(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113496019 B
(45)授权公告日 2021.11.30

(21)申请号 202111046471.2
(22)申请日 2021.09.08
(65)同一申请的已公布的文献号
申请公布号 CN 113496019 A
(43)申请公布日 2021.10.12
(73)专利权人 环球数科集团有限公司
地址 518063 广东省深圳市南山区粤海街道高新南九道10号深圳湾科技生态园10栋B座17层01-03号
(72)发明人 张卫平 丁烨 张浩宇
(74)专利代理机构 北京清控智云知识产权代理事务所(特殊普通合伙) 11919
代理人 马肃
(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/45(2013.01)
G06F 21/14(2013.01)
(56)对比文件
CN 103106555 A,2013.05.15
CN 110378087 A,2019.10.25
CN 111314346 A,2020.06.19
JP 2014167675 A,2014.09.11
CN 107896237 A,2018.04.10
审查员 简文雨

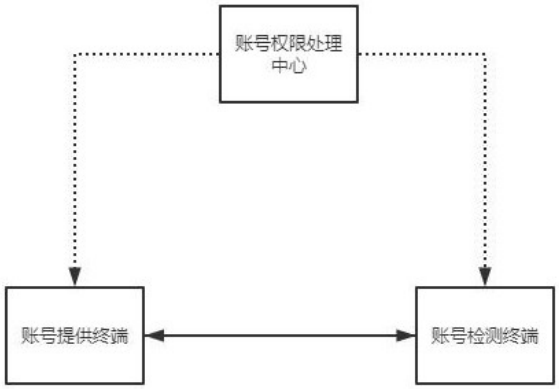
权利要求书2页 说明书7页 附图3页

(54)发明名称

一种兼容在线离线的账号权限控制系统

(57)摘要

本发明提供了一种兼容在线离线的账号权限控制系统，其特征在于，包括账号权限处理中心，账号检测终端和账号提供终端，所述账号检测终端与所述账号提供终端通过短距通讯连接，所述账号检测终端检测所述账号提供终端的账号权限来开放相应的功能，所述账号提供终端和所述账号检测终端包括代码处理器，所述代码生成器由所述账号权限处理中心赋予并在离线状态时进行权限确认。本系统在离线状态时也能对账号的权限进行高安全性和防伪性的确认，尤其在一些信号较差的地区或天气环境下能够确保业务的正常进行。



CN 113496019 B

1.一种兼容在线离线的账号权限控制系统,其特征在于,包括账号权限处理中心,账号检测终端和账号提供终端,所述账号检测终端与所述账号提供终端通过短距通讯连接,所述账号检测终端检测所述账号提供终端的账号权限来开放相应的功能;

所述账号提供终端包括代码生成器和代码处理器,所述账号检测终端包括代码生成器和代码处理器,所述账号提供终端的代码生成器和所述账号检测终端的代码生成器由所述账号权限处理中心赋予;

当所述账号检测终端与所述账号提供终端均与所述账号权限处理中心处于离线状态时,通过下述步骤进行权限认证:

S1、所述账号提供终端的代码生成器随机生成一段第一代码,并将所述第一代码发送至所述账号检测终端;

S2、所述账号检测终端将所述第一代码与目标权限代码经账号检测终端的代码处理器处理后得到第二代码,并将所述第二代码发送至所述账号提供终端;

S3、所述账号提供终端将账号拥有的所有权限代码分别与第一代码经账号提供终端的代码处理器处理后得到若干伪第二代码,并与所述第二代码对比确定目标权限代码;

S4、所述账号提供终端将所述目标权限代码与所述第二代码经账号提供终端的代码处理器处理后得到第三代码,并将所述第三代码与目标权限代码发送至所述账号检测终端;

S5、所述账号检测终端将目标权限代码与第二代码经账号检测终端的代码处理器处理后得到第三代码,并对接收到的目标权限代码与第三代码进行核对,核对无误后对所述账号提供终端开放相应的功能;

