

车载设备的升级方法及设备

5 技术领域

本申请涉及信息与通信技术领域，尤其涉及车载设备的升级方法及设备。

背景技术

随着计算机技术和互联网技术地不断发展，车载设备的功能越来越丰富。为了不断完善车载设备的功能，车载设备的固件或软件需要定期升级。通常，车载设备的固件或软件是通过将车辆召回的方式来升级的，这种升级方式成本高并且升级周期较长。

为了解决这个问题，通过空中下载（over the air，OTA）技术升级车载设备的方案被提出了。例如，车辆的外部设备向服务器请求升级包，并将请求到的升级包发送给车载设备，以便车载设备升级自己的固件或软件。但是，这种方法存在很大的安全隐患。

发明内容

本申请实施例提供车载设备的升级方法及设备，可以保障车载设备升级的安全性。

为达到上述目的，本申请的实施例采用如下技术方案：

第一方面，提供了一种车载设备的升级方法，该方法可以由服务器执行；或者，也可以由应用于服务器中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分服务器功能的逻辑模块或软件实现，对此不作限定。为了便于描述，下面以由服务器执行为例进行说明。

该方法包括：接收来自电子设备的第一签名信息和第一公钥信息，该第一签名信息是用该电子设备的私钥对第一升级请求进行签名得到的，该第一升级请求用于请求至少一个车载设备的升级包，该第一公钥信息用于验证该电子设备的身份，该第一公钥信息包括该电子设备的公钥的公钥证书，或者，该第一公钥信息包括该电子设备的公钥；在该第一签名信息和该第一公钥信息验证成功的情况下，向该电子设备发送该升级包。

基于上述第一方面提供的方法，服务器可以通过第一公钥信息验证电子设备的合法性，如电子设备是否有下载升级包的权限等，通过第一签名信息验证接收到的信息是否被篡改，以保障车载设备升级的安全性。

在一种可能的实现方式中，该方法还包括：根据该电子设备的公钥验证该第一签名信息。

基于上述可能的实现方式，可以验证第一签名信息是否被篡改，以提高通信安全。

在一种可能的实现方式中，该方法还包括：接收来自车载控制设备的该电子设备

的公钥；向该车载控制设备发送该公钥证书，该公钥证书是根据该服务器的私钥生成的。

基于上述可能的实现方式，服务器可以为电子设备的公钥生成公钥证书，以便服务器根据该公钥证书验证电子设备的合法性。

5 在一种可能的实现方式中，该方法还包括：根据该服务器的公钥验证该公钥证书。

基于上述可能的实现方式，若该公钥证书是服务器根据自己的私钥生成的，则服务器可以根据自己的公钥验证该公钥证书。

10 在一种可能的实现方式中，该公钥证书是根据车载控制设备的私钥生成的，该方法还包括：根据该车载控制设备的公钥验证该公钥证书。

基于上述可能的实现方式，若该公钥证书是根据车载控制设备的私钥生成的，则服务器可以根据车载控制设备的公钥验证该公钥证书。

在一种可能的实现方式中，该方法还包括：接收来自车载控制设备的该电子设备的公钥；生成该电子设备的公钥的授权信息。

15 基于上述可能实现方式，服务器可以为电子设备的公钥生成该公钥的授权信息，以便服务器根据该授权信息验证电子设备的合法性。

在一种可能的实现方式中，该方法还包括：根据该授权信息验证该电子设备的公钥。

20 基于上述可能的实现方式，服务器不需要公钥证书来验证电子设备的合法性，而是通过该授权信息验证电子设备的合法性，整个验证过程不需要使用证书链，验证效率高。

在一种可能的实现方式中，该方法还包括：删除该授权信息。

基于上述可能的实现方式，服务器可以取消对电子设备的授权。

25 在一种可能的实现方式中，该第一升级请求包括该至少一个车载设备的待升级信息。

30 基于上述可能的实现方式，服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。例如，若服务器中存储的最新发布的软件的版本信息与待升级信息中的版本信息相同，则服务器确定至少一个车载设备不需要升级；若服务器中存储的最新发布的软件的版本信息比待升级信息中的版本信息更高，则服务器确定至少一个车载设备需要升级。

在一种可能的实现方式中，该公钥证书包括以下至少一项：该至少一个车载设备的待升级信息、车载控制设备的标识、该服务器的标识、该电子设备的标识、授权期限或授权目的信息。

35 基于上述可能的实现方式，若公钥证书包括至少一个车载设备的待升级信息，则表示该公钥证书的授权期限为短期或一次性授权。可选的，若该公钥证书包括至少一个车载设备的待升级信息，还表示该公钥证书用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。若公钥证书包括车载控制设备的标识，则表示该公钥证书是车载控制设备生成或授权的。若公钥证书包括服务器的标识，则表示该公钥证书是服务器生成或授权的。若公钥证书包括电子设备的标识，则表示该公钥证书是

授权给电子设备的。

- 第二方面，提供了一种车载设备的升级方法，该方法可以由电子设备执行；或者，也可以由应用于电子设备中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分电子设备功能的逻辑模块或软件实现，对此不作限定。为了
5 便于描述，下面以由电子设备执行为例进行说明。

该方法包括：向服务器发送第一签名信息和第一公钥信息，该第一签名信息是用该电子设备的私钥对第一升级请求进行签名得到的，该第一升级请求用于请求至少一个车载设备的升级包，该第一公钥信息用于验证该电子设备的身份，该第一公钥信息包括该电子设备的公钥的公钥证书，或者，该第一公钥信息包括该电子设备的公钥；
10 接收来自该服务器的该升级包；向车载控制设备发送该升级包。

基于上述第二方面提供的方法，电子设备可以向服务器发送第一签名信息和第一公钥信息，使得服务器可以通过第一公钥信息验证电子设备的合法性，如电子设备是否有下载升级包的权限等，通过第一签名信息验证接收到的信息是否被篡改，以保障车载设备升级的安全性。

- 15 在一种可能的实现方式中，该方法还包括：接收来自该车载控制设备的该公钥证书，该公钥证书是根据该车载控制设备的私钥生成的，或者，该公钥证书是根据该服务器的私钥生成的。

基于上述可能的实现方式，电子设备可以获取到公钥证书，以便后续通过公钥证书向服务器请求至少一个车载设备的升级包。

- 20 在一种可能的实现方式中，该方法还包括：获取该电子设备的公钥和该电子设备的私钥；向该车载控制设备发送该电子设备的公钥。

基于上述可能的实现方式，电子设备获取到自己的公钥后，可以向车载控制设备发送该公钥，以便车载控制设备或服务器为该公钥生成公钥证书。

- 25 在一种可能的实现方式中，该第一升级请求包括该至少一个车载设备的待升级信息。

基于上述可能的实现方式，服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。例如，若服务器中存储的最新发布的软件的版本信息与待升级信息中的版本信息相同，则服务器确定至少一个车载设备不需要升级；若服务器中存储的最新发布的软件的版本信息比待升级信息中的版本信息更高，则服务器确定至少一个车载设备需要升级。
30

在一种可能的实现方式中，该公钥证书包括以下至少一项：该至少一个车载设备的待升级信息、该车载控制设备的标识、该服务器的标识、该电子设备的标识、授权期限或授权目的信息。

- 35 基于上述可能的实现方式，若公钥证书包括至少一个车载设备的待升级信息，则表示该公钥证书的授权期限为短期或一次性授权。可选的，若该公钥证书包括至少一个车载设备的待升级信息，还表示该公钥证书用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。若公钥证书包括车载控制设备的标识，则表示该公钥证书是车载控制设备生成或授权的。若公钥证书包括服务器的标识，则表示该公钥证书是服务器生成或授权的。若公钥证书包括电子设备的标识，则表示该公钥证书是

授权给电子设备的。

在一种可能的实现方式中，该方法还包括：接收来自该车载控制设备的该至少一个车载设备的待升级信息。

5 基于上述可能的实现方式，电子设备可以从车载控制设备获取至少一个车载设备的待升级信息，以便电子设备向服务器发送该待升级信息，使得服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。

第三方面，提供了一种车载设备的升级方法，该方法可以由车载控制设备执行；或者，也可以由应用于车载控制设备中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分车载控制设备功能的逻辑模块或软件实现，对此不作
10 限定。为了便于描述，下面以由车载控制设备执行为例进行说明。

该方法包括：接收来自电子设备的该电子设备的公钥；向该电子设备发送该电子设备的公钥的公钥证书，该公钥证书是根据该车载控制设备的私钥生成的，或者，该公钥证书是根据服务器的私钥生成的。

15 基于上述第三方面提供的方法，车载控制设备可以向电子设备发送电子设备的公钥的公钥证书，以便电子设备根据该公钥证书向服务器请求升级包。

在一种可能的实现方式中，该公钥证书是根据服务器的私钥生成的，该方法还包括：向该服务器发送该电子设备的公钥；接收来自该服务器的该公钥证书。

基于上述可能的实现方式，车载控制设备可以向服务器发送电子设备的公钥，以便服务器为该公钥生成公钥证书。

20 在一种可能的实现方式中，该公钥证书包括以下至少一项：至少一个车载设备的待升级信息、该车载控制设备的标识、该服务器的标识、该电子设备的标识、授权期限或授权目的信息。

基于上述可能的实现方式，若公钥证书包括至少一个车载设备的待升级信息，则表示该公钥证书的授权期限为短期或一次性授权。可选的，若该公钥证书包括至少一个车载设备的待升级信息，还表示该公钥证书用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。若公钥证书包括车载控制设备的标识，则表示该公钥证书是车载控制设备生成或授权的。若公钥证书包括服务器的标识，则表示该公钥证书是服务器生成或授权的。若公钥证书包括电子设备的标识，则表示该公钥证书是
25 授权给电子设备的。

30 在一种可能的实现方式中，该方法还包括：向所电子设备发送该至少一个车载设备的待升级信息。

基于上述可能的实现方式，车载控制设备可以向电子设备发送至少一个车载设备的待升级信息，以便电子设备向服务器发送该待升级信息，使得服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。

35 第四方面，提供了一种车载设备的升级方法，该方法可以由车载控制设备执行；或者，也可以由应用于车载控制设备中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分车载控制设备功能的逻辑模块或软件实现，对此不作限定。为了便于描述，下面以由车载控制设备执行为例进行说明。

该方法包括：接收来自电子设备的该电子设备的公钥；向服务器发送第一指示信

息和该电子设备的公钥，该第一指示信息用于指示生成该电子设备的公钥的授权信息。

基于上述第四方面提供的方法，车载控制设备可以指示服务器为电子设备的公钥生成授权信息。这样，在电子设备向服务器请求升级包时，服务器不需要公钥证书来验证电子设备的合法性，而是通过该授权信息验证电子设备的合法性，整个验证过程不需要使用证书链，验证效率高。

在一种可能的实现方式中，该方法还包括：向该电子设备发送至少一个车载设备的待升级信息。

基于上述可能的实现方式，车载控制设备可以向电子设备发送至少一个车载设备的待升级信息，以便电子设备向服务器发送该待升级信息，使得服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。

第五方面，提供了一种车载设备的升级方法，该方法可以由服务器执行；或者，也可以由应用于服务器中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分服务器功能的逻辑模块或软件实现，对此不作限定。为了便于描述，下面以由服务器执行为例进行说明。

该方法包括：接收来自电子设备的第二签名信息，该第二签名信息用于验证该电子设备的身份，该第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，该代理签名密钥是根据车载控制设备的私钥和该代理签名密钥的授权信息得到的，该第一升级请求用于请求至少一个车载设备的升级包；在该第二签名信息验证成功的情况下，向该电子设备发送该升级包。

基于上述第五方面提供的方法，服务器可以通过第二签名信息验证电子设备的合法性，如电子设备是否有下载升级包的权限等，以及验证接收到的信息是否被篡改，以保障车载设备升级的安全性。

