(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117319085 A
(43)申请公布日 2023.12.29

(21)申请号 202311594824.1

(22)申请日 2023.11.28

(71)申请人 深圳市蓝鲸智联科技股份有限公司
地址 518102 广东省深圳市宝安区西乡街道南昌社区航城大道华丰国际机器人产业园C栋七层

(72)发明人 秦保勇 陈浪 甘茂煌

(74)专利代理机构 重庆莫斯专利代理事务所(普通合伙) 50279
专利代理师 王升兰

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)

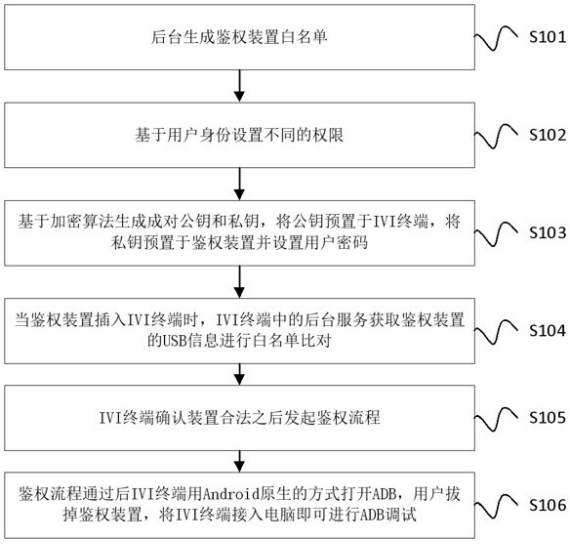
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种开启车载信息娱乐系统ADB的方法及鉴权装置

(57)摘要

本发明涉及汽车电子产品技术领域,具体涉及一种开启车载信息娱乐系统ADB的方法及鉴权装置,包括:后台生成鉴权装置白名单;基于用户身份设置不同的权限;基于加密算法生成成对公钥和私钥,将公钥预置于IVI终端,将私钥预置于鉴权装置并设置用户密码;当鉴权装置插入IVI终端时,IVI终端中的后台服务获取鉴权装置的USB信息进行白名单比对;IVI终端确认装置合法之后发起鉴权流程;鉴权流程通过后IVI终端用Android原生的方式打开ADB,用户拔掉鉴权装置,将IVI终端接入电脑即可进行ADB调试,从而通过增加鉴权装置以进行身份识别,然后配合加密方法以进行双重认证,在方便对不同的用户匹配不同的访问权限的同时,提高了安全性。



CN 117319085 A

1.一种开启车载信息娱乐系统ADB的方法,其特征在于,

包括:后台生成鉴权装置白名单;

基于用户身份设置不同的权限;

基于加密算法生成成对公钥和私钥,将公钥预置于IVI终端,将私钥预置于鉴权装置并设置用户密码;

当鉴权装置插入IVI终端时,IVI终端中的后台服务获取鉴权装置的USB信息进行白名单比对;

IVI终端确认装置合法之后发起鉴权流程;

鉴权流程通过后IVI终端用Android原生的方式打开ADB,用户拔掉鉴权装置,将IVI终端接入电脑即可进行ADB调试。

2.如权利要求1所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

所述基于用户身份设置不同的权限的具体步骤包括:

获取ADB中的权限信息;

基于权限信息和用户身份生成不同的访问权限;

将访问权限写入鉴权装置中。

3.如权利要求2所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

所述加密算法包括RSA、DSA、ECC。

4.如权利要求3所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

所述设置用户密码的具体方式包括采用数字密码或者生物密码的形式来设置密码,生物密码需在鉴权装置上设置采集模块。

5.如权利要求4所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

所述USB信息包括vid、pid、接口类型和版本号。

6.如权利要求5所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

所述IVI终端确认装置合法之后发起鉴权流程的具体步骤包括:

IVI终端弹出对话框提示输入用户密码;

IVI终端选择与装置RSA私钥匹配的RSA公钥加密用户密码和一个随机字符串,将密文通过USB endpoint传输给鉴权装置;

鉴权装置用RSA私钥解密得到密码和随机字符串的明文,将解密后的用户密码与装置内保存的密码进行比对;

如果密码不匹配则鉴权失败,如果密码匹配,鉴权装置将随机字符串用RSA私钥加密后回传给IVI终端;IVI终端将鉴权装置返回的密文用RSA公钥解密得到明文,将明文与步骤B生成的随机字符串比较,如果字符串相同则整个鉴权成功,反之认为鉴权失败。