所述账号提供终端的代码处理器和所述账号检测终端的代码处理器的处理公式为:

$$C(i)=q\left((A(i)+2)^{(B(i)+2)}\div\sqrt{A(i)+B(i)+2},\ j\right);$$

其中,A、B表示代码处理器的两个输入代码,C表示代码处理器的输出代码,A(i)、B(i)和C(i)表示代码的第i个字符对应的值,函数q(a,j)表示取a的第j位小数位的值;

当所述账号检测终端和所述账号提供终端至少有一个终端与所述账号权限处理中心处于在线状态时,所述账号检测终端对从所述账号权限处理中心获取的账号权限进行确认并判断是否开放相应的功能。

2.如权利要求1所述的一种兼容在线离线的账号权限控制系统,其特征在于,所述账号提供终端包括防伪标记的生成器,所述账号权限处理中心包括防伪标记的解析器,当所述账号提供终端与所述账号权限处理中心处于离线状态,所述账号检测终端与所述账号权限处理中心处于在线状态时,所述账号检测终端从所述账号提供终端处获得所述防伪标记并上传至所述账号权限处理中心,所述账号权限处理中心解析无误后将对应账号的权限信息发送至所述账号检测终端进行权限确认。

3.如权利要求2所述的一种兼容在线离线的账号权限控制系统,其特征在于,所述账号权限处理中心和所述账号检测终端拥有一个相同的密钥,当所述账号提供终端与所述账号权限处理中心处于在线状态,所述账号检测终端与所述账号权限处理中心处于离线状态时,所述账号权限处理中心将对应账号的权限用密钥进行加密打包成权限包发送给所述账号提供终端,所述账号提供终端将所述权限包转发至所述账号检测终端,所述账号检测终端对所述权限包用密钥解密后对其中的权限进行确认。

4.如权利要求3所述的一种兼容在线离线的账号权限控制系统,其特征在于,所述账号提供终端与账号检测终端均设有连线状态检测器用于检测当前的状态,所述终端通过接收对方的连线状态并结合自身的连线状态选择对应的一种模式来进行权限确认。

5.如权利要求4所述的一种兼容在线离线的账号权限控制系统,其特征在于,所述代码处理器处理的代码采用16进制字符,代码处理器中的计算结果采用16进制进行结算。

一种兼容在线离线的账号权限控制系统

技术领域

[0001] 本发明涉及账号管理技术领域，尤其涉及一种兼容在线离线的账号权限控制系统。

背景技术

[0002] 在当前的业务处理过程中，不同的账号拥有不同的权限，能够进行相应的业务处理，在良好的网络环境下，对账号的权限确认快捷而可靠，但当网络环境不佳时，账号的权限确认会出现较大的安全漏洞，容易被不法分子钻漏洞从而造成较大的损失。本发明主要针对离线状态时如何提高安全性作出改进。

[0003] 现在已经开发出了很多权限控制系统，经过我们大量的检索与参考，发现现有的权限控制系统有如公开号为KR100727085B1，KR101026607B1、CN106709319B和KR101453826B1所公开的系统，方法包括：获取二维码信息，对所述二维码信息进行识别，得到加密数据和数据权限分配表；获取用户权限，查找数据权限分配表，得到所述加密数据中所述用户权限授权的加密数据；对所述目标加密数据进行解密，得到解密后的目标数据。装置包括：二维码识别模块、数据获取模块和数据解密模块。通过对二维码信息识别并获取数据权限分配表和目标加密数据，不仅能在本地对二维码进行解码，而且能够在本地获取数据权限分配表。但该系统在离线状态时能够通过仿造账号及权限来使用相应的功能，安全性不够高。

发明内容

[0004] 本发明的目的在于，针对所存在的不足，提出了一种兼容在线离线的账号权限控制系统，

[0005] 本发明采用如下技术方案：

[0006] 一种兼容在线离线的账号权限控制系统，包括账号权限处理中心，账号检测终端和账号提供终端，所述账号检测终端与所述账号提供终端通过短距通讯连接，所述账号检测终端检测所述账号提供终端的账号权限来开放相应的功能；