在一种可能的实现方式中，该方法还包括：根据该车载控制设备的公钥验证该第二签名信息。

基于上述可能的实现方式，服务器可以根据车载控制设备的公钥验证第二签名信息，以验证电子设备的合法性，以及接收到的信息是否被篡改。

在一种可能的实现方式中，该方法还包括：将该授权信息存入授权信息取消列表。

基于上述可能的实现方式，服务器可以通过将授权信息存入授权信息取消列表，来取消对电子设备的授权。

在一种可能的实现方式中，该第一升级请求包括该至少一个车载设备的待升级信息。

基于上述可能的实现方式，服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。例如，若服务器中存储的最新发布的软件的版本信息与待升级信息中的版本信息相同，则服务器确定至少一个车载设备不需要升级；若服务器中存储的最新发布的软件的版本信息比待升级信息中的版本信息更高，则服务器确定至少一个车载设备需要升级。

在一种可能的实现方式中，该授权信息包括以下至少一项：该至少一个车载设备

的待升级信息、该车载控制设备的标识、该服务器的标识、该电子设备的标识、授权期限或授权目的信息。

基于上述可能的实现方式，若授权信息包括至少一个车载设备的待升级信息，则表示该代理签名密钥的授权期限为短期或一次性授权。可选的，若该授权信息包括至少一个车载设备的待升级信息，还表示该代理签名密钥用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。若授权信息包括车载控制设备的标识，则表示该代理签名密钥是车载控制设备生成或授权的。若授权信息包括服务器的标识和电子设备的标识，则表示该代理签名密钥是用于服务器和电子设备之间的验证的。

第六方面，提供了一种车载设备的升级方法，该方法可以由电子设备执行；或者，也可以由应用于电子设备中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分电子设备功能的逻辑模块或软件实现，对此不作限定。为了便于描述，下面以由电子设备执行为例进行说明。

该方法包括：向服务器发送第二签名信息，该第二签名信息用于验证该电子设备的身份，该第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，该代理签名密钥是根据车载控制设备的私钥和该代理签名密钥的授权信息得到的，该第一升级请求用于请求至少一个车载设备的升级包；接收来自该服务器的该升级包；向车载控制设备发送该升级包。

基于上述第六方面提供的方法，电子设备可以向服务器发送第二签名信息，以便服务器通过第二签名信息验证电子设备的合法性，如电子设备是否有下载升级包的权限等，以及验证接收到的信息是否被篡改，以保障车载设备升级的安全性。

在一种可能的实现方式中，该方法还包括：接收来自该车载控制设备的该代理签名密钥。

基于上述可能的实现方式，电子设备可以从车载控制设备获取代理签名密钥。

在一种可能的实现方式中，该第一升级请求包括该至少一个车载设备的待升级信息。

基于上述可能的实现方式，电子设备可以向服务器发送至少一个车载设备的待升级信息，以便服务器根据该待升级信息验证升级包与至少一个车载设备的适配性。例如，若服务器中存储的最新发布的软件的版本信息与待升级信息中的版本信息相同，则服务器确定至少一个车载设备不需要升级；若服务器中存储的最新发布的软件的版本信息比待升级信息中的版本信息更高，则服务器确定至少一个车载设备需要升级。

在一种可能的实现方式中，该授权信息包括以下至少一项：该至少一个车载设备的待升级信息、该车载控制设备的标识、该服务器的标识、该电子设备的标识、授权期限或授权目的信息。

基于上述可能的实现方式，若授权信息包括至少一个车载设备的待升级信息，则表示该代理签名密钥的授权期限为短期或一次性授权。可选的，若该授权信息包括至少一个车载设备的待升级信息，还表示该代理签名密钥用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。若授权信息包括车载控制设备的标识，则表示该代理签名密钥是车载控制设备生成或授权的。若授权信息包括服务器的标识和电子设备的标识，则表示该代理签名密钥是用于服务器和电子设备之间的验证的。

在一种可能的实现方式中，该方法还包括：接收来自该车载控制设备的该至少一个车载设备的待升级信息。

基于上述可能的实现方式，电子设备可以从车载控制设备获取至少一个车载设备的待升级信息，以便电子设备向服务器发送该待升级信息，使得服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。

5 第七方面，提供了一种车载设备的升级方法，该方法可以由车载控制设备执行；或者，也可以由应用于车载控制设备中的模块，例如芯片、芯片系统或电路执行；或者，还可以由能实现全部或部分车载控制设备功能的逻辑模块或软件实现，对此不作限定。为了便于描述，下面以由车载控制设备执行为例进行说明。

10 该方法包括：获取代理签名密钥，该代理签名密钥是根据该车载控制设备的私钥和该代理签名密钥的授权信息得到的；向电子设备发送该代理签名密钥。

基于上述第七方面提供的方法，车载控制设备可以获取代理签名密钥并发送给电子设备，以便服务器通过代理签名密钥验证电子设备的合法性。

15 在一种可能的实现方式中，该授权信息包括以下至少一项：至少一个车载设备的待升级信息、该车载控制设备的标识、服务器的标识、该电子设备的标识、授权期限或授权目的信息。

基于上述可能的实现方式，若授权信息包括至少一个车载设备的待升级信息，则表示该代理签名密钥的授权期限为短期或一次性授权。可选的，若该授权信息包括至少一个车载设备的待升级信息，还表示该代理签名密钥用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。若授权信息包括车载控制设备的标识，则表示该代理签名密钥是车载控制设备生成或授权的。若授权信息包括服务器的标识和电子设备的标识，则表示该代理签名密钥是用于服务器和电子设备之间的验证的。

在一种可能的实现方式中，该方法还包括：向该电子设备发送该至少一个车载设备的待升级信息。

25 基于上述可能的实现方式，车载控制设备可以向电子设备发送至少一个车载设备的待升级信息，以便电子设备向服务器发送该待升级信息，使得服务器可以根据该待升级信息验证升级包与至少一个车载设备的适配性。

第八方面，提供了一种通信设备用于实现上述方法。该通信设备可以为上述第一方面中的服务器，或者包含上述服务器的装置，或者为上述第一方面中的服务器中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部服务器功能的逻辑模块或软件实现；或者，该通信设备可以为上述第五方面中的服务器，或者包含上述服务器的装置，或者为上述第五方面中的服务器中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部服务器功能的逻辑模块或软件实现；或者，该通信设备可以为上述第七方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第七方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现。该通信设备包括实现上述方法相应的模块、单元、或手段（means），该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

结合上述第八方面，在一种可能的实现方式中，该通信设备可以包括处理模块和收发模块。该处理模块，可以用于实现上述第一方面、第五方面、第七方面及其任意可能的实现方式中的处理功能。该处理模块例如可以为处理器。该收发模块，也可以称为收发单元，用以实现上述第一方面、第五方面、第七方面及其任意可能的实现方式中的发送和/或接收功能。该收发模块可以由收发电路，收发机，收发器或者通信接口构成。

结合上述第八方面，在一种可能的实现方式中，收发模块包括发送模块和接收模块，分别用于实现上述第一方面、第五方面、第七方面及其任意可能的实现方式中的发送和接收功能。

第九方面，提供了一种通信设备用于实现上述方法。该通信设备可以为上述第二方面中的电子设备，或者包含上述电子设备的装置，或者为上述第二方面中的电子设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部电子设备功能的逻辑模块或软件实现。该通信设备包括实现上述方法相应的模块、单元、或 means，该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

结合上述第九方面，在一种可能的实现方式中，该通信设备可以包括收发模块。该收发模块，也可以称为收发单元，用以实现上述第二方面及其任意可能的实现方式中的发送和/或接收功能。该收发模块可以由收发电路，收发机，收发器或者通信接口构成。

结合上述第九方面，在一种可能的实现方式中，收发模块包括发送模块和接收模块，分别用于实现上述第二方面及其任意可能的实现方式中的发送和接收功能。

结合上述第九方面，在一种可能的实现方式中，该通信设备还可以包括处理模块。该处理模块，可以用于实现上述第二方面及其任意可能的实现方式中的处理功能。该处理模块例如可以为处理器。

第十方面，提供了一种通信设备用于实现上述方法。该通信设备可以为上述第三方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第三方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第四方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第四方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第六方面中的电子设备，或者包含上述电子设备的装置，或者为上述第六方面中的电子设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现。该通信设备包括实现上述方法相应的模块、单元、或手段 means，该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

结合上述第十方面，在一种可能的实现方式中，该通信设备可以包括收发模块。该收发模块，也可以称为收发单元，用以实现上述第三方面、第四方面、第六方面及其任意可能的实现方式中的发送和/或接收功能。该收发模块可以由收发电路，收发

机，收发器或者通信接口构成。

结合上述第十方面，在一种可能的实现方式中，收发模块包括发送模块和接收模块，分别用于实现上述第三方面、第四方面、第六方面及其任意可能的实现方式中的发送和接收功能。

- 5 第十一方面，提供了一种通信设备，包括：处理器；该处理器用于与存储器耦合，并读取存储器中的指令之后，根据该指令执行如上述任一方面所述的方法。该通信设备可以为上述第一方面中的服务器，或者包含上述服务器的装置，或者为上述第一方面中的服务器中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部服务器功能的逻辑模块或软件实现；或者，该通信设备可以为上述第二方面中的电子设备，或者包含上述电子设备的装置，或者为上述第二方面中的电子设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部电子设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第三方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第三方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现；或者，
10 该通信设备可以为上述第四方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第四方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第五方面中的服务器，或者包含上述服务器的装置，或者为上述第五方面中的服务器中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部服务器功能的逻辑模块或软件实现；或者，该通信设备可以为上述第六方面中的电子设备，或者包含上述电子设备的装置，或者为上述第六方面中的电子设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部电子设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第七方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第七方面中的车载控制设备中的模块，如芯片、芯片系统或电
20 路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现。
25

结合上述第十一方面，在一种可能的实现方式中，该通信设备还包括存储器，该存储器，用于保存必要的程序指令和数据。

- 结合上述第十一方面，在一种可能的实现方式中，该通信设备为芯片或芯片系统。可选的，该通信设备是芯片系统时，可以由芯片构成，也可以包含芯片和其他分立器件。
30

- 第十二方面，提供了一种通信设备，包括：处理器和接口电路；接口电路，用于接收计算机程序或指令并传输至处理器；处理器用于执行所述计算机程序或指令，以使该通信设备执行如上述任一方面所述的方法。该通信设备可以为上述第一方面中的服务器，或者包含上述服务器的装置，或者为上述第一方面中的服务器中的模块，
35 如芯片、芯片系统或电路，或者为能实现部分或全部服务器功能的逻辑模块或软件实现；或者，该通信设备可以为上述第二方面中的电子设备，或者包含上述电子设备的装置，或者为上述第二方面中的电子设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部电子设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第三方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第

三方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第四方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第四方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第五方面中的服务器，或者包含上述服务器的装置，或者为上述第五方面中的服务器中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部服务器功能的逻辑模块或软件实现；或者，该通信设备可以为上述第六方面中的电子设备，或者包含上述电子设备的装置，或者为上述第六方面中的电子设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部电子设备功能的逻辑模块或软件实现；或者，该通信设备可以为上述第七方面中的车载控制设备，或者包含上述车载控制设备的装置，或者为上述第七方面中的车载控制设备中的模块，如芯片、芯片系统或电路，或者为能实现部分或全部车载控制设备功能的逻辑模块或软件实现。

结合上述第十二方面，在一种可能的实现方式中，该通信设备为芯片或芯片系统。可选的，该通信设备是芯片系统时，可以由芯片构成，也可以包含芯片和其他分立器件。

第十三方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述任一方面所述的方法。

第十四方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述任一方面所述的方法。

第十五方面，提供了一种车辆，该车辆包括用于执行上述第三方面所述的方法的车载控制设备，或者用于执行上述第四方面所述的方法的车载控制设备，或者用于执行上述第七方面所述的方法的车载控制设备。

第十六方面，提供了一种升级系统，该升级系统包括用于执行上述第一方面所述的方法的服务器、用于执行上述第二方面所述的方法的电子设备以及用于执行上述第三方面所述的方法的车载控制设备。

第十七方面，提供了一种升级系统，该升级系统包括用于执行上述第一方面所述的方法的服务器、用于执行上述第二方面所述的方法的电子设备以及用于执行上述第四方面所述的方法的车载控制设备。

第十八方面，提供了一种升级系统，该升级系统包括用于执行上述第五方面所述的方法的服务器、用于执行上述第六方面所述的方法的电子设备以及用于执行上述第七方面所述的方法的车载控制设备。

