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;

using the generated device key to authenticate a device associated with the device identifier, including

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, without storing the generated device key at the core network node prior to and after authenticating the device.

2. The method of claim 1, 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.

3. The method of claim 1, 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.

4. The method of claim 3, 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.

5. The method of claim 3, 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.

6. The method of claim 1, 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.

7. 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;

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;

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, without storing the device key at the first core network node prior to and after authenticating the device.

8. The method of claim 7, 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.

9. The method of claim 7, 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.

10. The method of claim 7, 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.

11. The method of any of claims 7 to 10, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.

12. A key generation and authentication system comprising:

a first core network node;

a key generation unit provided at the 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;

an authentication vector generation unit provided at the 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, wherein the first core network node is configured to be free of storing the device key therein prior to and after authenticating a device associated with the device identifier.

13. The system of claim 12, 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.

14. The system of claim 12, 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.

15. The system of claim 12, 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.

16. The system of any of claims 12 to 15, wherein the first core network node includes one of Home Subscriber Server (HSS) and Authentication, Authorization and Accounting (AAA) server.