7.如权利要求6所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

在IVI终端接入电脑即可进行ADB调试完成后,IVI终端如果重启则默认关闭ADB。

8.一种开启车载信息娱乐系统ADB的鉴权装置,应用于权利要求1~7任意一项所述的一种开启车载信息娱乐系统ADB的方法,其特征在于,

包括:外壳、加密模块、接口模块和固件保护模块,所述加密模块设置在所述外壳内,所述接口模块与所述加密模块连接,所述固件保护模块设置在所述外壳内。

9.如权利要求8所述的一种开启车载信息娱乐系统ADB的鉴权装置,其特征在于,

所述开启车载信息娱乐系统ADB的鉴权装置还包括定位模块,所述定位模块用于对装置进行定位并在条件达成时撤销权限。

10.如权利要求9所述的一种开启车载信息娱乐系统ADB的鉴权装置,其特征在于,

所述开启车载信息娱乐系统ADB的鉴权装置还包括生物识别模块,所述生物识别模块与所述加密模块连接,用于获取用户的生物信息进行身份认证。

一种开启车载信息娱乐系统ADB的方法及鉴权装置

技术领域

[0001] 本发明涉及汽车电子产品技术领域,尤其涉及一种开启车载信息娱乐系统ADB的方法及鉴权装置。

背景技术

[0002] 随着技术发展,越来越多的车载信息娱乐终端(后文简称IVI终端)使用了Android操作系统。出于安全考虑,IVI终端的ADB(ADB是Android Debug Bridge,是一个客户端-服务器端程序,用于调试桥的作用。它是Android SDK中的一个工具,可以直接操作管理Android模拟器或者真实的Android设备)默认是不会对用户开放的,所以Android原生的从开发者选项里打开ADB的方式会被移除。但IVI终端在生产、测试以及售后问题排查时,研发及售后人员不可避免地要用到ADB。

[0003] 我国专利CN113961931A 公开了一种adb工具使用方法、装置和电子设备。该方法包括:通信连接终端将用户输入的明文信息加密为密文信息,并将密文信息传输至移动终端。在移动终端上,基于接收到的密文信息,配置adb工具待开启的目标使用权限。移动终端的操作系统基于目标使用权限的配置信息,确定adb工具的目标使用权限是否满足开启要求,并且在adb工具的目标使用权限满足开启要求的前提下,开启adb工具的目标使用权限。

[0004] 该发明缺少对连接终端的合法性检查,使得安全性较低。

发明内容

[0005] 本发明的目的在于提供一种开启车载信息娱乐系统ADB的方法及鉴权装置,旨在可以通过增加鉴权装置以进行身份识别,然后配合加密方法以进行双重认证,在方便对不同的用户匹配不同的访问权限的同时,提高了安全性。

[0006] 为实现上述目的,第一方面,本发明提供了一种开启车载信息娱乐系统ADB的方法,包括后台生成鉴权装置白名单;

基于用户身份设置不同的权限;

基于加密算法生成成对公钥和私钥,将公钥预置于IVI终端,将私钥预置于鉴权装置并设置用户密码;

当鉴权装置插入IVI终端时,IVI终端中的后台服务获取鉴权装置的USB信息进行白名单比对;

IVI终端确认装置合法之后发起鉴权流程;

鉴权流程通过后IVI终端用Android原生的方式打开ADB,用户拔掉鉴权装置,将IVI终端接入电脑即可进行ADB调试。

[0007] 其中,所述基于用户身份设置不同的权限的具体步骤包括:

获取ADB中的权限信息;

基于权限信息和用户身份生成不同的访问权限;

将访问权限写入鉴权装置中。

[0008] 其中,所述加密算法包括RSA、DSA、ECC。

[0009] 其中,所述设置用户密码的具体方式包括采用数字密码或者生物密码的形式来设置密码,生物密码需在鉴权装置上设置采集模块。

[0010] 其中,所述USB信息包括vid、pid、接口类型和版本号。

[0011] 其中,所述IVI终端确认装置合法之后发起鉴权流程的具体步骤包括:

IVI终端弹出对话框提示输入用户密码;

