(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114710284 B
(45)授权公告日 2022.08.16

(21)申请号 202210528669.2

(22)申请日 2022.05.16

(65)同一申请的已公布的文献号
申请公布号 CN 114710284 A

(43)申请公布日 2022.07.05

(73)专利权人 北京智芯微电子科技有限公司
地址 100192 北京市海淀区西小口路66号中关村东升科技园A区3号楼

(72)发明人 李德建 刁明响 王于波 崔炳荣 张喆 蒋名扬 唐小飞 王岩

(74)专利代理机构 北京智信四方知识产权代理有限公司 11519
专利代理师 彭杰

(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/0433(2021.01)
H04W 12/30(2021.01)
H04W 12/42(2021.01)

(56)对比文件
WO 2017166791 A1,2017.10.05
WO 2017028375 A1,2017.02.23
US 2010250936 A1,2010.09.30
US 2003161064 A1,2003.08.28
US 2002073415 A1,2002.06.13

审查员 王伦杰

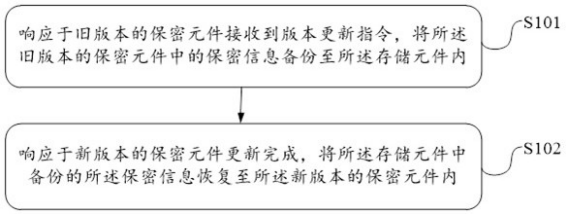
权利要求书3页 说明书11页 附图6页

(54)发明名称

通信保密元件的版本更新方法、设备及存储介质

(57)摘要

本公开涉及计算机数据技术领域，具体涉及公开了一种通信保密元件的版本更新方法、设备及存储介质，该方法包括：响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内；响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内。该技术方案可以解决保密信息外泄的问题，主要用于增强保密元件在版本更新时的安全性。



CN 114710284 B

1.一种通信保密元件的版本更新方法,其特征在于,所述方法应用于电子用户身份识别芯片,所述电子用户身份识别芯片上设置有保密元件和存储元件,所述方法包括:

响应于旧版本的保密元件接收到版本更新指令,将所述旧版本的保密元件中的保密信息备份至所述存储元件内;

响应于新版本的保密元件更新完成,将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内。

2.根据权利要求1所述的方法,其特征在于,在将所述旧版本的保密元件中的保密信息备份至所述存储元件内之后,所述方法还包括:

所述存储元件向服务器返回备份成功消息,以便所述服务器下发新版本的保密元件的安装包;

响应于接收到所述服务器下发的新版本的保密元件的安装包,删除旧版本的保密元件,下载所述新版本的保密元件的安装包并安装,完成所述新版本的保密元件的更新。

3.根据权利要求2所述的方法,其特征在于,所述响应于新版本的保密元件更新完成,将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内,包括:

响应于新版本的保密元件更新完成,向所述电子用户身份识别芯片所在的通讯模组发送更新成功消息,以便所述通讯模组向所述新版本的保密元件下发恢复保密信息请求消息;

响应于所述新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息,将所述存储元件内备份的所述保密信息恢复至所述新版本的保密元件内。

4.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述旧版本的保密元件接收服务器发送的版本更新指令。

5.根据权利要求1所述的方法,其特征在于,所述将所述旧版本的保密元件中的保密信息备份至所述存储元件内,包括:

所述旧版本的保密元件调用第一共享接口将所述保密信息发送给所述存储元件;

所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置。

6.根据权利要求5所述的方法,其特征在于,所述将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内,包括:

所述新版本的保密元件调用第二共享接口向所述存储元件发送信息恢复指令;

所述存储元件响应于接收到所述信息恢复指令,通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件;

所述新版本的保密元件接收并写入所述保密信息。

7.根据权利要求6所述的方法,其特征在于,所述第一共享接口和/或所述第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和所述存储元件的接口。

8.一种通信保密元件的版本更新方法,其特征在于,所述方法应用于通讯模组,所述通讯模组内嵌电子用户身份识别芯片,所述电子用户身份识别芯片上设置有保密元件和存储元件,所述方法包括:

所述通讯模组将服务器下发的版本更新指令转发至旧版本的保密元件;

所述旧版本的保密元件响应于接收到所述版本更新指令,将所述旧版本的保密元件内

的保密信息备份至所述存储元件内；

所述电子用户身份识别芯片响应于检测到新版本的保密元件更新完成，向所述通讯模组发送更新成功消息；

所述通讯模组接收到所述更新成功消息时，向所述新版本的保密元件发送恢复保密信息请求消息；

所述新版本的保密元件响应于接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内。

9.根据权利要求8所述的方法，其特征在于，所述方法还包括：

所述存储元件在将所述保密信息备份成功后，向所述通讯模组发送备份成功消息；

所述通讯模组响应于接收到所述备份成功消息，将所述备份成功消息转发给服务器，以便所述服务器响应于接收到所述备份成功消息向所述通讯模组发送新版本的保密元件的安装包；

所述通讯模组接收所述服务器发送的新版本的保密元件的安装包并转发给所述电子用户身份识别芯片；

所述电子用户身份识别芯片删除旧版本的保密元件，接收所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新。

10.根据权利要求8所述的方法，其特征在于，所述将所述旧版本的保密元件内的保密信息备份至所述存储元件内，包括：

所述旧版本的保密元件调用第一共享接口将所述保密信息发送给所述存储元件；

所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置。

11.根据权利要求10所述的方法，其特征在于，所述将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内，包括：

所述新版本的保密元件调用第二共享接口向所述存储元件发送信息恢复指令；

所述存储元件响应于接收到所述信息恢复指令，通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件；

所述新版本的保密元件接收并写入所述保密信息。

12.根据权利要求11所述的方法，其特征在于，所述第一共享接口和/或所述第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和所述存储元件的接口。

13.一种电子用户身份识别芯片，其特征在于，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述电子用户身份识别芯片被配置为执行权利要求1至7任一项所述的通信保密元件的版本更新方法。

14.一种通讯模组，其特征在于，所述通讯模组内嵌入有电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述通讯模组被配置为执行权利要求8至12任一项所述的通信保密元件的版本更新方法。

15.一种电子设备，其特征在于，包括存储器和处理器，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行以实现权利要求1至12任一项所述的方法。

16.一种可读存储介质，其特征在于，其上存储有计算机指令，该计算机指令被处理器

执行时实现权利要求1至12任一项所述的方法步骤。

通信保密元件的版本更新方法、设备及存储介质

技术领域

[0001] 本公开涉及计算机数据技术领域，具体涉及一种通信保密元件的版本更新方法、设备及存储介质。

背景技术

[0002] 随着计算机数据通信技术的发展，以及通信终端技术的完善和用户需求的提高，数据通信的安全问题越来越被重视，针对数据安全和保密方面的技术也汹涌而出，各种针对数据安全和保密的方法层出不穷。

[0003] 目前，通信终端中需要保密的保密信息通常都存储在终端的ESIM(Embedded-SIM，电子用户身份识别)芯片中，该电子用户身份识别芯片中设置有SE(Secure Element，保密元件)(也可称为安全元件)，该保密元件采用java card(智能卡开发)标准开发而来，可以提供对敏感信息的安全存储和对交易事务提供一个安全的执行环境，通常都会将SEID(Secure Element Identity，SE身份标识)，白名单，安全启动标识等这些个人化的保密信息存储在该保密元件中。

