (KAF_ENC_IND) explained in connection with step 203d.

204c: The hAAnF responds to the external AF with the application key response. In an example embodiment, the application key response comprises the K_{AF}.

204d: The hAAnF pushes or otherwise provides the

K_{AF} to the vAAnF together with the application encryption indication (KAF_ENC_IND).

[0016] In an example embodiment, if the indication value received at hAAnF has a third value (e.g., 3), indicating that a special AKMA encryption key is used for encryption', the hAAnF shall provide only the indication to VPLMN without any keys, unless the hAAnF has received the special AKMA encryption key from the NEF. Fig. 3 shows an example embodiment in which the external AF has provided the NEF with the special AKMA encryption key and the same has been forwarded by the NEF to the hAAnF.

[0017] The application encryption indication provides certainty on the key material delivered by HPLMN to VPLMN. Without this indication, the VPLMN could not be certain whether the K_{AF} is used as the AKMA encryption key or a K_{AF} derivative is used for as the AKMA encryption key, or a key independent of K_{AF} is used as the AKMA encryption key.

[0018] 204e: The vAAnF stores the AKMA encryption key for enabling a subsequent lawful interception.

[0019] 204f: The external AF sends an application session establishment response message to the UE, as the internal AF in 203e.

[0020] Fig. 3 shows a simplified signalling diagram of some features of example embodiments related to an external AF, comprising steps:

201-202: as in Fig. 2.

303: This is a process of an example embodiment wherein the external AF is used.

303a: The UE sends an application session establishment request with the A-KID to the external AF.

303b: The external AF sends the application key request, (Naanf AKMA ApplicationKey_Get request) to the hAAnF. In an example embodiment, the application key request comprises the A-KID, the AF_ID, and a key sharing responsibility indication AF_responsible for Key_sharing set to Boolean value True. Based on this indication, AAnF does not share any key to VPLMN.

303c: The hAAnF responds with the application key response (Naanf AKMA ApplicationKey_Get response) message with K_{AF} to the external AF.

303d: The external AF generates the AKMA encryption key.

303e: The external AF sends an encryption key indication message (Nnef_AKMA_AF_Encryption_Key_Indication) to the NEF. Note: as the interface here is the Nnef, the message is accordingly named as the Nnef_AKMA _AF_Encryption_Key_Indication. In an example embodiment, the encryption key indication message comprises the A-KID, KAF_ENC_IND, AKMA_ENC_key and GPSI. Note: if the external AF has formed the AKMA_ENC_key of or based on the KAF, AKMA_ENC_key may be omitted in an example embodiment. In another example embodiment, the KAF_ENC_IND is omitted.

303f: The NEF forwards the AKMA encryption key (AKMA_ENC_KEY) by an encryption key indication message (Naanf AKMA AF_Encryption_Key_Indication) to the hAAnF.

303g: the hAAnF sends the KAF_ENC_IND and/or the AKMA encryption key by an encryption key indication message (Naanf_AKMA_AF_Encryption_Key_Indication) to the vAAnF. In an example embodiment, this message further comprises the A-KID.

303h: At some point of time, the external AF sends the Application session establishment response to the UE.

[0021] Fig. 4 shows a block diagram of an apparatus 400 according to an embodiment of the invention. In an example embodiment, the apparatus 400 is used to implement one or more of the network functions or the UE. Moreover, it is possible that the apparatus 400 be used to implement one or more network functions for a given number or particular users. For example, the hAAnF may be implemented for one user by the apparatus 400 and with other equipment for another user.

