a wearable device, or a computing device that has a wireless communication function. For example, the UE may be a mobile phone (mobile phone), a tablet computer, or a computer with a wireless transceiver function. Alternatively, the terminal device may be a virtual reality (virtual reality, VR) terminal device, an augmented reality (augmented reality, AR) terminal device, a wireless terminal in industrial control, or the like.

[00123] The vehicle-mounted control device in embodiments of this application, for example, the vehicle-mounted control device 103, is any vehicle-mounted device having a communication capability and a computing capability. For example, the vehicle-mounted control device is an OTA manager (OTA Manager), a telematics box (telematics box, T-Box), a gateway (gateway), a multi-domain controller (multi-domain controller, MDC), a vehicle control unit (vehicle control unit, VCU), or an electronic control unit (electronic control unit, ECU).

[00124] In FIG. 1A, the server 101 and the vehicle-mounted control device 103 are mutual-trust devices, and the vehicle-mounted control device 103 and the electronic device 102 are mutual-trust devices. In other words, a trust relationship is established between the server 101 and the vehicle-mounted control device 103, and a trust relationship is established between the vehicle-mounted control device 103 and the electronic device 102. In this way, the electronic device 102 may request an upgrade package of at least one vehicle-mounted device from the server 101 based on an identity authentication credential (first public key information or a proxy signature key in the following) provided by the vehicle-mounted control device 103 for the electronic device 102. After verifying that the identity authentication credential is valid, the server 101 sends the upgrade package to the electronic device 102, so that the electronic device 102 sends the upgrade package to the vehicle-mounted control device 103 at an appropriate time, to ensure security of upgrading the vehicle-mounted device.

[00125] Optionally, the electronic device 102 may further assist in storing software information or firmware information of the vehicle-mounted device, for example, at least one of current version information of software/firmware, a size of software/firmware, or developer information of software/firmware.

[00126] Optionally, the electronic device 102 may further convert a security mechanism between the server 101 and the vehicle-mounted control device 103. For example, the server 101 sends, to the electronic device 102, information obtained by encrypting first information according to a first algorithm. After receiving the information, the electronic device 102 decrypts the information to obtain the first information, and sends, to the vehicle-mounted control device 103, information obtained by encrypting the first information according to a second algorithm. It may be understood that after receiving the information obtained by encrypting the first information according to the first algorithm, the electronic device 102 may further detect the information via a

CLAIMS

1. A vehicle-mounted device upgrade method, applied to a server, wherein the method comprises:

receiving first signature information and first public key information from an electronic device, wherein the first signature information is obtained by signing a first upgrade request based on a private key of the electronic device, the first upgrade request is used to request an upgrade package of at least one vehicle-mounted device, the first public key information is used to verify an identity of the electronic device, and the first public key information comprises a public key certificate of a public key of the electronic device, or the first public key information comprises a public key of the electronic device; and

when verification of the first signature information and the first public key information succeeds, sending the upgrade package to the electronic device.

2. The method according to claim 1, wherein the method further comprises:

verifying the first signature information based on the public key of the electronic device.

3. The method according to claim 1 or 2, wherein the method further comprises:

receiving the public key of the electronic device from a vehicle-mounted control device; and

sending the public key certificate to the vehicle-mounted control device, wherein the public key certificate is generated based on a private key of the server.

4. A vehicle-mounted device upgrade method, applied to an electronic device, wherein the method comprises:

sending first signature information and first public key information to a server, wherein the first signature information is obtained by signing a first upgrade request based on a private key of the electronic device, the first upgrade request is used to request an upgrade package of at least one vehicle-mounted device, the first public key information is used to verify an identity of the electronic device, and the first public key information comprises a public key certificate of a public key of the electronic device, or the first public key information comprises a public key of the electronic device;

receiving the upgrade package from the server; and

sending the upgrade package to a vehicle-mounted control device.

5. The method according to claim 4, wherein the method further comprises:

receiving the public key certificate from the vehicle-mounted control device, wherein the public key certificate is generated based on a private key of the vehicle-mounted control device, or the public key certificate is generated based on a private key of the server.

6. The method according to claim 5, wherein the method further comprises:

obtaining the public key of the electronic device and the private key of the electronic device; and

sending the public key of the electronic device to the vehicle-mounted control device.

7. The method according to any one of claims 4 to 6, wherein the first upgrade request comprises upgrade information of the at least one vehicle-mounted device.

8. The method according to any one of claims 4 to 7, wherein the public key certificate comprises at least one of the following: the upgrade information of the at least one vehicle-mounted device, an identifier of the vehicle-mounted control device, an identifier of the server, an identifier of the electronic device, an authorization period, or authorization purpose information.

9. A vehicle-mounted device upgrade method, applied to a vehicle-mounted control device, wherein the method comprises:

receiving a public key of an electronic device from the electronic device; and

sending a public key certificate of the public key of the electronic device to the electronic device, wherein the public key certificate is generated based on a private key of the vehicle-mounted control device, or the public key certificate is generated based on a private key of a server.

10. The method according to claim 9, wherein the public key certificate is generated based on the private key of the server, and the method further comprises:

sending the public key of the electronic device to the server; and

receiving the public key certificate from the server.

11. The method according to claim 9 or 10, wherein the public key certificate comprises at least one of the following: upgrade information of at least one vehicle-mounted device, an identifier of the vehicle-mounted control device, an identifier of the server, an identifier of the electronic device, an authorization period, or authorization purpose information.

12. The method according to claim 11, wherein the method further comprises:

sending the upgrade information of the at least one vehicle-mounted device to the electronic device.

13. A communication device, comprising: a processor, wherein the processor is coupled to a memory, the memory is configured to store a program or instructions, and when the program or the instructions are executed by the processor, the apparatus is enabled to perform the method according to any one of claims 1 to 3, or perform the method according to any one of claims 4 to 8, or perform the method according to any one of claims 9 to 12.

14. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program or instructions, and when the computer program or the instructions are executed, a computer is enabled to perform the method according to any one of claims 1 to 3, or perform the method according to any one of claims 4 to 8, or perform the method according to any

one of claims 9 to 12.

15. A vehicle, comprising a transceiver module, wherein

the transceiver module is configured to receive a public key of an electronic device from the electronic device; and

the transceiver module is further configured to send a public key certificate of the public key of the electronic device to the electronic device, wherein the public key certificate is generated based on a private key of the communication device, or the public key certificate is generated based on a private key of a server.