其中，第八方面至第十八方面中任一种可能的实现方式所带来的技术效果可参见上述第一方面至第二方面中任一方面或任一方面中不同可能的实现方式所带来的技术效果，此处不再赘述。

可以理解的是，在方案不矛盾的前提下，上述各个方面中的方案均可以结合。

附图说明

图 1A 为本申请实施例提供的升级系统架构示意图；

- 图 1B 为本申请实施例提供的网络架构示意图；
- 图 2 为本申请实施例提供的通信设备的硬件结构示意图；
- 图 3 为本申请实施例提供的车载设备的升级方法的流程示意图一；
- 图 4 为本申请实施例提供的车载设备的升级方法的流程示意图二；
- 5 图 5 为本申请实施例提供的车载设备的升级方法的流程示意图三；
- 图 6 为本申请实施例提供的车载设备的升级方法的流程示意图四；
- 图 7 为本申请实施例提供的车载设备的升级方法的流程示意图五；
- 图 8 为本申请实施例提供的通信设备的结构示意图一；
- 图 9 为本申请实施例提供的通信设备的结构示意图二；
- 10 图 10 为本申请实施例提供的通信设备的结构示意图三。

具体实施方式

下面结合附图对本申请实施例的实施方式进行详细描述。

本申请实施例提供的方法可用于各种升级系统。下面以图 1A 所示升级系统 10 为例，对本申请实施例提供的方法进行描述。图 1A 仅为示意图，并不构成对本申请提供的技术方案的适用场景的限定。

如图 1A 所示，为本申请实施例提供的升级系统 10 的架构示意图。图 1A 中，升级系统 10 可以包括服务器 101，可以与服务器 101 通信连接的电子设备 102，以及可以与服务器 101 和电子设备 102 都通信连接的车载控制设备 103。

其中，服务器 101 和电子设备 102 之间可通过蜂窝网络或 Wi-Fi 系统等方式通信连接。服务器 101 和车载控制设备 103 之间可通过蜂窝网络或 Wi-Fi 系统等方式通信连接。电子设备 102 和车载控制设备 103 之间可通过蜂窝网络、Wi-Fi 系统、近距离无线通信（near field communication, NFC）、蓝牙或数据线等方式通信连接。本申请实施例中，蜂窝网络可以包括任意一种或多种第三代合作伙伴计划（3rd generation partnership project, 3GPP）相关的网络，如第四代（4th generation, 4G）网络、第五代（5th generation, 5G）或未来演进的网络等。

本申请实施例中的服务器，如服务器 101，是一种具有通信能力和计算能力的设备。例如，服务器为计算机、计算设备或云服务器等。

本申请实施例中的电子设备，如电子设备 102，是一种具有通信能力和计算能力的设备。例如，电子设备为终端、充电桩或通用串行总线（universal serial bus, USB）卡等。其中，终端还可以称为终端设备，终端设备可以是用户设备（user equipment, UE）。其中，UE 包括具有无线通信功能的手持式设备、可穿戴设备或计算设备。示例性地，UE 可以是手机（mobile phone）、平板电脑或带无线收发功能的电脑。终端设备还可以是虚拟现实（virtual reality, VR）终端设备、增强现实（augmented reality, AR）终端设备或工业控制中的无线终端等等。

本申请实施例中的车载控制设备，如车载控制设备 103，是任意一种具备通信能力和计算能力的车内设备。例如，该车载控制设备为 OTA 控制设备（OTA Manger）、通信盒子（telematics box, T-Box）、网关（gateway）、多域控制器（multiple domain controller, MDC）、整车控制单元（vehicle control unit, VCU）或电

子控制单元（electronic control unit，ECU）等。

在图 1A 中，服务器 101 和车载控制设备 103 为互信设备，车载控制设备 103 和电子设备 102 为互信设备。换言之，服务器 101 和车载控制设备 103 建立了信任关系，车载控制设备 103 和电子设备 102 建立了信任关系。这样，电子设备 102 可以通过车载控制设备 103 为电子设备 102 提供的身份认证凭证（如下文中的第一公钥信息或代理签名密钥），向服务器 101 请求至少一个车载设备的升级包。服务器 101 在验证该身份认证凭证合法后，向电子设备 102 发送该升级包，以便电子设备 102 在合适的时间将该升级包发送给车载控制设备 103，并且保障了车载设备升级的安全性。

可选的，电子设备 102 还可以协助存储车内设备的软件信息或固件信息，如：软件/固件的当前版本信息、软件/固件的大小或软件/固件的开发者信息中的至少一种。

可选的，电子设备 102 还可以转换服务器 101 和车载控制设备 103 之间的安全机制。例如，服务器 101 向电子设备 101 发送采用第一算法对第一信息加密得到的信息。电子设备 102 接收到该信息后，解密该信息得到第一信息，并向车载控制设备 103 发送采用第二算法对第一信息加密得到的信息。可以理解的，电子设备 102 接收到采用第一算法对第一信息加密得到的信息后，还可以通过电子设备 102 内的安全模块（如安装的安全软件）检测该信息，以提高通信安全。

可选的，电子设备 102 还可以采用密钥分享（secret sharing）的方式与车载控制设备 103 共同保管车辆用于通信的密钥，以提高车辆通信安全。

图 1A 所示的升级系统 10 仅用于举例，并非用于限制本申请的技术方案。本领域的技术人员应当明白，在具体实现过程中，升级系统 10 还可以包括其他设备，同时也可根据具体需要来确定服务器、车载控制设备或电子设备的数量，不予限制。

在一种可能的实现方式中，图 1A 所示的升级系统 10 可以应用于图 1B 所示的网络架构中。

如图 1B 所示，为本申请实施例提供的一种网络架构。图 1B 中，该网络架构包括：服务器，与服务器通信连接的电子设备，以及与服务器和电子设备通信连接的车辆。该车辆包括 T-BOX、与 T-BOX 通信连接的车载控制设备以及与车载控制设备通信连接的待升级设备。

可以理解的，图 1A 中的服务器 101 在图 1B 中对应的设备为服务器，图 1A 中的电子设备 102 在图 1B 中对应的设备为电子设备，图 1A 中的车载控制设备 103 在图 1B 中对应的设备为车载控制设备。

在图 1B 中，电子设备可以用于向服务器请求至少一个待升级设备的升级包，并将请求到的升级包发送给车载控制设备。服务器用于接收来自电子设备的用于请求至少一个待升级设备的升级包的信息，并验证电子设备的身份，在电子设备的身份合法的情况下，向电子设备发送所请求的升级包。车载控制设备用于接收来自电子设备的至少一个待升级设备的升级包，并将该升级包发送给对应的待升级设备。T-Box 用于将接收到的来自车外设备的信息转发给车内设备，将来自车内设备的信息转发给车外设备。例如，T-Box 转发服务器和车载控制设备之间的信息。应理解，服务器和车载控制设备也可以直接通信，而不是通过 T-Box 通信，不予限制。

在图 1B 中，待升级设备可以是任一个等待升级的车载设备，例如，为任意一种

具备人机交互界面（human machine interface, HMI）的设备、电池管理系统（battery management system, BMS）或 ECU 等。

在图 1B 中，车载控制设备是独立部署在车辆中的。而在具体应用中，车载控制设备也可以不独立部署在车辆中，而是作为一个或多个车载设备的功能模块，换言之，车载控制设备的功能可以部署在车辆中的任意一个或多个设备上。例如，车载控制设备的功能部署在 T-BOX、网关或某个待升级设备上，不予限制。

本申请实施例中，多个可以理解为两个或两个以上，在此做出统一说明，后面不再赘述。

可以理解的，图 1B 所示的网络架构仅用于举例，并非用于限制本申请的技术方案。本领域的技术人员应当明白，在具体实现过程中，该网络架构还可以包括其他设备，同时也可根据具体需要来确定服务器、车载控制设备、电子设备、待升级设备或车辆的数量，不予限制。

可选的，本申请实施例图 1A 或图 1B 中的各设备（例如服务器、电子设备或车载控制设备等）也可以称之为通信设备，其可以是一个通用设备或者是一个专用设备，本申请实施例对此不作具体限定。

可选的，本申请实施例图 1A 或图 1B 中的各设备（例如服务器、电子设备或车载控制设备等）的相关功能可以由一个设备实现，也可以由多个设备共同实现，还可以是由一个设备内的一个或多个功能模块实现，本申请实施例对此不作具体限定。可以理解的是，上述功能既可以是硬件设备中的元件，也可以是在专用硬件上运行的软件功能，或者硬件与软件的结合，或者平台（例如，云平台）上实例化的虚拟化功能。

在具体实现时，本申请实施例图 1A 或图 1B 中的各设备（例如服务器、电子设备或车载控制设备等）都可以采用图 2 所示的组成结构，或者包括图 2 所示的部件。图 2 所示为可适用于本申请实施例的通信设备的硬件结构示意图。该通信设备 20 包括至少一个处理器 201 和至少一个通信接口 204，用于实现本申请实施例提供的方法。该通信设备 20 还可以包括通信线路 202 和存储器 203。

处理器 201 可以是一个通用中央处理器（central processing unit, CPU），微处理器，特定应用集成电路（application-specific integrated circuit, ASIC），或一个或多个用于控制本申请方案程序执行的集成电路。

通信线路 202 可包括一通路，在上述组件之间传送信息，例如总线。

通信接口 204，用于与其他设备或通信网络通信。通信接口 204 可以是任何收发器一类的装置，如可以是以太网接口、无线接入网（radio access network, RAN）接口、无线局域网（wireless local area networks, WLAN）接口、收发器、管脚、总线、或收发电路等。

存储器 203 可以是只读存储器（read-only memory, ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory, RAM）或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only memory, EEPROM）、只读光盘

（compact disc read-only memory, CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储

设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过通信线路 202 与处理器 201 相耦合。存储器 203 也可以和处理器 201 集成在一起。本申请实施例提供的存储器通常可以具有非易失性。

5 其中，存储器 203 用于存储执行本申请实施例提供的方案所涉及的计算机执行指令，并由处理器 201 来控制执行。处理器 201 用于执行存储器 203 中存储的计算机执行指令，从而实现本申请实施例提供的方法。或者，可选的，本申请实施例中，也可以是处理器 201 执行本申请下述实施例提供的方法中的处理相关的功能，通信接口 204 负责与其他设备或通信网络通信，本申请实施例对此不作具体限定。

10 可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。

15 作为一种实施例，处理器 201 可以包括一个或多个 CPU，例如图 2 中的 CPU0 和 CPU1。

作为一种实施例，通信设备 20 可以包括多个处理器，例如图 2 中的处理器 201 和处理器 207。这些处理器中的每一个可以是一个单核（single-CPU）处理器，也可以是一个多核（multi-CPU）处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

20 作为一种实施例，通信设备 20 还可以包括输出设备 205 和/或输入设备 206。输出设备 205 和处理器 201 耦合，可以以多种方式来显示信息。例如，输出设备 205 可以是液晶显示器（liquid crystal display, LCD），发光二极管（light emitting diode, LED）显示设备，阴极射线管（cathode ray tube, CRT）显示设备，或投影仪（projector）等。输入设备 206 和处理器 201 耦合，可以以多种方式接收用户的输入。例如，输入设备 206 可以是鼠标、键盘、触摸屏设备或传感设备等。

25 可以理解的，图 2 中示出的组成结构并不构成对该通信设备的限定，除图 2 所示部件之外，该通信设备可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

下面将结合图 3 至图 7，对本申请实施例提供的方法进行描述。下述实施例中的各设备可以具备图 2 所示部件，不予赘述。

30 可以理解的，图 3 至图 7 所示的方法中是以服务器、电子设备和车载控制设备作为该交互示意的执行主体为例来示意该方法，但本申请并不限制该交互示意的执行主体。例如，图 3 至图 7 所示的方法中的服务器也可以是支持该服务器实现该方法的芯片、芯片系统、或处理器，还可以是能实现全部或部分服务器功能的逻辑模块或软件；图 3 至图 7 所示的方法的电子设备也可以是支持该电子设备实现该方法的芯片、芯片系统、或处理器，还可以是能实现全部或部分电子设备功能的逻辑模块或软件；图 3 至图 7 所示的方法的车载控制设备也可以是支持该车载控制设备实现该方法的芯片、芯片系统、或处理器，还可以是能实现全部或部分车载控制设备功能的逻辑模块或软件。