[0007] 所述账号提供终端包括代码生成器和代码处理器，所述账号检测终端包括代码生成器，所述代码生成器由所述账号权限处理中心赋予；

[0008] 当所述账号检测终端与所述账号提供终端均与所述账号权限处理中心处于离线状态时，通过下述步骤进行权限认证：

[0009] S1、所述账号提供终端的所述代码生成器随机生成一段第一代码，并将所述第一代码发送至所述账号检测终端；

[0010] S2、所述账号检测终端将所述第一代码与目标权限代码经所述代码处理器处理后得到第二代码，并将所述第二代码发送至所述账号提供终端；

[0011] S3、所述账号提供终端将账号拥有的所有权限代码分别与第一代码经所述代码处理器处理后得到若干伪第二代码，并与所述第二代码对比确定目标权限代码；

[0012] S4、所述账号提供终端将所述目标权限代码与所述第二代码经所述代码处理器处理后得到第三代码，并将所述第三代码与目标权限代码发送至所述账号检测终端；

[0013] S5、所述账号检测终端将目标权限代码与第二代码经所述代码处理器处理后得到第三代码，并对接收到的目标权限代码与第三代码进行核对，核对无误后对所述账号提供终端开放相应的功能；

[0014] 所述代码处理器的处理公式为：

[0015] $$C(i)=q\left((A(i)+2)^{(B(i)+2)}\div\sqrt{A(i)+B(i)+2},\ j\right)$$；

[0016] 其中，A、B表示代码处理器的两个输入代码，C表示代码处理器的输出代码，A(i)、B(i)和C(i)表示代码的第i个字符对应的值，函数q(a,j)表示取a的第j位小数位的值；

[0017] 当所述账号检测终端和所述账号提供终端至少有一个终端与所述账号权限处理中心处于在线状态时，所述账号检测终端对从所述账号权限处理中心获取的账号权限进行确认并判断是否开放相应的功能；

[0018] 进一步的，所述账号提供终端包括防伪标记的生成器，所述账号权限处理中心包括防伪标记的解析器，当所述账号提供终端与所述账号权限处理中心处于离线状态，所述账号检测终端与所述账号权限处理中心处于在线状态时，所述账号检测终端从所述账号提供终端处获得所述防伪标记并上传至所述账号权限处理中心，所述账号权限处理中心解析无误后将对应账号的权限信息发送至所述账号检测终端进行权限确认；

[0019] 进一步的，所述账号权限处理中心和所述账号检测终端拥有一个相同的密钥，当所述账号提供终端与所述账号权限处理中心处于在线状态，所述账号检测终端与所述账号权限处理中心处于离线状态时，所述账号权限处理中心将对应账号的权限用密钥进行加密打包成权限包发送给所述账号提供终端，所述账号提供终端将所述权限包转发至所述账号检测终端，所述账号检测终端对所述权限包用密钥解密后对其中的权限进行确认；

[0020] 进一步的，所述账号提供终端与账号检测终端均设有连线状态检测器用于检测当前的状态，所述终端通过接收对方的连线状态并结合自身的连线状态选择对应的一种模式来进行权限确认；

[0021] 进一步的，所述代码处理器处理的代码采用16进制字符，代码处理器中的计算结果采用16进制进行结算。

[0022] 本发明所取得的有益效果是：

[0023] 本系统采用了四种模式来进行权限确认，在不同的网络环境下使用合适的模式，在保证安全性的前提下提高权限确认的效率，在离线状态时，通过使用代码处理器对权限代码进行处理，提高了安全性，使得假冒者即使获取了正确的账号信息和权限代码信息也无法通过权限确认，本系统中的代码处理器为单向计算处理，无法通过逆向运算来获取权限代码，提高了暴力破解的难度和时间成本。

附图说明

[0024] 从以下结合附图的描述可以进一步理解本发明。图中的部件不一定按比例绘制，而是将重点放在示出实施例的原理上。在不同的视图中，相同的附图标记指定对应的部分。