IVI终端选择与装置RSA私钥匹配的RSA公钥加密用户密码和一个随机字符串,将密文通过USB endpoint传输给鉴权装置;

鉴权装置用RSA私钥解密得到密码和随机字符串的明文。将解密后的用户密码与装置内保存的密码进行比对;

如果密码不匹配则鉴权失败,如果密码匹配,鉴权装置将随机字符串用RSA私钥加密后回传给IVI终端;IVI终端将鉴权装置返回的密文用RSA公钥解密得到明文,将明文与步骤B生成的随机字符串比较,如果字符串相同则整个鉴权成功,反之认为鉴权失败。

[0012] 其中,在IVI终端接入电脑即可进行ADB调试完成后,IVI终端如果重启则默认关闭ADB。

[0013] 第二方面,本发明还提供一种开启车载信息娱乐系统ADB的鉴权装置,包括:外壳、加密模块、接口模块和固件保护模块,所述加密模块设置在所述外壳内,所述接口模块与所述加密模块连接,所述固件保护模块设置在所述外壳内。

[0014] 其中,所述开启车载信息娱乐系统ADB的鉴权装置还包括定位模块,所述定位模块用于对装置进行定位并在条件达成时撤销权限。

[0015] 其中,所述开启车载信息娱乐系统ADB的鉴权装置还包括生物识别模块,所述生物识别模块与所述加密模块连接,用于获取用户的生物信息进行身份认证。

[0016] 本发明的一种开启车载信息娱乐系统ADB的方法及鉴权装置,包括:后台生成鉴权装置白名单;基于用户身份设置不同的权限;基于加密算法生成成对公钥和私钥,将公钥预置于IVI终端,将私钥预置于鉴权装置并设置用户密码;

当鉴权装置插入IVI终端时,IVI终端中的后台服务获取鉴权装置的USB信息进行白名单比对;IVI终端确认装置合法之后发起鉴权流程;鉴权流程通过后IVI终端用Android原生的方式打开ADB,用户拔掉鉴权装置,将IVI终端接入电脑即可进行ADB调试,从而通过增加鉴权装置以进行身份识别,然后配合加密方法以进行双重认证,在方便对不同的用户匹配不同的访问权限的同时,提高了安全性。

附图说明

[0017] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例或现有技术描述中所需要使用的附图作简单的介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0018] 图1是本发明的第一实施例的一种开启车载信息娱乐系统ADB的方法的流程图。

[0019] 图2是本发明的第一实施例的基于用户身份设置不同的权限的流程图。

[0020] 图3是本发明的第一实施例的终端确认装置合法之后发起鉴权流程的流程图。

[0021] 图4是本发明的第二实施例的一种开启车载信息娱乐系统ADB的鉴权装置的结构图。

[0022] 图5是本发明的第二实施例的定位模块的结构图。

[0023] 外壳201、加密模块202、接口模块203、固件保护模块204、定位模块205、定位单元206、预警触发单元207、报警单元208、生物识别模块209、上传模块210。

具体实施方式

[0024] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0025] 第一实施例

请参阅图1~图3,图1是本发明的第一实施例的一种开启车载信息娱乐系统ADB的方法的流程图。图2是本发明的第一实施例的基于用户身份设置不同的权限的流程图。图3是本发明的第一实施例的终端确认装置合法之后发起鉴权流程的流程图。

[0026] 本发明提供一种开启车载信息娱乐系统ADB的方法,包括:

S101后台生成鉴权装置白名单;

通过生成白名单可以方便批量登记鉴权装置。

[0027] S102基于用户身份设置不同的权限;

可以针对不同的用户群体(比如研发工程师、工厂生产人员、售后人员等)签发不同的鉴权装置,IVI终端针对不同的用户开启不同的权限,具体步骤包括:

S201获取ADB中的权限信息;

首先获取ADB中可以开放连接的所有权限信息。

[0028] S202基于权限信息和用户身份生成不同的访问权限;

然后可以将这些获取到的权限信息和用户的身份进行绑定,从而可以生成不同的访问权限。

[0029] S203将访问权限写入鉴权装置中。

[0030] 最终将访问权限写入到鉴权装置中,可以根据用户的身份定制相应的鉴权装置。

[0031] S103基于加密算法生成成对公钥和私钥,将公钥预置于IVI终端,将私钥预置于鉴权装置并设置用户密码;