可以理解的是，本申请下述实施例中各个设备之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字，本申请实施例对此不作具体限定。

可以理解的是，在本申请实施例中，“/”可以表示前后关联的对象是一种“或”的关系，例如，A/B 可以表示 A 或 B；“和/或”可以用于描述关联对象存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A，B 可以是单数或者复数。此外，类似于“A、B 和 C 中的至少一项”或“A、B 或 C 中的至少一项”的表述通常用于表示如下中任一项：单独存在 A；单独存在 B；单独存在 C；同时存在 A 和 B；同时存在 A 和 C；同时存在 B 和 C；同时存在 A、B 和 C。以上是以 A、B 和 C 共三个元素进行举例来说明该项目的可选用条目，当表述中具有更多元素时，该表述的含义可以按照前述规则获得。

为了便于描述本申请实施例的技术方案，在本申请实施例中，可以采用“第一”、“第二”等字样对功能相同或相似的技术特征进行区分。该“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并不限定一定不同。在本申请实施例中，“示例性的”或者“例如”等词用于表示例子、例证或说明，被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念，便于理解。

可以理解，说明书通篇中提到的“实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各个实施例未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。可以理解，在本申请的各种实施例中，各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

可以理解，在本申请中，“当...时”、“若”以及“如果”均指在某种客观情况下会做出相应的处理，并非是限定时间，且也不要求实现时一定要有所判断的动作，也不意味着存在其它限定。

可以理解，本申请实施例中的一些可选的特征，在某些场景下，可以不依赖于其他特征，比如其当前所基于的方案，而独立实施，解决相应的技术问题，达到相应的效果，也可以在某些场景下，依据需求与其他特征进行结合。相应的，本申请实施例中给出的装置也可以相应的实现这些特征或功能，在此不予赘述。

可以理解的，本申请实施例中同一个步骤或者具有相同功能的步骤或者技术特征在不同实施例之间可以互相参考借鉴。

可以理解的，本申请实施例中，服务器，和/或，电子设备，和/或，车载控制设备可以执行本申请实施例中的部分或全部步骤，这些步骤仅是示例，本申请实施例还可以执行其它步骤或者各种步骤的变形。此外，各个步骤可以按照本申请实施例呈现的不同的顺序来执行，并且有可能并非要执行本申请实施例中的全部步骤。

如图 3 所示，为本申请实施例提供的一种车载设备的升级方法，该方法可以包括如下步骤：

S301: 电子设备向服务器发送第一签名信息和第一公钥信息。相应的, 服务器接收来自电子设备的第一签名信息和第一公钥信息。

本申请实施例中, 电子设备可以是图 1A 中的电子设备 102, 服务器可以是图 1A 中的服务器 101; 或者电子设备可以是图 1B 中的电子设备, 服务器可以是图 1B 中的服务器。

下面分别对第一签名信息和第一公钥信息进行介绍。

本申请实施例中, 第一签名信息是用电子设备的私钥对第一升级请求进行签名得到的。第一升级请求用于请求至少一个车载设备的升级包。其中, 至少一个车载设备可以是图 1B 中的待升级设备。

10 作为一种示例, 第一升级请求包括至少一个标志位, 该至少一个标志位与至少一个车载设备一一对应, 至少一个标志位中的任意一个标志位用于请求该标志位对应的车载设备的升级包。

作为另一种示例, 第一升级请求包括至少一个车载设备中每个车载设备的标识信息。

15 可选的, 第一升级请求还包括至少一个车载设备的待升级信息。示例性的, 至少一个车载设备的待升级信息包括以下至少一项: 至少一个车载设备当前安装的软件的名称、该软件的版本信息、至少一个车载设备的名称、该软件的开发者的信息或至少一个车载设备所在车辆的标识。

20 可选的, 该待升级信息可以是电子设备从车载控制设备上获取的。例如, 在 S301 之前, 车载控制设备向电子设备发送该待升级信息。相应的, 电子设备接收该待升级信息。

可以理解的, 至少一个车载设备的待升级信息可以使得服务器确定至少一个车载设备是否需要升级, 或者, 使得服务器验证升级包与至少一个车载设备的适配性。例如, 若服务器中存储的最新发布的软件的版本信息与待升级信息中的版本信息相同, 25 则服务器确定至少一个车载设备不需要升级; 若服务器中存储的最新发布的软件的版本信息比待升级信息中的版本信息更高, 则服务器确定至少一个车载设备需要升级。

可选的, 服务器中存储上述待升级信息。此时, 第一升级请求中可以不包括待升级信息。服务器接收到第一签名信息后, 可以在本地查找待升级信息, 以确定至少一个车载设备是否需要升级。

30 本申请实施例中, 第一公钥信息用于验证电子设备的身份, 或者说, 第一公钥信息用于验证电子设备是否合法。示例性的, 第一公钥信息包括电子设备的公钥的公钥证书, 或者, 第一公钥信息包括电子设备的公钥。这样, 服务器可以根据公钥证书或电子设备的公钥验证电子设备的身份, 或者验证电子设备是否合法。

35 其中, 该公钥证书可以包括以下至少一项: 至少一个车载设备的待升级信息、车载控制设备的标识、服务器的标识、电子设备的标识、授权期限或授权目的信息。其中, 授权期限可以包括长期、短期或一次性授权。一次性授权是指该公钥证书能被验证一次。或者, 授权期限包括 1 个月、两个月、半年或一年。可以理解的, 长期授权可以使得公钥证书能够使用较长时间, 不需要频繁生成公钥证书。短期授权或一次性授权虽然要频繁生成公钥证书, 但是安全性较高。另外, 一次性授权还不需要取消授

权。

可选的，公钥证书还包括保护上述全部或部分信息的完整性和源真实性的标签，如数字签名。

- 5 可以理解的，若该公钥证书中未包括授权期限，该公钥证书可以隐性指示授权期限。例如，若该公钥证书包括至少一个车载设备的待升级信息，则表示该公钥证书的授权期限为短期或一次性授权。可选的，若该公钥证书包括至少一个车载设备的待升级信息，则表示该公钥证书用于车载设备的升级，而不能用于除车载设备升级业务之外的其他业务。

- 10 一种可能的设计，该公钥证书包括至少一个域，上述信息可以包括在对应的域中。例如，公钥证书包括发行（Issuer）域、有效性（Validity）域或扩展密钥使用域（Extended key usage field）中的至少一个。Issuer 域可以包括授权人相关的信息，如车载控制设备的标识或服务器的标识。Validity 域可以包括授权期限等。Extended key usage field 可以包括除授权人信息和授权期限之外的信息，如电子设备的标识、至少一个车载设备的待升级信息和授权目的信息。

- 15 可以理解的，在授权期限内，服务器若要取消对电子设备的授权，可采用常规的公钥证书取消机制进行授权取消，如将该公钥证书放入证书取消列表中。

可以理解的，上述域仅是公钥证书包括的域的示例，在具体应用中，公钥证书可以包括比上述示例更多或更少的域，不予限制。

- 20 一种可能的实现方式，该公钥证书是根据服务器的私钥生成的；或者，该公钥证书是根据车载控制设备的私钥生成的。其中，车载控制设备为图 1A 中的车载控制设备 103，或者为图 1B 中的车载控制设备。

S302：在第一签名信息和第一公钥信息验证成功的情况下，服务器向电子设备发送至少一个车载设备的升级包。相应的，电子设备接收来自服务器的至少一个车载设备的升级包。

- 25 可以理解的，服务器接收到第一签名信息和第一公钥信息后，可以验证第一签名信息和第一公钥信息，并在第一签名信息和第一公钥信息验证成功的情况下，向电子设备发送至少一个车载设备的升级包。

- 30 作为一种示例，服务器根据电子设备的公钥验证第一签名信息。若第一签名信息验证成功，则表示第一签名信息未被篡改；或第一签名信息验证失败，则表示第一签名信息被篡改。

- 35 作为另一种示例，若第一公钥信息包括电子设备的公钥的公钥证书，该公钥证书是根据服务器的私钥生成的，则服务器根据服务器的公钥验证该公钥证书。或者，若第一公钥信息包括电子设备的公钥的公钥证书，该公钥证书是根据车载控制设备的私钥生成的，则服务器根据车载控制设备的公钥验证该公钥证书（在 S302 之前，服务器可以从车载控制设备获取车载控制设备的公钥）。可以理解的，服务器的公钥或车载控制设备的公钥可以有自己的公钥证书，该公钥证书可以通过其他设备的公钥进行验证，其他设备的公钥也可以有自己的公钥证书，以此类推，可以形成证书链，最终通过证书链中的根证书验证证书链中其他证书的合法性。应理解，若公钥证书验证成功，则表示电子设备合法，或电子设备被授权下载升级包，若公钥证书验证失败，则

表示电子设备不合法，或电子设备未被授权下载升级包。

作为另一种示例，若第一公钥信息包括电子设备的公钥，服务器根据电子设备的公钥的授权信息验证该电子设备的公钥。其中，该电子设备的公钥的授权信息用于指示该电子设备的公钥是否被授权，或该电子设备是否合法。例如，若该授权信息包括

- 5 该电子设备的公钥，则该授权信息指示该电子设备的公钥被授权或该电子设备合法；若该授权信息未包括该电子设备的公钥，则该授权信息指示该电子设备的公钥未被授权或该电子设备不合法。又例如，该授权信息包括一个标志位，该标志位指示该电子设备的公钥是否被授权，或该电子设备是否合法。又例如，该授权信息包括该电子设备的公钥以及该公钥对应的标志位，该标志位用于指示该电子设备的公钥是否被授
10 权，或该电子设备是否合法。

可以理解的，服务器通过该授权信息验证电子设备的合法性，可以避免使用证书链的形式验证电子设备，可以提高验证效率。

可以理解的，若在授权期限内，服务器若想取消对电子设备的授权，可以删除该授权信息。

- 15 S303: 电子设备向车载控制设备发送至少一个车载设备的升级包。相应的，车载控制设备接收来自电子设备的至少一个车载设备的升级包。

可以理解的，电子设备可以在适合的时间（如车载控制设备的网络空闲或车载控制设备连接到网络上的情况下）向车载控制设备发送至少一个车载设备的升级包。

可以理解的，车载控制设备通过电子设备向服务器请求升级包有以下好处：

- 20 （1）可以节省车载网络的开销；（2）在车载控制设备无法通信时，电子设备可以及时获取到升级包；（3）在用户（如车主或电子设备的主人）不在车内，无法操作车载控制设备时，电子设备可以及时获取到升级包。

S304: 车载控制设备分别向至少一个车载设备发送每个车载设备的升级包。相应的，每个车载设备接收升级包。

- 25 可以理解的，车载设备接收到自己的升级包后，可以进行升级。

其中，上述 S301-S304 中的电子设备或者服务器或者车载控制设备的动作可以由图 2 所示的通信设备 20 中的处理器 201 调用存储器 203 中存储的应用程序代码来执行，本申请实施例对此不做任何限制。

- 30 基于图 3 所示的方法，服务器可以通过第一公钥信息验证电子设备的合法性，如电子设备是否有下载升级包的权限等，通过第一签名信息验证接收到的信息是否被篡改，以保障车载设备升级的安全性。

可选的，在图 3 所示方法的一种可能的场景中，上述公钥证书是车载控制设备或服务器为电子设备生成的。具体的，如图 4 所示，若第一公钥信息包括电子设备的公钥的公钥证书，则图 3 所示的方法还包括 S300a~S300c 或者 S300A~S300E。

- 35 S300a: 电子设备获取电子设备的公钥和电子设备的私钥。

一种可能的实现方式，电子设备生成电子设备的公钥和电子设备的私钥；或者，密钥生成装置为电子设备生成电子设备的公钥和电子设备的私钥，并发送给电子设备，相应的，电子设备接收该公钥和该私钥。

S300b: 电子设备向车载控制设备发送电子设备的公钥。相应的，车载控制设备

接收来自电子设备的电子设备的公钥。

S300c: 车载控制设备向电子设备发送电子设备的公钥的公钥证书。相应的, 电子设备接收该公钥证书。

5 一种可能的实现方式, 车载控制设备作为授权者使用自己的私钥为电子设备的公钥(被授权者)生成公钥证书。或者, 车载控制设备通过证书签发机构使用车载控制设备的私钥为电子设备的公钥生成公钥证书。可以理解的, 该公钥证书可以作为授权书。