[0004] 在保密元件进行版本更新时，为了避免这些个人化的保密信息丢失或损坏而导致保密元件不可用，需要对这些保密信息进行妥善处理。现有技术中采用的方案是在保密元件进行版本更新时，将这些保密信息通过7816接口读出，在电子用户身份识别芯片所在的通讯模组中备份，当保密元件的版本更新完成后，再将个人化保密信息通过7816指令写入保密元件内，完成信息恢复，在保密信息的备份和恢复时，均需要将这些保密信息在7816通道上进行传输，容易被截获，存在信息泄露的风险。

发明内容

[0005] 为了解决相关技术中的问题，本公开实施例提供一种通信保密元件的版本更新方法、设备及存储介质。

[0006] 第一方面，本公开实施例中提供了一种通信保密元件的版本更新方法。

[0007] 具体地，所述通信保密元件的版本更新方法应用于电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述方法包括：

[0008] 响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内；

[0009] 响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内。

[0010] 在一种可能的实现方式中，在将所述旧版本的保密元件中的保密信息备份至所述存储元件内后，所述方法还包括：

[0011] 所述存储元件向服务器返回备份成功消息，以便所述服务器下发新版本的保密元件的安装包；

[0012] 响应于接收到所述服务器下发的新版本的保密元件的安装包，删除旧版本的保密

元件，下载所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新。

[0013] 在一种可能的实现方式中，所述响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内，包括：

[0014] 响应于新版本的保密元件更新完成，向所述电子用户身份识别芯片所在的通讯模组发送更新成功消息，以便所述通讯模组向所述新版本的保密元件下发恢复保密信息请求消息；

[0015] 响应于所述新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至所述新版本的保密元件内。

[0016] 在一种可能的实现方式中，所述方法还包括：

[0017] 所述旧版本的保密元件接收服务器发送的版本更新指令。

[0018] 在一种可能的实现方式中，所述将所述旧版本的保密元件中的保密信息备份至所述存储元件内，包括：

[0019] 所述旧版本的保密元件调用第一共享接口将所述保密信息发送给所述存储元件；

[0020] 所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置。

[0021] 在一种可能的实现方式中，所述将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内，包括：

[0022] 所述新版本的保密元件调用第二共享接口向所述存储元件发送信息恢复指令；

[0023] 所述存储元件响应于接收到所述信息恢复指令，通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件；

[0024] 所述新版本的保密元件接收并写入所述保密信息。

[0025] 在一种可能的实现方式中，所述第一共享接口和/或第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和存储元件的接口。

[0026] 第二方面，本公开实施例中提供了一种通信保密元件的版本更新方法。

[0027] 具体地，所述通信保密元件的版本更新方法应用于通讯模组，所述通讯模组内嵌电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述方法包括：

[0028] 所述通讯模组将服务器下发的版本更新指令转发至旧版本的保密元件；

[0029] 所述旧版本的保密元件响应于接收到所述版本更新指令，将所述旧版本的保密元件内的保密信息备份至所述存储元件内；

[0030] 所述电子用户身份识别芯片响应于检测到新版本的保密元件更新完成，向所述通讯模组发送更新成功消息；

[0031] 所述通讯模组接收到所述更新成功消息时，向所述新版本的保密元件发送恢复保密信息请求消息；

[0032] 所述新版本的保密元件响应于接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内。

[0033] 在一种可能的实现方式中，所述方法还包括：

[0034] 所述存储元件在将所述保密信息备份成功后，向所述通讯模组发送备份成功消息；

[0035] 所述通讯模组响应于接收到所述备份成功消息，将所述备份成功消息转发给服务器，以便所述服务器响应于接收到所述备份成功消息向所述通讯模组发送新版本的保密元件的安装包；

[0036] 所述通讯模组接收所述服务器发送的新版本的保密元件的安装包并转发给所述电子用户身份识别芯片；

[0037] 所述电子用户身份识别芯片删除旧版本的保密元件，接收所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新。

[0038] 在一种可能的实现方式中，所述将所述旧版本的保密元件内的保密信息备份至所述存储元件内，包括：

[0039] 所述旧版本的保密元件调用第一共享接口将所述保密信息发送给所述存储元件；

[0040] 所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置。

[0041] 在一种可能的实现方式中，所述将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内，包括：

[0042] 所述新版本的保密元件调用第二共享接口向所述存储元件发送信息恢复指令；

[0043] 所述存储元件响应于接收到所述信息恢复指令，通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件；

[0044] 所述新版本的保密元件接收并写入所述保密信息。

[0045] 在一种可能的实现方式中，所述第一共享接口和/或所述第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和所述存储元件的接口。

[0046] 第三方面，本公开实施例中提供了一种电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述电子用户身份识别芯片被配置为执行上述第一方面提供的通信保密元件的版本更新方法。

[0047] 第四方面，本公开实施例中提供了一种通讯模组，所述通讯模组内嵌入有电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述通讯模组被配置为执行上述第二方面提供的通信保密元件的版本更新方法。

[0048] 第五方面，本公开实施例提供了一种电子设备，包括存储器和处理器，其中，所述存储器用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器执行以实现如第一方面和第二方面中任一项所述的方法。

[0049] 第六方面，本公开实施例中提供了一种计算机可读存储介质，其上存储有计算机指令，该计算机指令被处理器执行时实现如第一方面和第二方面中任一项所述的方法。

[0050] 根据本公开实施例提供的技术方案，可以响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内；响应于新版本的保密元件更新完成，再将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内，如此通过在电子用户身份识别芯片内部进行保密信息的备份和恢复，对于外界来说，属于完全不透明状态，保密信息完全与外界物理隔离，保证了保密信息的安全，而且在保密元件的升级过程中，将保密信息存储在电子用户身份识别芯片的存储元件中，可以借助电子用户身份识别芯片的防火墙标准，利用电子用户身份识别芯片暴力破解数据难度大的优势，进一步保证保密信息的储存安全。

附图说明

[0051] 结合附图，通过以下非限制性实施方式的详细描述，本公开的其它特征、目的和优点将变得更加明显。在附图中。

[0052] 图1示出根据本公开的实施例的应用于电子用户身份识别芯片的通信保密元件的版本更新方法的流程图。

[0053] 图2示出根据本公开的实施例的应用于电子用户身份识别芯片的通信保密元件的版本更新方法的流程图。

[0054] 图3示出根据本公开的实施例的应用于电子用户身份识别芯片的通信保密元件的版本更新方法的流程图。

[0055] 图4示出根据本公开的实施例的应用于通讯模组的通信保密元件的版本更新方法的流程图。

[0056] 图5示出根据本公开的实施例的应用于通讯模组的通信保密元件的版本更新方法的流程图。

[0057] 图6示出根据本公开的实施例的通信保密元件的版本更新方法的整体流程图。

[0058] 图7示出根据本公开的实施例的电子设备的结构框图。

[0059] 图8示出适于用来实现根据本公开实施例的通信保密元件的版本更新方法的计算机系统的结构示意图。

具体实施方式

[0060] 下文中，将参考附图详细描述本公开的示例性实施例，以使本领域技术人员可容易地实现它们。此外，为了清楚起见，在附图中省略了与描述示例性实施例无关的部分。

