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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 September 2017 (21.09.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/160227 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)
H04W 12/04 (2009.01) *H04W 4/00* (2009.01)

(21) International Application Number:
PCT/SG2017/050095

(22) International Filing Date:
1 March 2017 (01.03.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10201602129U 18 March 2016 (18.03.2016) SG

(71) Applicant: **HUAWEI INTERNATIONAL PTE. LTD.** [SG/SG]; 15A, Changi Business Park Central 1, #03-03, Singapore 486035 (SG).

(72) Inventors: **SHI, Jie**; 20, Teletech Park, Singapore Science Park II, Science Park Road, #03-31, Singapore 117674 (SG). **KANG, Xin**; 20, Teletech Park, Singapore Science Park II, Science Park Road, #03-31, Singapore 117674 (SG). **WANG, Haiguang**; 20, Teletech Park, Singapore Science Park II, Science Park Road, #03-31, Singapore 117674 (SG).

(74) Agent: **ALLEN & GLEDHILL LLP**; One Marina Boulevard #28-00, Singapore 018989 (SG).

(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, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: METHOD AND SYSTEM FOR KEY GENERATION AND SERVICE-BASED AUTHENTICATION IN MOBILE NETWORK

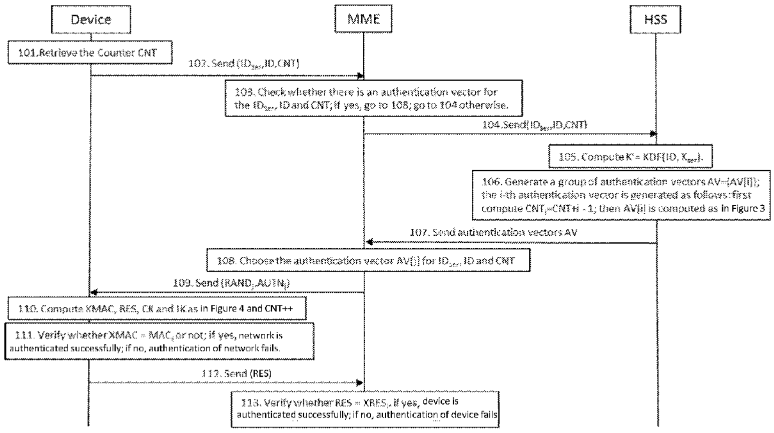
Device
MME
HSS
101.Retrieve the Counter CNT
102. Send (ID_{ser},ID,CNT)
103. Check whether there is an authentication vector for the ID_{ser}, ID and CNT; if yes, go to 108; go to 104 otherwise.
104.Send(ID_{ser},ID,CNT)
105. Compute K' = KDF(ID, K_{ser}).
106. Generate a group of authentication vectors AV={AV[i]}; the i-th authentication vector is generated as follows: first compute CNT_i=CNT+i - 1; then AV[i] is computed as in Figure 3
107. Send authentication vectors AV
108. Choose the authentication vector AV[j] for ID_{ser}, ID and CNT
109. Send ($RAND_j$,$AUTN_j$)
110. Compute XMAC, RES, CK and IK as in Figure 4 and CNT++
111. Verify whether XMAC = MAC_j or not; if yes, network is authenticated successfully; if no, authentication of network fails.
112. Send (RES)
113. Verify whether RES = $XRES_j$, if yes, device is authenticated successfully; if no, authentication of device fails

Figure 2

(57) **Abstract**: Embodiments of the invention provide key generation and authentication methods that dynamically generate device credentials e.g. device key, at the core network during authentication procedure, and thereby eliminating the need to store device credentials, e.g. device key, at the core network. Particularly, at a core network node, e.g. HSS, upon receiving an authentication message which at least includes a device identifier and a service identifier, the core network node generates a device key based at least on the device identifier and a service key which is stored at the core network node and associated with the service identifier; and uses the generated device key to authenticate a device associated with the device identifier.

WO 2017/160227 A1

METHOD AND SYSTEM FOR KEY GENERATION AND SERVICE-BASED AUTHENTICATION IN MOBILE NETWORK

Field of Invention

The invention relates to method, system and apparatus for service-based authentication in mobile/cellular/telecommunication networks between a core network and Internet of Things (IoT) devices.

Background

In current mobile network, i.e. third generation (3G)/ fourth generation (4G), each User Equipment (UE) performs mutual authentication with core network while connecting to mobile network. Figure 1 shows a mutual authentication for 4G called Evolved Packet System Authentication and Key Agreement (EPS AKA). In the EPS AKA procedure, UE first sends an Attach Request to a Mobility Management Entity (MME). The MME forwards the Attach Request to the Home Subscriber Server (HSS) which subsequently generates authentication vectors based on the credentials shared with UE. The authentication vectors are sent to MME which subsequently sends authentication material to UE. UE authenticates the network and then sends an authentication code to MME. MME verifies the authentication code and authenticates the UE. After authentication, UE exchanges key material with MME and eNB to further generate session keys for control and data plane. The credential material used in EPS AKA is shared between UE and HSS, and is different for different UEs. Since the EPS AKA protocol is based on symmetric key cryptography, which requires that the UE and core network (i.e., HSS) share a same credential, it is necessary for the HSS to store the credentials of all UEs.

In the future Internet of Things (IoT) era, the number of IoT devices will be huge and is believed to reach up to 50 billion by year 2020. If the EPS AKA authentication procedure were applied for these IoT devices, it is necessary for the HSS to store the credentials of all these devices. The costs, including setting up and maintaining HSS and potential license fee, will be huge to mobile operators. Another problem is that the EPS AKA protocol is irrelative to IoT services which may be not suitable for fifth generation mobile networks (5G), which is defined to be service-centric.

U.S. patent application publication no. US2011/0269423A1 proposed a method of distributing user access credentials to a client device (e.g. UE) through a services manager. The client device will use the access credentials to authenticate with network. Particularly, a network service provider such as a mobile operator may distribute user access (e.g., Universal Subscriber Identity Module or "USIM") credentials to a services manager via a USIM vendor. A client device will authenticate with the services manager to obtain a set of USIM credentials upon successful authentication and further use the received USIM credential to authenticate with the network service provider. After successful authentication, the network service provider may provide the client device with wireless services.

While US 2011/0269423 A1 provides a method to distribute user access credential to a client device through a service manager, which is service-relative and may be suitable for 5G, the costs of HSS are still very high.

In view of the above and other issues, authentication schemes that would reduce HSS storage requirements and HSS costs would be highly desirable.

Summary

Embodiments of the invention provide key generation and authentication methods that provide dynamic generation of device credentials e.g. device key, at a core network, e.g. HSS, during authentication procedure. This eliminates the need to store device credentials at the core network prior to and after authentication procedure and thereby reduces storage requirements at the core network, e.g. HSS.

According to a first aspect of the invention, a key generation and authentication method is provided, wherein the method comprises:

receiving, at a core network node, an authentication message which at least includes a device identifier and a service identifier;

generating, at the core network node, a device key based at least on the device identifier and a service key which is stored at the core network node and associated with the service identifier; and

using the generated device key to authenticate a device associated with the device identifier.

With reference to the first aspect, in a first possible implementation manner of the first aspect, the step of using the generated device key to authenticate a device associated with the device identifier further comprises:

generating at least one authentication vector based at least on the device key;

transmitting the at least one authentication vector to the device;

receiving, from the device, a response to the at least one authentication vector; and

authenticating the device based on the received response.

With reference to the first possible implementation manner of the first aspect, in a second possible implementation manner of the first aspect, wherein the authentication message further includes an initial counter value;wherein the core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server; andwherein generating at least one authentication vector based at least on the device key is performed at the one of HSS and AAA server, and wherein generating at least one authentication vector based at least on the device key, comprises:

generating a random number (RAND);

generating a sequential counter value based on the initial counter value;

generating a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generating an authentication token (AUTN) based on the message authentication code (MAC); and

acquiring the authentication vector according to the RAND, the XRES and the AUTN;

wherein after generating at least one authentication vector based at least on the device key, the method further comprises: transmitting the at least one authentication vector to a MME; and choosing, at the MME, a corresponding one of the at least one authentication vector based on the device identifier, the service identifier and the initial counter value;

wherein transmitting the at least one authentication vector to the device further includes:

transmitting, to a device, a corresponding random number and a corresponding authentication token which are included in the corresponding one of the at least one authentication vector; and

wherein authenticating the device based on the received response further includes:

successfully authenticating the device, at the MME, if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal, wherein the XRES is included in the authentication vector.

With reference to the second possible implementation manner of the first aspect, in a third possible implementation manner of the first aspect,

the step of wherein the authentication message further includes a nonce;

wherein the generating at least one authentication vector based at least on the generated device key comprises :

generating a random number (RAND); and

generating a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

wherein after the generating at least one authentication vector based at least on the generated device key, the method further comprises:

generating an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);wherein the transmitting the at least one the authentication vector to the device comprises:

Transmitting the random number and the message authentication code (MAC) to the device; and

wherein authenticating the device based on the received response comprises:

successfully authenticating the device, at the MME, if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal.

With reference to the third possible implementation manner of the first aspect, in a fourth possible implementation manner of the first aspect,
generating a random number (RAND) is performed at the one of HSS and AAA server; and wherein generating at least one authentication vector based at least on the device key is performed at the one of HSS and AAA server.

With reference to the third possible implementation manner of the first aspect, in a fifth possible implementation manner of the first aspect, wherein generating a random number (RAND) is performed at the MME; and wherein generating at least one authentication vector based at least on the device key is performed at the MME.

With reference to the first possible implementation manner of the first aspect, in a sixth possible implementation manner of the first aspect, wherein the core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server; and wherein generating at least one authentication vector based at least on the device key is performed at the one of HSS and AAA server, wherein the generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND);

generating a message authentication code (MAC) based at least on the device key and a sequence number which is stored at the HSS and associated with the device identifier;

generating an authentication token (AUTN) based on the message authentication code (MAC); and

acquiring the authentication vector according to the random number and the authentication token;

wherein after the generating at least one authentication vector based at least on the device key, the method further comprises:

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number (RAND); transmitting the at least one authentication vector to a MME; and

choosing, at the MME, a corresponding one of the at least one authentication vector based on the device identifier and the service identifier ;

wherein transmitting the at least one authentication vector to the device comprises:

transmitting, to a device, a corresponding random number and a corresponding authentication token included in the corresponding one of the at least one authentication vector; and

wherein authenticating the device based on the received response comprises:

successfully authenticating the device if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal.

According to a second aspect of the invention, a key generation and authentication system is provided wherein the system comprises:a key generation unit provided at a core network node, the key generation unit is configured to:

receive an authentication message which at least includes a device identifier and a service identifier;

generate a device key based at least on the device identifier and a service key which is stored at the core network node and associated with the service identifier; and

an authentication unit provided at a core network node, the authentication unit is configured to:

use the generated device key to authenticate a device associated with the device identifier.

With reference to the second aspect, in a first possible implementation manner of the second aspect, the system further comprises an authentication vector generation unit and a communications unit:

a communications unit configured to: transmit the at least one authentication vector to the device; and

the authentication vector generation unit is further configured to: generate at least one authentication vector based at least on the device key; and

the authentication unit is further configured to: receive from the device a response to the at least one authentication vector; and authenticate the device based on the received response.