可以理解的, 通过 S300a~S300c, 车载控制设备可以为电子设备生成授权书(如: 电子设备的公钥的公钥证书)。之后, 电子设备可以根据该授权书向服务器请求升级包。由于授权书具有不可修改和不可伪造性, 将授权书作为电子设备向服务器证明电子设备的合法性的凭证, 可以保证车载设备的升级安全。

S300A: 电子设备获取电子设备的公钥和电子设备的私钥。

S300B: 电子设备向车载控制设备发送电子设备的公钥。相应的, 车载控制设备接收来自电子设备的电子设备的公钥。

15 上述 S300A~S300B 的过程与 S300a~S300b 的过程类似, 因此可以参考上述 S300a~S300b 中对应的描述, 在此不做赘述。

S300C: 车载控制设备向服务器发送电子设备的公钥。相应的, 服务器接收来自车载控制设备的电子设备的公钥。

20 S300D: 服务器向车载控制设备发送电子设备的公钥的公钥证书。相应的, 车载控制设备接收该公钥证书。

一种可能的实现方式, 服务器作为授权者使用自己的私钥为电子设备的公钥(被授权者)生成公钥证书。或者, 服务器通过证书签发机构使用服务器的私钥为电子设备的公钥生成公钥证书。可以理解的, 该公钥证书可以作为授权书。

25 作为一种示例, 车载控制设备可以使用自己的私钥作为身份认证登录服务器, 为电子设备的公钥申请公钥证书。服务器可以使用自己的私钥为电子设备的公钥生成公钥证书, 或者调用第三方证书签发机构使用服务器的私钥为电子设备的公钥生成公钥证书。

S300E: 车载控制设备向电子设备发送电子设备的公钥的公钥证书。相应的, 电子设备接收该公钥证书。

30 可以理解的, 通过 S300A~S300E, 服务器可以为电子设备生成授权书(如: 电子设备的公钥的公钥证书)。之后, 电子设备可以根据该授权书向服务器请求升级包。由于授权书具有不可修改和不可伪造性, 将授权书作为电子设备向服务器证明电子设备的合法性的凭证, 可以保证车载设备的升级安全。

35 其中, 上述 S300a-S300E 中的电子设备或者车载控制设备或者服务器的动作可以由图 2 所示的通信设备 20 中的处理器 201 调用存储器 203 中存储的应用程序代码来执行, 本申请实施例对此不做任何限制。

可选的, 在图 3 所示方法的一种可能的场景中, 服务器可以为电子设备的公钥生成授权信息。具体的, 如图 5 所示, 若第一公钥信息包括电子设备的公钥, 则图 3 所示的方法还包括 S3001~S3004。

S3001: 电子设备获取电子设备的公钥和电子设备的私钥。

S3002: 电子设备向车载控制设备发送电子设备的公钥。相应的, 车载控制设备接收来自电子设备的电子设备的公钥。

上述 S3001~S3002 的过程与 S300a~S300b 的过程类似, 因此可以参考上述

5 S300a~S300b 中对应的描述, 在此不做赘述。

S3003: 车载控制设备向服务器发送电子设备的公钥。相应的, 服务器接收来自车载控制设备的电子设备的公钥。

可选的, 车载控制设备还向服务器发送第一指示信息。相应的, 服务器接收该第一指示信息。其中, 该第一指示信息用于指示生成电子设备的公钥的授权信息。

10 例如, 第一指示信息包括 1 比特, 该 1 比特的值为“0”或“1”时, 指示生成电子设备的公钥的授权信息。

S3004: 服务器生成电子设备的公钥的授权信息。

示例性的, 车载控制设备使用自己的私钥作为身份认证登录服务器, 并请求对电子设备的公钥进行授权。服务器可以生成并保存该授权信息。这样, 服务器接收到电

15 子设备发送的升级请求后, 可以查询授权信息, 以验证电子设备是否合法。

可以理解的, 通过上述 S3001~S3004, 服务器可以为电子设备的公钥生成授权信息。这样, 在电子设备向服务器请求升级包时, 服务器不需要公钥证书来验证电子设备的合法性, 而是通过该授权信息验证电子设备的合法性, 整个验证过程不需要使用证书链, 验证效率高。

20 其中, 上述 S3001-S3004 中的电子设备或者车载控制设备或者服务器的动作可以由图 2 所示的通信设备 20 中的处理器 201 调用存储器 203 中存储的应用程序代码来执行, 本申请实施例对此不做任何限制。

可以理解的, 在上述图 3 至图 5 所示的方法中, 服务器是通过公钥证书或者电子设备的公钥的授权信息验证电子设备的身份是否合法。在具体应用中, 可以通过代理

25 签名 (proxy signature) 的方式为电子设备生成身份凭证, 以便服务器验证电子设备的合法性。

其中, 代理签名涉及原签名者和代理签名者。原签名者通过为代理签名者生成代理签名密钥 (proxy signing key), 将自己的签名能力授权给代理签名者。代理签名密钥的生成可以使用原签名者的私钥, 也可以使用代理签名者的私钥。如果代理签名密

30 钥的生成使用代理签名者的私钥, 则需要原签名者和代理签名者双方交互共同生成; 如果代理签名密钥的生成不使用代理签名者的私钥, 则通常由原签名者单独生成。本申请实施例以使用原签名者单独生成代理签名密钥为例进行介绍。

如图 6 所示, 为本申请实施例提供的又一种车载设备的升级方法, 该方法可以包括如下步骤:

35 S601: 电子设备向服务器发送第二签名信息。相应的, 服务器接收来自电子设备的第二签名信息。

本申请实施例中, 电子设备可以是图 1A 中的电子设备 102, 服务器可以是图 1A 中的服务器 101; 或者电子设备可以是图 1B 中的电子设备, 服务器可以是图 1B 中的服务器。

本申请实施例中，第二签名信息用于验证电子设备的身份。第二签名信息是用代理签名密钥对第一升级请求进行签名得到的。其中，代理签名密钥是根据车载控制设备的私钥和代理签名密钥的授权信息得到的。例如，代理签名密钥可以用算法对应授权信息的哈希值以及车载控制设备的私钥进行计算得到。该授权信息还可以称为保证书（warranty）。第一升级请求的介绍可以参考上述 S301 中对应的描述，在此不做赘述。

本申请实施例中，代理签名密钥的授权信息可以包括以下至少一项：至少一个车载设备的待升级信息、车载控制设备的标识、服务器的标识、电子设备的标识、授权期限或授权目的信息。其中，至少一个车载设备的待升级信息和授权期限的介绍可以参考上述 S301 中对应的描述，在此不做赘述。

S602：服务器在第二签名信息验证成功的情况下，向电子设备发送至少一个车载设备的升级包。相应的，电子设备接收来自服务器的至少一个车载设备的升级包。

可以理解的，服务器接收到第二签名信息后，可以验证第二签名信息，并在第二签名信息验证成功的情况下，向电子设备发送至少一个车载设备的升级包。

一种可能的实现方式，服务器根据车载控制设备的公钥验证第二签名信息。可以理解的，代理签名密钥是根据车载控制设备的私钥和代理签名密钥的授权信息得到的，第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，所以服务器可以用车载控制设备的公钥验证第二签名信息。

可以理解的，若第二签名信息验证成功，则表示电子设备合法，或电子设备被授权下载升级包，并且接收到的信息未被篡改，若第二签名信息验证失败，则表示电子设备不合法，或电子设备未被授权下载升级包，或接收到的信息被篡改。

一种可能的实现方式，若在授权期限内，服务器要取消对电子设备的授权，可以将上述授权信息存入授权信息取消列表中。

S603：电子设备向车载控制设备发送至少一个车载设备的升级包。相应的，车载控制设备接收来自电子设备的至少一个车载设备的升级包。

S604：车载控制设备分别向至少一个车载设备发送每个车载设备的升级包。相应的，每个车载设备接收升级包。

上述 S603~S604 的过程与上述 S303~S304 的过程类似，因此，可以参考上述 S303~S304 中对应的描述，在此不做赘述。

其中，上述 S601-S604 中的电子设备或者服务器或者车载控制设备的动作可以由图 2 所示的通信设备 20 中的处理器 201 调用存储器 203 中存储的应用程序代码来执行，本申请实施例对此不做任何限制。

基于图 6 所示的方法，服务器可以通过第二签名信息验证电子设备的合法性，如电子设备是否有下载升级包的权限等，以及验证接收到的信息是否被篡改，以保障车载设备升级的安全性。

可选的，在图 6 所示方法的一种可能的场景中，车载控制装置为电子设备生成代理签名密钥。具体的，如图 7 所示，图 6 所示的方法还包括以下步骤：

S600a：车载控制设备获取代理签名密钥。

一种可能的实现方式，车载控制设备作为原签名者，使用自己的私钥为电子设备

(作为代理签名者)生成代理签名密钥。其中,代理签名密钥包括代理签名密钥的授权信息。代理签名密钥可以作为授权书,用于服务器验证电子设备的合法性。

S600b: 车载控制设备向电子设备发送代理签名密钥。相应的,电子设备接收来自车载控制设备的代理签名密钥。

- 5 可以理解的,通过 S600a~S600b,车载控制设备可以为电子设备生成授权书(如:代理签名密钥)。之后,电子设备可以根据该授权书向服务器请求升级包。由于授权书具有不可修改和不可伪造性,将授权书作为电子设备向服务器证明电子设备的合法性的凭证,可以保证车载设备的升级安全。另外,上述授权书的生成不需要服务器的参与,过程简单实用。而且代理签名密钥产生的数字签名(如第二签名信息)的合法性由原签名者(车载控制设备)的公钥验证,不涉及被授权者(电子设备)的公钥证书,与通过电子设备的公钥的公钥证书进行认证的方法相比,减少了证书链的长度,可以提高验证效率。
- 10

- 其中,上述 S600a~S600b 中的电子设备或者车载控制设备的动作可以由图 2 所示的通信设备 20 中的处理器 201 调用存储器 203 中存储的应用程序代码来执行,本申
- 15 请实施例对此不做任何限制。

 本申请上文中提到的各个实施例之间在方案不矛盾的情况下,均可以进行结合,不作限制。

- 上述主要从各个设备之间交互的角度对本申请实施例提供的方案进行了介绍。相应的,本申请实施例还提供了通信设备,该通信设备可以为上述方法实施例中的服务器,或者包含上述服务器的装置,或者为可用于服务器的部件;或者,该通信设备可以为上述方法实施例中的电子设备,或者包含上述电子设备的装置,或者为可用于电子设备的部件;或者,该通信设备可以为上述方法实施例中的车载控制设备,或者包含上述车载控制设备的装置,或者为可用于车载控制设备的部件。可以理解的是,服务器、电子设备或车载控制设备等为了实现上述功能,其包含了执行各个功能相应的
- 20 硬件结构和/或软件模块。本领域技术人员应该很容易意识到,结合本文中所公开的实施例描述的各示例的单元及算法操作,本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。
- 25

- 30 本申请实施例可以根据上述方法示例对服务器、电子设备或车载控制设备进行功能模块的划分,例如,可以对应各个功能划分各个功能模块,也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现,也可以采用软件功能模块的形式实现。可以理解的是,本申请实施例中对模块的划分是示意性的,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式。

- 35 比如,以采用集成的方式划分各个功能模块的情况下,图 8 示出了一种通信设备 80 的结构示意图。通信设备 80 包括收发模块 801 和处理模块 802。收发模块 801,也可以称为收发单元用于执行收发操作,例如可以是收发电路,收发机,收发器或者通信接口等。处理模块 802,也可以称为处理单元用于执行除了收发操作之外的操作,例如可以是处理电路或者处理器等。

在一些实施例中，该通信设备 80 还可以包括存储模块（图 8 中未示出），用于存储程序指令和数据。

示例性地，通信设备 80 用于实现服务器的功能。通信设备 80 例如为图 3 所示的实施例，图 4 所示的实施例或图 5 所示的实施例所述的服务器。

5 其中，收发模块 801，用于接收来自电子设备的**第一签名信息**和**第一公钥信息**。其中，**第一签名信息**是用电子设备的私钥对**第一升级请求**进行签名得到的，**第一升级请求**用于请求至少一个车载设备的升级包，**第一公钥信息**用于验证电子设备的身份，**第一公钥信息**包括电子设备的公钥的公钥证书，或者，**第一公钥信息**包括电子设备的公钥。例如，收发模块 801 可以用于执行 S301。