[0061] 在本公开中，应理解，诸如“包括”或“具有”等的术语旨在指示本说明书中所公开的特征、数字、步骤、行为、部件、部分或其组合的存在，并且不欲排除一个或多个其他特征、数字、步骤、行为、部件、部分或其组合存在或被添加的可能性。

[0062] 另外还需要说明的是，在不冲突的情况下，本公开中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本公开。

[0063] 上文提及，在保密元件进行版本更新时，为了避免这些个人化的保密信息丢失或损坏而导致保密元件不可用，需要对这些保密信息进行妥善处理。现有技术中采用的方案是在保密元件进行版本更新时，将这些保密信息通过7816接口读出，在电子用户身份识别芯片所在的通讯模组中备份，当保密元件的版本更新完成后，再将个人化保密信息通过7816指令写入保密元件内，完成信息恢复，在保密信息的备份和恢复时，均需要将这些保密信息在7816通道上进行传输，容易被截获，存在信息泄露的风险。

[0064] 为了解决上述问题，本公开提供了一种通信保密元件的版本更新方法、设备及存储介质。

[0065] 图1示出根据本公开的实施例的应用于电子用户身份识别芯片的通信保密元件的版本更新方法的流程图。如图1所示，所述通信保密元件的版本更新方法包括以下步骤S101-S102：

[0066] 在步骤S101中，响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内；

[0067] 在步骤S102中，响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内。

[0068] 这里，所述通信保密元件的版本更新方法指的是通信场景中的保密元件的版本更新方法，可应用于设置有保密元件的电子用户身份识别芯片，该电子用户身份识别芯片中除了设置有保密元件，还设置有存储元件，该保密元件可以提供对保密信息的安全存储和对交易事务提供一个安全的执行环境，该存储元件可以提供对数据的安全存储。

[0069] 这里，在研发出新版本的保密元件的程序后，会将该新版本的保密元件的安装包上传至对应的服务器中，服务器在获取到新版本的保密元件的安装包后，确定其服务的电子用户身份识别芯片中的旧版本的保密元件需要进行版本升级，此时，服务器会向电子用户身份识别芯片中的旧版本的保密元件下发版本更新指令，该旧版本的保密元件在接收到该版本更新指令时，会将该旧版本的保密元件内的保密信息备份至所述存储元件内，然后就可以安装新版本的保密元件，在新版本的保密元件安装完成后，该新版本的保密元件就可以从存储元件内将备份的保密信息读出，并将这些保密信息写入新版本的保密元件，完成保密信息的恢复。

[0070] 本实施方式通过在电子用户身份识别芯片内部进行保密信息的备份和恢复，对于外界来说，属于完全不透明状态，保密信息完全与外界物理隔离，保证了保密信息安全，而且在保密元件的升级过程中，将保密信息存储在电子用户身份识别芯片的存储元件中，可以借助电子用户身份识别芯片的防火墙标准，利用电子用户身份识别芯片暴力破解数据难度大的优势，进一步保证保密信息的存储安全。另外，由于保密信息仅在电子用户身份识别芯片内部传输，传输速度更快，提高了备份和恢复的效率，也进一步提升了整个升级过程的效率。

[0071] 在本公开一种可能的实施方式中，图2示出根据本公开的实施例的应用于电子用户身份识别芯片的通信保密元件的版本更新方法的流程图，如图2所示，在将所述旧版本的保密元件中的保密信息备份至所述存储元件内之后，所述方法还包括以下步骤：

[0072] 在步骤S103中，所述存储元件向服务器返回备份成功消息，以便所述服务器下发新版本的保密元件的安装包；

[0073] 在步骤S104中，响应于接收到所述服务器下发的新版本的保密元件的安装包，删除旧版本的保密元件，下载所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新。

[0074] 这里，在将所述旧版本的保密元件中的保密信息备份至所述存储元件内之后，就可以执行保密元件的版本更新操作，删除旧版本的保密元件，下载新版本的保密元件的安装包并进行安装，得到更新后的新版本的保密元件。

[0075] 这里，可以是存储元件向服务器返回备份成功消息，所述服务器响应于接收到该备份成功消息，可以向电子用户身份识别芯片下发保密元件的新安装包，电子用户身份识别芯片接收到该新版本的保密元件的安装包后，可以删除旧版本的保密元件，下载所述新版本的保密元件的安装包并安装，得到更新后的新版本的保密元件。

[0076] 在本公开一种可能的实施方式中，图3示出根据本公开的实施例的应用于电子用户身份识别芯片的通信保密元件的版本更新方法的流程图，如图3所示，上述步骤S102即响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版

本的保密元件内，可以实现为以下步骤：

[0077] 在步骤S1021中，响应于新版本的保密元件更新完成，向所述电子用户身份识别芯片所在的通讯模组发送更新成功消息，以便所述通讯模组向所述新版本的保密元件下发恢复保密信息请求消息；

[0078] 在步骤S1022中，响应于所述新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至所述新版本的保密元件内。

[0079] 这里，该通讯模组指的是该电子用户身份识别芯片嵌入的通讯模组，电子用户身份识别芯片在更新好新版本的保密元件之后，可以向通讯模组发送更新成功消息，所述通讯模组响应于接收到该更新成功消息，会向该新版本的保密元件下发恢复保密信息请求消息，指示该新版本的保密元件进行保密信息恢复，该新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息时，可以读取所述存储元件内备份的所述保密信息，写入该新版本的保密元件内。

[0080] 这里需要说明的是，该新版本的保密元件在恢复该备份的保密信息后，可以向服务器返回恢复成功消息，告知服务器该保密元件版本更新成功。

[0081] 在本公开一种可能的实施方式中，所述方法还可以包括以下步骤：

[0082] 所述旧版本的保密元件接收服务器发送的版本更新指令。

[0083] 这里，在研发出新版本的保密元件的程序后，会将该新版本的保密元件的安装包上传至对应的服务器中，服务器在获取到新版本的保密元件的安装包后，确定其服务的电子用户身份识别芯片中的旧版本的保密元件需要进行版本升级，此时，服务器会向电子用户身份识别芯片中的旧版本的保密元件下发版本更新指令，该旧版本的保密元件在接收到该版本更新指令时，会将该旧版本的保密元件内的保密信息备份至所述存储元件内。

[0084] 在本公开一种可能的实施方式中，上述通信保密元件的版本更新方法中的步骤S101中将所述旧版本的保密元件中的保密信息备份至所述存储元件内的部分可以包括以下步骤A1和A2：

[0085] 在步骤A1中，所述旧版本的保密元件调用第一共享接口将所述保密信息发送给所述存储元件；

[0086] 在步骤A2中，所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置。

[0087] 这里，旧版本的保密元件可以通过存储元件的AID(Application Identifier，应用标识)调用系统API(Application Programming Interface，应用程序接口)获得第一共享接口的句柄(Handle)，然后可以基于该第一共享接口的句柄调用该第一共享接口，通过第一共享接口将所述保密信息发送给所述预设存储位置如备份文件处，该存储元件通过所述第一共享接口接收所述保密信息后，可以将该保密信息写入所述存储元件中的预设存储位置，如该存储元件中的备份文件处。这里需要说明的是，该第一共享接口指的是用于将保密元件中待备份的保密信息传输至该存储元件的数据备份共享接口。

[0088] 在本公开一种可能的实施方式中，上述通信保密元件的版本更新方法中的步骤S102中将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内的部分可以包括以下步骤B1至B3：