所述加密算法包括RSA、DSA、ECC。RSA、DSA和ECC都是非对称加密算法,这是由于它们都需要两个密钥:公钥和私钥。这两个密钥是配对的,如果用公钥对数据进行加密,那么只有对应的私钥才能解密;反之,如果用私钥对数据进行加密,则只能用对应的公钥进行解密。

[0032] RSA是一种非常著名的非对称加密算法,其安全性主要基于大数分解的困难性。在实际应用中,RSA广泛应用于数字签名、加密通信等场景。

[0033] DSA是一种标准的非对称加密算法,主要用于数字签名和验证。与RSA不同,它并不适用于大规模的数据加密。

[0034] ECC是一种新兴的非对称加密算法。相比于RSA,ECC在安全性能上具有明显的优势。比如,在相同密钥长度下,160位的ECC与1024位的RSA或DSA具有相同的安全强度。此外,

ECC的计算量小,处理速度快,特别是在私钥的处理速度上,ECC比RSA和DSA都快。因此,ECC已经在许多领域得到了广泛的应用。

[0035] 设置用户密码的具体方式包括采用数字密码或者生物密码的形式来设置密码,生物密码需在鉴权装置上设置采集模块。

[0036] S104当鉴权装置插入IVI终端时,IVI终端中的后台服务获取鉴权装置的USB信息进行白名单比对;

所述USB信息包括vid、pid、接口类型和版本号。通过采用上述信息进行比对后以确定其合法性,从而完成身份认证。

[0037] S105IVI终端确认装置合法之后发起鉴权流程;

具体步骤包括:

S301IVI终端弹出对话框提示输入用户密码;

S302IVI终端选择与装置RSA私钥匹配的RSA公钥加密用户密码和一个随机字符串,将密文通过USB endpoint传输给鉴权装置;

S303鉴权装置用RSA私钥解密得到密码和随机字符串的明文。将解密后的用户密码与装置内保存的密码进行比对;

S304如果密码不匹配则鉴权失败,如果密码匹配,鉴权装置将随机字符串用RSA私钥加密后回传给IVI终端;IVI终端将鉴权装置返回的密文用RSA公钥解密得到明文,将明文与步骤B生成的随机字符串比较,如果字符串相同则整个鉴权成功,反之认为鉴权失败。

[0038] 通过上述方式可以进行加密算法的鉴权。

[0039] S106鉴权流程通过后IVI终端用Android原生的方式打开ADB,用户拔掉鉴权装置,将IVI终端接入电脑即可进行ADB调试。

[0040] 在IVI终端接入电脑即可进行ADB调试完成后,IVI终端如果重启则默认关闭ADB,以提高操作的安全性。

[0041] 本发明的一种开启车载信息娱乐系统ADB的方法,通过增加鉴权装置以进行身份识别,然后配合加密方法以进行双重认证,在方便对不同的用户匹配不同的访问权限的同时,提高了安全性。

[0042] 第二实施例

请参阅图4~图5,图4是本发明的第二实施例的一种开启车载信息娱乐系统ADB的鉴权装置的结构图。图5是本发明的第二实施例的定位模块的结构图。在第一实施例的基础上,本发明还提供一种开启车载信息娱乐系统ADB的鉴权装置,包括:外壳201、加密模块202、接口模块203和固件保护模块204,所述加密模块202设置在所述外壳201内,所述接口模块203与所述加密模块202连接,所述固件保护模块204设置在所述外壳201内。

[0043] 在本实施方式中,通过所述外壳201进行保护,在所述外壳201内设置有加密模块202,用于写入相关的私钥信息,然后通过所述接口模块203可以和外界设备进行对接,所述固件保护模块204具有防拆卸功能,设置在所述外壳201内,以提高设备的安全性能。

[0044] 所述开启车载信息娱乐系统ADB的鉴权装置还包括定位模块205,所述定位模块205用于对装置进行定位并在条件达成时撤销权限。为了进一步提高装置的安全性能,本申请通过所述定位模块205可以对装置的位置进行定位,以使得当检测到装置定位异常时撤销对该装置的白名单授权,提高安全性能。