10 处理模块 802，用于在**第一签名信息**和**第一公钥信息**验证成功的情况下，通过收发模块 801 向电子设备发送升级包。例如，处理模块 802 可以用于执行 S302。

在一种可能的实现方式中，处理模块 802，还用于根据电子设备的公钥验证**第一签名信息**。

15 在一种可能的实现方式中，收发模块 801，还用于接收来自车载控制设备的电子设备的公钥；收发模块 801，还用于向车载控制设备发送公钥证书，公钥证书是根据通信设备 80 的私钥生成的。

在一种可能的实现方式中，处理模块 802，还用于根据通信设备 80 的公钥验证公钥证书。

20 在一种可能的实现方式中，公钥证书是根据车载控制设备的私钥生成的，处理模块 802，还用于根据车载控制设备的公钥验证公钥证书。

在一种可能的实现方式中，收发模块 801，还用于接收来自车载控制设备的电子设备的公钥；处理模块 802，还用于生成电子设备的公钥的授权信息。

在一种可能的实现方式中，处理模块 802，还用于根据授权信息验证电子设备的公钥。

25 在一种可能的实现方式中，处理模块 802，还用于删除授权信息。

在一种可能的实现方式中，**第一升级请求**包括至少一个车载设备的待升级信息。

在一种可能的实现方式中，公钥证书包括以下至少一项：至少一个车载设备的待升级信息、车载控制设备的标识、通信设备 80 的标识、电子设备的标识、授权期限或授权目的信息。

30 当用于实现服务器的功能时，关于通信设备 80 所能实现的其他功能，可参考图 3 所示的实施例，图 4 所示的方法实施例或图 5 所示的实施例的相关介绍，不多赘述。

或者，示例性地，通信设备 80 用于实现服务器的功能。通信设备 80 例如为图 6 所示的实施例或图 7 所示的实施例所述的服务器。

35 其中，收发模块 801，用于接收来自电子设备的**第二签名信息**。其中，**第二签名信息**用于验证电子设备的身份，**第二签名信息**是用代理签名密钥对**第一升级请求**进行签名得到的，代理签名密钥是根据车载控制设备的私钥和代理签名密钥的授权信息得到的，**第一升级请求**用于请求至少一个车载设备的升级包。例如，收发模块 801 可以用于执行 S601。

处理模块 802, 用于在第二签名信息验证成功的情况下, 通过收发模块 801 向电子设备发送升级包。例如, 处理模块 802 可以用于执行 S602。

在一种可能的实现方式中, 处理模块 802, 还用于根据车载控制设备的公钥验证第二签名信息。

- 5 在一种可能的实现方式中, 处理模块 802, 还用于将授权信息存入授权信息取消列表。

在一种可能的实现方式中, 第一升级请求包括至少一个车载设备的待升级信息。

- 10 在一种可能的实现方式中, 授权信息包括以下至少一项: 至少一个车载设备的待升级信息、车载控制设备的标识、通信设备 80 的标识、电子设备的标识、授权期限或授权目的信息。

当用于实现服务器的功能时, 关于通信设备 80 所能实现的其他功能, 可参考图 6 所示的实施例或图 7 所示的实施例的相关介绍, 不多赘述。

或者, 示例性地, 通信设备 80 用于实现车载控制设备的功能。通信设备 80 例如为图 7 所示的实施例所述的车载控制设备。

- 15 其中, 处理模块 802, 用于获取代理签名密钥。其中, 代理签名密钥是根据通信设备 80 的私钥和代理签名密钥的授权信息得到的。例如, 处理模块 802 可以用于执行 S600a。

收发模块 801, 用于向电子设备发送代理签名密钥。例如, 收发模块 801 可以用于执行 S600b。

- 20 在一种可能的实现方式中, 授权信息包括以下至少一项: 至少一个车载设备的待升级信息、通信设备 80 的标识、服务器的标识、电子设备的标识、授权期限或授权目的信息。

在一种可能的实现方式中, 收发模块 801, 还用于向电子设备发送至少一个车载设备的待升级信息。

- 25 当用于实现车载控制设备的功能时, 关于通信设备 80 所能实现的其他功能, 可参考图 7 所示的实施例的相关介绍, 不多赘述。

在一个简单的实施例中, 本领域的技术人员可以想到通信设备 80 可以采用图 2 所示的形式。比如, 图 2 中的处理器 201 可以通过调用存储器 203 中存储的计算机执行指令, 使得通信设备 80 执行上述方法实施例中所述的方法。

- 30 示例性的, 图 8 中的收发模块 801 和处理模块 802 的功能/实现过程可以通过图 2 中的处理器 201 调用存储器 203 中存储的计算机执行指令来实现。或者, 图 8 中的处理模块 802 的功能/实现过程可以通过图 2 中的处理器 201 调用存储器 203 中存储的计算机执行指令来实现, 图 8 中的收发模块 801 的功能/实现过程可以通过图 2 中的通信接口 204 来实现。

- 35 比如, 以采用集成的方式划分各个功能模块的情况下, 图 9 示出了一种通信设备 90 的结构示意图。通信设备 90 包括收发模块 901。可选的, 该通信设备 90 还包括处理模块 902。收发模块 901, 也可以称为收发单元用于执行收发操作, 例如可以是收发电路, 收发机, 收发器或者通信接口等。处理模块 902, 也可以称为处理单元用于执行除了收发操作之外的操作, 例如可以是处理电路或者处理器等。

在一些实施例中，该通信设备 90 还可以包括存储模块（图 9 中未示出），用于存储程序指令和数据。

示例性地，通信设备 90 用于实现电子设备的功能。通信设备 90 例如为图 3 所示的实施例，图 4 所示的实施例或图 5 所示的实施例所述的电子设备。

5 其中，收发模块 901，用于向服务器发送第一签名信息和第一公钥信息。其中，第一签名信息是用通信设备 90 的私钥对第一升级请求进行签名得到的，第一升级请求用于请求至少一个车载设备的升级包，第一公钥信息用于验证通信设备 90 的身份，第一公钥信息包括通信设备 90 的公钥的公钥证书，或者，第一公钥信息包括通信设备 90 的公钥。例如，收发模块 901 可以用于执行 S301。

10 收发模块 901，还用于接收来自服务器的升级包。例如，收发模块 901 可以用于执行 S302。

收发模块 901，还用于向车载控制设备发送升级包。例如，收发模块 901 可以用于执行 S303。

15 在一种可能的实现方式中，收发模块 901，还用于接收来自车载控制设备的公钥证书，公钥证书是根据车载控制设备的私钥生成的，或者，公钥证书是根据服务器的私钥生成的。

在一种可能的实现方式中，处理模块 902，用于获取通信设备 90 的公钥和通信设备 90 的私钥；收发模块 901，还用于向车载控制设备发送通信设备 90 的公钥。

在一种可能的实现方式中，第一升级请求包括至少一个车载设备的待升级信息。

20 在一种可能的实现方式中，公钥证书包括以下至少一项：至少一个车载设备的待升级信息、车载控制设备的标识、服务器的标识、通信设备 90 的标识、授权期限或授权目的信息。

在一种可能的实现方式中，收发模块 901，还用于接收来自车载控制设备的至少一个车载设备的待升级信息。

25 当用于实现电子设备的功能时，关于通信设备 90 所能实现的其他功能，可参考图 3 所示的实施例，图 4 所示的方法实施例或图 5 所示的实施例的相关介绍，不多赘述。

30 在一个简单的实施例中，本领域的技术人员可以想到通信设备 90 可以采用图 2 所示的形式。比如，图 2 中的处理器 201 可以通过调用存储器 203 中存储的计算机执行指令，使得通信设备 90 执行上述方法实施例中所述的方法。

35 示例性的，图 9 中的收发模块 901 和处理模块 902 的功能/实现过程可以通过图 2 中的处理器 201 调用存储器 203 中存储的计算机执行指令来实现。或者，图 9 中的处理模块 902 的功能/实现过程可以通过图 2 中的处理器 201 调用存储器 203 中存储的计算机执行指令来实现，图 9 中的收发模块 901 的功能/实现过程可以通过图 2 中的通信接口 204 来实现。

比如，以采用集成的方式划分各个功能模块的情况下，图 10 示出了一种通信设备 100 的结构示意图。通信设备 100 包括收发模块 1001。收发模块 1001，也可以称为收发单元用于执行收发操作，例如可以是收发电路，收发机，收发器或者通信接口等。

示例性地，通信设备 100 用于实现车载控制设备的功能。通信设备 100 例如为图 4 所示的实施例所述的车载控制设备。

其中，收发模块 1001，用于接收来自电子设备的电子设备的公钥。例如，收发模块 1001 可以用于执行 S300b 或 S300B。

- 5 收发模块 1001，用于向电子设备发送电子设备的公钥的公钥证书，公钥证书是根据通信设备 100 的私钥生成的，或者，公钥证书是根据服务器的私钥生成的。例如，收发模块 1001 可以用于执行 S300c 或 S300E。

- 10 在一种可能的实现方式中，公钥证书是根据服务器的私钥生成的，收发模块 1001，还用于向服务器发送电子设备的公钥；收发模块 1001，还用于接收来自服务器的公钥证书。

在一种可能的实现方式中，公钥证书包括以下至少一项：至少一个车载设备的待升级信息、通信设备 100 的标识、服务器的标识、电子设备的标识、授权期限或授权目的信息。

- 15 在一种可能的实现方式中，收发模块 1001，还用于向所电子设备发送至少一个车载设备的待升级信息。

当用于实现车载控制设备的功能时，关于通信设备 100 所能实现的其他功能，可参考图 4 所示的实施例的相关介绍，不多赘述。

或者，示例性地，通信设备 100 用于实现车载控制设备的功能。通信设备 100 例如为图 5 所示的实施例所述的车载控制设备。

- 20 其中，收发模块 1001，用于接收来自电子设备的电子设备的公钥。例如，收发模块 1001 可以用于执行 S3002。

收发模块 1001，还用于向服务器发送第一指示信息和电子设备的公钥，第一指示信息用于指示生成电子设备的公钥的授权信息。例如，收发模块 1001 可以用于执行 S3003。

- 25 在一种可能的实现方式中，收发模块 1001，还用于向电子设备发送至少一个车载设备的待升级信息。

当用于实现车载控制设备的功能时，关于通信设备 100 所能实现的其他功能，可参考图 5 所示的实施例的相关介绍，不多赘述。

- 30 或者，示例性地，通信设备 100 用于实现电子设备的功能。通信设备 100 例如为图 6 所示的实施例或图 7 所示的实施例所述的电子设备。

- 35 其中，收发模块 1001，用于向服务器发送第二签名信息。其中，第二签名信息用于验证通信设备 100 的身份，第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，代理签名密钥是根据车载控制设备的私钥和代理签名密钥的授权信息得到的，第一升级请求用于请求至少一个车载设备的升级包。例如，收发模块 1001 用于执行 S601。

收发模块 1001，还用于接收来自服务器的升级包。例如，收发模块 1001 还用于执行 S602。

收发模块 1001，还用于向车载控制设备发送升级包。例如，收发模块 1001 还用于执行 S603。

在一种可能的实现方式中，收发模块 1001，还用于接收来自车载控制设备的代理签名密钥。

在一种可能的实现方式中，第一升级请求包括至少一个车载设备的待升级信息。

在一种可能的实现方式中，授权信息包括以下至少一项：至少一个车载设备的待升级信息、车载控制设备的标识、服务器的标识、通信设备 100 的标识、授权期限或授权目的信息。

在一种可能的实现方式中，收发模块 1001，还用于接收来自车载控制设备的至少一个车载设备的待升级信息。

当用于实现电子设备的功能时，关于通信设备 100 所能实现的其他功能，可参考图 6 所示的实施例或图 7 所示的实施例的相关介绍，不多赘述。

在一个简单的实施例中，本领域的技术人员可以想到通信设备 100 可以采用图 2 所示的形式。比如，图 2 中的处理器 201 可以通过调用存储器 203 中存储的计算机执行指令，使得通信设备 100 执行上述方法实施例中所述的方法。