[0089] 在步骤B1中,所述新版本的保密元件调用第二共享接口向所述存储元件发送信息恢复指令;

[0090] 在步骤B2中,所述存储元件响应于接收到所述信息恢复指令,通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件;

[0091] 在步骤B3中,所述新版本的保密元件接收并写入所述保密信息。

[0092] 这里,新版本的保密元件可以通过存储元件的AID调用系统API获得第二共享接口的句柄,然后可以基于该第二共享接口的句柄调用该第二共享接口,通过第二共享接口向所述存储元件发送信息恢复指令,所述存储元件接收到所述信息恢复指令后,可以通过所述第二共享接口将备份的所述保密信息发送给所述保密元件,所述新版本的保密元件接收该保密信息并将该保密信息一次性写入新版本的保密元件中,比如说,一次性写入SEID,白名单,安全启动标识等保密信息。

[0093] 本实施方式通过在电子用户身份识别芯片内部设置共享接口完成保密信息的备份和恢复,实现简单方便。

[0094] 在本公开一实施方式中,所述第一共享接口和/或第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和存储元件的接口。

[0095] 这里,可以设计一共享接口包,这个共享接口包里声明了第一共享接口和/或第二共享接口,这两个共享接口是java card的标准共享接口,保密元件在版本更新阶段可以直接调用第一共享接口和第二共享接口,第一共享接口、第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和存储元件的接口,这样即使后续存储元件被删除进行重新安装,也不会影响该第一共享接口和/或第二共享接口的使用,可以保证存储元件能够被自由删除安装,使存储元件的版本也可以在线更新。

[0096] 图4示出根据本公开的实施例的应用于通讯模组的通信保密元件的版本更新方法的流程图。如图4所示,所述通信保密元件的版本更新方法包括以下步骤S401-S405:

[0097] 在步骤S401中,所述通讯模组将服务器下发的版本更新指令转发至旧版本的保密元件;

[0098] 在步骤S402中,所述旧版本的保密元件响应于接收到所述版本更新指令,将所述旧版本的保密元件内的保密信息备份至所述存储元件内;

[0099] 在步骤S403中,所述电子用户身份识别芯片响应于检测到新版本的保密元件更新完成,向所述通讯模组发送更新成功消息;

[0100] 在步骤S404中,所述通讯模组接收到所述更新成功消息时,向所述新版本的保密元件发送恢复保密信息请求消息;

[0101] 在步骤S405中,所述新版本的保密元件响应于接收到所述通讯模组发送的恢复保密信息请求消息,将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内。

[0102] 这里,所述通信保密元件的版本更新方法可适用于通讯模组,如可以是5G远程通讯模组,该通讯模组内嵌电子用户身份识别芯片,该电子用户身份识别芯片中设置有保密元件和存储元件,该保密元件可以提供对敏感信息的安全存储和对交易事务提供一个安全的执行环境,该存储元件可以提供对数据的安全存储。

[0103] 这里,在研发出新版本的保密元件的程序后,会将该新版本的保密元件的安装包上传至对应的服务器中,服务器在获取到新版本的保密元件的安装包后,确定其服务的电

子用户身份识别芯片中的旧版本的保密元件需要进行版本升级，此时，服务器会向该通讯模组发送保密元件的版本更新指令，该通讯模组接收到该版本更新指令时，会将服务器下发的版本更新指令转发至旧版本的保密元件，示例的，通讯模组与电子用户身份识别芯片之间的通信格式为APDU(Application Protocol Data Unit，应用协议数据单元)结构，该通讯模组会将服务器下发的版本更新指令以APDU指令的格式发送给旧版本的保密元件，该旧版本的保密元件接收到该版本更新指令时，可以将所述旧版本的保密元件内的保密信息备份至所述存储元件内。

[0104] 在该实施方式中，将旧版本的保密元件内的保密信息备份后，电子用户身份识别芯片就可以删除该旧版本的保密元件并安装新版本的保密元件，在新版本的保密元件安装完成后，电子用户身份识别芯片可以向该通讯模组发送更新成功消息，所述通讯模组接收到所述更新成功消息时，向所述新版本的保密元件发送恢复保密信息请求消息，指示该新版本的保密元件进行数据恢复，该恢复保密信息请求消息也是APDU指令，所述新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息时，可以将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内。

[0105] 在本公开的一种可能实施方式中，图5示出根据本公开的实施例的应用于通讯模组的通信保密元件的版本更新方法的流程图，如图5所示，所述方法还包括以下步骤：

[0106] 在步骤S406中，所述存储元件在将所述保密信息备份成功后，向所述通讯模组发送备份成功消息；

[0107] 在步骤S407中，所述通讯模组响应于接收到所述备份成功消息，将所述备份成功消息转发给服务器，以便所述服务器响应于接收到所述备份成功消息向所述通讯模组发送新版本的保密元件的安装包；

[0108] 在步骤S408中，所述通讯模组接收所述服务器发送的新版本的保密元件的安装包并转发给所述电子用户身份识别芯片；

[0109] 在步骤S409中，所述电子用户身份识别芯片删除旧版本的保密元件，接收所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新。

[0110] 这里，所述存储元件在将所述保密信息备份完成后，向所述通讯模组发送备份成功消息，所述通讯模组响应于所述备份成功消息，可以将该备份成功消息转发给服务器，服务器接收到该备份成功消息后，会向该通讯模组发送新版本的保密元件的安装包，如此，该通讯模组就可以从服务器下载新版本的保密元件的安装包并发送给所述电子用户身份识别芯片；所述电子用户身份识别芯片接收所述新版本的保密元件的安装包时，就可以删除旧版本的保密元件以及旧安装包，下载所述新版本的保密元件的安装包并安装，得到更新后的新版本的保密元件，然后就可以执行步骤S403－S405，将存储元件内备份的所述保密信息恢复至该新版本的保密元件内，该新版本的保密元件在写入该备份的保密信息后，可以向服务器返回恢复成功消息，告知服务器该保密元件升级成功，如此，保密元件的整个升级流程就结束了。

[0111] 在本公开一种可能的实施方式中，上述通信保密元件的版本更新方法中的步骤S402中将所述旧版本的保密元件中的保密信息备份至所述存储元件内的部分可以包括以下步骤C1和C2：

[0112] 在步骤C1中，所述旧版本的保密元件调用第一共享接口将所述保密信息发送给所

述存储元件；

[0113] 在步骤C2中，所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置。

[0114] 这里，旧版本的保密元件可以通过存储元件的AID调用系统API获得第一共享接口的句柄，然后可以基于该第一共享接口的句柄调用该第一共享接口，通过第一共享接口将所述保密信息发送给所述存储元件，该存储元件通过所述第一共享接口接收所述保密信息后，可以将该保密信息写入所述存储元件中的预设存储位置如该存储元件中的备份文件处。这里需要说明的是，该第一共享接口指的是用于将保密元件中待备份的保密信息传输至该存储元件的数据备份共享接口。

[0115] 在本公开一种可能的实施方式中，上述通信保密元件的版本更新方法中的步骤S405中将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内的部分可以包括以下步骤D1至D3：

[0116] 在步骤D1中，所述新版本的保密元件调用第二共享接口向所述存储元件发送信息恢复指令；

[0117] 在步骤D2中，所述存储元件响应于接收到所述信息恢复指令，通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件；