With reference to the first possible implementation manner of the second aspect, in a second possible implementation,

the key generation unit is further configured to: receive an initial counter value;

the authentication vector generation unit is further configured to:

generate a random number (RAND);

generate a sequential counter value based on the initial counter value;

generate a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generate an authentication token (AUTN) based on the message authentication code (MAC); and

acquire the authentication vector according to the RAND, the XRES and the AUTN;

the communications unit is further configured to: transmit the at least one authentication vector to a Mobility Management Entity (MME);

the authentication vector generation unit is further configured to: choose, at the MME, a corresponding one of the at least one authentication vector based on the device identifier, the service identifier and the initial counter value;

the communications unit is further configured to: transmit, to the device, a corresponding random number and a corresponding authentication token (AUTN) included in the corresponding one of the at least one authentication vector; and

the authentication unit is further configured to: successfully authenticate the device if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the XRES are equal, wherein the XRES is included in the authentication vector.

With reference to the first possible implementation manner of the second aspect, in a third possible implementation,

the authentication message further includes a nonce;

the authentication vector generation unit is further configured to:

generate a random number (RAND); and

generate a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

the communications unit is further configured to: transmit the random number (RAND) and the message authentication code (MAC) to the device; and

the authentication unit is further configured to: successfully authenticate the device, at the MME, if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal.

With reference to the first possible implementation manner of the second aspect, in a fourth possible implementation,

the authentication vector generation unit is further configured to:

generate a random number (RAND);

generate a message authentication code (MAC) based at least on the device key and a sequence number which is stored at the HSS and associated with the device identifier;

generate an authentication token (AUTN) based on the message authentication code (MAC); and

acquire the authentication vector according to the random number and the authentication token;

generate an expected response value (XRES) for network authentication of the device based at least on the device key and the random number (RAND);

the communications unit is further configured to: transmit the at least one authentication vector to a Mobility Management Entity (MME);

the authentication vector generation unit is further configured to: choose, at the MME, a corresponding one of the at least one authentication vector based on the device identifier and the service identifier ;

the communications unit is further configured to: transmit, to the device, a corresponding random number and a corresponding authentication token included in the corresponding one of the at least one authentication vector;

the authentication unit is further configured to: successfully authenticate the device if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal.

According to a third aspect of the invention, an authentication method is provided, wherein the method comprises:

initiating mutual authentication with a core network by transmitting, to the core network, an authentication message which at least includes a device identifier and a service identifier;

receiving an authentication vector from the core network, wherein the authentication vector is generated based at least on a device key which is generated at the core network based at least on the device identifier in the authentication message;

generating an expected message authentication code (XMAC) and a response value (RES), based on the authentication vector received from the core network and the device key stored in the device;

authenticating the core network based at least on a MAC and the authentication vector and the expected message authentication code (XMAC), wherein the MAC is included in the authentication vector; and

sending the response value (RES) to the core network, upon successfully authenticating the core network.

With reference to the third aspect, in a first possible implementation manner of the third aspect, wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes an initial counter value; wherein based on the authentication vector received from the core network, generating an expected message authentication code (XMAC) comprises:

generating the expected message authentication code (XMAC), based at least on the random number (RAND), the initial counter value and the device key stored in the device; and

wherein authenticating the core network based on the authentication vector and the expected message authentication code (XMAC) comprises:

successfully authenticating the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

With reference to the third aspect, in a second possible implementation manner of the third aspect,

wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes a nonce;

wherein based on the authentication vector received from the core network, generating an expected message authentication code (XMAC) comprises:

generating the expected message authentication code (XMAC), based at least on the random number (RAND) and the device key stored in the device;

wherein authenticating the core network based on the authentication vector and the expected message authentication code (XMAC) comprises:

successfully authenticating the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

With reference to the third aspect, in a third possible implementation manner of the third aspect,

wherein the authentication vector at least includes a random number (RAND) and an authentication token (AUTN),

wherein based on the authentication vector received from the core network, generating an expected message authentication code (XMAC) comprises:

generating the expected message authentication code (XMAC), based at least on the random number (RAND) and the device key stored in the device; and

wherein authenticating the core network based on the authentication vector and the expected message authentication code (XMAC) comprises:

successfully authenticating the core network if the message authentication code (MAC) which is included in the authentication token (AUTN) and the expected message authentication code (XMAC) are equal.

According to a fourth aspect of the invention, an authentication system is provided, wherein the system comprises:

a communications unit configured to:

initiate mutual authentication with a core network by transmitting, to the core network, an authentication message which at least includes a device identifier and a service identifier;

receive an authentication vector from the core network, wherein the authentication vector is generated based at least on a device key which is generated at the core network based at least on the device identifier in the authentication message; and

an authentication unit configured to:

generate an expected message authentication code (XMAC) and a response value (RES), based on the authentication vector received from the network and the device key stored in the device;

authenticate the core network based at least on a MAC and the authentication vector and the expected message authentication code (XMAC), wherein the MAC is included in the authentication vector;

send a response value (RES) to the core network, upon successful authentication of the core network.

With reference to the fourth aspect, in a first possible implementation manner of the fourth aspect, wherein the authentication message further includes an initial counter value;

wherein the authentication vector at least includes a random number and a message authentication code (MAC); and

wherein the authentication unit is further configured to:

generate the expected message authentication code (XMAC), based on the random number (RAND) ,the initial counter value and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

With reference to the fourth aspect, in a second possible implementation manner of the fourth aspect,

wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes a nonce; and

wherein the authentication unit is further configured to:

generate the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

With reference to the fourth aspect, in a third possible implementation manner of the fourth aspect,

wherein the authentication vector at least includes a random number and an authentication token (AUTN); and

wherein the authentication unit is further configured to:

generate the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) which is included in the authentication token (AUTN) and the expected message authentication code (XMAC) are equal.

According to a fifth aspect of the invention, an authentication system is provided, wherein the system comprises:

a processor;

a storage medium;

instructions stored on the storage medium and executable by the processor to:

initiate mutual authentication with a core network by transmitting, to the core network, an authentication message which at least includes a device identifier and a service identifier;

receive an authentication vector from the core network, wherein the authentication vector is generated based at least on a device key which is generated at the core network based at least on the device identifier in the authentication message; and

generate an expected message authentication code (XMAC) and a response value (RES), based on the authentication vector received from the network and the device key stored in the device;

authenticate the core network based at least on a MAC and the expected message authentication code (XMAC), wherein the MAC is included in the authentication vector;

send a response value (RES) to the core network, upon successful authentication of the core network.

With reference to the fifth aspect, in a first possible implementation manner of the fifth aspect, wherein the authentication message further includes an initial counter value;

wherein the authentication vector at least includes a random number and a message authentication code (MAC); and

wherein the instructions stored on the storage medium and executable by the processor to:

generate the expected message authentication code (XMAC) based at least on the random number (RAND) ,the initial counter value and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

With reference to the fifth aspect, in a second possible implementation manner of the fifth aspect,

wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes a nonce; and

wherein the instructions stored on the storage medium and executable by the processor to:

generate the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

With reference to the fifth aspect, in a third possible implementation manner of the fifth aspect,

wherein the authentication vector at least includes a random number and an authentication token (AUTN); and

wherein the instructions stored on the storage medium and executable by the processor to:

generate the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

According to a sixth aspect of the invention, a key generation and authentication method is provided, wherein the method comprises:

at a first core network node:

receiving, an authentication message which at least includes a device identifier and a service identifier; and

generating, a device key based at least on the device identifier and a service key which is stored at the first core network node and associated with the service identifier.

With reference to the sixth aspect, in a first possible implementation manner of the sixth aspect,

generating at least one authentication vector based at least on the device key; and

transmitting the at least one authentication vector to a second core network node.

With reference to the first possible implementation manner of the sixth aspect, in a second possible implementation manner of the sixth aspect, wherein the authentication message further includes an initial counter value; and

wherein generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND);

generating a sequential counter value based on the initial counter value;

generating a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generating an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the RAND, the XRES and the AUTN.

With reference to the first possible implementation manner of the sixth aspect, in a third possible implementation manner of the sixth aspect, wherein the authentication message further includes a nonce;

wherein generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND); and

generating a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

wherein after the generating at least one authentication vector based at least on the generated device key, the method further comprises:

generating an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

wherein the transmitting the at least one authentication vector to a second core network node comprises:

transmitting the XRES and the MAC vector to a second core network node.

With reference to the first possible implementation manner of the sixth aspect, in a fourth possible implementation manner of the sixth aspect, wherein the first core network node includes a sequence number associated with the device identifier; wherein generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND);

generating a message authentication code (MAC) based at least on the device key and the sequence number;

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number (RAND); and

generating an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the random number and the authentication token.

With reference to anyone of the above possible implementation manner of the sixth aspect, in a fifth possible implementation manner of the sixth aspect, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.

According to a seventh aspect of the invention, a key generation and authentication system , the system comprises:

a key generation unit provided at a first core network node and configured to:

receive an authentication message which at least includes a device identifier and a service identifier; and

generate, a device key based at least on the device identifier and a service key which is stored at the first core network node and associated with the service identifier.

With reference to the seventh aspect, in a first possible implementation manner of the seventh aspect,

an authentication vector generation unit provided at a first core network node and configured to:

generate at least one authentication vector based at least on the device key; and

a communications unit provided at a first core network node and configured to: transmit the at least one authentication vector to a second core network node.

With reference to the first possible implementation manner of the seventh aspect, in a second possible implementation manner of the seventh aspect,wherein the authentication message further includes an initial counter value; and wherein the authentication vector generation unit is configured to:

for each of the at least one authentication vector:

generate a random number (RAND);

generate a sequential counter value based on the initial counter value;

generate a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generate an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the RAND, the XRES and the AUTN.

With reference to the first possible implementation manner of the seventh aspect, in a third possible implementation manner of the seventh aspect, wherein the authentication message further includes a nonce;

wherein the authentication vector generation unit is configured to:

generate a random number (RAND); and

generate a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

wherein the communications unit is configured to:

transmit the XRES and the MAC to a second core network node.

With reference to the first possible implementation manner of the seventh aspect, in a fourth possible implementation manner of the seventh aspect wherein the core network node includes a sequence number associated with the device identifier;

wherein the authentication vector generation unit is configured to:

generate a random number (RAND);

generate a message authentication code (MAC) based at least on the device key and the sequence number;

generate an authentication token (AUTN) based on the message authentication code (MAC); and

acquire the authentication vector according to the random number and the authentication token.

With reference to anyone of the above possible implementation manner of the seventh aspect, in a fifth possible implementation manner of the seventh aspect, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.

According to a seventh aspect of the invention, a key generation and authentication system , the system comprises:

a processor;

a storage medium;

instructions stored on the storage medium and executable by the processor to:

receive an authentication message which at least includes a device identifier and a service identifier; and

generate, a device key based at least on the device identifier and a service key which is stored at the first core network node and associated with the service identifier.

With reference to the eighth aspect, in a first possible implementation manner of the eigth aspect,

an authentication vector generation unit provided at a first core network node and configured to:

generate at least one authentication vector based at least on the device key; and

a communications unit provided at a first core network node and configured to: transmit the at least one authentication vector to a second core network node.

With reference to the first possible implementation manner of the eighth aspect, in a second possible implementation manner of the eighth aspect,wherein the authentication message further includes an initial counter value; and

wherein the instructions stored on the storage medium and executable by the processor to:

for each of the at least one authentication vector:

generate a random number (RAND);

generate a sequential counter value based on the initial counter value;

generate a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generate an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the RAND, the XRES and the AUTN.