示例性的，图 10 中的收发模块 1001 的功能/实现过程可以通过图 2 中的处理器 201 调用存储器 203 中存储的计算机执行指令来实现。或者，图 10 中的收发模块 1001 的功能/实现过程可以通过图 2 中的通信接口 204 来实现。

可以理解的是，以上模块或单元的一个或多个可以软件、硬件或二者结合来实现。当以上任一模块或单元以软件实现的时候，所述软件以计算机程序指令的方式存在，并被存储在存储器中，处理器可以用于执行所述程序指令并实现以上方法流程。该处理器可以内置于 SoC（片上系统）或 ASIC，也可是一个独立的半导体芯片。该处理器内处理用于执行软件指令以进行运算或处理的核外，还可进一步包括必要的硬件加速器，如现场可编程门阵列（field programmable gate array, FPGA）、PLD（可编程逻辑器件）、或者实现专用逻辑运算的逻辑电路。

当以上模块或单元以硬件实现的时候，该硬件可以是 CPU、微处理器、数字信号处理（digital signal processing, DSP）芯片、微控制单元（microcontroller unit, MCU）、人工智能处理器、ASIC、SoC、FPGA、PLD、专用数字电路、硬件加速器或非集成的分立器件中的任一个或任一组合，其可以运行必要的软件或不依赖于软件以执行以上方法流程。

可选的，本申请实施例还提供了一种芯片系统，包括：至少一个处理器和接口，该至少一个处理器通过接口与存储器耦合，当该至少一个处理器执行存储器中的计算机程序或指令时，使得上述任一方法实施例中的方法被执行。在一种可能的实现方式中，该芯片系统还包括存储器。可选的，该芯片系统可以由芯片构成，也可以包含芯片和其他分立器件，本申请实施例对此不作具体限定。

可选的，本申请实施例还提供了一种计算机可读存储介质。上述方法实施例中的全部或者部分流程可以由计算机程序来指令相关的硬件完成，该程序可存储于上述计算机可读存储介质中，该程序在执行时，可包括如上述各方法实施例的流程。计算机可读存储介质可以是前述任一实施例的通信设备的内部存储单元，例如通信设备的硬盘或内存。上述计算机可读存储介质也可以是上述通信设备的外部存储设备，例如上述通信设备上配备的插接式硬盘，智能存储卡（smart media card, SMC），安全数字

(secure digital, SD)卡, 闪存卡(flash card)等。进一步地, 上述计算机可读存储介质还可以既包括上述通信设备的内部存储单元也包括外部存储设备。上述计算机可读存储介质用于存储上述计算机程序以及上述通信设备所需的其他程序和数据。上述计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

5 可选的, 本申请实施例还提供了一种计算机程序产品。上述方法实施例中的全部或者部分流程可以由计算机程序来指令相关的硬件完成, 该程序可存储于上述计算机程序产品中, 该程序在执行时, 可包括如上述各方法实施例的流程。

10 可选的, 本申请实施例还提供了一种计算机指令。上述方法实施例中的全部或者部分流程可以由计算机指令来指令相关的硬件(如计算机、处理器、服务器、电子设备或车载控制设备等)完成。该程序可被存储于上述计算机可读存储介质中或上述计算机程序产品中。

可选的, 本申请实施例还提供了一种车辆, 包括上述实施例中的车载控制设备。

可选的, 本申请实施例还提供了一种升级系统, 包括: 图3所示实施例、图4所示实施例或图5所示实施例中的服务器、电子设备和车载控制设备。

15 可选的, 本申请实施例还提供了一种升级系统, 包括: 图6所示实施例或图7所示实施例中的服务器、电子设备和车载控制设备。

20 通过以上的实施方式的描述, 所属领域的技术人员可以清楚地了解到, 为描述的方便和简洁, 仅以上述各功能模块的划分进行举例说明, 实际应用中, 可以根据需要而将上述功能分配由不同的功能模块完成, 即将装置的内部结构划分成不同的功能模块, 以完成以上描述的全部或者部分功能。

25 在本申请所提供的几个实施例中, 应该理解到, 所揭露的装置和方法, 可以通过其它的方式实现。例如, 以上所描述的装置实施例仅仅是示意性的, 例如, 所述模块或单元的划分, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式, 例如多个单元或组件可以结合或者可以集成到另一个装置, 或一些特征可以忽略, 或不执行。另一点, 所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口, 装置或单元的间接耦合或通信连接, 可以是电性, 机械或其它的形式。

30 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的, 作为单元显示的部件可以是一个物理单元或多个物理单元, 即可以位于一个地方, 或者也可以分布到多个不同地方。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外, 在本申请各个实施例中的各功能单元可以集成在一个处理单元中, 也可以是各个单元单独物理存在, 也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现, 也可以采用软件功能单元的形式实现。

35 以上所述, 仅为本申请的具体实施方式, 但本申请的保护范围并不局限于此, 任何在本申请揭露的技术范围内的变化或替换, 都应涵盖在本申请的保护范围之内。因此, 本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种车载设备的升级方法，其特征在于，应用于服务器，所述方法包括：
接收来自电子设备的第二签名信息和第二公钥信息，所述第二签名信息是用所述
电子设备的私钥对第二升级请求进行签名得到的，所述第二升级请求用于请求至少一个
5 个车载设备的升级包，所述第二公钥信息用于验证所述电子设备的身份，所述第二公
钥信息包括所述电子设备的公钥的公钥证书，或者，所述第二公钥信息包括所述电子
设备的公钥；
在所述第二签名信息和所述第二公钥信息验证成功的情况下，向所述电子设备发
送所述升级包。
- 10 2. 根据权利要求1所述的方法，其特征在于，所述方法还包括：
根据所述电子设备的公钥验证所述第二签名信息。
3. 根据权利要求1或2所述的方法，其特征在于，所述方法还包括：
接收来自车载控制设备的所述电子设备的公钥；
向所述车载控制设备发送所述公钥证书，所述公钥证书是根据所述服务器的私钥
15 生成的。
4. 根据权利要求3所述的方法，其特征在于，所述方法还包括：
根据所述服务器的公钥验证所述公钥证书。
5. 根据权利要求1或2所述的方法，其特征在于，所述公钥证书是根据车载控
制设备的私钥生成的，所述方法还包括：
20 根据所述车载控制设备的公钥验证所述公钥证书。
6. 根据权利要求1或2所述的方法，其特征在于，所述方法还包括：
接收来自车载控制设备的所述电子设备的公钥；
生成所述电子设备的公钥的授权信息。
7. 根据权利要求6所述的方法，其特征在于，所述方法还包括：
25 根据所述授权信息验证所述电子设备的公钥。
8. 根据权利要求6或7所述的方法，其特征在于，所述方法还包括：
删除所述授权信息。
9. 根据权利要求1-8中任一项所述的方法，其特征在于，所述第一升级请求包
括所述至少一个车载设备的待升级信息。
- 30 10. 根据权利要求1-9中任一项所述的方法，其特征在于，所述公钥证书包括以
下至少一项：所述至少一个车载设备的待升级信息、车载控制设备的标识、所述服务
器的标识、所述电子设备的标识、授权期限或授权目的信息。
11. 一种车载设备的升级方法，其特征在于，应用于电子设备，所述方法包括：
向服务器发送第二签名信息和第二公钥信息，所述第二签名信息是用所述电子设
35 备的私钥对第二升级请求进行签名得到的，所述第二升级请求用于请求至少一个车载
设备的升级包，所述第二公钥信息用于验证所述电子设备的身份，所述第二公钥信息
包括所述电子设备的公钥的公钥证书，或者，所述第二公钥信息包括所述电子设备的
公钥；
接收来自所述服务器的所述升级包；

向车载控制设备发送所述升级包。

12. 根据权利要求 11 所述的方法，其特征在于，所述方法还包括：

接收来自所述车载控制设备的所述公钥证书，所述公钥证书是根据所述车载控制设备的私钥生成的，或者，所述公钥证书是根据所述服务器的私钥生成的。

5 13. 根据权利要求 12 所述的方法，其特征在于，所述方法还包括：

获取所述电子设备的公钥和所述电子设备的私钥；

向所述车载控制设备发送所述电子设备的公钥。

14. 根据权利要求 11-13 中任一项所述的方法，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。

10 15. 根据权利要求 11-14 中任一项所述的方法，其特征在于，所述公钥证书包括以下至少一项：所述至少一个车载设备的待升级信息、所述车载控制设备的标识、所述服务器的标识、所述电子设备的标识、授权期限或授权目的信息。

16. 根据权利要求 14 或 15 所述的方法，其特征在于，所述方法还包括：

接收来自所述车载控制设备的所述至少一个车载设备的待升级信息。

15 17. 一种车载设备的升级方法，其特征在于，应用于车载控制设备，所述方法包括：

接收来自电子设备的所述电子设备的公钥；

向所述电子设备发送所述电子设备的公钥的公钥证书，所述公钥证书是根据所述车载控制设备的私钥生成的，或者，所述公钥证书是根据服务器的私钥生成的。

20 18. 根据权利要求 17 所述的方法，其特征在于，所述公钥证书是根据服务器的私钥生成的，所述方法还包括：

向所述服务器发送所述电子设备的公钥；

接收来自所述服务器的所述公钥证书。

25 19. 根据权利要求 17 或 18 所述的方法，其特征在于，所述公钥证书包括以下至少一项：至少一个车载设备的待升级信息、所述车载控制设备的标识、所述服务器的标识、所述电子设备的标识、授权期限或授权目的信息。

20. 根据权利要求 19 所述的方法，其特征在于，所述方法还包括：

向所述电子设备发送所述至少一个车载设备的待升级信息。

30 21. 一种车载设备的升级方法，其特征在于，应用于车载控制设备，所述方法包括：

接收来自电子设备的所述电子设备的公钥；

向服务器发送第一指示信息和所述电子设备的公钥，所述第一指示信息用于指示生成所述电子设备的公钥的授权信息。

22. 根据权利要求 21 所述的方法，其特征在于，所述方法还包括：

35 向所述电子设备发送至少一个车载设备的待升级信息。

23. 一种车载设备的升级方法，其特征在于，应用于服务器，所述方法包括：

接收来自电子设备的第二签名信息，所述第二签名信息用于验证所述电子设备的身份，所述第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，所述代理签名密钥是根据车载控制设备的私钥和所述代理签名密钥的授权信息得到的，所述

- 第一升级请求用于请求至少一个车载设备的升级包；
在所述第二签名信息验证成功的情况下，向所述电子设备发送所述升级包。
24. 根据权利要求 23 所述的方法，其特征在于，所述方法还包括：
根据所述车载控制设备的公钥验证所述第二签名信息。
- 5 25. 根据权利要求 23 或 24 所述的方法，其特征在于，所述方法还包括：
将所述授权信息存入授权信息取消列表。
26. 根据权利要求 23-25 中任一项所述的方法，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。
27. 根据权利要求 23-26 中任一项所述的方法，其特征在于，所述授权信息包括
10 以下至少一项：所述至少一个车载设备的待升级信息、所述车载控制设备的标识、所述服务器的标识、所述电子设备的标识、授权期限或授权目的信息。
28. 一种车载设备的升级方法，其特征在于，应用于电子设备，所述方法包括：
向服务器发送第二签名信息，所述第二签名信息用于验证所述电子设备的身份，
所述第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，所述代理签名
15 密钥是根据车载控制设备的私钥和所述代理签名密钥的授权信息得到的，所述第一升级请求用于请求至少一个车载设备的升级包；
接收来自所述服务器的所述升级包；
向车载控制设备发送所述升级包。
29. 根据权利要求 28 所述的方法，其特征在于，所述方法还包括：
20 接收来自所述车载控制设备的所述代理签名密钥。
30. 根据权利要求 28 或 29 所述的方法，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。
31. 根据权利要求 28-30 中任一项所述的方法，其特征在于，所述授权信息包括
25 以下至少一项：所述至少一个车载设备的待升级信息、所述车载控制设备的标识、所述服务器的标识、所述电子设备的标识、授权期限或授权目的信息。
32. 根据权利要求 30 或 31 所述的方法，其特征在于，所述方法还包括：
接收来自所述车载控制设备的所述至少一个车载设备的待升级信息。
33. 一种车载设备的升级方法，其特征在于，应用于车载控制设备，所述方法包括：
30 获取代理签名密钥，所述代理签名密钥是根据所述车载控制设备的私钥和所述代理签名密钥的授权信息得到的；
向电子设备发送所述代理签名密钥。
34. 根据权利要求 33 所述的方法，其特征在于，所述授权信息包括以下至少一项：至少一个车载设备的待升级信息、所述车载控制设备的标识、服务器的标识、所述
35 所述电子设备的标识、授权期限或授权目的信息。
35. 根据权利要求 34 所述的方法，其特征在于，所述方法还包括：
向所述电子设备发送所述至少一个车载设备的待升级信息。
36. 一种通信设备，其特征在于，所述通信设备包括：收发模块和处理模块；
所述收发模块，用于接收来自电子设备的第一签名信息和第一公钥信息，所述第