[0118] 在步骤D3中，所述新版本的保密元件接收并写入所述保密信息。

[0119] 这里，新版本的保密元件可以通过存储元件的AID调用系统API获得第二共享接口的句柄，然后可以基于该第二共享接口的句柄调用该第二共享接口，通过第二共享接口向所述存储元件发送信息恢复指令，所述存储元件接收到所述信息恢复指令后，可以通过所述第二共享接口将备份的所述保密信息发送给所述保密元件，所述新版本的保密元件接收该保密信息并将该保密信息一次性写入新版本的保密元件中，比如说，一次性写入SEID，白名单，安全启动标识等保密信息。

[0120] 本实施方式通过在电子用户身份识别芯片内部设置共享接口完成保密信息的备份和恢复，实现简单方便。

[0121] 在本公开一种可能的实施方式中，所述第一共享接口和/或第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和存储元件的接口。

[0122] 这里，可以设计一共享接口包，这个共享接口包里声明了第一共享接口和/或第二共享接口，这两个共享接口是java card的标准共享接口，保密元件在版本更新阶段可以直接调用第一共享接口和第二共享接口，第一共享接口、第二共享接口为所述电子用户身份识别芯片内独立于所述保密元件和存储元件的接口，这样即使后续存储元件被删除进行重新安装，也不会影响该第一共享接口和/或第二共享接口的使用，可以保证存储元件能够被自由删除安装，使存储元件的版本也可以在线更新。

[0123] 示例的，图6示出根据本公开的实施例的通信保密元件的版本更新方法的整体流程图，如图6所示，该方法包括以下步骤：

[0124] 在步骤S601中，服务器在保密元件出现新版本需要进行保密元件的版本更新时，通过通讯模组向旧版本的保密元件发送保密元件的版本更新指令；

[0125] 在步骤S602中，旧版本的保密元件调用第一共享接口将所述保密信息发送给所述存储元件；

[0126] 在步骤S603中，所述存储元件通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置；

[0127] 在步骤S604中，所述存储元件在将所述保密信息备份完成后，通过所述通讯模组向服务器发送备份成功消息；

[0128] 在步骤S605中，所述服务器通过该通讯模组向该电子用户身份识别芯片发送新版本的保密元件的安装包；

[0129] 在步骤S606中，该电子用户身份识别芯片删除旧版本的保密元件，下载所述新版本的保密元件的安装包并安装，得到更新后的新版本的保密元件；

[0130] 在步骤S607中，该电子用户身份识别芯片响应于检测到新版本的保密元件更新完成，向所述通讯模组发送更新成功消息；

[0131] 在步骤S608中，所述通讯模组接收到所述更新成功消息时，向所述新安全应用单元发送恢复保密信息请求消息；

[0132] 在步骤S609中，所述新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息时，调用第二共享接口向所述存储元件发送信息恢复指令；

[0133] 在步骤S610中，所述存储元件响应于接收到所述信息恢复指令，通过所述第二共享接口将备份的所述保密信息发送给所述新版本的保密元件；

[0134] 在步骤S611中，所述新版本的保密元件接收并写入所述保密信息；

[0135] 在步骤S612中，所述新版本的保密元件向服务器返回恢复成功消息。

[0136] 本公开还提供了一种电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述电子用户身份识别芯片被配置为执行前述应用于电子用户身份识别芯片的通信保密元件的版本更新方法。

[0137] 本公开还提供了一种通讯模组，所述通讯模组内嵌入有电子用户身份识别芯片，所述电子用户身份识别芯片上设置有保密元件和存储元件，所述通讯模组被配置为执行前述应用于该通讯模组的通信保密元件的版本更新方法。

[0138] 本公开还公开了一种电子设备，图7示出根据本公开的实施例的电子设备的结构框图。

[0139] 如图7所示，所述电子设备700包括存储器701和处理器702，其中，存储器701用于存储一条或多条计算机指令，其中，所述一条或多条计算机指令被所述处理器702执行以实现根据本公开的实施例的方法。

[0140] 图8示出适于用来实现根据本公开实施例的通信保密元件的版本更新方法的计算机系统的结构示意图。

[0141] 如图8所示，计算机系统800包括处理单元801，其可以根据存储在只读存储器(ROM)802中的程序或者从存储部分808加载到随机访问存储器(RAM)803中的程序而执行上述实施例中的各种处理。在RAM803中，还存储有计算机系统800操作所需的各种程序和数据。处理单元801、ROM802以及RAM803通过总线804彼此相连。输入/输出(I/O)接口805也连接至总线804。

[0142] 以下部件连接至I/O接口805：包括键盘、鼠标等的输入部分806；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分807；包括硬盘等的存储部分808；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分809。通信部分809经由诸如因

特网的网络执行通信处理。驱动器810也根据需要连接至I/O接口805。可拆卸介质811，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器810上，以便于从其上读出的计算机程序根据需要被安装入存储部分808。其中，所述处理单元801可实现为CPU、GPU、TPU、FPGA、NPU等处理单元。

[0143] 特别地，根据本公开的实施例，上文描述的方法可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括计算机指令，该计算机指令被处理器执行时实现上文所述的方法步骤。在这样的实施例中，该计算机程序产品可以通过通信部分809从网络上被下载和安装，和/或从可拆卸介质811被安装。

[0144] 附图中的流程图和框图，图示了按照本公开各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0145] 描述于本公开实施例中所涉及到的单元或模块可以通过软件的方式实现，也可以通过可编程硬件的方式来实现。所描述的单元或模块也可以设置在处理器中，这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0146] 作为另一方面，本公开还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中电子设备或计算机系统中所包含的计算机可读存储介质；也可以是单独存在，未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序，所述程序被一个或者一个以上的处理器用来执行描述于本公开的方法。

[0147] 以上描述仅为本公开的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本公开中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离所述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本公开中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

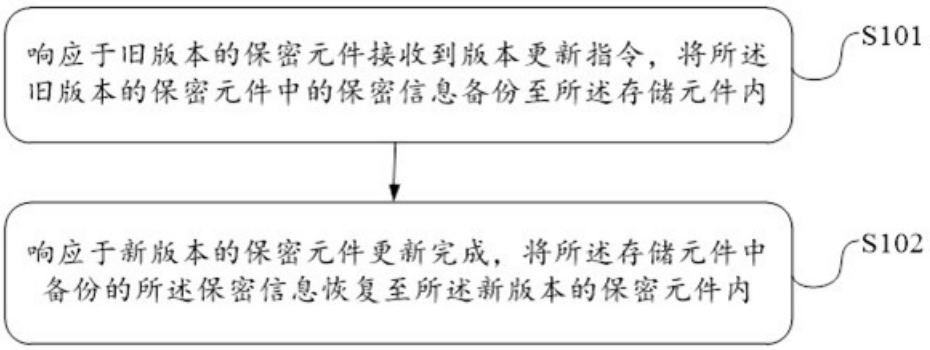

响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内
S101
响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内
S102