[0045] 所述定位模块205包括定位单元206、预警触发单元207和报警单元208,所述定位单元206用于对装置的地理位置进行定位,所述预警触发单元207,用于对地理位置的合法性进行匹配,所述报警单元208,用于当地理位置非法时发送报警信号并从白名单中撤销装置授权。通过所述定位单元206可以采用GPS等方式进行定位,然后通过所述预警触发单元207以对地理位置的合法性进行匹配检测,具体方式是可以限定区域检测,或者是与移动终端的位置进行绑定,当超出移动终端预设距离后则处于报警区域,所述报警单元208,用于当装置持续处于报警区域一定时间后,则发送警报和撤销授权,以提高安全性。

[0046] 所述开启车载信息娱乐系统ADB的鉴权装置还包括生物识别模块209,所述生物识别模块209与所述加密模块202连接,用于获取用户的生物信息进行身份认证。所述生物识别模块209用于可以采集人体的生物信息进行授权,使得使用更加方便。

[0047] 所述开启车载信息娱乐系统ADB的鉴权装置还包括上传模块210,所述上传模块210用于上传调试数据。所述上传模块210可以将调试产生的数据上传,使得使用更加方便。

[0048] 以上所揭露的仅为本发明一种较佳实施例而已,当然不能以此来限定本发明之权利范围,本领域普通技术人员可以理解实现上述实施例的全部或部分流程,并依本发明权利要求所作的等同变化,仍属于发明所涵盖的范围。