一签名信息是用所述电子设备的私钥对第一升级请求进行签名得到的，所述第一升级请求用于请求至少一个车载设备的升级包，所述第一公钥信息用于验证所述电子设备的身份，所述第一公钥信息包括所述电子设备的公钥的公钥证书，或者，所述第一公钥信息包括所述电子设备的公钥；

- 5 所述处理模块，用于在所述第一签名信息和所述第一公钥信息验证成功的情况下，通过所述收发模块向所述电子设备发送所述升级包。

37. 根据权利要求 36 所述的通信设备，其特征在于，
所述处理模块，还用于根据所述电子设备的公钥验证所述第一签名信息。

38. 根据权利要求 36 或 37 所述的通信设备，其特征在于，
10 所述收发模块，还用于接收来自车载控制设备的所述电子设备的公钥；
所述收发模块，还用于向所述车载控制设备发送所述公钥证书，所述公钥证书是根据所述通信设备的私钥生成的。

39. 根据权利要求 38 所述的通信设备，其特征在于，
所述处理模块，还用于根据所述通信设备的公钥验证所述公钥证书。

- 15 40. 根据权利要求 36 或 37 所述的通信设备，其特征在于，所述公钥证书是根据车载控制设备的私钥生成的，

所述处理模块，还用于根据所述车载控制设备的公钥验证所述公钥证书。

41. 根据权利要求 36 或 37 所述的通信设备，其特征在于，
所述收发模块，还用于接收来自车载控制设备的所述电子设备的公钥；

- 20 所述处理模块，还用于生成所述电子设备的公钥的授权信息。

42. 根据权利要求 41 所述的通信设备，其特征在于，
所述处理模块，还用于根据所述授权信息验证所述电子设备的公钥。

43. 根据权利要求 41 或 42 所述的通信设备，其特征在于，
所述处理模块，还用于删除所述授权信息。

- 25 44. 根据权利要求 36-43 中任一项所述的通信设备，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。

45. 根据权利要求 36-44 中任一项所述的通信设备，其特征在于，所述公钥证书包括以下至少一项：所述至少一个车载设备的待升级信息、车载控制设备的标识、所述通信设备的标识、所述电子设备的标识、授权期限或授权目的信息。

- 30 46. 一种通信设备，其特征在于，所述通信设备包括：收发模块；

所述收发模块，用于向服务器发送第一签名信息和第一公钥信息，所述第一签名信息是用所述通信设备的私钥对第一升级请求进行签名得到的，所述第一升级请求用于请求至少一个车载设备的升级包，所述第一公钥信息用于验证所述通信设备的身份，所述第一公钥信息包括所述通信设备的公钥的公钥证书，或者，所述第一公钥信息包括所述通信设备的公钥；

- 35 所述收发模块，还用于接收来自所述服务器的所述升级包；

所述收发模块，还用于向车载控制设备发送所述升级包。

47. 根据权利要求 46 所述的通信设备，其特征在于，
所述收发模块，还用于接收来自所述车载控制设备的所述公钥证书，所述公钥证

书是根据所述车载控制设备的私钥生成的，或者，所述公钥证书是根据所述服务器的私钥生成的。

48. 根据权利要求 47 所述的通信设备，其特征在于，所述通信设备还包括：处理模块；

5 所述处理模块，用于获取所述通信设备的公钥和所述通信设备的私钥；

所述收发模块，还用于向所述车载控制设备发送所述通信设备的公钥。

49. 根据权利要求 46-48 中任一项所述的通信设备，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。

10 50. 根据权利要求 46-49 中任一项所述的通信设备，其特征在于，所述公钥证书包括以下至少一项：所述至少一个车载设备的待升级信息、所述车载控制设备的标识、所述服务器的标识、所述通信设备的标识、授权期限或授权目的信息。

51. 根据权利要求 49 或 50 所述的通信设备，其特征在于，

所述收发模块，还用于接收来自所述车载控制设备的所述至少一个车载设备的待升级信息。

15 52. 一种通信设备，其特征在于，所述通信设备包括：收发模块；

所述收发模块，用于接收来自电子设备的所述电子设备的公钥；

所述收发模块，还用于向所述电子设备发送所述电子设备的公钥的公钥证书，所述公钥证书是根据所述通信设备的私钥生成的，或者，所述公钥证书是根据服务器的私钥生成的。

20 53. 根据权利要求 52 所述的通信设备，其特征在于，所述公钥证书是根据服务器的私钥生成的，

所述收发模块，还用于向所述服务器发送所述电子设备的公钥；

所述收发模块，还用于接收来自所述服务器的所述公钥证书。

25 54. 根据权利要求 52 或 53 所述的通信设备，其特征在于，所述公钥证书包括以下至少一项：至少一个车载设备的待升级信息、所述通信设备的标识、所述服务器的标识、所述电子设备的标识、授权期限或授权目的信息。

55. 根据权利要求 54 所述的通信设备，其特征在于，

所述收发模块，还用于向所述电子设备发送所述至少一个车载设备的待升级信息。

56. 一种通信设备，其特征在于，所述通信设备包括：收发模块；

30 所述收发模块，用于接收来自电子设备的所述电子设备的公钥；

所述收发模块，还用于向服务器发送第一指示信息和所述电子设备的公钥，所述第一指示信息用于指示生成所述电子设备的公钥的授权信息。

57. 根据权利要求 56 所述的通信设备，其特征在于，

所述收发模块，还用于向所述电子设备发送至少一个车载设备的待升级信息。

35 58. 一种通信设备，其特征在于，所述通信设备包括：收发模块和处理模块；

所述收发模块，用于接收来自电子设备的第二签名信息，所述第二签名信息用于验证所述电子设备的身份，所述第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，所述代理签名密钥是根据车载控制设备的私钥和所述代理签名密钥的授权信息得到的，所述第一升级请求用于请求至少一个车载设备的升级包；

所述处理模块，用于在所述第二签名信息验证成功的情况下，通过所述收发模块向所述电子设备发送所述升级包。

59. 根据权利要求 58 所述的通信设备，其特征在于，
所述处理模块，还用于根据所述车载控制设备的公钥验证所述第二签名信息。

5 60. 根据权利要求 58 或 59 所述的通信设备，其特征在于，
所述处理模块，还用于将所述授权信息存入授权信息取消列表。

61. 根据权利要求 58-60 中任一项所述的通信设备，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。

62. 根据权利要求 58-61 中任一项所述的通信设备，其特征在于，所述授权信息
10 包括以下至少一项：所述至少一个车载设备的待升级信息、所述车载控制设备的标识、所述通信设备的标识、所述电子设备的标识、授权期限或授权目的信息。

63. 一种通信设备，其特征在于，所述通信设备包括：收发模块；

所述收发模块，用于向服务器发送第二签名信息，所述第二签名信息用于验证所述通信设备的身份，所述第二签名信息是用代理签名密钥对第一升级请求进行签名得到的，所述代理签名密钥是根据车载控制设备的私钥和所述代理签名密钥的授权信息
15 得到的，所述第一升级请求用于请求至少一个车载设备的升级包；

所述收发模块，还用于接收来自所述服务器的所述升级包；

所述收发模块，还用于向车载控制设备发送所述升级包。

64. 根据权利要求 63 所述的通信设备，其特征在于，
20 所述收发模块，还用于接收来自所述车载控制设备的所述代理签名密钥。

65. 根据权利要求 63 或 64 所述的通信设备，其特征在于，所述第一升级请求包括所述至少一个车载设备的待升级信息。

66. 根据权利要求 63-65 中任一项所述的通信设备，其特征在于，所述授权信息
25 包括以下至少一项：所述至少一个车载设备的待升级信息、所述车载控制设备的标识、所述服务器的标识、所述通信设备的标识、授权期限或授权目的信息。

67. 根据权利要求 65 或 66 所述的通信设备，其特征在于，

所述收发模块，还用于接收来自所述车载控制设备的所述至少一个车载设备的待升级信息。

68. 一种通信设备，其特征在于，所述通信设备包括：处理模块和收发模块；

30 所述处理模块，用于获取代理签名密钥，所述代理签名密钥是根据所述通信设备的私钥和所述代理签名密钥的授权信息得到的；

所述收发模块，用于向电子设备发送所述代理签名密钥。

69. 根据权利要求 68 所述的通信设备，其特征在于，所述授权信息包括以下至少一项：至少一个车载设备的待升级信息、所述通信设备的标识、服务器的标识、所述
35 电子设备的标识、授权期限或授权目的信息。

70. 根据权利要求 69 所述的通信设备，其特征在于，

所述收发模块，还用于向所述电子设备发送所述至少一个车载设备的待升级信息。

71. 一种通信设备，其特征在于，包括：处理器，所述处理器与存储器耦合，所述存储器用于存储程序或指令，当所述程序或指令被所述处理器执行时，使得所述装

置执行如权利要求 1 至 10 中任一项所述的方法,或者执行如权利要求 11 至 16 中任一项所述的方法,或者执行如权利要求 17 至 20 中任一项所述的方法,或者执行如权利要求 21 至 22 中任一项所述的方法,或者执行如权利要求 23 至 27 中任一项所述的方法,或者执行如权利要求 28 至 32 中任一项所述的方法,或者执行如权利要求 33 至 35 中任一项所述的方法。

72. 一种计算机可读存储介质,其上存储有计算机程序或指令,其特征在于,所述计算机程序或指令被执行时使得计算机执行如权利要求 1 至 10 中任一项所述的方法,或者执行如权利要求 11 至 16 中任一项所述的方法,或者执行如权利要求 17 至 20 中任一项所述的方法,或者执行如权利要求 21 至 22 中任一项所述的方法,或者执行如权利要求 23 至 27 中任一项所述的方法,或者执行如权利要求 28 至 32 中任一项所述的方法,或者执行如权利要求 33 至 35 中任一项所述的方法。

73. 一种计算机程序产品,所述计算机程序产品中包括计算机程序代码,其特征在于,当所述计算机程序代码在计算机上运行时,使得计算机执行如权利要求 1 至 10 中任一项所述的方法,或者执行如权利要求 11 至 16 中任一项所述的方法,或者执行如权利要求 17 至 20 中任一项所述的方法,或者执行如权利要求 21 至 22 中任一项所述的方法,或者执行如权利要求 23 至 27 中任一项所述的方法,或者执行如权利要求 28 至 32 中任一项所述的方法,或者执行如权利要求 33 至 35 中任一项所述的方法。

74. 一种芯片,其特征在于,包括:处理器,所述处理器与存储器耦合,所述存储器用于存储程序或指令,当所述程序或指令被所述处理器执行时,使得所述芯片执行如权利要求 1 至 10 中任一项所述的方法,或者如权利要求 11 至 16 中任一项所述的方法,或者执行如权利要求 17 至 20 中任一项所述的方法,或者执行如权利要求 21 至 22 中任一项所述的方法,或者执行如权利要求 23 至 27 中任一项所述的方法,或者执行如权利要求 28 至 32 中任一项所述的方法,或者执行如权利要求 33 至 35 中任一项所述的方法。

75. 一种车辆,其特征在于,包括:如权利要求 52 至 55 中任一项所述的通信设备,或者如权利要求 56 至 57 中任一项所述的通信设备,或者如权利要求 68 至 70 中任一项所述的通信设备。