图1

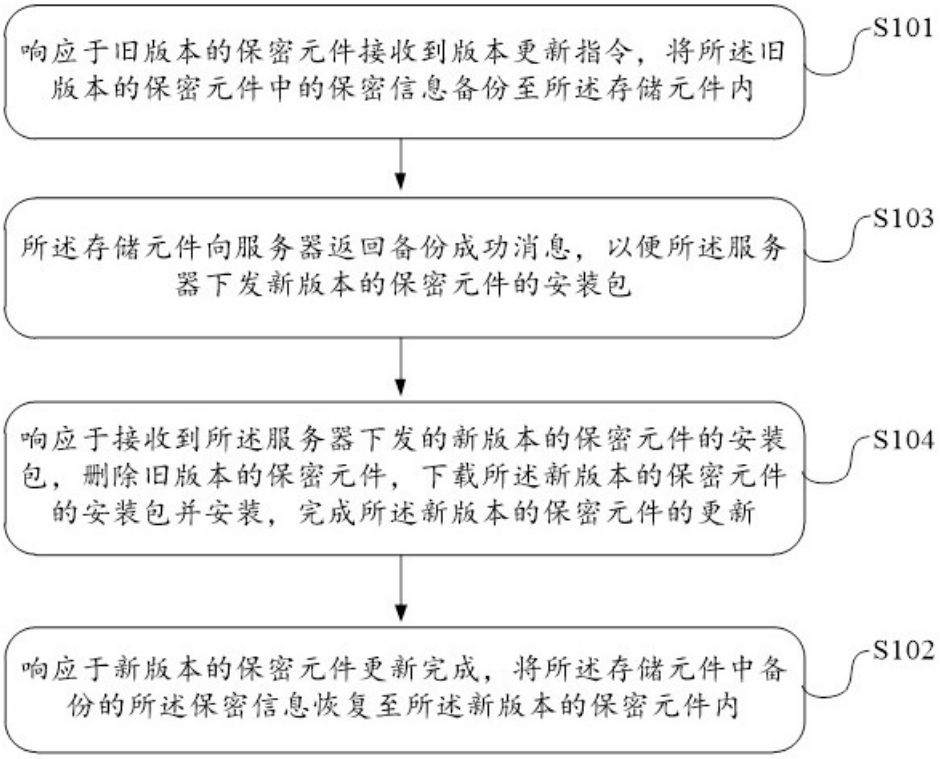

响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内
S101
所述存储元件向服务器返回备份成功消息，以便所述服务器下发新版本的保密元件的安装包
S103
响应于接收到所述服务器下发的新版本的保密元件的安装包，删除旧版本的保密元件，下载所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新
S104
响应于新版本的保密元件更新完成，将所述存储元件中备份的所述保密信息恢复至所述新版本的保密元件内
S102

图2

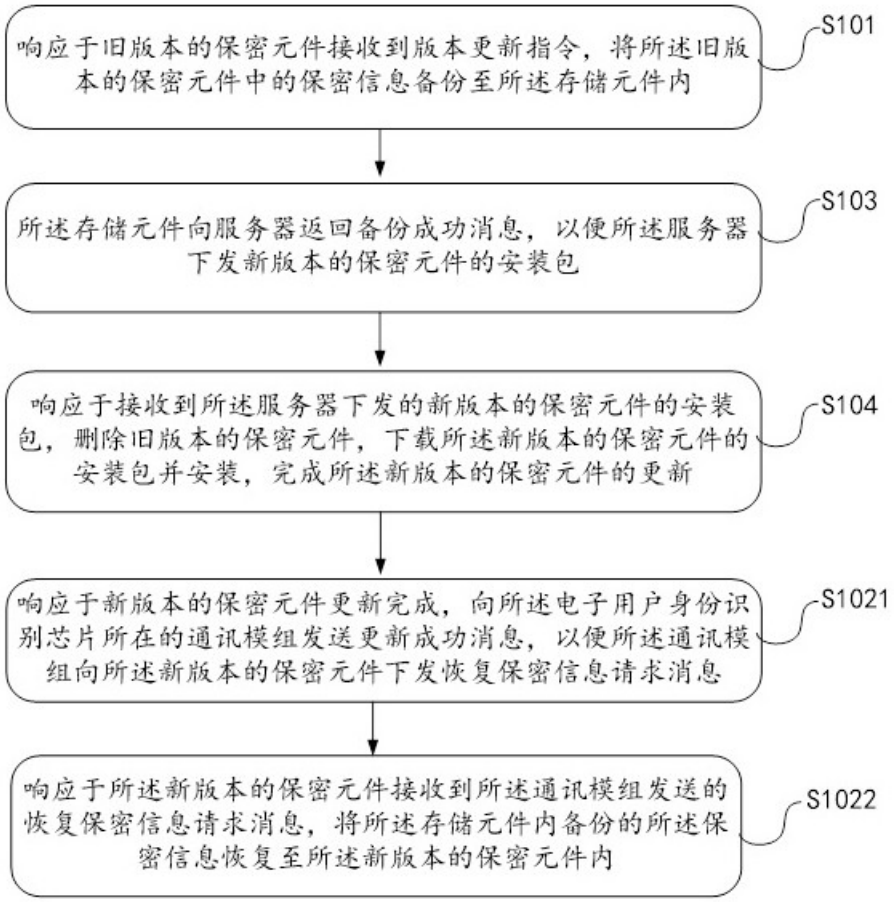

响应于旧版本的保密元件接收到版本更新指令，将所述旧版本的保密元件中的保密信息备份至所述存储元件内
S101
所述存储元件向服务器返回备份成功消息，以便所述服务器下发新版本的保密元件的安装包
S103
响应于接收到所述服务器下发的新版本的保密元件的安装包，删除旧版本的保密元件，下载所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新
S104
响应于新版本的保密元件更新完成，向所述电子用户身份识别芯片所在的通讯模组发送更新成功消息，以便所述通讯模组向所述新版本的保密元件下发恢复保密信息请求消息
S1021
响应于所述新版本的保密元件接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至所述新版本的保密元件内
S1022