[0022] The apparatus 400 comprises at least one memory 440 comprising instructions 446 and/or data 448. The at least one memory 440 may comprise non-volatile memory 444 and/or main memory 442. The apparatus 400 further comprises at least one processor 420 configured to execute the instructions 446 stored in the at least one memory 440 for controlling the operation of the apparatus 400, and at least one communication unit 410 for communicating with other nodes. The instructions 446 and/or the data 448, or parts thereof, may be transferred by the at least one processor 420 between the non-volatile memory 444 and the main memory 442. The at least one memory 440 may comprise random access memory (RAM) and/or read-only memory (ROM). The at least one memory 440 may comprise at least one RAM chip, and/or at least one ROM chip, and/or at least one flash memory chip. The at least one memory 440 may comprise solid-state, magnetic, and/or optical memory, for example. The at least one memory 440 may be at least in part accessible to the at least one processor 420. The at least one memory 440 may be at least in part external to the apparatus 400. The at least one communication unit 410 may comprise, for example, at least one of: a local area network (LAN) port; a wireless local area network (WLAN) unit; a Bluetooth unit; a cellular data communication unit; or a satellite data communication unit. The at least one processor 420 may comprise, 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; or a microcontroller. The apparatus may comprise a user interface 430, such as a keyboard and/or a graphical user interface (GUI).

[0023] The apparatus 400 as drawn can be a dedicated computer or server computer, for example. In an example embodiment, the apparatus is implemented using cloud computing such that the apparatus comprises a plurality of processors and memories that implement a large number of different functionalities including, for example, one or more of the network functions described in the foregoing. The apparatus can further support virtualization such that one or more of different functionalities provided by the apparatus may be implemented on a virtualization platform, comprising for example one or more virtualized computers, virtualized computer servers, and/or virtualized network entities running on one or more virtualization servers.

[0024] As used in this application, the term "circuitry" may refer to one or more or all of the following:

(a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry) and;

(b) combinations of hardware circuits and software, such as (as applicable):

(i) a combination of analog and/or digital hardware circuit(s) with software/firmware; and

(ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions); and

(c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

[0025] This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other computing or network device.

[0026] 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 lawful interception support can be improved in 5G networks. Another technical effect of one or more of the example embodiments disclosed herein is that processing related to application function encryption may be reduced for roaming UE.

[0027] 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 transitory or 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. 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.

[0028] 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.

[0029] 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.

[0030] 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.

[0031] As used herein, "at least one of the following: <a list of two or more elements>" and "at least one of <a list of two or more elements>" and similar wording, where the list of two or more elements are joined by "and" or "or", mean at least any one of the elements, or at least any two or more of the elements, or at least all the elements.

Claims

1. An apparatus, comprising

means for receiving from user equipment an application session establishment request comprising as a key identifier an Authentication and Key management for Applications, AKMA, Key Identifier, A-KID;

means for producing an application key request (Naanf AKMA ApplicationKey_Get request) comprising as information elements the A-KID, an application function identifier, AF_ID, and a key sharing responsibility indication of a home AKMA Anchor Function, hAAnF, of a home public land mobile network, HPLMN, of a mobile operator whose cellular subscription is in use by the mobile station;

wherein the key sharing responsibility indication is informative on whether or not the hAAnF should share application encryption key material;

means for sending the application key request to the hAAnF;

means for receiving an application key response (Naanf AKMA ApplicationKey_Get response) responsively to the sending of the application key request to the hAAnF, the application key response comprising an AKMA Application Key, K_{AF};

means for producing application encryption key material, based at least on the received application key response; and

means for providing a visited AKMA Anchor Function, vAAnF, of the user equipment, with an application encryption indication (KAF_ENC_IND) and the application encryption key material, for enabling lawful interception in the visited public land mobile network.

2. The apparatus of claim 1, wherein the apparatus is an application function of the HPLMN.

3. The apparatus of claim 1 or 2, wherein the means for producing the application encryption key material is further configured to perform:

in case that the K_{AF} as such is used as an AKMA encryption key, arranging that the application encryption key material comprises or consists of the K_{AF}, and the application encryption indication (KAF_ENC_IND) is assigned a first value;

in case that a derivative of the K_{AF} is used as the AKMA encryption key, arranging that the application encryption key material comprises the K_{AF} and/or further information such as a replay attack protector or nonce, and the application encryption indication (KAF_ENC_IND) is assigned a second value; and

in case that a special key independent of the K_{AF} is used as an AKMA encryption key, arranging that the application encryption key material comprises the special key, and the application encryption indication (KAF_ENC_IND) is assigned a third value.