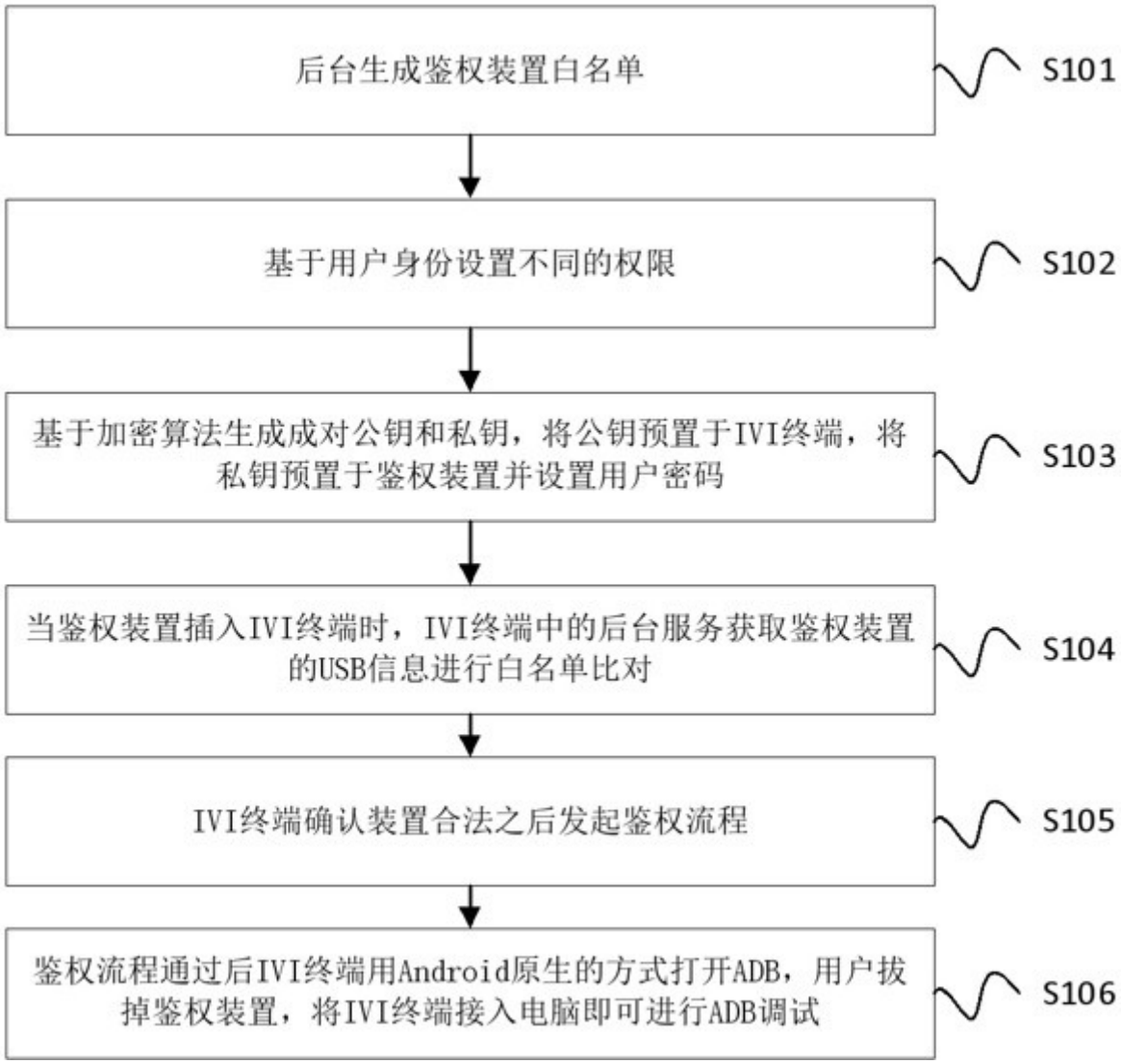

后台生成鉴权装置白名单
S101
基于用户身份设置不同的权限
S102
基于加密算法生成成对公钥和私钥，将公钥预置于IVI终端，将私钥预置于鉴权装置并设置用户密码
S103
当鉴权装置插入IVI终端时，IVI终端中的后台服务获取鉴权装置的USB信息进行白名单比对
S104
IVI终端确认装置合法之后发起鉴权流程
S105
鉴权流程通过后IVI终端用Android原生的方式打开ADB，用户拔掉鉴权装置，将IVI终端接入电脑即可进行ADB调试
S106

