Claims

1. An authentication and/or key management method, comprising:

receiving, by a first device, a session establishment request message initiated by a user equipment (UE), wherein the request message carries a key identifier, the first device comprises an Authentication and Key Management for Applications (AKMA) application proxy, or an authentication proxy, or an AKMA authentication proxy, and the first device is configured to a proxy of a group of application functions (AF)/application servers (AS) or to a proxy of AF/AS in a same trust domain;

acquiring, by the first device, a first key between the first device and the UE according to the key identifier;

the method further comprises:

receiving, by the first device, a data which is protected by the UE based on a third key, and sending the data to a second device, wherein the third key is generated by the UE and is the same as the first key;

and/or,

receiving, by the first device, data sent by the second device, protecting the data based on the first key, and sending the data to the UE.

2. The method according to claim 1, further comprising:

generating, by the first device, a second key between the UE and the second device for the second device according to the first key.

3. The method according to claim 2, wherein the generating, by the first device, the second key between the UE and the second device for the second device according to the first key comprises:

generating, by the first device, a second key based on the first key and identification information of the second device.

4. The method according to claim 1, wherein the acquiring the first key between the first device and the UE according to the key identifier comprises:

acquiring, by the first device, a local first key corresponding to the key identifier according to the key identifier;

or,

acquiring, by the first device, a first key corresponding to the key identifier from an AKMA Anchor Function (AAnF) according to the key identifier.

5. The method according to claim 1, further comprising: providing for the UE, by the first device, a list of second devices that the UE is able to access.

6. The method according to claim 1, further comprising: establishing, by the first device, a transport layer security (TLS) secure channel with the UE.

7. The method according to claim 6, wherein the establishing by the first device the TLS secure channel with the UE comprises:

generating, by the first device, a premaster key or an external pre-shared key of the TLS secure channel based on the first key or a key derived from the first key.

8. The method according to any one of claims 1, 6 and 7, further comprising:

sending, by the first device, first protected data to the UE, wherein the first protected data comprises data protected by the first device based on the first key or the key derived from the first key.

9. The method according to any one of claims 1, 6 and 7, further comprising:

receiving, by the first device, data sent by the UE and protected based on the third key or a key derived from the third key.

10. An authentication and/or key management method, comprising:

sending, by a user equipment (UE), a session establishment request message to a first device, wherein the request message carries a key identifier, the first device comprises an Authentication and Key Management for Applications (AKMA) application proxy, or an authentication proxy, or an AKMA authentication proxy, and the first device is configured to a proxy of a group of application functions (AF)/application servers (AS) or to a proxy of AF/AS in a same trust domain;

receiving, by the UE, a first protected data sent by the first device, wherein the first protected data comprises a data protected by the first device based on a first key or a key derived from the first key, wherein the first key is acquired by the first device according to the key identifier;

the method further comprises:

generating, by the UE, a third key that is the same as the first key, and sending, to the first device, a data protected by the third key or a key derived from the third key, to enable the first device to send the data to a second device;

and/or,

receiving, by the UE, a data protected and forwarded by the first device based on the first key.

11. The method according to claim 10, further comprising:

generating, by the UE, a fourth key that is the same as a second key, and receiving a second protected data sent by the second device, wherein the second

protected data comprises a data protected by the second device based on the second key, wherein the second key is generated by the first device for the second device based on the first key.

12. The method according to claim 10, further comprising:

acquiring, by the UE, from the first device, a list of second devices that the UE is able to access.

13. The method according to claim 10, further comprising:

establishing, by the UE, a transport layer security (TLS) secure channel with the first device.

14. The method according to claim 10, wherein the establishing by the UE the TLS secure channel with the first device comprises:

generating, by the UE, a third key that is the same as the first key;

generating, by the UE, a premaster key or an external pre-shared key of the TLS secure channel based on the third key or a key derived from the third key.

15. A communication device, comprising a memory, a processor, and a program stored in the memory and executable on the processor; the processor is configured to execute the program to perform the authentication and/or key management method according to any one of claims 1 to 9.

16. A communication device, comprising a memory, a processor, and a program stored in the memory and executable on the processor; the processor is configured to execute the program to perform the authentication and/or key management method according to any one of claims 10 to 14.