With reference to the first possible implementation manner of the eighth aspect, in a third possible implementation manner of the eighth aspect, wherein the authentication message further includes a nonce;

wherein the instructions stored on the storage medium and executable by the processor to:

generate a random number (RAND); and

generate a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

wherein the communications unit is configured to:

transmit the XRES and the MAC to a second core network node.

With reference to the first possible implementation manner of the eighth aspect, in a fourth possible implementation manner of the eighth aspect, wherein the core network node includes a sequence number associated with the device identifier; wherein the instructions stored on the storage medium and executable by the processor to:

generate a random number (RAND);

generate a message authentication code (MAC) based at least on the device key and the sequence number;

generate an authentication token (AUTN) based on the message authentication code (MAC); and

acquire the authentication vector according to the random number and the authentication token.

With reference to anyone of the above possible implementation manner of the eighth aspect, in a fifth possible implementation manner of the eighth aspect, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.

According to a ninth aspect of the invention, a key generation and authentication method, the method comprises:

at a second core network node:

having at least one authentication vector,wherein the at least one authentication vector includes a random number and an expected response value (XRES);

transmitting at least the random number to a device;

receiving a response value (RES) from the device, which is generated based at least on a second device key stored at the device, and the random number; and

successfully authenticating the device if the response value (RES) and an expected response value (XRES) are equal.

With reference to the ninth aspect, in a first possible implementation manner of the ninth aspect,

wherein the having at least one authentication vector comprises:

receiving the at least one authentication vector from the first core network node.

With reference to the ninth aspect, in a second possible implementation manner of the eighth aspect, wherein before the having at least one authentication vector, the method further comprises:

receiving an authentication message from a device; and

transmitting the authentication message to a first core network node for generating a first device key;

wherein the having at least one authentication vector comprises:

receiving the first device key from the first core network node; and

generating the at least one authentication vector at the second core network node.

With reference to anyone of the above possible implementation manner of the ninth aspect, in a third possible implementation manner of the ninth aspect, wherein the second core network node includes a Mobility Management Entity (MME).

According to a tenth aspect of the invention, a key generation and authentication system, the system comprises:

a communications unit provided at a second core network node and configured to:

have at least one authentication vector, wherein the at least one authentication vector includes a random number and an expected response value (XRES);

transmit at least the random number to a device;

receive a response value (RES) from the device, which is generated based at least on a second device key stored at the device, and the random number; and

an authentication unit provided at the second core network node and configured to:

successfully authenticate the device if the response value (RES) and an expected response value (XRES) are equal.

With reference to the tenth aspect, in a first possible implementation manner of the tenth aspect, wherein the communications unit is further configured to: receive the at least one authentication vector from the first core network node.

With reference to the tenth aspect, in a first possible implementation manner of the tenth aspect, wherein the communications unit is further configured to:

receive an authentication message from a device; and

transmit the authentication message to a first core network node for generating a first device key;

receive the first device key from the first core network node; and

generate the at least one authentication vector at the second core network node.

With reference to anyone of the above possible implementation manner of the tenth aspect, in a third possible implementation manner of the tenth aspect, wherein the second core network node includes a Mobility Management Entity (MME).

According to a eleventh aspect of the invention, a key generation and authentication system, the system comprises:

a communications unit provided at a second core network node and configured to:

have at least one authentication vector, wherein the at least one authentication vector includes a random number and an expected response value (XRES);

transmit at least the random number to a device;

receive a response value (RES) from the device, which is generated based at least on a second device key stored at the device, and the random number; and

an authentication unit provided at the second core network node and configured to:

successfully authenticate the device if the response value (RES) and an expected response value (XRES) are equal.

With reference to the eleventh aspect, in a first possible implementation manner of the eleventh aspect, wherein the communications unit is further configured to: receive the at least one authentication vector from the first core network node.

With reference to the eleventh aspect, in a first possible implementation manner of the eleventh aspect, wherein the communications unit is further configured to:

receive an authentication message from a device; and

transmit the authentication message to a first core network node for generating a first device key;

receive the first device key from the first core network node; and

generate the at least one authentication vector at the second core network node.

With reference to anyone of the above possible implementation manner of the eleventh aspect, in a third possible implementation manner of the eleventh aspect, wherein the second core network node includes a Mobility Management Entity (MME).

Brief Description of the Drawings

Embodiments of the invention are disclosed hereinafter with reference to the drawings, in which:

Figure 1 illustrates an EPS AKA procedure for 4G network;

Figure 2 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention;

Figure 3 illustrates a method for generating authentication vectors;

Figure 4 illustrates a user authentication function in a device;

Figure 5 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention;

Figure 6 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention;

Figure 7 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention;

Figure 8 illustrates another method for generating authentication vectors;

Figure 9 illustrates another user authentication function in a device;

Figure 10 illustrates a system for key generation and authentication, which may be deployed at a network; and

Figure 11 illustrates a system for key generation and authentication, which may be deployed at a device.

Detailed Description

In the following description, numerous specific details are set forth in order to provide a thorough understanding of various illustrative embodiments of the invention. It will be understood, however, to one skilled in the art, that embodiments of the invention may be practiced without some or all of these specific details. In other instances, well known process operations have not been described in detail in order not to unnecessarily obscure pertinent aspects of embodiments being described. In the drawings, like reference numerals refer to same or similar functionalities or features throughout the several views.

As used in the description and claims, unless otherwise specified the use of the ordinal adjectives "first", "second", "third", etc., to describe a common element, merely indicate that different instances of like elements are being referred to, and are not intended to imply that the elements so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

In this disclosure, the phrase “core network” refers to a network entity including Mobility Management Entity (MME), Home Subscriber Server (HSS), Authentication, Authorization, Accounting server (AAA) server, user gateway, network service gateway, Radio Access Network (RAN) controller. The phrase “core network node” refers to any of the above-listed network entities.

In this disclosure, the phrase “authentication vector” is comprised of a plurality of components or parameters that provide temporary authentication data that enables authentication of a core network and/or a device, e.g. IoT device. Examples of authentication vector (AV) components include, but are not limited to, random number (RAND), expected response value (XRES), cipher key (CK), integrity key (IK), message authentication code (MAC), network authentication token (AUTN). An authentication vector may include a plurality of components which are selected from the above-mentioned component examples and may include other suitable components.

In this disclosure, the phrase "authentication message" refers to a request, a message or data that initiates authentication procedure or is generated during authentication procedure. Examples of "authentication message" include, but are not limited to, authentication request, authentication vector request.

Embodiments of the invention provide methods for key generation and authentication between a core network and IoT devices, e.g., smart sensors, smart phones, user equipment, etc. The invention does not require the core network (or HSS) to store a credential for each IoT device. Further, the authentication methods are service-relative, which may be suitable for 5G.

A method for key generation and distribution of IoT device credentials to IoT devices is described as follows.

I. An IoT service provider performs authentication with a network service provider (e.g., mobile operator). After successful authentication, the IoT service provider and the network service provider share a service identifier ID_{ser}, a service key K_{ser} and other optional parameters such as valid time. ID_{ser} is a unique service identifier of a service, e.g., service name.

II. For each IoT device D, the IoT service provider generates a device key K, as K = KDF(K_{ser},ID), where ID is a unique device identifier of device D, KDF is a key generation function such as HMAC. Examples of device identifier ID include, but not limited to, device name and IMEI (International Mobile Equipment Identity). The parameters of KDF at least include ID and K_{ser}, and may include other suitable parameters such as valid time.

III. The IoT service provider distributes a device key K to device D in a secured way using Wi-Fi, embedded Universal Integrated Circuit Card (eUICC)-based mechanism or other suitable techniques.

Methods for key generation and authentication between a core network and devices are described with reference to Figures 2 to 9.

Figure 2 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention. In this embodiment, an IoT device has obtained its device key K from IoT service provider as K = KDF (K_{ser}, ID); a Home Subscriber Server (HSS) in a core network has obtained and stored each service identity ID_{ser} and its corresponding service key K_{ser}. Further, the device stores a counter.

In block 101, the device retrieves an initial counter value as CNT.

In block 102, the device transmits an authentication message, e.g. authentication request, which at least includes ID_{ser}, ID and CNT to a MME at the core network.

In block 103, after receiving the authentication message containing ID_{ser}, ID and CNT, the MME checks whether an authentication vector for the ID_{ser}, ID and CNT exists. If an authentication vector is present or exists at the MME, the flow sequence proceeds to block 108. If an authentication vector is not present or does not exist at the MME, the flow sequence proceeds to block 104.

In block 104, the MME transmits a request message, e.g. authentication vector request, which at least includes ID_{ser}, ID and CNT to the HSS.

In block 105, the HSS retrieves the service key K_{ser} which is stored in the HSS and corresponds to the received ID_{ser}, and generates a device key K' = KDF (K_{ser}, ID) for this particular device ID and this particular service.

In block 106, the HSS generates a plurality of authentication vectors AV={AV[i]}. The i-th authentication vector is generated as follows:

(a) CNT_i = CNT + i – 1, wherein CNT_i is a sequential counter value;

(b) compute or generate AV[i] = ($RAND_i$, CNT_i, $XRES_i$, CK_i, IK_i, $AUTN_i$) and $AUTN_i$=(AMF_i, MAC_i) as shown in Figure 3, where AMF is authentication management field.

Particularly, for each authentication vector, the HSS generates a random number $RAND_i$ and other AV components of each authentication vector as follows:

- A message authentication code MAC_i = f1(K',CNT_i||$RAND_i$||AMF_i), wherein f1 is a message authentication function;

- An expected response value $XRES_i = f2(K', RAND_i)$, wherein f2 is a message authentication function;
- A cipher key $CK_i = f3 (K',RAND_i)$, wherein f3 is a key generating function;
- An integrity key $IK_i = f4 (K',RAND_i)$, wherein f4 is a key generating function.

In block 107, the HSS transmits the plurality of authentication vectors AV to the MME.

In block 108, the MME selects a corresponding authentication vector AV[j] for ID_{ser}, ID and CNT, where $AV[j] = RAND_j||CNT_j||XRES_j||CK_j||IK_j||AUTN_j$ and $AUTN_j = AMF_j||MAC_j$.

In block 109, based on the selected corresponding authentication vector AV[j], the MME transmits a message which includes a subset of AV components from the selected authentication vector, i.e., $RAND_j$ and $AUTN_j$, to the device, where $AUTN_j = AMF_j||MAC_j$;

In block 110, based on the received message containing the subset of AV components, i.e., $RAND_j$ and $AUTN_j$, the device generates XMAC, RES, CK and IK based on the device key K as shown in Figure 4 and increase current counter value in the device by one:

- An expected message authentication code XMAC = f1(K,CNT||RAND||AMF), wherein f1 is a message authentication function;
- A response value RES = f2(K,RAND), wherein f2 is a message authentication function;
- A cipher key CK = f3(K,RAND), wherein f3 is a key generating function;
- An integrity key IK = f4(K,RAND), wherein f4 is a key generating function.

In block 111, the device verifies whether XMAC = MAC_j. If XMAC and MAC_j are equal, the network is successfully authenticated. Otherwise, authentication of the network fails.

In block 112, the device transmits a message which includes RES to the MME.

In block 113, after receiving the message containing RES, the MME verifies whether RES = $XRES_j$. If RES and XRES are equal, the device is successfully authenticated. Otherwise, authentication of the device fails.

Figure 5 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention. In this embodiment, an IoT device has obtained its device key K from IoT service provider as K = KDF (K_{ser}, ID); a HSS in a core network has obtained and stored each service identity ID_{ser} and its corresponding service key K_{ser}.

