CLAIMS

1. A key management method, comprising:

performing, by a communication apparatus, a primary authentication procedure, and generating a first authentication and key management for applications, AKMA, key and an identifier of the first AKMA key, wherein the identifier of the first AKMA key identifies the first AKMA key, wherein the communication apparatus is a terminal device or a chip system in the terminal device;

sending, by the communication apparatus, a first application session establishment request message to an application function network element, wherein the first application session establishment request message comprises the identifier of the first AKMA key;

receiving, by the communication apparatus, a response message for the first application session establishment request message from the application function network element, wherein the response message for the first application session establishment request message comprises a first failure indication, and the first failure indication indicates an application session establishment failure; and

sending, by the communication apparatus, a second application session establishment request message to the application function network element, wherein the second application session establishment request message comprises an identifier of a second AKMA key, the identifier of the second AKMA key is generated after re-authentication, and the identifier of the second AKMA key identifies the second AKMA key;

wherein after sending the first application session establishment request message to an application function network element, and before receiving a response message for the first application session establishment request message, performing, by the communication apparatus, a procedure of re-authentication to obtain the second AKMA key and the identifier of the second AKMA key.

2. The method according to claim 1, wherein after the performing the procedure of re-authentication, the method further comprises:

deleting the first AKMA key and the first identifier.

3. The method according to claim 1 or 2, wherein the procedure of the re-authentication comprises:

receiving, by the communication apparatus, an authentication request message from a security anchor function network element, wherein the authentication request message comprises a first authentication parameter;

calculating, by the communication apparatus, a second authentication parameter by using a locally stored root key, and checking the first authentication parameter of the security anchor function network element; and

after the check succeeds, sending, by the communication apparatus, a response message for the authentication

request message in the procedure of the re-authentication to the security anchor function network element, wherein the response message for the authentication request message comprises a third authentication parameter.

4. The method according to claim 3, wherein the authentication request message is a non-access stratum, NAS, message authentication request, and the response message for the authentication request message is a NAS message authentication response.

5. The method according to claim 3 or 4, wherein after the sending, by the communication apparatus, a response message for the authentication request message in the procedure of the re-authentication to the security anchor function network element, the method further comprises:

generating, by the communication apparatus, the second AKMA key and the identifier of the second AKMA key.

6. The method according to any one of claims 1 to 5, wherein the first application session establishment request message is an application session establishment request message, and the response message for the first application session establishment request message is an application session establishment response.

7. A key management method, comprising:

receiving, by an application function network element, a first application session establishment request message from a terminal device, wherein the first application session establishment request message comprises an identifier of a first authentication and key management for applications, AKMA, key, and the identifier of the first AKMA key identifies the first AKMA key;

sending, by the application function network element, a first request message to an AKMA anchor function network element, wherein the first request message is for requesting a communication key between the terminal device and the application function network element;

receiving, by the application function network element, a second failure indication from the AKMA anchor function network element, wherein the second failure indication indicates a request failure in the communication key;

sending, by the application function network element, a response message for the first application session establishment request message to the terminal device based on the second failure indication, wherein the response message comprises a first failure indication, and the first failure indication indicates an application session establishment failure; and

receiving, by the application function network element, a second application session establishment request message from the terminal device, wherein the second application session establishment request message comprises an identifier of a second AKMA key, the identifier of the second AKMA key is generated after re-authentication, and the identifier of the second AKMA key identifies the second AKMA key.

8. The method according to claim 7, further comprising:

receiving, by the AKMA anchor function network element, the first request message; and

sending, by the AKMA anchor function network element, the second failure indication to the application function network element.

9. The method according to claim 7 or 8, wherein the first application session establishment request message is an application session establishment request message, and the response message for the first application session establishment request message is an application session establishment response.

10. A communication apparatus, comprising a processing unit, a sending unit, and a receiving unit, wherein

the processing unit is configured to: perform a primary authentication procedure, and generate a first authentication and key management for applications, AKMA, key and an identifier of the first AKMA key, wherein the identifier of the first AKMA key identifies the first AKMA key;

the sending unit is configured to send a first application session establishment request message to an application function network element, wherein the first application session establishment request message comprises the identifier of the first AKMA key;

the processing unit is configured to perform a procedure of re-authentication to obtain a second AKMA key and an identifier of the second AKMA key

the receiving unit is configured to receive a response message for the first application session establishment request message from the application function network element, wherein the response message for the first application session establishment request message comprises a first failure indication, and the first failure indication indicates an application session establishment failure; and

the sending unit is further configured to send a second application session establishment request message to the application function network element, wherein the second application session establishment request message comprises the identifier of the second AKMA key, the identifier of the second AKMA key is generated after re-authentication, and the identifier of the second AKMA key identifies the second AKMA key.

11. The apparatus according to claim 10, wherein

the procedure of the re-authentication comprises:

receiving an authentication request message from a security anchor function network element, wherein the authentication request message comprises a first authentication parameter;

calculating a second authentication parameter by using a locally stored root key, and checking the first authentication parameter of the security anchor function network element; and

after the check succeeds, sending a response message for the authentication request message in the procedure of the re-authentication to the security anchor function network element, wherein the response message for the

authentication request message comprises a third authentication parameter.

12. A communication apparatus, comprising a receiving unit, a sending unit, and a processing unit, wherein

the receiving unit is configured to receive a first application session establishment request message from a terminal device, wherein the first application session establishment request message comprises an identifier of a first authentication and key management for applications AKMA key, and the identifier of the first AKMA key identifies the first AKMA key;

the sending unit is configured to send a first request message to an AKMA anchor function network element, wherein the first request message is for requesting a communication key between the terminal device and the apparatus;

the receiving unit is further configured to receive a second failure indication from the AKMA anchor function network element, wherein the second failure indication indicates a request failure in the communication key;

the processing unit is configured to send a response message for the first application session establishment request message to the terminal device based on the second failure indication through the sending unit, wherein the response message comprises a first failure indication, and the first failure indication indicates an application session establishment failure; and

the receiving unit is further configured to receive a second application session establishment request message from the terminal device, wherein the second application session establishment request message comprises an identifier of a second AKMA key, the identifier of the second AKMA key is generated after re-authentication, and the identifier of the second AKMA key identifies the second AKMA key.

13. A computer-readable storage medium, comprises instructions, wherein when the instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 9.

14. A computer program product comprising instructions, wherein when the computer program product runs on a computer, the computer is enabled to perform the method according to any one of claims 1 to 9.