4. An apparatus, wherein the apparatus is a visited AKMA Anchor Function, vAAnF, of a visited public land mobile network, VPLMN; the apparatus comprising

means for receiving from another AKMA Anchor Function or from an application function, an application encryption indication (KAF_ENC_IND) and optionally application encryption key material, for lawful interception in the VPLMN; and

means for providing a decrypting entity with the application encryption key material or an AKMA encryption key obtained using the AKMA encryption key, responsively to receiving a request from an authorized entity to enable lawful interception.

5. The apparatus of claim 4, further comprising means for obtaining the AKMA encryption key based on at least the application encryption key material and/or the value of the application encryption indication (KAF_ENC_ID).

6. The apparatus of claim 5, wherein the means for obtaining the AKMA encryption key further comprises

means for arranging that the AKMA encryption key comprises or consists of the K_{AF}, responsively to the application encryption indication (KAF_ENC_IND) indicating that the K_{AF} is used as the AKMA encryption key;

means for arranging that the AKMA encryption key comprises at least one of: the AKMA encryption key derived from K_{AF}, or source data from which the AKMA encryption key is derivable from using the K_{AF}, responsively to the application encryption indication (KAF_ENC_IND) indicating that the AKMA encryption key is derived the from K_{AF};

means for arranging that the AKMA encryption key comprises or consists of an indication indicating that the K_{AF} is not used for encryption, responsively to the application encryption indication (KAF_ENC_IND) indicating that the K_{AF} is not used for encryption; and

means for storing the AKMA encryption key.

7. The apparatus of any one of claims 4 to 6, wherein the means for providing decrypting entity with the AKMA encryption key further comprises

means for providing the decrypting entity with the AKMA encryption key , responsively to the application encryption indication (KAF_ENC_IND) indicating that the K_{AF} is used as the AKMA encryption key;

means for providing the decrypting entity with at least one of the following , responsively to the application encryption indication (KAF_ENC_IND) indicating that the AKMA encryption key is derived the from K_{AF}:

the AKMA encryption key derived from K_{AF}, or

the application encryption key material from which the AKMA encryption key is derivable using the K_{AF}; and

means for providing the decrypting entity with an indication that the K_{AF} is not used for encryption, responsively to the application encryption indication (KAF_ENC_IND) indicating that the K_{AF} is not used for encryption.

8. The apparatus of claim 7, wherein the means for providing an indication that the K_{AF} is not used for encryption to the decrypting entity, responsively to the application encryption indication (KAF_ENC_IND) indicating that the K_{AF} is not used for encryption, is further configured to provide the decrypting entity with a special encryption key when available.

9. An apparatus comprising

means for receiving an application session establishment request comprising an authentication and key management for applications, AKMA, Key Identifier, A-KID;
means for producing an application key request (Naanf AKMA ApplicationKey_Get request) comprising information elements AKMA Key Identifier A-KID; an application function identifier, AF_ID; and an application encryption key indication (Nnef_AKMA_AF_Encryption_Key_Indication); and
means for sending the produced application key request (Naanf AKMA ApplicationKey_Get request) to a home AKMA anchor function, hAAnF, or to a network exposure function, NEF, for enabling lawful interception in the VPLMN.

10. The apparatus of claim 9, further comprising means for receiving, responsively to the sent application key request, an application key response (Naanf AKMA ApplicationKey_Get response) comprising an AKMA Application Key (K_{AF}).

11. The apparatus of claim 10, further comprising means for generating an AKMA encryption key (AKMA_ENC_key) using the AKMA Application Key (K_{AF}), responsively to the receiving of the application key response (Naanf AKMA ApplicationKey_Get response).

12. The apparatus of claim 11 further comprising

means for generating an application function encryption key indication message (Nnef_AKMA_AF_Encryption_Key_Indication) comprising or indicating each of the following: the A-KID; the AKMA encryption key; and a generic public subscriber identifier; and
means for sending the application function encryption key indication message (Nnef_AKMA_AF_Encryption_Key_Indication) to the network exposure function.

13. The apparatus of claim 9, further comprising

means for deriving the AKMA encryption key from application encryption key material comprising the AKMA Application Key (K_{AF}); wherein
the means for producing an application key request is configured to contain the application encryption key material in the application key request.