[0025] 图1为整体结构框架示意图；

[0026] 图2为连线状态一的权限确认框架示意图；

[0027] 图3为连线状态二的权限确认框架示意图；

[0028] 图4为连线状态三的权限确认框架示意图；

[0029] 图5为连线状态四的权限确认流程示意图。

具体实施方式

[0030] 为了使得本发明的目的、技术方案及优点更加清楚明白，以下结合其实施例，对本发明进行进一步详细说明；应当理解，此处所描述的具体实施例仅用于解释本发明，并不用于限定本发明。对于本领域技术人员而言，在查阅以下详细描述之后，本实施例的其它系统、方法和/或特征将变得显而易见。旨在所有此类附加的系统、方法、特征和优点都包括在本说明书内，包括在本发明的范围内，并且受所附权利要求书的保护。在以下详细描述描述了所公开的实施例的另外的特征，并且这些特征根据以下将详细描述将是显而易见的。

[0031] 本发明实施例的附图中相同或相似的标号对应相同或相似的部件；在本发明的描述中，需要理解的是，若有术语“上”、“下”、“左”、“右”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或组件必须具有特定的方位，以特定的方位构造和操作，因此附图中描述位置关系的用语仅用于示例性说明，不能理解为对本专利的限制，对于本领域的普通技术人员而言，可以根据具体情况理解上述术语的具体含义。

[0032] 实施例一。

[0033] 本实施例提供了一种兼容在线离线的账号权限控制系统，结合图1，包括账号权限处理中心，账号检测终端和账号提供终端，所述账号检测终端与所述账号提供终端通过短距通讯连接，所述账号检测终端检测所述账号提供终端的账号权限来开放相应的功能；

[0034] 所述账号提供终端包括代码生成器和代码处理器，所述账号检测终端包括代码生成器，所述代码生成器由所述账号权限处理中心赋予；

[0035] 当所述账号检测终端与所述账号提供终端均与所述账号权限处理中心处于离线状态时，通过下述步骤进行权限认证：

[0036] S1、所述账号提供终端的所述代码生成器随机生成一段第一代码，并将所述第一代码发送至所述账号检测终端；

[0037] S2、所述账号检测终端将所述第一代码与目标权限代码经所述代码处理器处理后得到第二代码，并将所述第二代码发送至所述账号提供终端；

[0038] S3、所述账号提供终端将账号拥有的所有权限代码分别与第一代码经所述代码处理器处理后得到若干伪第二代码，并与所述第二代码对比确定目标权限代码；

[0039] S4、所述账号提供终端将所述目标权限代码与所述第二代码经所述代码处理器处理后得到第三代码，并将所述第三代码与目标权限代码发送至所述账号检测终端；

[0040] S5、所述账号检测终端将目标权限代码与第二代码经所述代码处理器处理后得到第三代码，并对接收到的目标权限代码与第三代码进行核对，核对无误后对所述账号提供终端开放相应的功能；

[0041] 所述代码处理器的处理公式为：

[0042] $C(i)=q\left((A(i)+2)^{(B(i)+2)}\div\sqrt{A(i)+B(i)+2},\ j\right)$；

[0043] 其中，A、B表示代码处理器的两个输入代码，C表示代码处理器的输出代码，A(i)、B(i)和C(i)表示代码的第i个字符对应的值，函数q(a,j)表示取a的第j位小数位的值；

[0044] 当所述账号检测终端和所述账号提供终端至少有一个终端与所述账号权限处理中心处于在线状态时，所述账号检测终端对从所述账号权限处理中心获取的账号权限进行确认并判断是否开放相应的功能；

[0045] 所述账号提供终端包括防伪标记的生成器，所述账号权限处理中心包括防伪标记的解析器，当所述账号提供终端与所述账号权限处理中心处于离线状态，所述账号检测终端与所述账号权限处理中心处于在线状态时，所述账号检测终端从所述账号提供终端处获得所述防伪标记并上传至所述账号权限处理中心，所述账号权限处理中心解析无误后将对应账号的权限信息发送至所述账号检测终端进行权限确认；