In block 201, the device chooses a nonce x.

In block 202, the device transmits a message, e.g. authentication request, which at least includes ID_{ser}, ID and x to a MME at the core network.

In block 203, the MME transmits a message, e.g. authentication vector request, which at least includes ID_{ser}, ID and x to a HSS.

In block 204, the HSS retrieves the service key K_{ser} which is stored in the HSS and corresponds to $ID_{ser,}$ and generates a key K'= KDF (K_{ser}, ID).

In block 205, the HSS generates a random number RAND, generates an authentication vector AV = (MAC, XRES, CK', IK') where MAC, XRES, CK' and IK' are generated as follows:

- MAC = f1(K', x||RAND), wherein f1 is a message authentication function;
- XRES = f2(K', x||RAND), wherein f2 is a message authentication function;
- CK' = f3(K', x||RAND), wherein f3 is a key generation function;
- IK' = f4(K', x||RAND), wherein f4 is a key generation function.

In block 206, the HSS transmits a message which includes the authentication vector AV to the MME where AV=(RAND, MAC, XRES, CK', IK').

In block 207, the MME transmits a message which includes a subset of AV components from the authentication vector, i.e., RAND and MAC, to the device.

In block 208, the device generates XMAC, RES, CK and IK as follows:

- XMAC = f1(K, x||RAND)
- RES = f2(K, x||RAND)
- CK = f3(K, x||RAND)
- IK = f4(K, x||RAND)

In block 209, the device verifies whether XMAC = MAC. If XMAC and MAC are equal, the network is successfully authenticated. Otherwise, authentication of the network fails.

In block 210, the device transmits a message which includes RES to the MME.

In block 211, the MME verifies whether XRES = RES. If XRES and RES are equal, the device is successfully authenticated. Otherwise, authentication of the device fails.

Figure 6 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention. In this embodiment, an IoT device has obtained its device key K from IoT service provider as K = KDF (K_{ser}, ID); a HSS in a core network has obtained and stored each service identity ID_{ser} and its corresponding service key K_{ser}.

In block 301, the device chooses or generates a nonce x.

In block 302, the device transmits an authentication message, e.g. authentication request, which at least includes ID_{ser}, ID and x to the MME.

In block 303, the MME checks whether a device key exists for the device ID and the service associated with $ID_{ser.}$ If a device key for the device ID and the service associated with ID_{ser} exists or is present in the MME, the flow sequence proceeds to block 307. If a device key for the device ID and the service associated with ID_{ser} does not exist or is not present in the MME, the flow sequence proceeds to block 304.

In block 304, the MME transmits a message, e.g. authentication vector request, which at least includes ID_{ser}, ID and x to the HSS.

In block 305, the HSS retrieves the service key K_{ser} which is stored in the HSS and corresponds to the received ID_{ser}, and generates a device key K' = KDF (ID, K_{ser}) for this particular device ID and this particular service.

In block 306, the HSS transmits device key K' to the MME, wherein K' = KDF (ID, K_{ser}).

In block 307, the MME generates a random number RAND, and generates MAC, XRES, CK' and IK' as follows:

- MAC = f1(K', x||RAND), wherein f1 is a message authentication function;
- XRES = f2(K', x||RAND), wherein f2 is a message authentication function;
- CK' = f3(K', x||RAND), wherein f3 is a key generation function;
- IK' = f4(K', x||RAND), wherein f4 is a key generation function.

In block 308, the MME transmits a message which includes selected components from the authentication vector, i.e., RAND and MAC, to the device.

In block 309, the device generates XMAC, RES, CK' and IK' as follows:

- XMAC = f1(K, x||RAND), wherein f1 is a message authentication function;
- RES = f2(K, x||RAND), wherein f2 is a message authentication function;

- CK = f3(K, x||RAND), wherein f3 is a key generation function;
- IK = f4(K, x||RAND), wherein f4 is a key generation function.

In block 310, the device verifies whether MAC = XMAC. If XMAC and MAC are equal, the network is successfully authenticated. Otherwise, authentication of the network fails.

In block 311, the device transmits a message which includes RES to the MME.

In block 312, the MME verifies whether XRES = RES. If XRES and RES are equal, the device is successfully authenticated. Otherwise, authentication of the device fails.

Figure 7 is a flow chart illustrating a method for key generation and authentication according to one embodiment of the invention. In this embodiment, an IoT device has obtained its device key K from IoT service provider as K = KDF (K_{ser}, ID); a HSS in a core network has obtained the corresponding service identity ID_{ser}, service key K_{ser} and a sequence number SQN which is associated with each device.

In block 401, the device transmits an authentication message, e.g. authentication request, which at least includes ID_{ser} and ID to the MME.

In block 402, the MME checks whether an authentication vector for the ID_{ser} and ID exists. If an authentication vector is present or exists at the MME, the flow sequence proceeds to block 407. If an authentication vector is not present or does not exist at the MME, the flow sequence proceeds to block 404.

In block 403, the MME transmits a message, e.g. authentication vector request, which at least includes ID_{ser}, ID and x to the HSS.

In block 404, the HSS retrieves the service key K_{ser} which is stored in the HSS and corresponds to ID_{ser}, and generates a device key K’ = KDF (K_{ser}, ID).

In block 405, the HSS generates a plurality of authentication vectors AV = {AV[i]} where components of each authentication vector AV[i] are generated using the method in Figure 8 which is the same as USIM-AKA described in 3GPP TS 33.102.

In block 406, the HSS transmits the plurality of authentication vectors and their AV components to the MME.

In block 407, the MME selects a corresponding authentication vector AV[j] for

ID_{ser} and ID.

In block 408, the MME transmits a message which includes a subset of AV components from the selected authentication vector, i.e., RAND and AUTN, to the device.

In block 409, the device generates XMAC, RES, CK and IK using the method in Figure 9 which is the same as USIM-AKA described in 3GPP TS 33.102.

In block 410, the device verifies whether XMAC = MAC and whether SQN is in the predetermined correct range. If XMAC and MAC are equal and SQN is within the predetermined correct range, the network is successfully authenticated. Otherwise, authentication of the network fails.

In block 411, the device transmits a message which includes RES to the MME.

In block 412, the MME verifies whether XRES = RES. If XRES and RES are equal, the device is successfully authenticated. Otherwise, authentication of the device fails.

In the above-described embodiments, it is to be appreciated that the HSS may be replaced with any other core network node which is responsible for authentication, such as Authentication, Authorization and Accounting (AAA) server; the MME may be replaced with any other core network node which is responsible for performing authentication operation, such as a local controller.

Figure 10 illustrates a system for key generation and authentication, which may be deployed at a core network node. The system comprises:

- a key generation unit;
- an authentication vector (AV) generation unit;
- a communications unit; and
- an authentication unit.

The key generation unit, provided at a core network node, is configured to: receive an authentication message which at least includes a device identifier and a service identifier, generate a device key based at least on the device identifier and a service key which is stored at the core network node and associated with the service identifier.

The authentication vector (AV) generation unit and authentication unit are configured to: use the generated device key to authenticate a device associated with the device identifier.

The authentication vector generation unit is further configured to: generate at least one authentication vector based at least on the device key. Such authentication vector generation unit may include one or more units provided at same or different locations.

The communications unit is configured to: transmit the at least one authentication vector to the device. Such communications unit may include one or more transmission units and receiving units, provided as separate units or otherwise.

The authentication unit is further configured to: receive from the device a response to the at least one authentication vector; and authenticate the device based on the received response.

In various embodiments wherein the system for key generation and authentication is deployed at a core network, the system is operative according to any of the accompanying claims.

Figure 11 illustrates an authentication system which may be deployed at a device. The system comprises:

a communications unit; and

an authentication unit.

The communications unit is configured to: initiate mutual authentication with a core network by transmitting, to the core network, an authentication message which at least includes a device identifier and a service identifier; receive an authentication vector from the core network , wherein the authentication vector is generated based at least on a device key which is generated at the core network based at least on the device identifier in the authentication message. Such communications unit may include one or more transmission units and receiving units, provided as separate units or otherwise.

The authentication unit is configured to: based on the authentication vector received from the network, generate an expected message authentication code (XMAC) and a response value (RES); core network based on the authentication vector and the expected message authentication code (XMAC); upon successful authentication of the core network, send a response value (RES) to the core network.

In various embodiments wherein the authentication system is deployed at a device, the system is operative according to any of the accompanying claims, for example.

The above-mentioned units are coupled or connected as illustrated in Figures 10 and 11, and are not necessarily limited to a direct physical connection or coupling. Thus, for example, two units may be coupled directly, or via one or more intermediary devices. In another example, two units may be coupled in such a way that information can be passed therebetween while not sharing any physical connection with one another.

Embodiments of the invention provide several advantages including, but not limited to:

- Reduced storage requirements at the core network e.g. HSS or AAA. Since the core network dynamically generates the device keys upon receipt of device credentials with initiation of mutual authentication procedure, the core network is not required to store credentials for each IoT device.
- Flexible management of credentials of IoT devices by IoT service providers since the credentials of IoT devices are transmitted to the core network only at the time of initiating mutual authentication or requesting authentication vector and would not be stored at the core network both prior to initiating mutual authentication and after mutual authentication procedure completes.

Other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention. Furthermore, certain terminology has been used for the purposes of descriptive clarity, and not to limit the disclosed embodiments of the invention. The embodiments and features described above should be considered exemplary.

Claims:

1. A key generation and authentication method comprising:

receiving, at a core network node, an authentication message which at least includes a device identifier and a service identifier;

generating, at the core network node, a device key based at least on the device identifier and a service key which is stored at the core network node and associated with the service identifier; and

using the generated device key to authenticate a device associated with the device identifier.

2. The method of claim 1, wherein using the generated device key to authenticate a device associated with the device identifier further comprises:

generating at least one authentication vector based at least on the device key;

transmitting the at least one authentication vector to the device;

receiving, from the device, a response to the at least one authentication vector; and

authenticating the device based on the received response.

3. The method of claim 2, wherein the authentication message further includes an initial counter value;

wherein the core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server; and

wherein generating at least one authentication vector based at least on the device key is performed at the one of HSS and AAA server, and

wherein generating at least one authentication vector based at least on the device key, comprises:

generating a random number (RAND);

generating a sequential counter value based on the initial counter value;

generating a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and generating an authentication token (AUTN) based on the message authentication code (MAC); and

acquiring the authentication vector according to the RAND, the XRES and the AUTN;

wherein after generating at least one authentication vector based at least on the device key, the method further comprises: transmitting the at least one authentication vector to a MME; and

choosing, at the MME, a corresponding one of the at least one authentication vector based on the device identifier, the service identifier and the initial counter value;

wherein transmitting the at least one authentication vector to the device further includes:

transmitting, to a device, a corresponding random number and a corresponding authentication token which are included in the corresponding one of the at least one authentication vector; and

wherein authenticating the device based on the received response further includes:

successfully authenticating the device, at the MME, if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal, wherein the XRES is included in the authentication vector.

4. The method of claim 2, wherein the authentication message further includes a nonce;

wherein the generating at least one authentication vector based at least on the generated device key comprises :

generating a random number (RAND); and

generating a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

wherein after the generating at least one authentication vector based at least on the generated device key, the method further comprises:

generating an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

wherein the transmitting the at least one the authentication vector to the device comprises:

transmitting the random number and the message authentication code (MAC) to the device; and

wherein authenticating the device based on the received response comprises:

successfully authenticating the device, at the MME, if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal.