图3

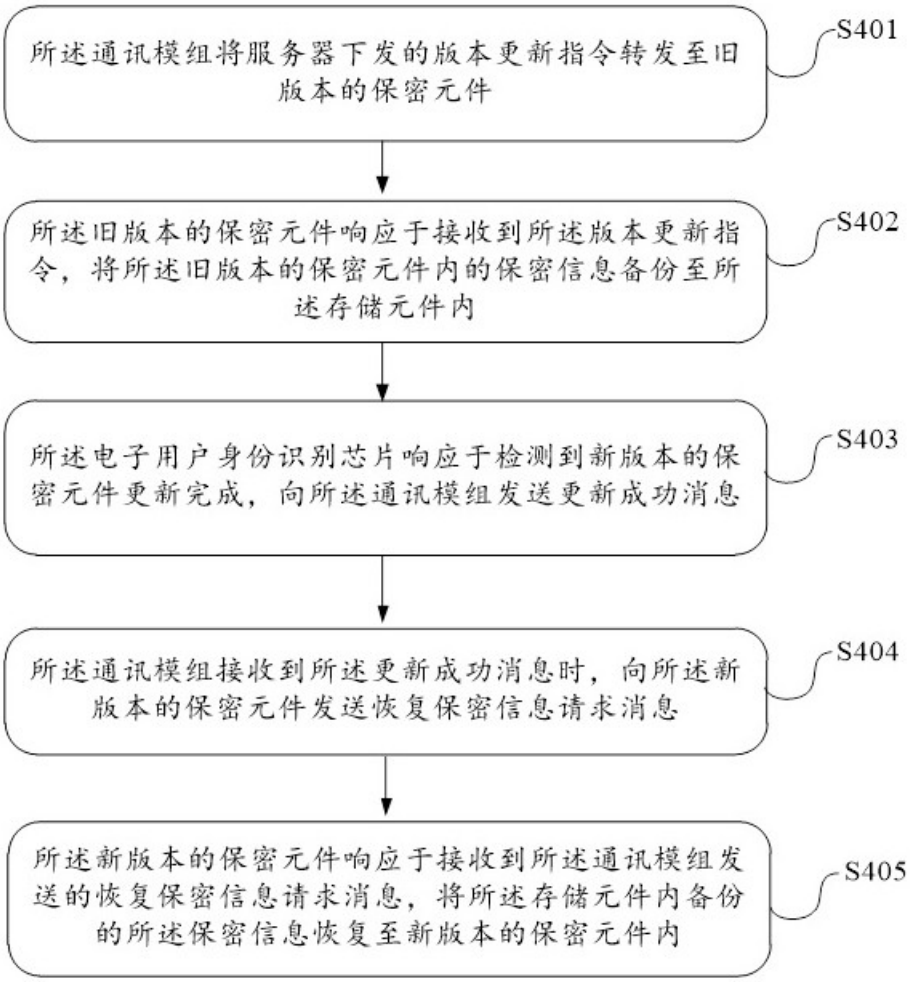

所述通讯模组将服务器下发的版本更新指令转发至旧版本的保密元件
S401
所述旧版本的保密元件响应于接收到所述版本更新指令，将所述旧版本的保密元件内的保密信息备份至所述存储元件内
S402
所述电子用户身份识别芯片响应于检测到新版本的保密元件更新完成，向所述通讯模组发送更新成功消息
S403
所述通讯模组接收到所述更新成功消息时，向所述新版本的保密元件发送恢复保密信息请求消息
S404
所述新版本的保密元件响应于接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内
S405

图4

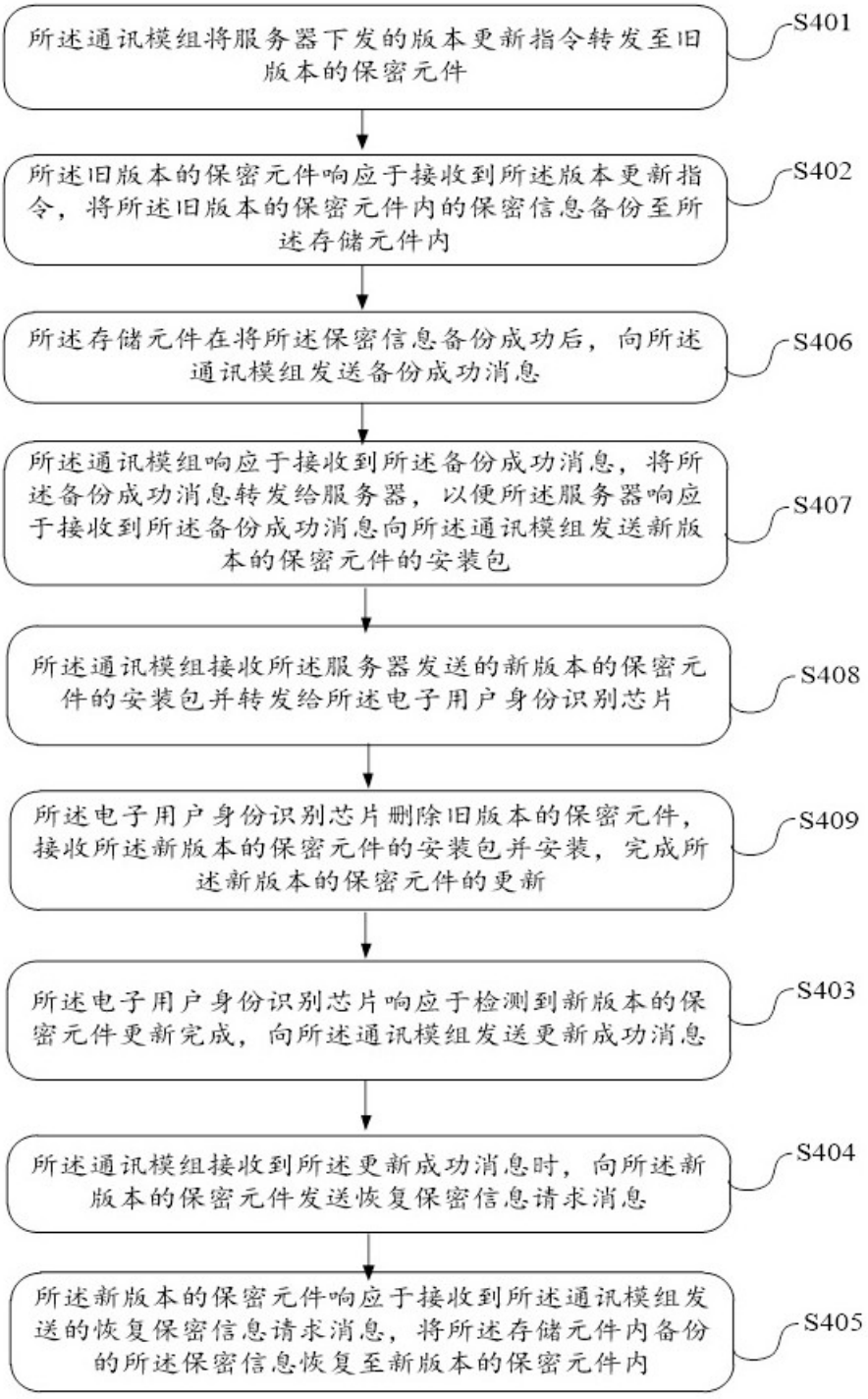

所述通讯模组将服务器下发的版本更新指令转发至旧版本的保密元件
S401
所述旧版本的保密元件响应于接收到所述版本更新指令，将所述旧版本的保密元件内的保密信息备份至所述存储元件内
S402
所述存储元件在将所述保密信息备份成功后，向所述通讯模组发送备份成功消息
S406
所述通讯模组响应于接收到所述备份成功消息，将所述备份成功消息转发给服务器，以便所述服务器响应于接收到所述备份成功消息向所述通讯模组发送新版本的保密元件的安装包
S407
所述通讯模组接收所述服务器发送的新版本的保密元件的安装包并转发给所述电子用户身份识别芯片
S408
所述电子用户身份识别芯片删除旧版本的保密元件，接收所述新版本的保密元件的安装包并安装，完成所述新版本的保密元件的更新
S409
所述电子用户身份识别芯片响应于检测到新版本的保密元件更新完成，向所述通讯模组发送更新成功消息
S403
所述通讯模组接收到所述更新成功消息时，向所述新版本的保密元件发送恢复保密信息请求消息
S404
所述新版本的保密元件响应于接收到所述通讯模组发送的恢复保密信息请求消息，将所述存储元件内备份的所述保密信息恢复至新版本的保密元件内
S405

