CLAIMS

1. A method for configuring a terminal device, characterized by, comprising:

performing, by a Universal Subscriber Identity Module (USIM) of the terminal device, a Generic Bootstrapping Architecture (GBA) authentication process or an Authentication and Key Management for Applications (AKMA) authentication process with a network device, and generating, by the USIM, at least one first key, wherein the at least one first key is generated by the USIM through negotiation with a Bootstrapping Server Function (BSF);

generating, by the USIM of the terminal device, at least one second key based on the at least one first key, and performing, by the USIM of the terminal device, at least encryption or integrity protection on at least one certificate request message based on the at least one second key;

transmitting, by the USIM of the terminal device to an application client included in the terminal device, at least one message which comprises the at least one certificate request message at least encrypted or integrity-protected by the at least one second key; and

transmitting, by the application client to a server, at least one first request message which comprises the at least one certificate request message at least encrypted or integrity-protected by the at least one second key, and comprises a Bootstrapping-Transaction Identifier (B-TID) and a Fully Qualified Domain Name (FQDN) of the server .

2. The method of claim 1, further comprising:

receiving, by the terminal device, at least one first response message from a server, and performing, by the terminal device, at least integrity verification or decryption on the at least one first response message based on the at least one second key, and obtaining, by the terminal device, at least one digital certificate carried in the at least one first response message.

3. The method of claim 1, wherein the terminal device comprises a modem, and

wherein the generating, by the USIM of the terminal device, the at least one second key based on the at least one first key, and performing, by the USIM of the terminal device, at least encryption or integrity protection on the at least one certificate request message based on the at least one second key comprises:

triggering, by the application client, the USIM through the modem, to generate the at least one second key based on the at least one first key;

generating, by the application client, at least one first certificate request message, and transmitting, by the application client, the at least one first certificate request message to the USIM through the modem;

generating, by the USIM, a public/private key pair, and adding, by the USIM, the public key in the public/private key pair to the at least one first certificate request message, and signing, by the USIM, the at least one first certificate request message with the private key in the public/private key pair, to obtain at least one second certificate request message;

performing, by the USIM, at least encryption or integrity protection on the at least one second certificate request message based on the at least one second key, thereby obtaining at least one processed certificate request message, wherein performing integrity protection includes: adding, by the USIM, a first verification value to the at least one second certificate request message; and

transmitting, by the USIM, the at least one processed second certificate request message to the application client through the modem.

4. The method of claim 2, wherein the terminal device comprises a modem, and

wherein the receiving, by the terminal device, the at least one first response message from the server, and performing, by the terminal device, at least integrity verification or decryption on the at least one first response message based on the at least one second key, and obtaining, by the terminal device, the at least one digital certificate carried in the at least one first response message comprises:

receiving, by the application client, the at least one first response message from the server, and transmitting, by the application client, the at least one first response message to the USIM through the modem;

performing, by the USIM, at least integrity verification or decryption on the at least one first response message based on the at least one second key; and

obtaining, by the USIM, the at least one digital certificate carried in the at least one first response message after the verification is passed, and storing, by the USIM, the at least one digital certificate in a security component.

5. A method for configuring a terminal device, characterized by, comprising:

receiving, by a server, at least one first request message, which comprises at least one certificate request message at least encrypted or integrity-protected by at least one second key, and comprises a Bootstrapping-Transaction Identifier (B-TID) and a Fully Qualified Domain Name (FQDN) of the server, from the terminal device;

obtaining, by the server, the at least one second key from a network device, comprising: transmitting, by the server, at least one second request message to the network device, the at least one second request message being configured to request the at least one second key and comprising

the B-TID and the FQDN; and receiving, by the server, at least one second response message transmitted by the network device, the at least one second response message comprising the at least one second key;

performing, by the server, at least integrity verification or decryption on the at least one first request message based on the at least one second key, and

wherein in a case that the server receives the at least one first request message, the method further comprises:

issuing, by the server, at least one digital certificate after authorization of the at least one first request message is passed; and

transmitting, by the server, at least one first response message to the terminal device, the at least one first response message comprising the at least one digital certificate.

6. The method of claim 5, wherein transmitting, by the server, the at least one first response message to the terminal device comprises:

constructing, by the server, the at least one first response message containing the at least one digital certificate, and performing, by the server, at least encryption or integrity protection on the at least one first response message based on the at least one second key, thereby obtaining at least one processed first response message, wherein performing integrity protection includes: adding, by the server, a second verification value to the at least one first response message; and

transmitting, by the server, the at least one processed first response message to the terminal device.

7. The method of claim 5, wherein

obtaining, by the server, the at least one second key from the network device comprises:

querying, by the server, whether there is at least one second key corresponding to the B-TID; and

obtaining, by the server, the at least one second key from the network device, in response to the querying result indicating that there is no second key corresponding to the B-TID.

8. A method for configuring a terminal device, characterized by, comprising:

acquiring, by a network device, at least one first key from a Bootstrapping Server Function (BSF), wherein the at least one first key is generated by the BSF through negotiation with a Universal Subscriber Identity Module (USIM) in the terminal device through performing a Generic Bootstrapping Architecture (GBA) authentication process or an Authentication and Key Management for Applications (AKMA) authentication process with the USIM in the terminal

device,

receiving, by the network device from a server, at least one second request message comprising a Bootstrapping-Transaction Identifier (B-TID) and a Fully Qualified Domain Name (FQDN) of the server, the at least one second request message being configured to request at least one second key,

generating, by the network device, the at least one second key based on the at least one first key, and

transmitting, by the network device, the at least one second key to the server.

9. The method of claim 8, wherein generating, by the network device, the at least one second key based on the at least one pre-negotiated first key, and transmitting, by the network device, the at least one second key to the server comprises:

generating, by the network device, at least one corresponding second key for the server based on the at least one pre-negotiated first key, and transmitting, by the network device, the corresponding second key to the server.

10. The method of any one of claims 8 and 9, wherein transmitting, by the network device, the at least one second key to the server comprises:

transmitting, by the network device, at least one second response message to the server, the at least one second response message comprising the at least one second key.

11. A communication device, comprising a memory, a processor, and a computer program stored on the memory and executable by the processor, the processor being configured to implement the method of any one of claims 1 to 4 when the processor executes the computer program,

or, the processor being configured to implement the method of any one of claims 5 to 7 when the processor executes the computer program,

or, the processor being configured to implement steps of the method of any one of claims 8 to 10 when the processor executes the computer program.