5. The method of claim 4, wherein generating a random number (RAND) is performed at the one of HSS and AAA server; and wherein generating at least one authentication vector based at least on the device key is performed at the one of HSS and AAA server.

6. The method of claim 4, wherein generating a random number (RAND) is performed at the MME; and wherein generating at least one authentication vector based at least on the device key is performed at the MME.

7. The method of claim 2, wherein the core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server; and

wherein generating at least one authentication vector based at least on the device key is performed at the one of HSS and AAA server, and

wherein the generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND);

generating a message authentication code (MAC) based at least on the device key and a sequence number which is stored at the HSS and associated with the device identifier;

generating an authentication token (AUTN) based on the message authentication code (MAC); and

acquiring the authentication vector according to the random number and the authentication token;

wherein after the generating at least one authentication vector based at least on the device key, the method further comprises:

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number (RAND);

transmitting the at least one authentication vector to a MME; and

choosing, at the MME, a corresponding one of the at least one authentication vector based on the device identifier and the service identifier ;

wherein transmitting the at least one authentication vector to the device comprises:

transmitting, to a device, a corresponding random number and a corresponding authentication token included in the corresponding one of the at least one authentication vector; and

wherein authenticating the device based on the received response comprises:

successfully authenticating the device if a response value (RES), which is received from the device and generated based at least on the random number and the device key stored in the device, and the expected response value (XRES) are equal.

8. An authentication method comprising:

initiating mutual authentication with a core network by transmitting, to the core network, an authentication message which at least includes a device identifier and a service identifier;

receiving an authentication vector from the core network, wherein the authentication vector is generated based at least on a device key which is generated at the core network based at least on the device identifier in the authentication message;

generating an expected message authentication code (XMAC) and a response value (RES), based on the authentication vector received from the core network and the device key stored in the device;

authenticating the core network based at least on a MAC and the expected message authentication code (XMAC), wherein the MAC is included in the authentication vector; and

sending the response value (RES) to the core network, upon successfully authenticating the core network.

9. The method of claim 8, wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes an initial counter value;

wherein based on the authentication vector received from the core network, generating an expected message authentication code (XMAC) comprises:

generating the expected message authentication code (XMAC), based at least on the random number (RAND), the initial counter value and the device key stored in the device; and

wherein authenticating the core network based on the authentication vector and the expected message authentication code (XMAC) comprises:

successfully authenticating the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

10. The method of claim 8, wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes a nonce;

wherein based on the authentication vector received from the core network, generating an expected message authentication code (XMAC) comprises:

generating the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device;

wherein authenticating the core network based on the authentication vector and the expected message authentication code (XMAC) comprises:

successfully authenticating the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

11. The method of claim 8, wherein the authentication vector at least includes a random number (RAND) and an authentication token (AUTN),

wherein based on the authentication vector received from the core network, generating an expected message authentication code (XMAC) comprises:

, generating the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device; and wherein authenticating the core network based on the authentication vector and the expected message authentication code (XMAC) comprises:

successfully authenticating the core network if the message authentication code (MAC) which is included in the authentication token (AUTN) and the expected message authentication code (XMAC) are equal.

12. An authentication system comprising:

a communications unit configured to:

initiate mutual authentication with a core network by transmitting, to the core network, an authentication message which at least includes a device identifier and a service identifier;

receive an authentication vector from the core network, wherein the authentication vector is generated based at least on a device key which is generated at the core network based at least on the device identifier in the authentication message; and

an authentication unit configured to:

generate an expected message authentication code (XMAC) and a response value (RES), based at least on the authentication vector received from the network;

authenticate the core network based on the authentication vector and the expected message authentication code (XMAC);

send a response value (RES) to the core network, upon successful authentication of the core network.

13. The system of claim 12, wherein the authentication message further includes an initial counter value;

wherein the authentication vector at least includes a random number and a message authentication code (MAC); and

wherein the authentication unit is further configured to:

generate the expected message authentication code (XMAC) based at least on the random number (RAND) and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

14. The system of claim 12, wherein the authentication vector at least includes a random number (RAND) and a message authentication code (MAC);

wherein the authentication message further includes a nonce; and

wherein the authentication unit is further configured to:

generate the expected message authentication code (XMAC) based on the random number (RAND) and the device key stored in the device; and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

15. The system of claim 12, wherein the authentication vector at least includes a random number and an authentication token (AUTN); and

wherein the authentication unit is further configured to:

based at least on the random number (RAND) and the device key stored in the device, generate the expected message authentication code (XMAC); and

successfully authenticate the core network if the message authentication code (MAC) and the expected message authentication code (XMAC) are equal.

16. A key generation and authentication method comprising:

at a first core network node:

receiving, an authentication message which at least includes a device identifier and a service identifier; and

generating, a device key based at least on the device identifier and a service key which is stored at the first core network node and associated with the service identifier.

17. The method of claim 16 further comprising:

generating at least one authentication vector based at least on the device key; and

transmitting the at least one authentication vector to a second core network node.

18. The method of claim 17, wherein the authentication message further includes an initial counter value; and

wherein generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND);

generating a sequential counter value based on the initial counter value;

generating a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generating an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the RAND, the XRES and the AUTN.

19. The method of claim 17, wherein the authentication message further includes a nonce;

wherein generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND); and

generating a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

wherein after the generating at least one authentication vector based at least on the generated device key, the method further comprises:

generating an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

wherein the transmitting the at least one authentication vector to a second core network node comprises:

transmitting the XRES and the MAC vector to a second core network node.

20. The method of claim 17, wherein the first core network node includes a sequence number associated with the device identifier;

wherein generating at least one authentication vector based at least on the device key comprises:

generating a random number (RAND);

generating a message authentication code (MAC) based at least on the device key and the sequence number;

generating an expected response value (XRES) for network authentication of the device based at least on the device key and the random number (RAND); and

generating an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the random number and the authentication token.

21. The method of any of claims 16 to 20, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.

22. A key generation and authentication system comprising:

a key generation unit provided at a first core network node and configured to:

receive an authentication message which at least includes a device identifier and a service identifier; and

generate, a device key based at least on the device identifier and a service key which is stored at the first core network node and associated with the service identifier.

23. The system of claim 22, further comprising:

an authentication vector generation unit provided at a first core network node and configured to:

generate at least one authentication vector based at least on the device key; and

a communications unit provided at a first core network node and configured to:

transmit the at least one authentication vector to a second core network node.

24. The system of claim 23, wherein the authentication message further includes an initial counter value; and

wherein the authentication vector generation unit is configured to:

for each of the at least one authentication vector:

generate a random number (RAND);

generate a sequential counter value based on the initial counter value;

generate a message authentication code (MAC) based at least on the device key, the sequential counter value and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key and the random number; and

generate an authentication token (AUTN) based on the message authentication code (MAC);

acquiring the authentication vector according to the RAND, the XRES and the AUTN.

25. The system of claim 23, wherein the authentication message further includes a nonce;

wherein the authentication vector generation unit is configured to:

generate a random number (RAND); and

generate a message authentication code (MAC) for device authentication of the network based at least on the device key and the random number (RAND);

generate an expected response value (XRES) for network authentication of the device based at least on the device key, the nonce and the random number (RAND);

wherein the communications unit is configured to:

transmit the XRES and the MAC to a second core network node.

26. The system of claim 23, wherein the core network node includes a sequence number associated with the device identifier;

wherein the authentication vector generation unit is configured to:

generate a random number (RAND);

generate a message authentication code (MAC) based at least on the device key and the sequence number;

generate an authentication token (AUTN) based on the message authentication code (MAC); and

acquire the authentication vector according to the random number and the authentication token.

27. The system of any of claims 22 to 26, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.

28. A key generation and authentication method comprising:

at a second core network node:

having at least one authentication vector, wherein the at least one authentication vector includes a random number and an expected response value (XRES);

transmitting at least the random number to a device;

receiving a response value (RES) from the device, which is generated based at least on a second device key stored at the device, and the random number; and

successfully authenticating the device if the response value (RES) and an expected response value (XRES) are equal.

29. The method of claim 28,

wherein the having at least one authentication vector comprises:

receiving the at least one authentication vector from the first core network node.

30. The method of claim 28, wherein before the having at least one authentication vector, the method further comprises:

receiving an authentication message from a device; and

transmitting the authentication message to a first core network node for generating a first device key;

wherein the having at least one authentication vector comprises:

receiving the first device key from the first core network node; and

generating the at least one authentication vector at the second core network node.

31. The method of any of claims 28 to 30, wherein the second core network node includes a Mobility Management Entity (MME).

32. A key generation and authentication system comprising:

a communications unit provided at a second core network node and configured to:

have at least one authentication vector, wherein the at least one authentication vector includes a random number and an expected response value (XRES);

transmit at least the random number to a device;

receive a response value (RES) from the device, which is generated based at least on a second device key stored at the device, and the random number; and

an authentication unit provided at the second core network node and configured to:

successfully authenticate the device if the response value (RES) and an expected response value (XRES) are equal.

33. The system of claim 32, wherein the communications unit is further configured to: receive the at least one authentication vector from the first core network node.

34. The system of claim 32, wherein the communications unit is further configured to:

receive an authentication message from a device; and

transmit the authentication message to a first core network node for generating a first device key;

receive the first device key from the first core network node; and

generate the at least one authentication vector at the second core network node.

35. The system of any of claims 32 to 34, wherein the second core network node includes a Mobility Management Entity (MME).

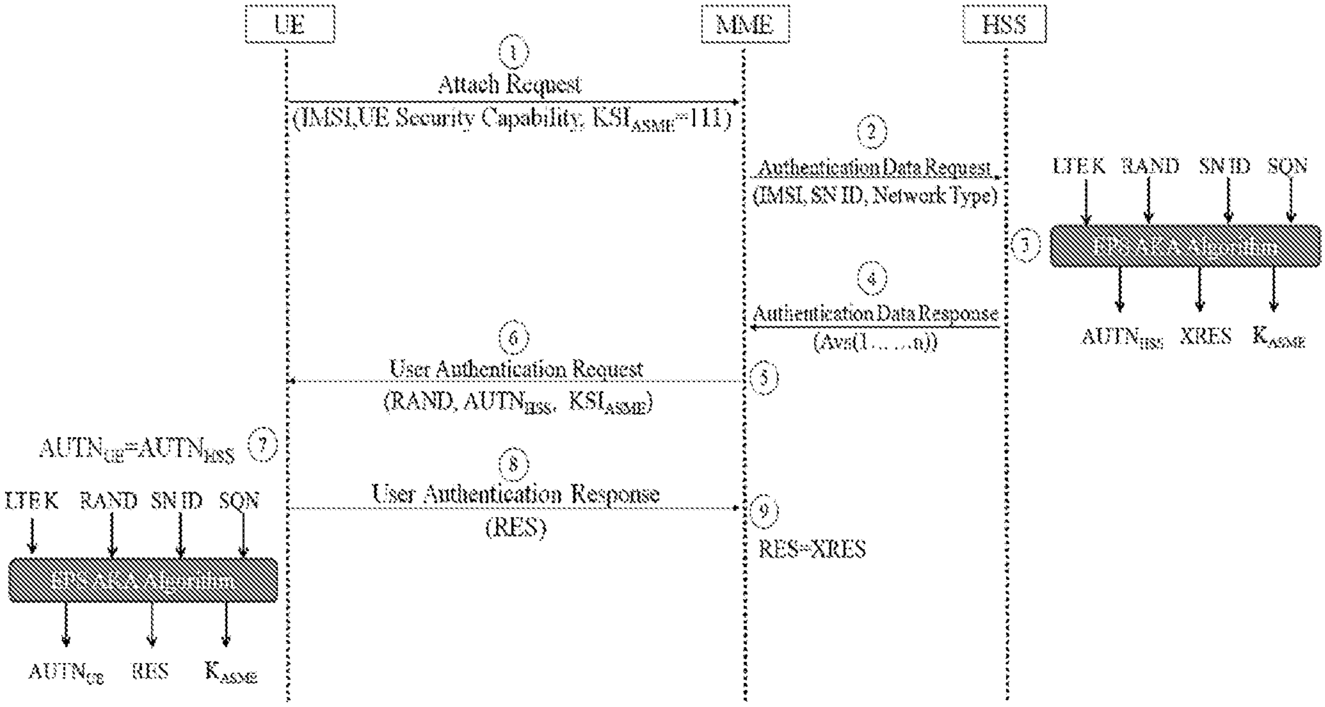
UE
MME
HSS
1
Attach Request
(IMSI,UE Security Capability, KSI$_{ASME}$=111)
2
Authentication Data Request
(IMSI, SN ID, Network Type)
LTE K
RAND
SN ID
SQN
3
EPS AKA Algorithm
AUTN$_{HSS}$
XRES
K$_{ASME}$
4
Authentication Data Response
(Avs(1……n))
5
6
User Authentication Request
(RAND, AUTN$_{HSS}$, KSI$_{ASME}$)
AUTN$_{UE}$=AUTN$_{HSS}$
7
8
User Authentication Response
(RES)
9
RES=XRES
LTE K
RAND
SN ID
SQN
EPS AKA Algorithm
AUTN$_{UE}$
RES
K$_{ASME}$