14. A system comprising the apparatus of any one of claims 1 to 3 and the apparatus of any one of claims 4, 5, 6, 7, or 8.

Fig. 1

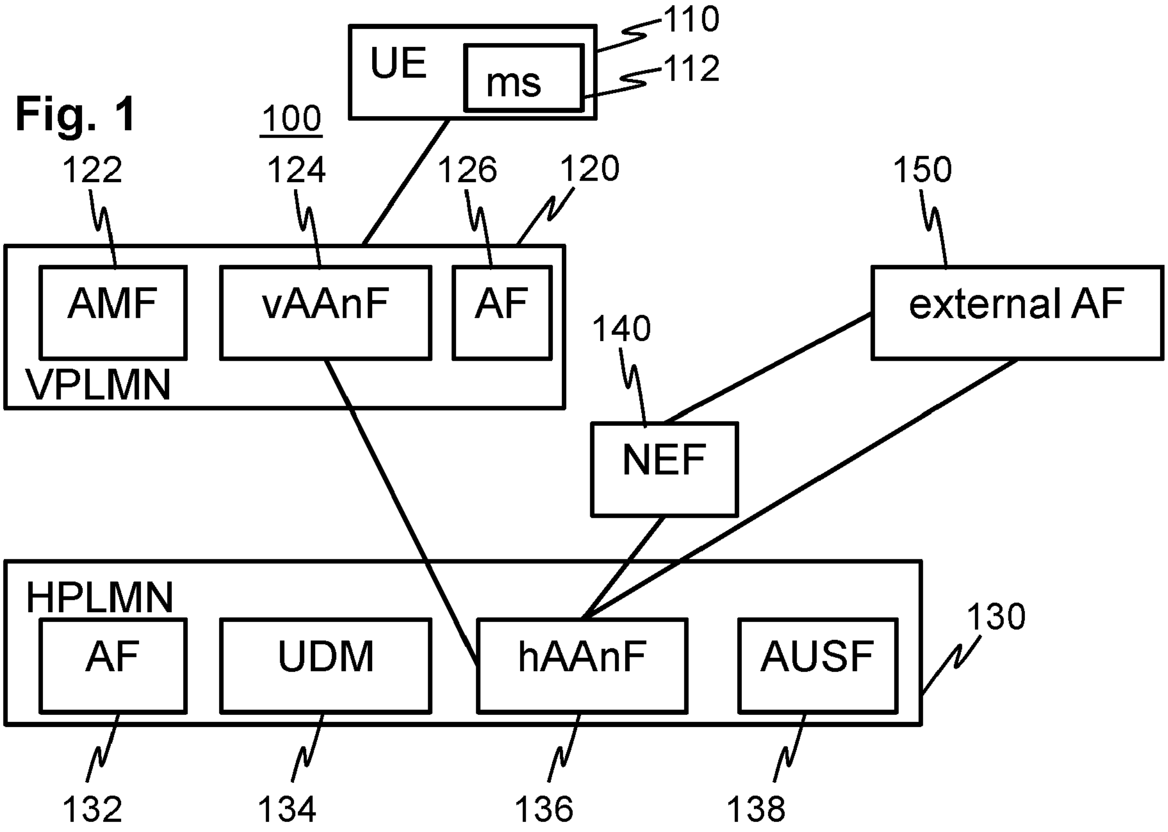

