CLAIMS

1. A method for secure channel establishment, applied to a fifth generation message (MSGin5G) user equipment (UE), the method comprising:

generating a first key based on an authentication and key management for application (AKMA) service; and

establishing a secure channel between the MSGin5G UE and an MSGin5G server based on the first key;

wherein establishing the secure channel between the MSGin5G UE and the MSGin5G server based on the first key comprises:

generating a third key based on the first key, and sending a client key exchange message comprising a first identity (ID) to the MSGin5G server, wherein the third key is a premaster key; and

establishing a transport layer security (TLS) secure channel between the MSGin5G UE and the MSGin5G server using the third key.

2. The method of claim 1, further comprising: before generating the first key based on the AKMA service,

performing primary authentication between the MSGin5G UE and a core network.

3. The method of claim 1, wherein generating the first key based on the AKMA service comprises:

sending a session establishment request to the MSGin5G server, the session establishment request comprising at least a first identity (ID); and

generating the first key using a second key identified by the first ID, the second key and the first ID being generated based on the AKMA service.

4. The method of claim 3, wherein generation of the first key using the second key identified by the first ID is performed before or after sending the session establishment request to the MSGin5G server.

5. The method of claim 3, further comprising:

receiving a session establishment response sent by the MSGin5G server,

wherein generation of the first key is performed before or after receiving the session establishment response.

6. A method for secure channel establishment, applied to a fifth generation message (MSGin5G) server, the method comprising:

acquiring a first key based on an authentication and key management for application (AKMA) service; and

establishing a secure channel between the MSGin5G server and an MSGin5G user equipment (UE) based on the first key;

wherein establishing the secure channel between the MSGin5G server and the MSGin5G UE based on the first key comprises:

receiving a client key exchange message sent by the MSGin5G UE, the client key exchange message comprising a first identity (ID); and

acquiring the first key from the MSGin5G server locally according to the first ID, generating a third key using the first key, and establishing a transport layer security (TLS) secure channel between the MSGin5G server and the MSGin5G UE using the third key, wherein the third key is a premaster key.

7. The method of claim 6, wherein acquiring the first key based on the AKMA service comprises:

receiving a session establishment request sent by the MSGin5G UE, the session establishment request comprising at least a first identity (ID);

sending a key request to a core network, the key request comprising at least the first ID; and

receiving first information sent by the core network, the first information comprising at least the first key, the first key being generated based on a second key identified by the first ID, the second key and the first ID being generated based on the AKMA service.

8. The method of claim 7, wherein first information further comprises a cycle of the first key, the cycle indicating a lifecycle specified by a policy.

9. A fifth generation message (MSGin5G) user equipment (UE), comprising:

a first processing unit, configured to generate a first key based on an authentication and key management for application (AKMA) service; and

a second processing unit, configured to establish a secure channel between the MSGin5G UE and an MSGin5G server based on the first key;

wherein the second processing unit is configured to:

generate a third key based on the first key, and send a client key exchange message comprising a first identity (ID) to the MSGin5G server, wherein the third key is a premaster key; and

establish a transport layer security (TLS) secure channel between the MSGin5G UE and the MSGin5G server using the third key.

10. The MSGin5G UE of claim 9, wherein the first processing unit is configured to, before generating the first key based on the AKMA service, perform primary authentication between the MSGin5G UE and a core network.

11. The MSGin5G UE of claim 9, wherein the first processing unit is configured to:

send a session establishment request to the MSGin5G server, the session establishment request comprising at least a first identity (ID); and

generate the first key using a second key identified by the first ID, the second key and the first ID being generated based on the AKMA service.

12. A fifth generation message (MSGin5G) server, comprising:

a third processing unit, configured to acquire a first key based on an authentication and key management for application (AKMA) service; and

a fourth processing unit, configured to establish a secure channel between the MSGin5G server and an MSGin5G user equipment (UE) based on the first key;

wherein the fourth processing unit is configured to:

receive a client key exchange message sent by the MSGin5G UE, the client key exchange message comprising a first identity (ID); and

acquire the first key from the MSGin5G server locally according to the first ID, generate

a third key using the first key, and establish a transport layer security (TLS) secure channel between the MSGin5G server and the MSGin5G UE using the third key, wherein the third key is a premaster key.

13. A storage medium, having stored thereon a computer program which, when executed by a processor, implements operations of the method of any one of claims 1 to 5, or implements operations of the method of any one of claims 6 to 8.