图5

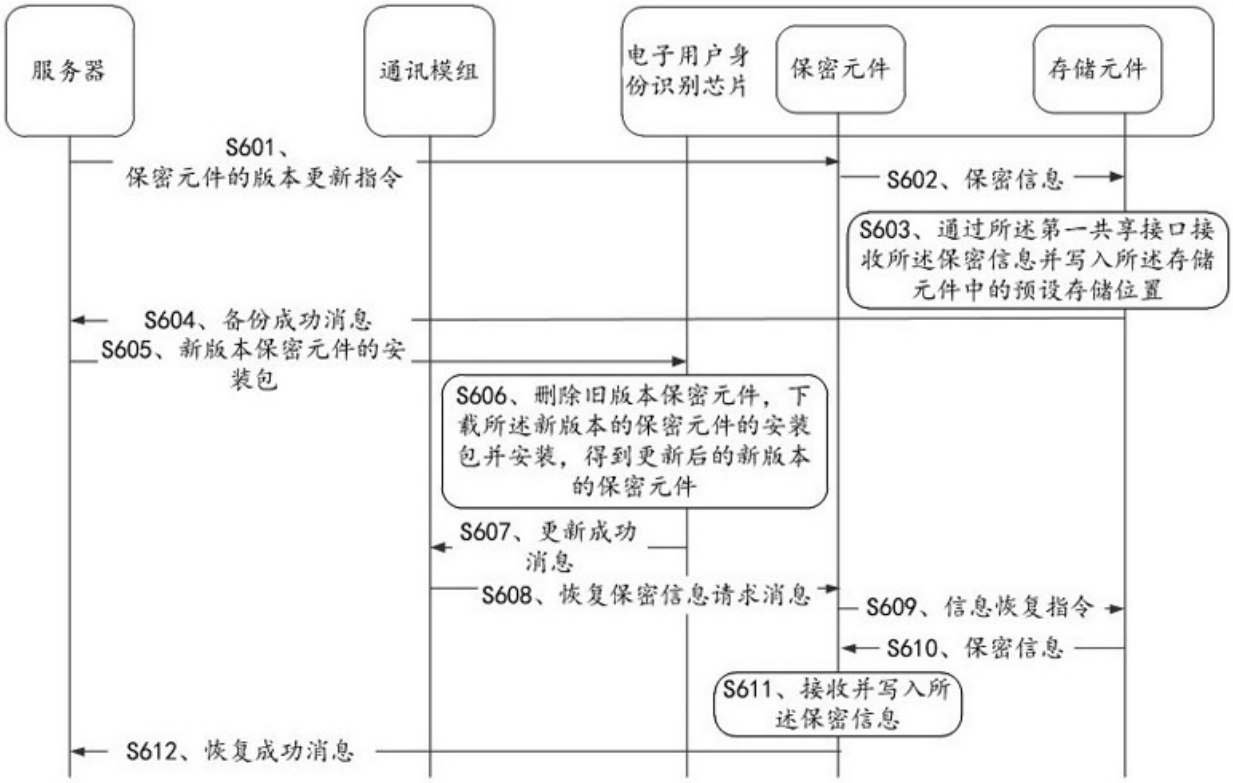

服务器
通讯模组
电子用户身份识别芯片
保密元件
存储元件
S601、保密元件的版本更新指令
S602、保密信息
S603、通过所述第一共享接口接收所述保密信息并写入所述存储元件中的预设存储位置
S604、备份成功消息
S605、新版本保密元件的安装包
S606、删除旧版本保密元件，下载所述新版本的保密元件的安装包并安装，得到更新后的新版本的保密元件
S607、更新成功消息
S608、恢复保密信息请求消息
S609、信息恢复指令
S610、保密信息
S611、接收并写入所述保密信息
S612、恢复成功消息

图6

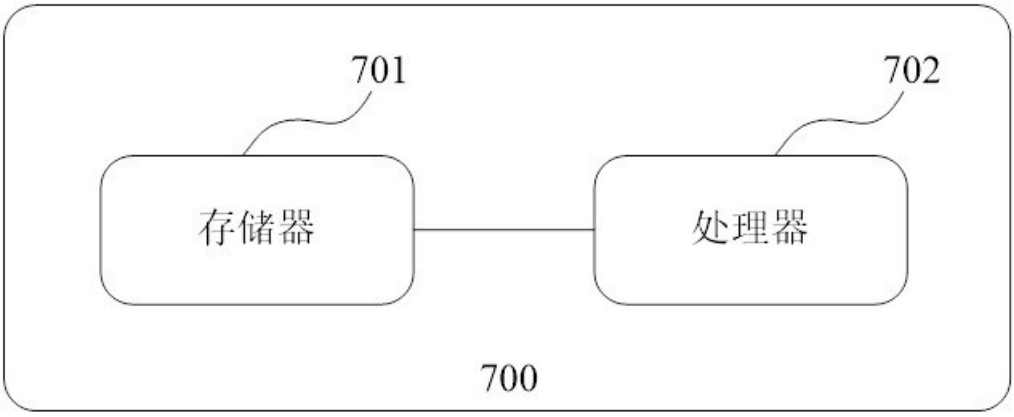

701
702
存储器
处理器
700

图7

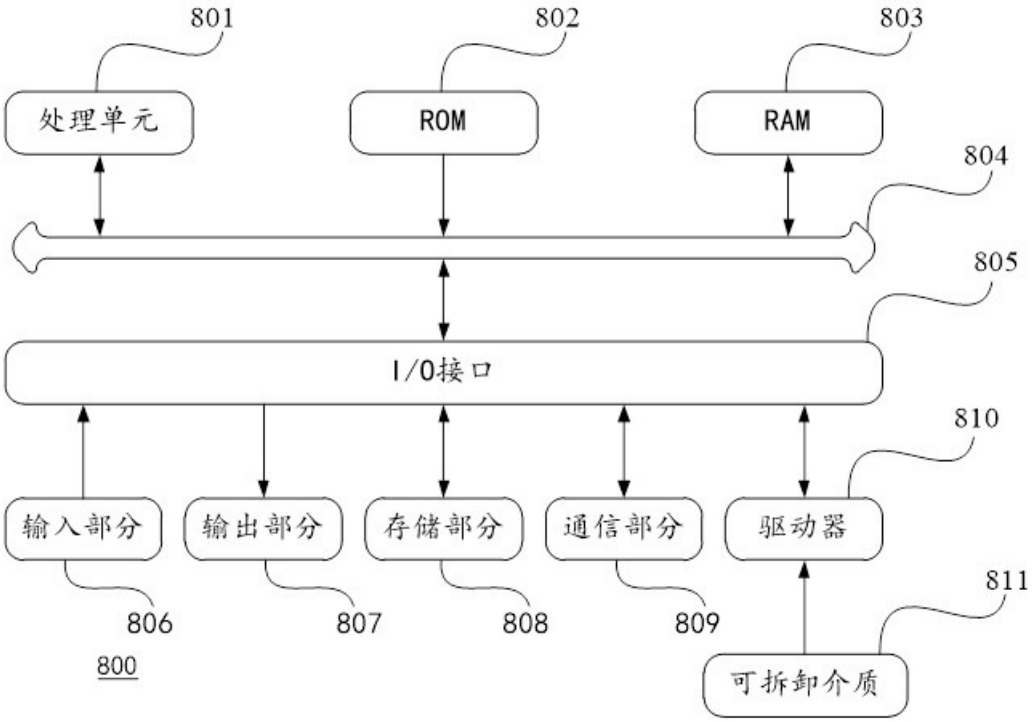

801
802
803
处理单元
ROM
RAM
804
805
I/O接口
810
输入部分
输出部分
存储部分
通信部分
驱动器
806
807
808
809
811
800
可拆卸介质

图8