110
UE
ms
112
100
122
124
126
120
150
AMF
vAAnF
AF
external AF
VPLMN
140
NEF
HPLMN
AF
UDM
hAAnF
AUSF
130
132
134
136
138

Fig. 4

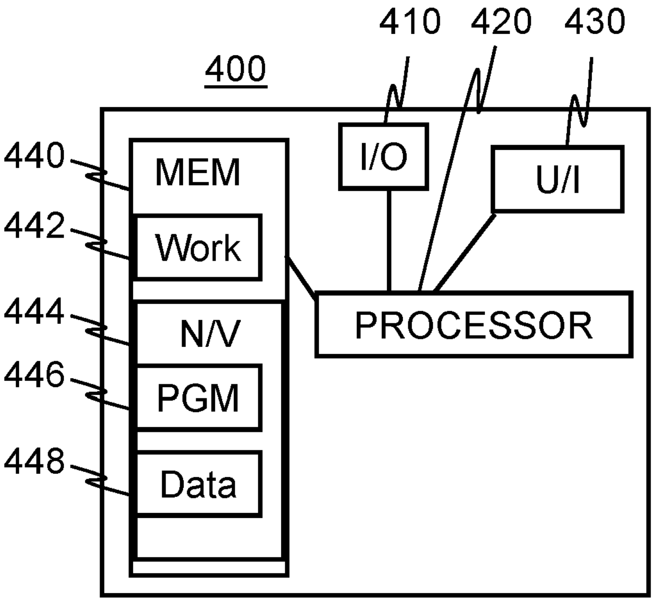