[0046] 所述账号权限处理中心和所述账号检测终端拥有一个相同的密钥，当所述账号提供终端与所述账号权限处理中心处于在线状态，所述账号检测终端与所述账号权限处理中心处于离线状态时，所述账号权限处理中心将对应账号的权限用密钥进行加密打包成权限包发送给所述账号提供终端，所述账号提供终端将所述权限包转发至所述账号检测终端，所述账号检测终端对所述权限包用密钥解密后对其中的权限进行确认；

[0047] 所述账号提供终端与账号检测终端均设有连线状态检测器用于检测当前的状态，所述终端通过接收对方的连线状态并结合自身的连线状态选择对应的一种模式来进行权限确认；

[0048] 所述代码处理器处理的代码采用16进制字符，代码处理器中的计算结果采用16进制进行结算。

[0049] 实施例二。

[0050] 本实施例包含了实施例一的全部内容，本实施例提供了一种兼容在线离线的账号权限控制系统，包括账号权限处理中心，账号检测终端和账号提供终端，所述账号权限处理中心与所述账号检测终端能够处于在线或离线状态，所述账号权限处理中心能够与所述账号提供终端处于在线或离线状态，所述账号检测终端与所述账号提供终端能够基于短距通讯基础在近距离范围内处于互联状态，所述账号检测终端能够在所述账号权限处理中心的四种连线状态下对所述账号提供终端的账号进行权限识别，并基于识别到的权限进行下一步操作；

[0051] 连线状态一：全在线状态，所述账号权限处理中心与所述账号检测终端处于在线状态，所述账号权限处理中心与所述账号提供终端处于在线状态；

[0052] 结合图2，所述账号检测终端获取所述账号提供终端的账号信息，所述账号检测终端向所述账号权限处理中心查询对应的账号信息并获取相应的权限信息，所述账号检测终端在所述权限信息中检索目标权限，检索到则开放相应功能，检索不到则向所述账号提供终端反馈无效应答；

[0053] 所述账号提供终端获取所述账号检测终端的物理地址码，所述账号提供终端向所述账号权限处理中心提供所述物理地址码并获得反馈信息；

[0054] 所述账号权限处理中心从所述账号提供终端获得所述账号检测终端的物理地址

码，所述账号权限处理中心接收到所述账号检测终端的查询信息，所述账号权限处理中心对所述账号检测终端的物理地址码进行比对，比对无误后向所述账号检测终端开放对应账号的权限信息，同时向所述账号提供终端返回反馈信息；

[0055] 连线状态二：半在线状态，所述账号权限处理中心与所述账号检测终端处于在线状态，所述账号权限处理中心与所述账号提供终端处于离线状态；

[0056] 结合图3，所述账号检测终端从所述账号提供终端获取到账号信息和防伪标记，所述账号检测终端向所述账号权限处理中心提供防伪标记并查询对应的账号信息，从而获得相应的权限信息，所述账号检测终端在所述权限信息中检索目标权限，检索到则开放相应功能，若防伪标记被所述账号权限处理中心无效化或者检索不到目标权限，则所述账号检测终端向所述账号提供终端反馈无效应答；

[0057] 所述账号权限处理中心接收到所述防伪标记后对所述防伪标记进行解析，解析正确后向所述账号检测终端开放对应账号的权限信息；

[0058] 所述账号提供终端包括防伪标记的生成器，所述生成器基于账号和当前时间段计算得到所述防伪标记，所述账号权限处理中心包括防伪标记的解析器，所述解析器基于账号和防伪标记计算得到当前时间段，若当前时间段与实际符合，则解析正确；

[0059] 连线状态三：半在线状态，所述账号权限处理中心与所述账号检测终端处于离线状态，所述账号权限处理中心与所述账号提供终端处于在线状态；

[0060] 结合图4，所述账号提供终端从所述账号检测终端获得物理地址码，所述账号提供终端向所述账号权限处理中心提供所述物理地址码并请求下载权限包，并将下载的权限包发送至所述账号检测终端；