图1

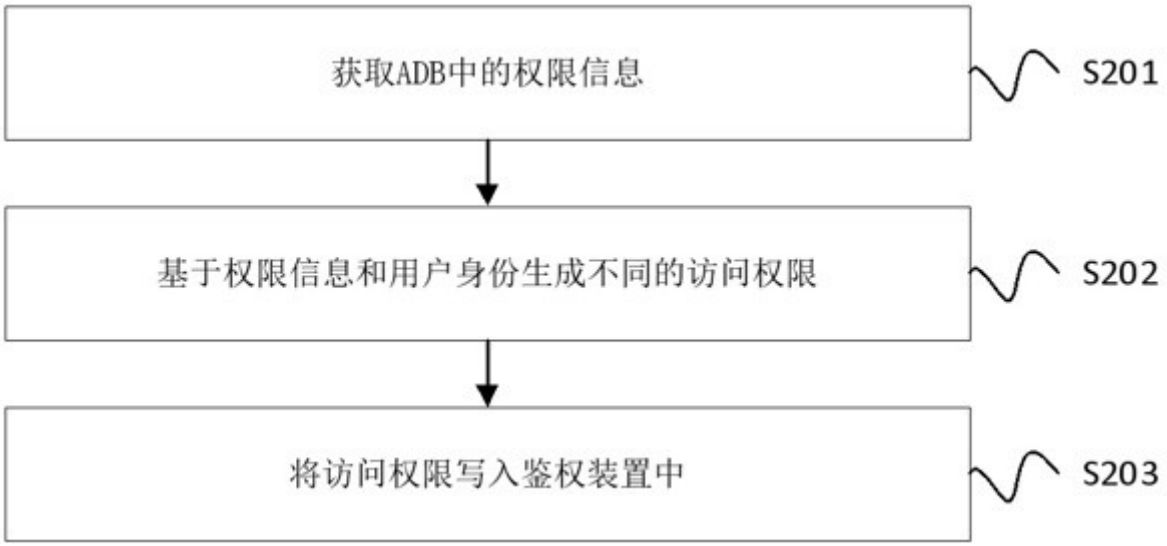

获取ADB中的权限信息
S201
基于权限信息和用户身份生成不同的访问权限
S202
将访问权限写入鉴权装置中
S203

图2

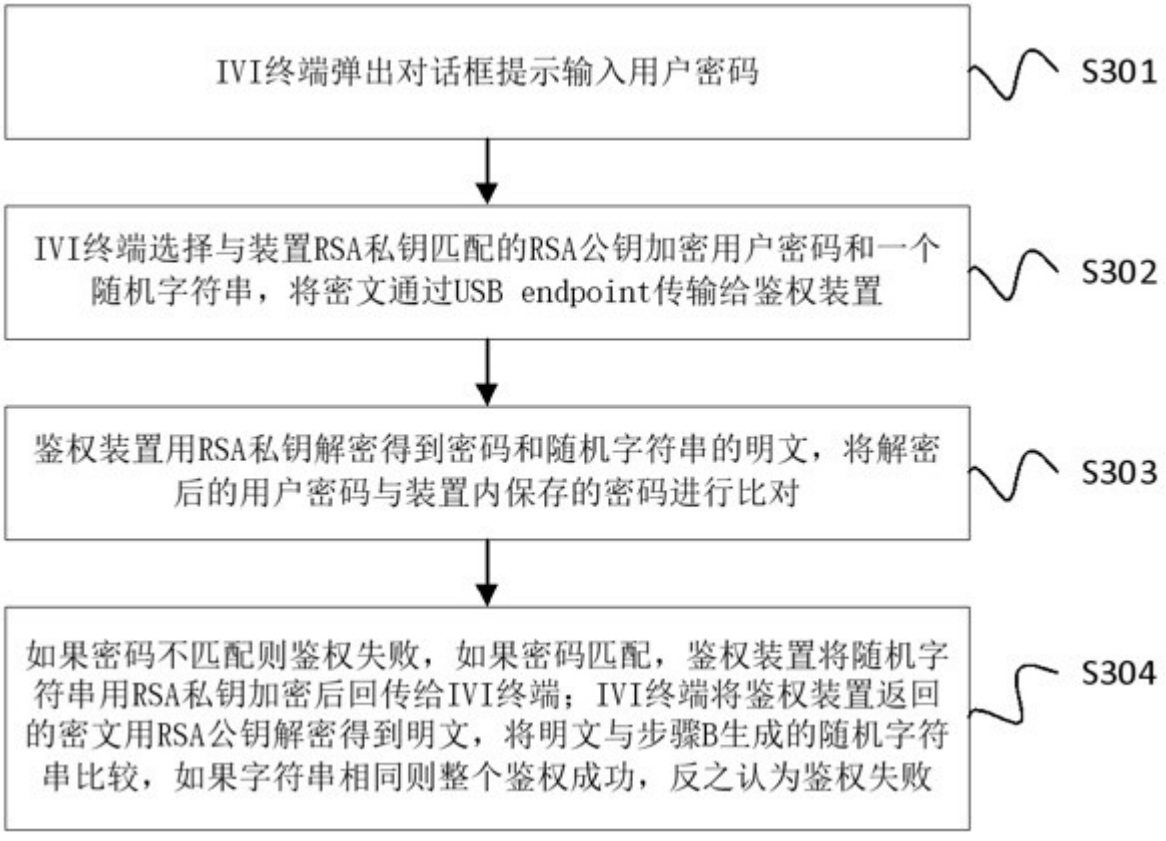

IVI终端弹出对话框提示输入用户密码
S301
IVI终端选择与装置RSA私钥匹配的RSA公钥加密用户密码和一个随机字符串，将密文通过USB endpoint传输给鉴权装置
S302
鉴权装置用RSA私钥解密得到密码和随机字符串的明文，将解密后的用户密码与装置内保存的密码进行比对
S303
如果密码不匹配则鉴权失败，如果密码匹配，鉴权装置将随机字符串用RSA私钥加密后回传给IVI终端；IVI终端将鉴权装置返回的密文用RSA公钥解密得到明文，将明文与步骤B生成的随机字符串比较，如果字符串相同则整个鉴权成功，反之认为鉴权失败
S304