410
420
430
400
440
MEM
442
Work
444
N/V
446
PGM
448
Data
I/O
U/I
PROCESSOR

Fig. 2

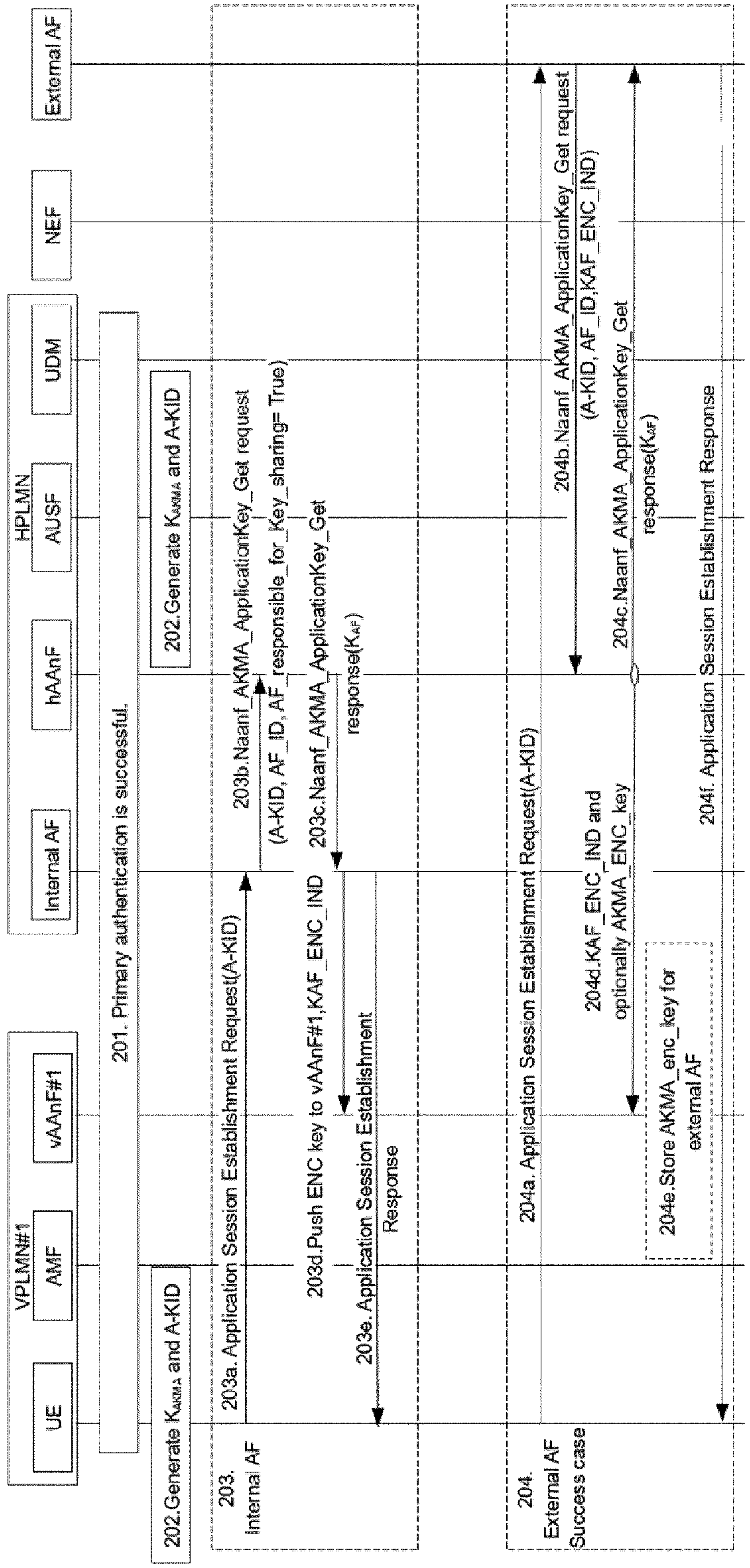
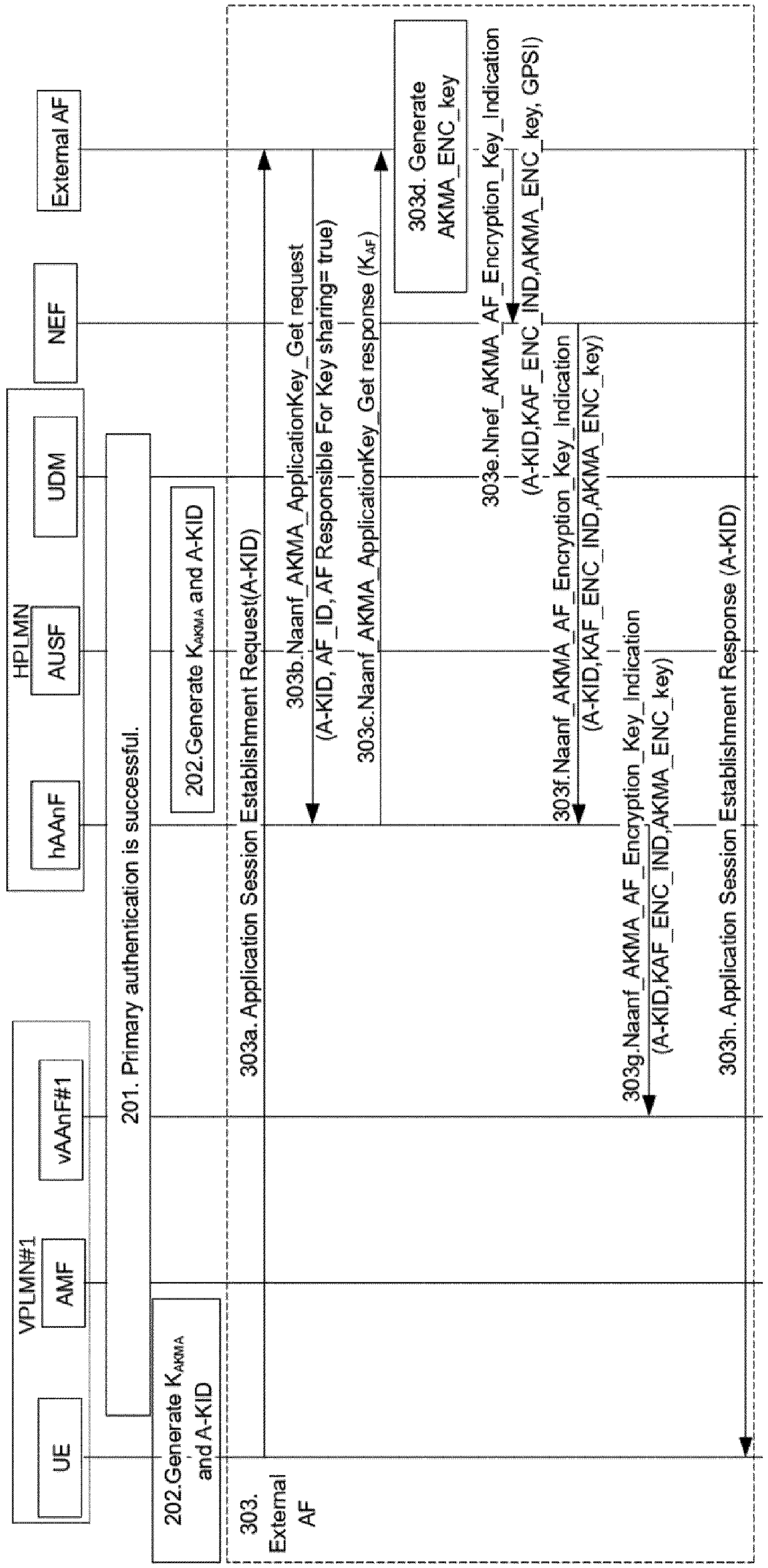