[0061] 所述账号检测终端向所述账号提供终端提供物理地址码并接收权限包，并利用所述密钥解锁权限包获得所述账号相关的权限，在所述权限中检索到目标权限则开放相应功能；

[0062] 所述账号权限处理中心接收到所述物理地址码后进行对比，对比无误后使用与所述物理地址码绑定的密钥对对应账号的权限进行加密打包处理得到权限包并发送给所述账号提供终端；

[0063] 所述账号权限处理中心中包括地址库，所述地址库用于存储所有账号检测终端的物理地址码及对应的密钥，所述密钥在所述账号检测终端初始化配置时生成并保存在所述账号权限处理中心和账号检测终端内；

[0064] 上述三个连线状态下所述账号检测终端最终都是获得所述账号权限处理中心的权限信息来判断是否对所述账号提供终端开放相应功能；

[0065] 连线状态四：离线状态，所述账号权限处理中心与所述账号检测终端处于离线状态，所述账号权限处理中心与所述账号提供终端处于离线状态；

[0066] 结合图5，所述账号提供终端向所述账号检测终端提供账号信息和第一代码，所述账号检测终端将所述第一代码与目标权限代码进行处理得到第二代码，并将所述第二代码发送给所述账号提供终端，所述账号提供终端将所述第一代码与所有的权限代码分别进行处理得到若干伪第二代码，所述账号提供终端从若干伪第二代码中找到与所述第二代码一致的伪第二代码进而确定目标权限，所述账号提供终端将所述第二代码与目标权限代码进行处理得到第三代码，并将所述第三代码与所述目标权限代码发送至所述账号检测单元，

所述账号检测单元将所述第二代码和所述目标权限代码进行处理得到第三代码，并对所述账号提供终端发送的目标权限代码和第三代码进行核对，核对无误后则开放相应功能；

[0067] 所述账号提供终端和所述账号检测终端拥有相同的代码处理器，所述代码处理器的输入端为两段代码，输出端为一段代码：具体可用下式表示：

[0068] $$A+B\xrightarrow{\text{代码处理器}}C$$；

[0069] 其中，A、B和C分别为一段代码；

[0070] 所述代码处理器具有单向性，不能通过A和C解析出B，也不能通过B和C解析出A；

[0071] 所述代码处理器由所述账号权限处理中心在在线状态时赋予给所述账号提供终端和所述账号检测终端；

[0072] 所述账号提供终端利用所述代码处理器计算得到伪第二代码和第三代码；

[0073] 所述账号检测终端利用所述代码处理器计算得到第二代码和第三代码；

[0074] 所述账号提供终端还包括代码生成器用于随机生成第一代码；

[0075] 所述第一代码、权限代码、第二代码、伪第二代码和第三代码具有相同的长度；

[0076] 所述代码处理器的处理公式为：

[0077] $$C(i)=q\left((A(i)+2)^{(B(i)+2)}\div\sqrt{A(i)+B(i)+2},\ j\right)$$；

[0078] 其中，A(i)、B(i)和C(i)表示代码的第i个字符对应的值，函数q(a,j)表示取a的第j位小数位的值；

[0079] 当所述代码采用16进制字符时，代码处理器中的计算也采用16进制计算；

[0080] 从上述公式中可知，在代码A不变的情况下，多个代码B经所述代码处理器处理后能够得到相同的代码C，故不能通过A和C解析出唯一的B；

[0081] 所述账号检测终端在发送第二代码以及接收第三代码时记录时间，当这两个时间差超过阈值时，直接终止权限确认；

[0082] 所述账号提供终端与账号检测终端均设有连线状态检测器，所述连线状态检测器用于检测所述终端与所述账号权限处理中心的连线状态，当所述账号提供终端与所述账号检测终端通过短距通讯连接时向对方发送当前的连线状态，所述终端通过接收的对方的连线状态与自身的连线状态选择上述四种模式中对应的一种模式来进行权限确认；