Figure 1
(Prior art)

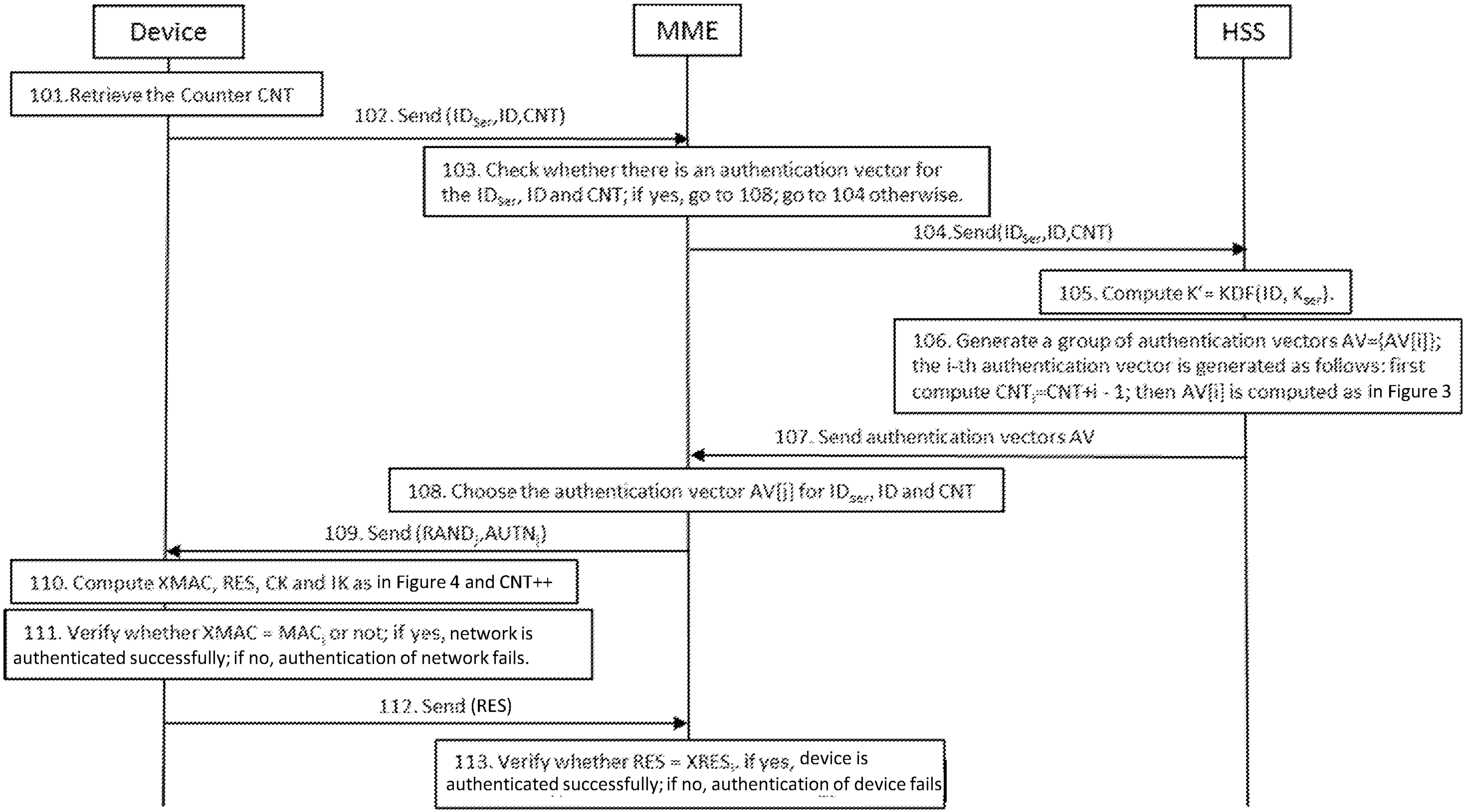
Device
MME
HSS
101.Retrieve the Counter CNT
102. Send {ID_{ser},ID,CNT}
103. Check whether there is an authentication vector for the ID_{ser}, ID and CNT; if yes, go to 108; go to 104 otherwise.
104.Send{ID_{ser},ID,CNT}
105. Compute K' = KDF(ID, K_{ser}).
106. Generate a group of authentication vectors AV={AV[i]}; the i-th authentication vector is generated as follows: first compute CNT_i=CNT+i - 1; then AV[i] is computed as in Figure 3
107. Send authentication vectors AV
108. Choose the authentication vector AV[j] for ID_{ser}, ID and CNT
109. Send {$RAND_j$,$AUTN_j$}
110. Compute XMAC, RES, CK and IK as in Figure 4 and CNT++
111. Verify whether XMAC = MAC_j or not; if yes, network is authenticated successfully; if no, authentication of network fails.
112. Send (RES)
113. Verify whether RES = $XRES_j$, if yes, device is authenticated successfully; if no, authentication of device fails

Figure 2

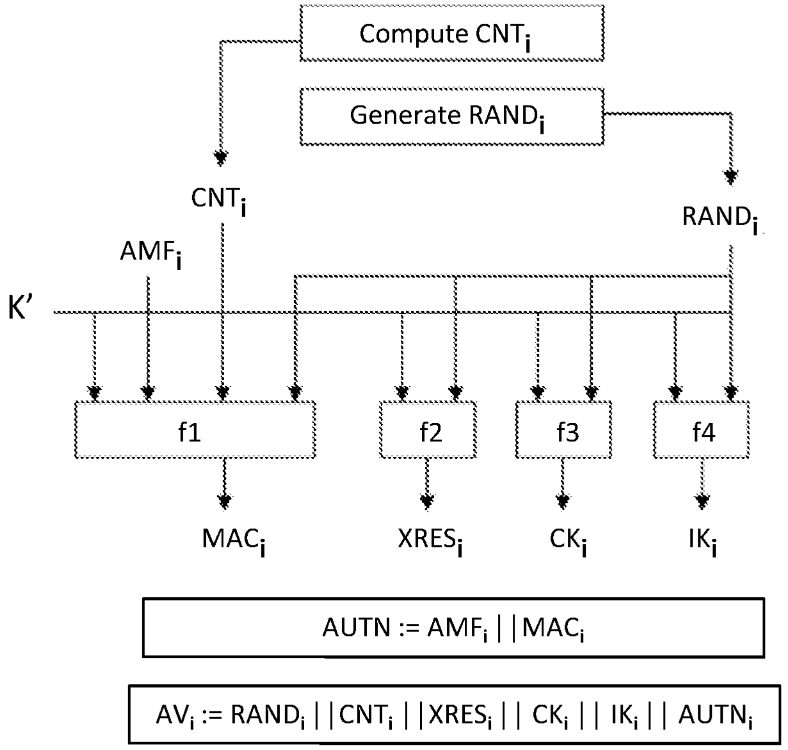
Compute CNT_i
Generate $RAND_i$
CNT_i
$RAND_i$
AMF_i
K'
f1
f2
f3
f4
MAC_i
$XRES_i$
CK_i
IK_i
AUTN := AMF_i | | MAC_i
AV_i := $RAND_i$ | | CNT_i | | $XRES_i$ | | CK_i | | IK_i | | $AUTN_i$