VPLMN#1
UE
AMF
vAAnF#1
HPLMN
Internal AF
hAAnF
AUSF
UDM
NEF
External AF
201. Primary authentication is successful.
202.Generate K_{AKMA} and A-KID
202.Generate K_{AKMA} and A-KID
203. Internal AF
203a. Application Session Establishment Request(A-KID)
203b.Naanf_AKMA_ApplicationKey_Get request
(A-KID, AF_ID, AF_responsible_for_Key_sharing= True)
203c.Naanf_AKMA_ApplicationKey_Get
response(K_{AF})
203d.Push ENC key to vAAnF#1,KAF_ENC_IND
203e. Application Session Establishment
Response
204. External AF Success case
204a. Application Session Establishment Request(A-KID)
204b.Naanf_AKMA_ApplicationKey_Get request
(A-KID, AF_ID,KAF_ENC_IND)
204c.Naanf_AKMA_ApplicationKey_Get
response(K_{AF})
204d.KAF_ENC_IND and
optionally AKMA_ENC_key
204e.Store AKMA_enc_key for
external AF
204f. Application Session Establishment Response

Fig. 3


UE
VPLMN#1
AMF
vAAnF#1
HPLMN
hAAnF
AUSF
UDM
NEF
External AF
201. Primary authentication is successful.
202.Generate K_{AKMA} and A-KID
202.Generate K_{AKMA} and A-KID
303. External AF
303a. Application Session Establishment Request(A-KID)
303b.Naanf_AKMA_ApplicationKey_Get request
(A-KID, AF_ID, AF Responsible For Key sharing= true)
303c.Naanf_AKMA_ApplicationKey_Get response (K_{AF})
303d. Generate AKMA_ENC_key
303e.Nnef_AKMA_AF_Encryption_Key_Indication
(A-KID,KAF_ENC_IND,AKMA_ENC_key, GPSI)
303f.Naanf_AKMA_AF_Encryption_Key_Indication
(A-KID,KAF_ENC_IND,AKMA_ENC_key)
303g.Naanf_AKMA_AF_Encryption_Key_Indication
(A-KID,KAF_ENC_IND,AKMA_ENC_key)
303h. Application Session Establishment Response (A-KID)

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 23 19 9458

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	NOKIA ET AL: "Solution on AKMA roaming", 3GPP DRAFT; S3-221634, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG3, no. e-meeting; 20220627 - 20220701 3 July 2022 (2022-07-03), XP052257894, Retrieved from the Internet: URL:https://ftp.3gpp.org/tsg_sa/WG3_Security/TSGS3_107e-AdHoc/Docs/S3-221634.zip S3-221634_was1352 Solution for AKMA Roaming.doc [retrieved on 2022-07-03]	1,2,5, 9-11,13, 14	INV. H04W8/12 H04W12/0431 H04W12/06
A	* figure 6.X.2.1 *	3,4,6-8, 12	

X	US 2022/210636 A1 (GUPTA VARINI [IN] ET AL) 30 June 2022 (2022-06-30)	4	TECHNICAL FIELDS SEARCHED (IPC)
Y	* paragraph [0119] - paragraph [0120]; figures 3,6 *	1,2,5, 9-11,13, 14	H04W
A		3,6-8,12	

The present search report has been drawn up for all claims

2

Place of search	Date of completion of the search	Examiner
Munich	1 February 2024	Padilla Serrano, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 23 19 9458

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

01-02-2024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2022210636 A1	30-06-2022	KR 20230125262 A	29-08-2023
		US 2022210636 A1	30-06-2022
		WO 2022146014 A1	07-07-2022

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82