[0083] 当在离线模式下通过权限确认后，所述账号检测终端会生成验证包，在下次与所述账号权限处理中心处于在线状态时，将所述验证包发送至所述账号权限处理中心，所述账号权限处理中心根据所述验证包的内容确认对应账号是否有目标权限，并向所述账号检测终端返回验证结果。

[0084] 虽然上面已经参考各种实施例描述了本发明，但是应当理解，在不脱离本发明的范围的情况下，可以进行许多改变和修改。也就是说上面讨论的方法，系统和设备是示例。各种配置可以适当地省略，替换或添加各种过程或组件。例如，在替代配置中，可以以与所描述的顺序不同的顺序执行方法，和/或可以添加，省略和/或组合各种部件。而且，关于某些配置描述的特征可以以各种其他配置组合，如可以以类似的方式组合配置的不同方面和元素。此外，随着技术发展其中的元素可以更新，即许多元素是示例，并不限制本公开或权利要求的范围。

[0085] 在说明书中给出了具体细节以提供对包括实现的示例性配置的透彻理解。然而，

可以在没有这些具体细节的情况下实践配置例如，已经示出了众所周知的电路，过程，算法，结构和技术而没有不必要的细节，以避免模糊配置。该描述仅提供示例配置，并且不限制权利要求的范围，适用性或配置。相反，前面对配置的描述将为本领域技术人员提供用于实现所描述的技术的使能描述。在不脱离本公开的精神或范围的情况下，可以对元件的功能和布置进行各种改变。

[0086] 综上，其旨在上述详细描述被认为是例示性的而非限制性的，并且应当理解，以上这些实施例应理解为仅用于说明本发明而不用于限制本发明的保护范围。在阅读了本发明的记载的内容之后，技术人员可以对本发明作各种改动或修改，这些等效变化和修饰同样落入本发明权利要求所限定的范围。