Figure 3

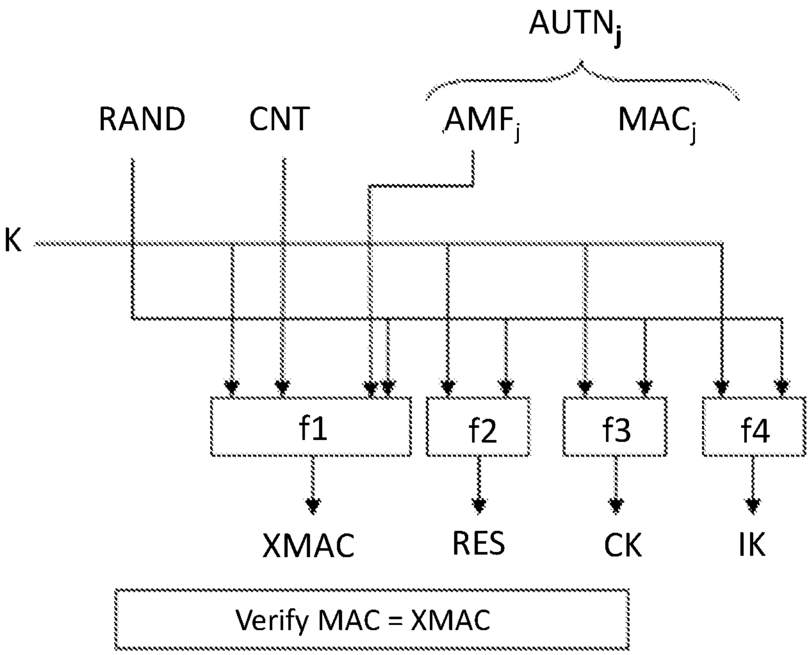

Figure 4

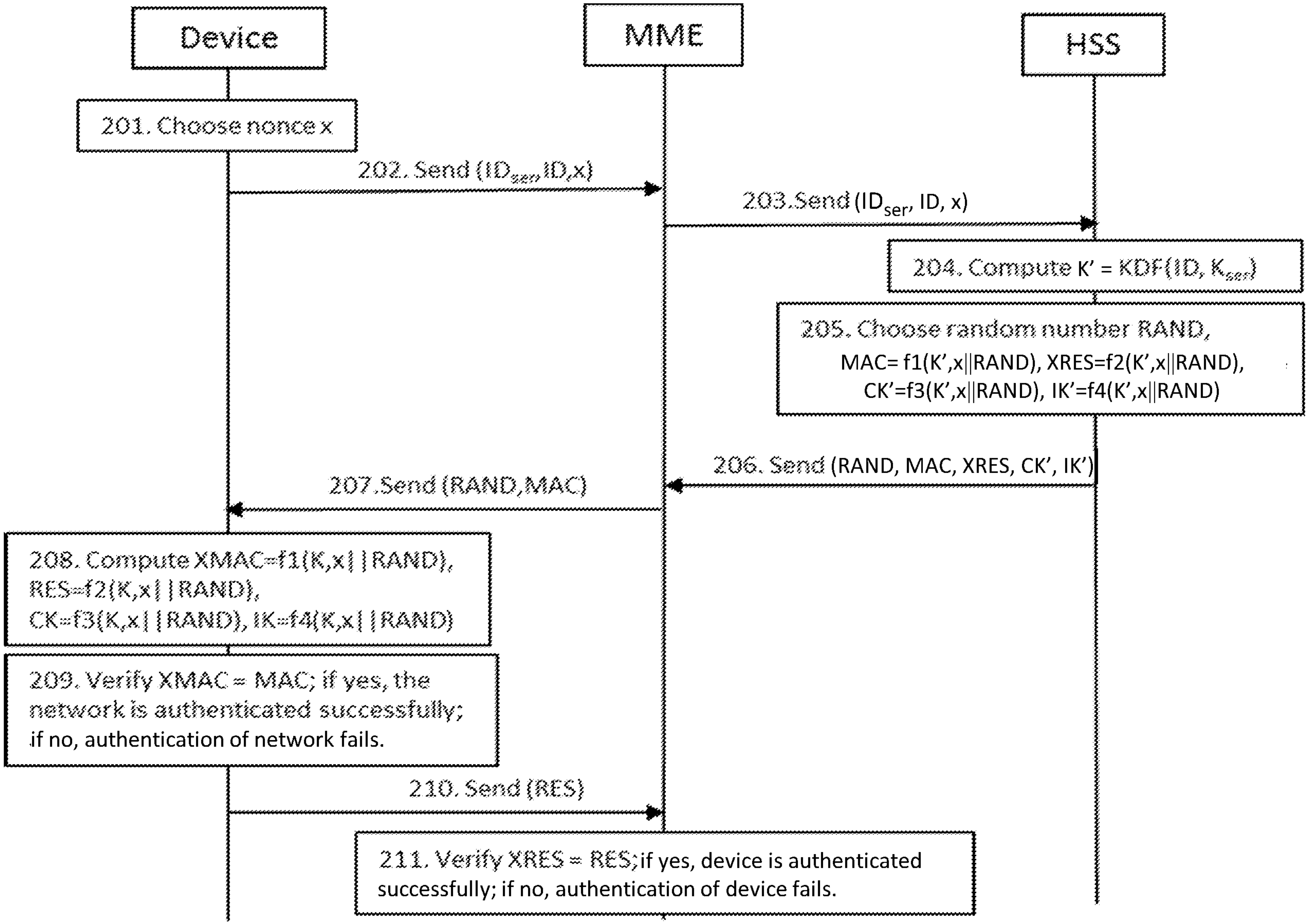
Device
MME
HSS
201. Choose nonce x
202. Send (ID$_{ser}$,ID,x)
203.Send (ID$_{ser}$, ID, x)
204. Compute K' = KDF(ID, K$_{ser}$)
205. Choose random number RAND,
MAC= f1(K',x||RAND), XRES=f2(K',x||RAND),
CK'=f3(K',x||RAND), IK'=f4(K',x||RAND)
206. Send (RAND, MAC, XRES, CK', IK')
207.Send (RAND,MAC)
208. Compute XMAC=f1(K,x| |RAND),
RES=f2(K,x| |RAND),
CK=f3(K,x| |RAND), IK=f4(K,x| |RAND)
209. Verify XMAC = MAC; if yes, the
network is authenticated successfully;
if no, authentication of network fails.
210. Send (RES)
211. Verify XRES = RES;if yes, device is authenticated
successfully; if no, authentication of device fails.

Figure 5

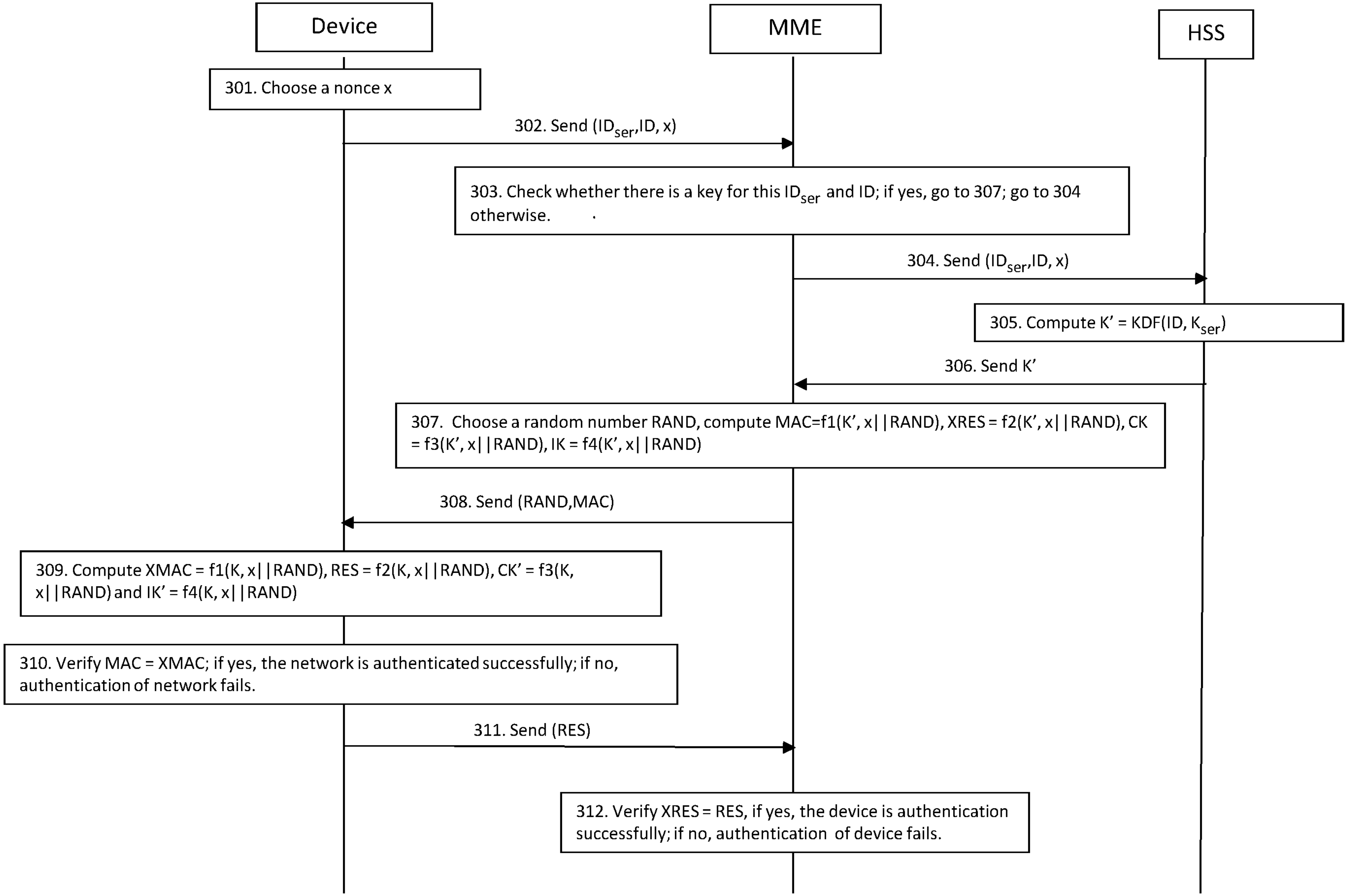
Device
MME
HSS
301. Choose a nonce x
302. Send (ID_{ser},ID, x)
303. Check whether there is a key for this ID_{ser} and ID; if yes, go to 307; go to 304 otherwise.
304. Send (ID_{ser},ID, x)
305. Compute K' = KDF(ID, K_{ser})
306. Send K'
307. Choose a random number RAND, compute MAC=f1(K', x||RAND), XRES = f2(K', x||RAND), CK = f3(K', x||RAND), IK = f4(K', x||RAND)
308. Send (RAND,MAC)
309. Compute XMAC = f1(K, x||RAND), RES = f2(K, x||RAND), CK' = f3(K, x||RAND) and IK' = f4(K, x||RAND)
310. Verify MAC = XMAC; if yes, the network is authenticated successfully; if no, authentication of network fails.
311. Send (RES)
312. Verify XRES = RES, if yes, the device is authentication successfully; if no, authentication of device fails.

Figure 6

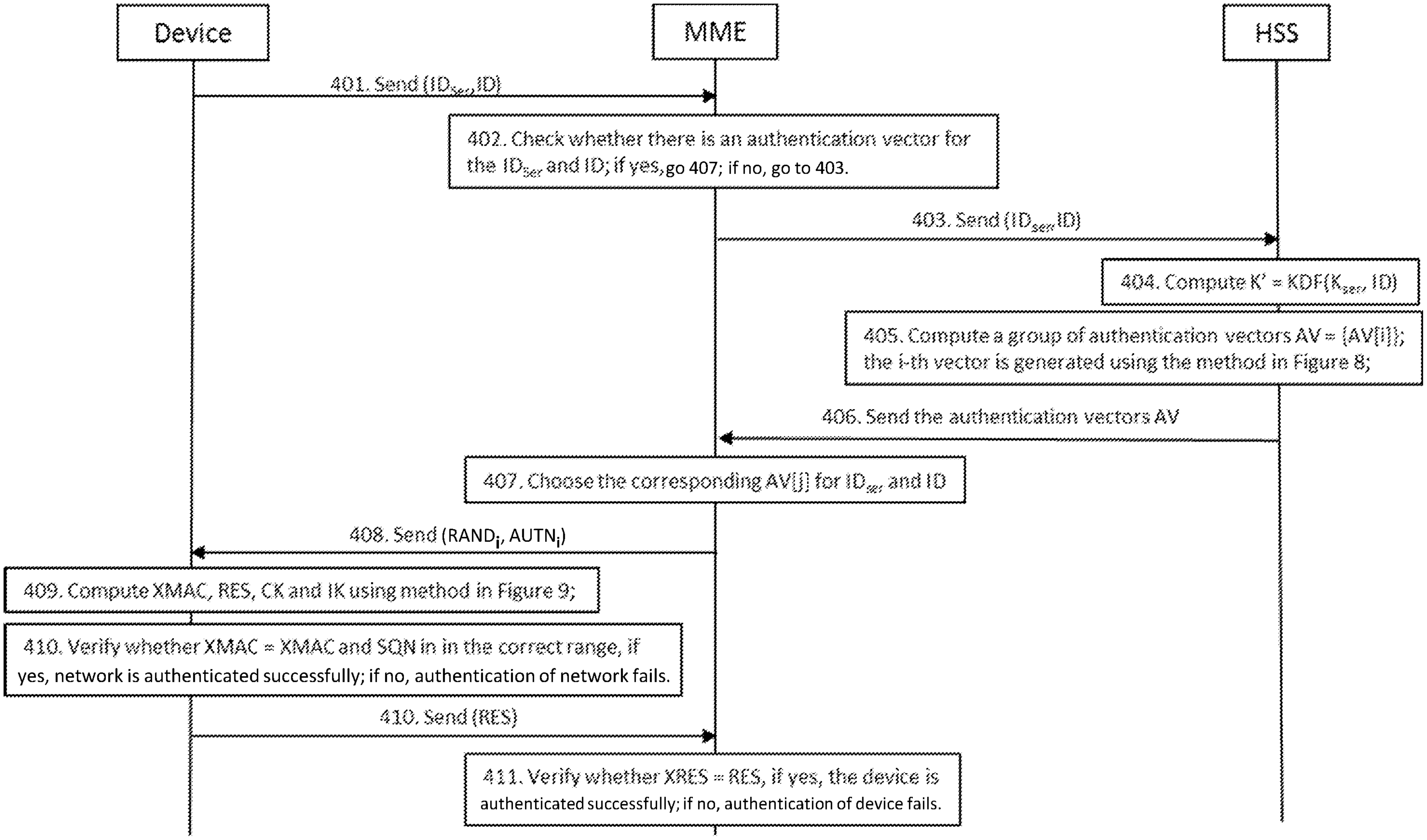
Device
MME
HSS
401. Send (ID$_{ser}$, ID)
402. Check whether there is an authentication vector for the ID$_{ser}$ and ID; if yes,go 407; if no, go to 403.
403. Send (ID$_{ser}$, ID)
404. Compute K' = KDF(K$_{ser}$, ID)
405. Compute a group of authentication vectors AV = {AV[i]}; the i-th vector is generated using the method in Figure 8;
406. Send the authentication vectors AV
407. Choose the corresponding AV[j] for ID$_{ser}$ and ID
408. Send (RAND$_i$, AUTN$_i$)
409. Compute XMAC, RES, CK and IK using method in Figure 9;
410. Verify whether XMAC = XMAC and SQN in in the correct range, if yes, network is authenticated successfully; if no, authentication of network fails.
410. Send (RES)
411. Verify whether XRES = RES, if yes, the device is authenticated successfully; if no, authentication of device fails.