图3

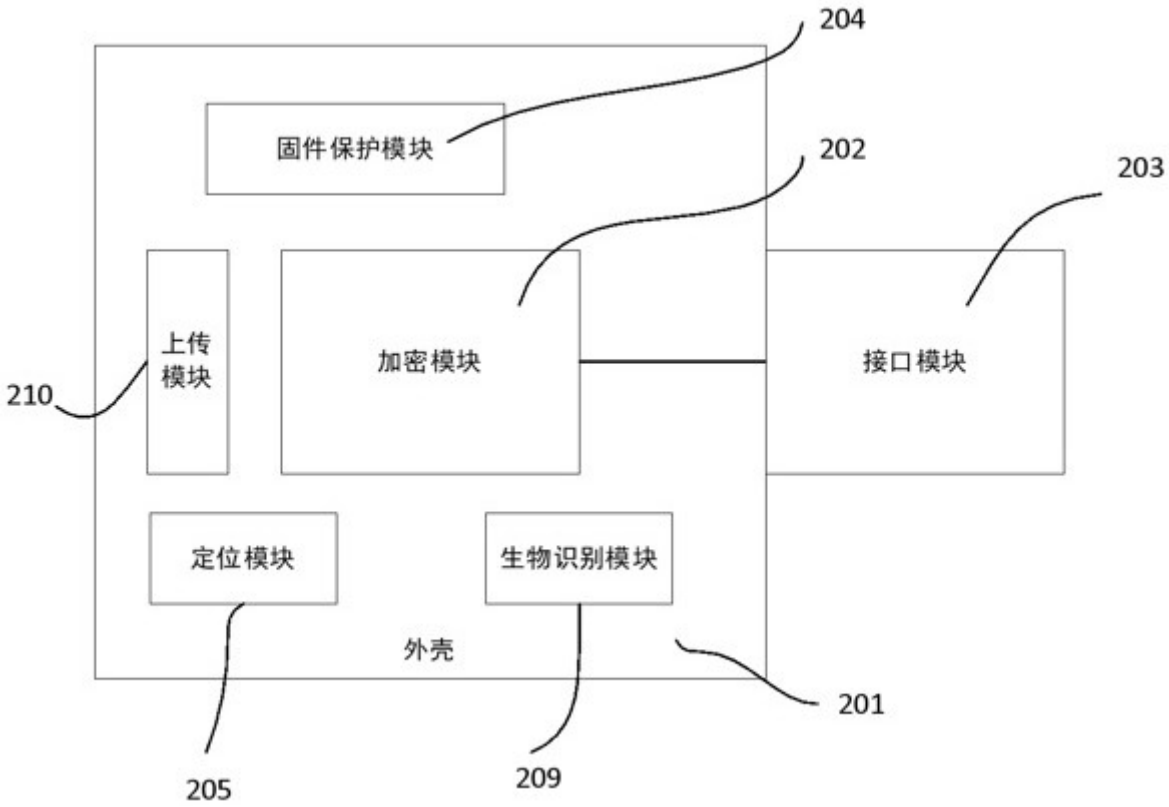

204
固件保护模块
202
203
上传模块
210
加密模块
接口模块
定位模块
生物识别模块
外壳
201
205
209

图4

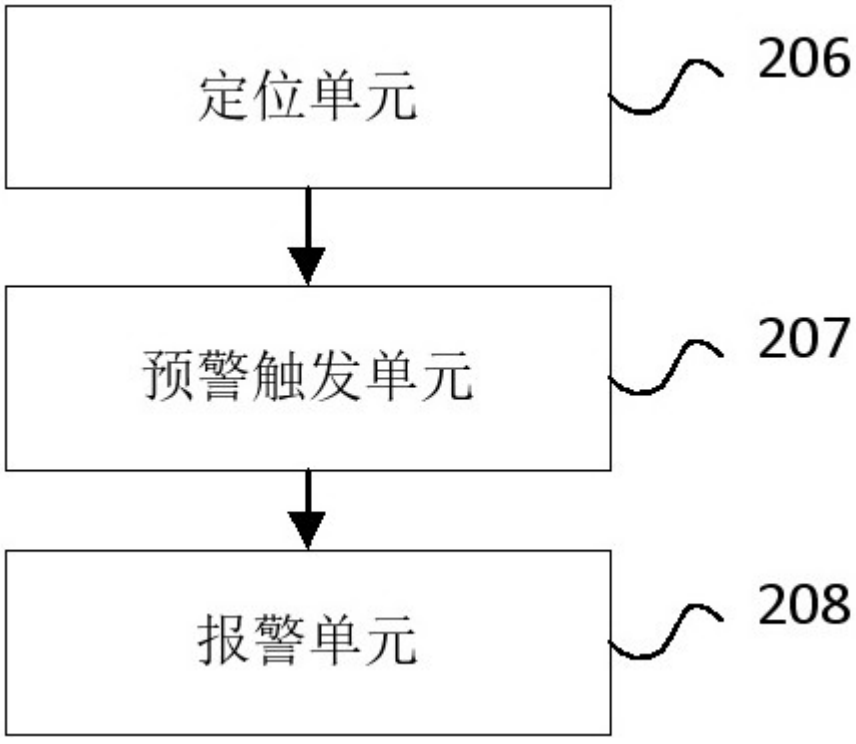

定位单元
206
预警触发单元
207
报警单元
208

图5