Figure 7

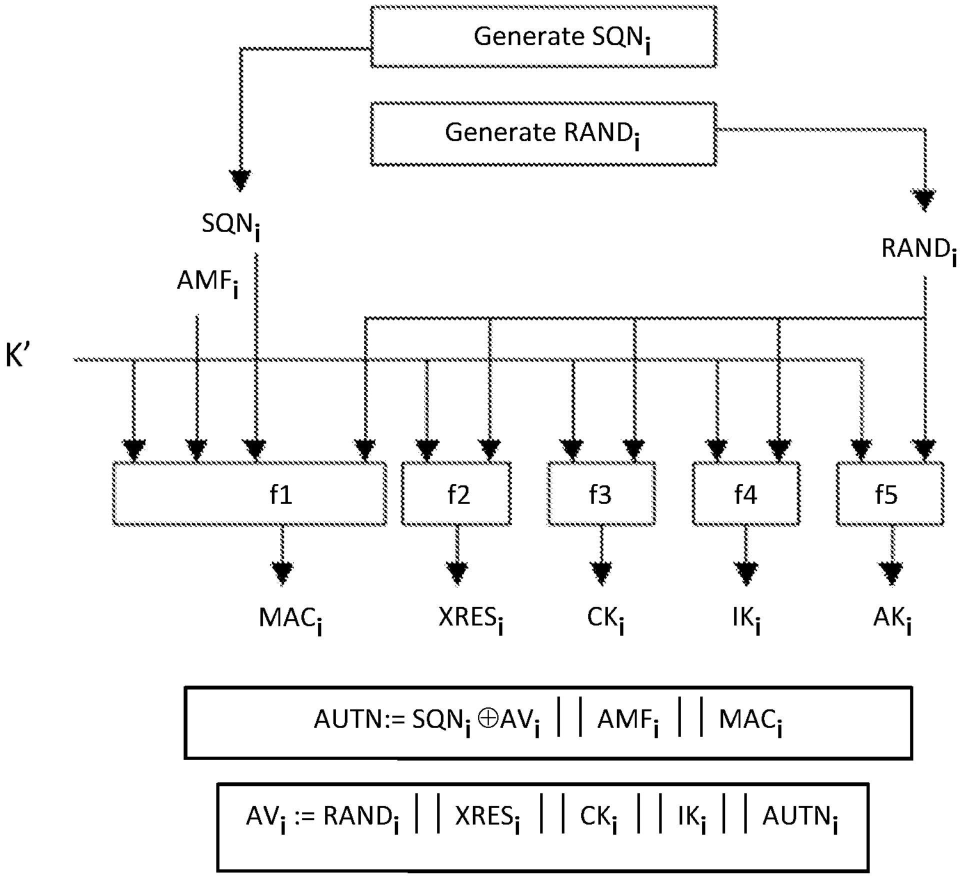
Generate SQN_i
Generate $RAND_i$
SQN_i
AMF_i
$RAND_i$
K'
f1
f2
f3
f4
f5
MAC_i
$XRES_i$
CK_i
IK_i
AK_i
AUTN:= $SQN_i \oplus AV_i$ | | AMF_i | | MAC_i
AV_i := $RAND_i$ | | $XRES_i$ | | CK_i | | IK_i | | $AUTN_i$

Figure 8

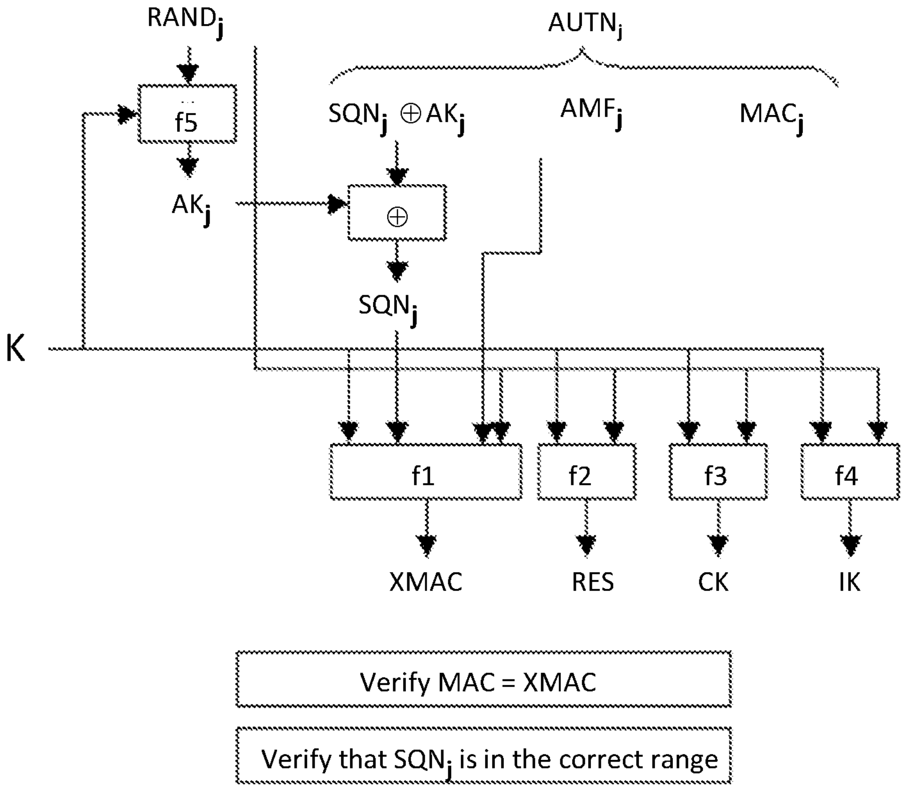

Figure 9

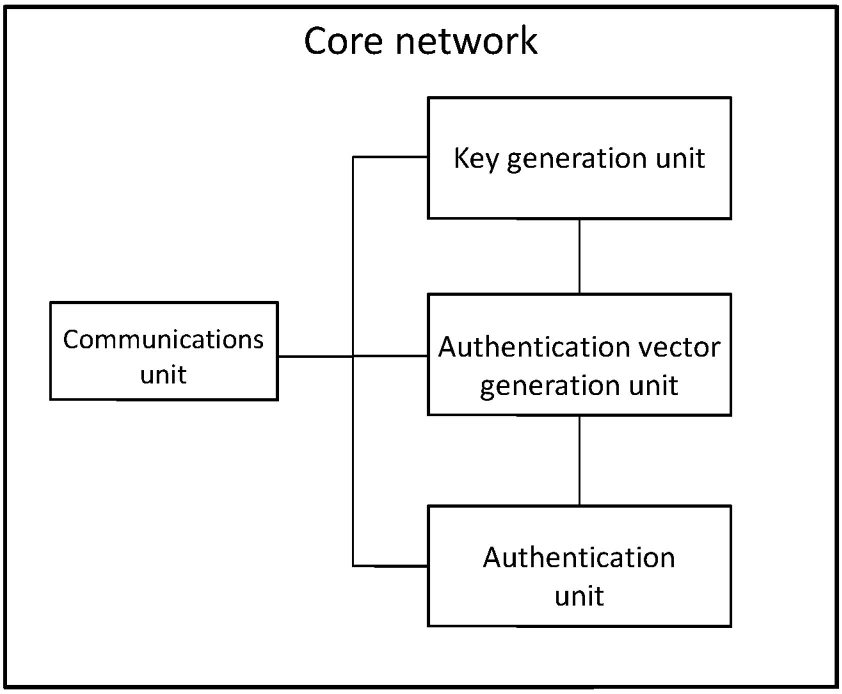

Figure 10

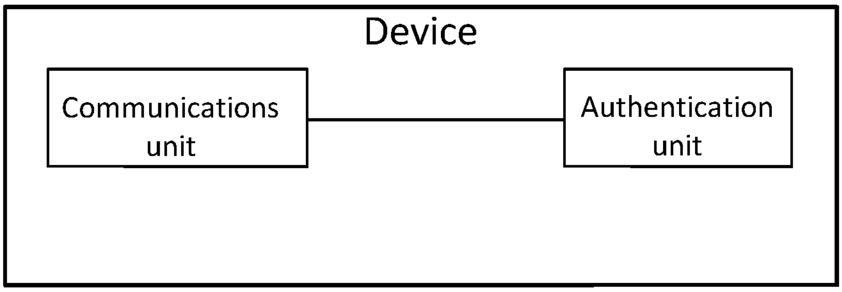

Figure 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/SG2017/050095

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/04 H04W12/06 H04W4/00
ADD.

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

B. FIELDS SEARCHED

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

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

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

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/012168 A1 (RAJADURAI RAJAVELSAMY [IN] ET AL) 10 January 2013 (2013-01-10) abstract; figures 1-4 paragraph [0020] - paragraph [0035] -----	1-7, 16-25,27
X	"Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220 version 6.3.0 Release 6); ETSI TS 133 220", IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. 3-SA3, no. V6.3.0, 1 December 2004 (2004-12-01), XP014028221, ISSN: 0000-0001 paragraph [4.5.2] - paragraph [4.5.3] -----	1-7, 16-27

□ 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
22 May 2017	21/07/2017

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2017/050095

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 additional 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 an 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.:

1-7, 16-27

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.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-7, 16-27

   how to generate an authentication key for the device

   ---

2. claims: 8-15

   how the device can authenticate the core network

   ---

3. claims: 28-35

   how the second core network node can authenticate the device

   ---

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/SG2017/050095

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013012168 A1	10-01-2013	US 2013012168 A1	10-01-2013
		WO 2011115407 A2	22-09-2011