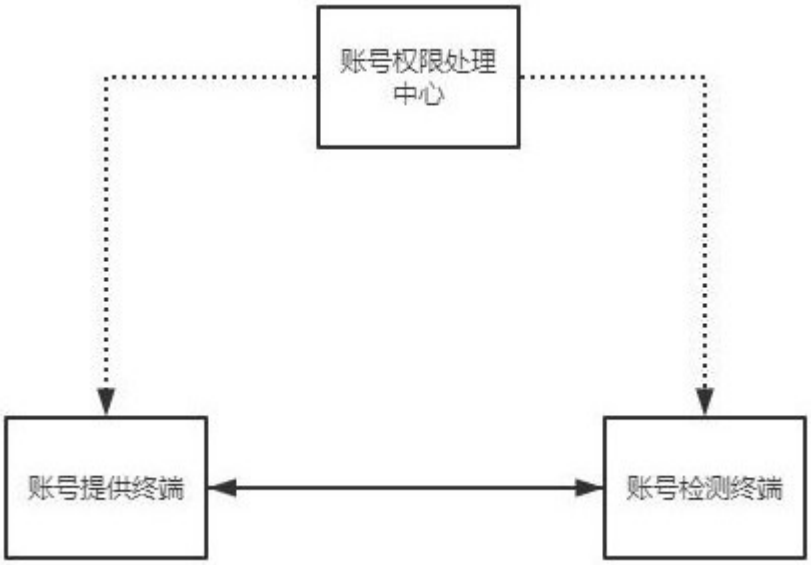

账号权限处理中心
账号提供终端
账号检测终端

图1

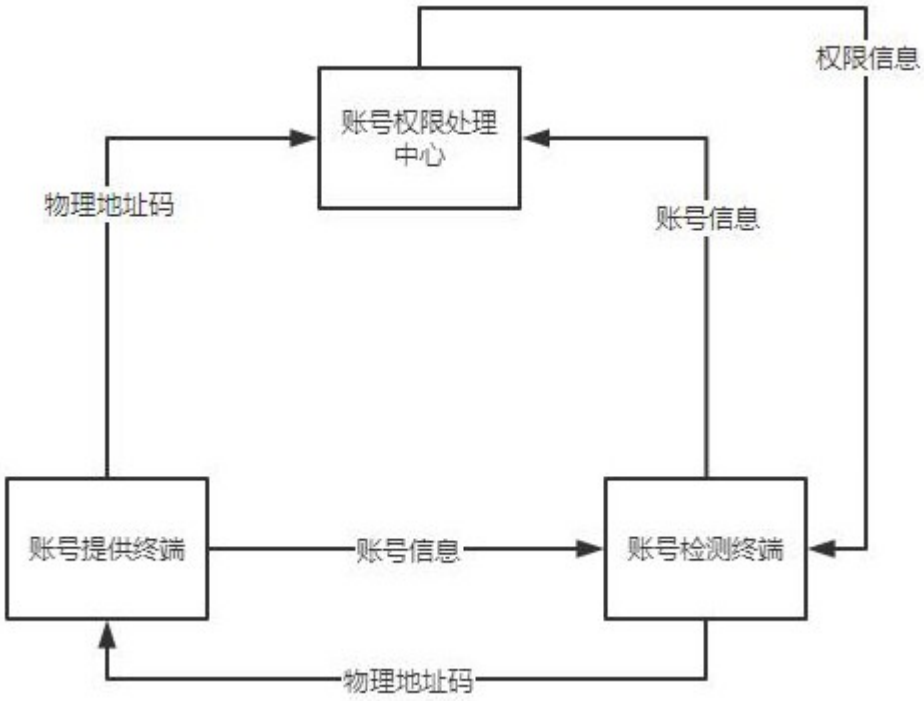

权限信息
账号权限处理中心
物理地址码
账号信息
账号提供终端
账号信息
账号检测终端
物理地址码

图2

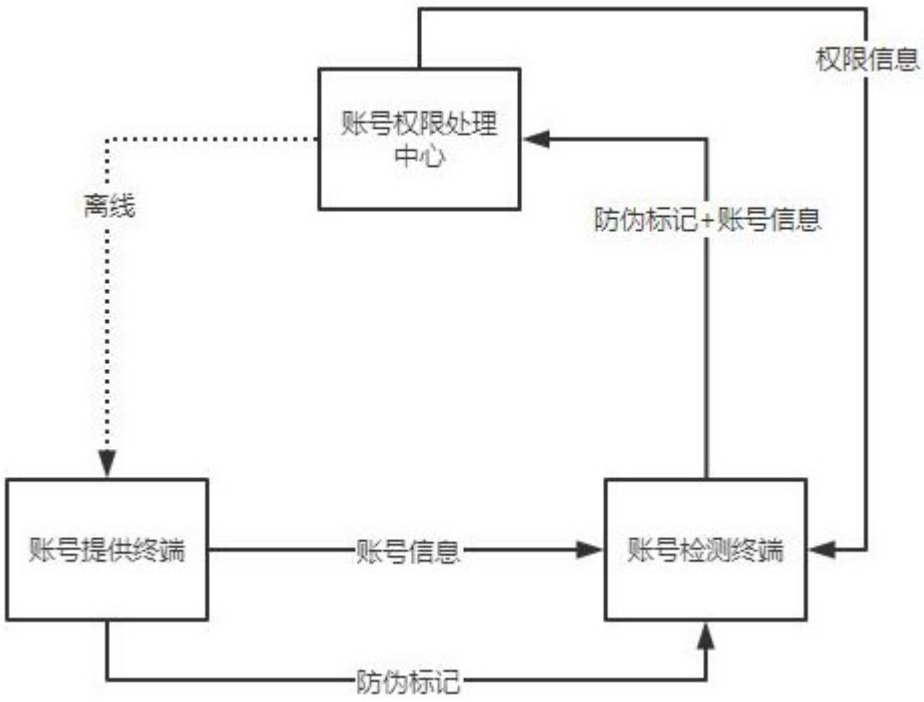

权限信息
账号权限处理中心
离线
防伪标记+账号信息
账号提供终端
账号信息
账号检测终端
防伪标记

图3

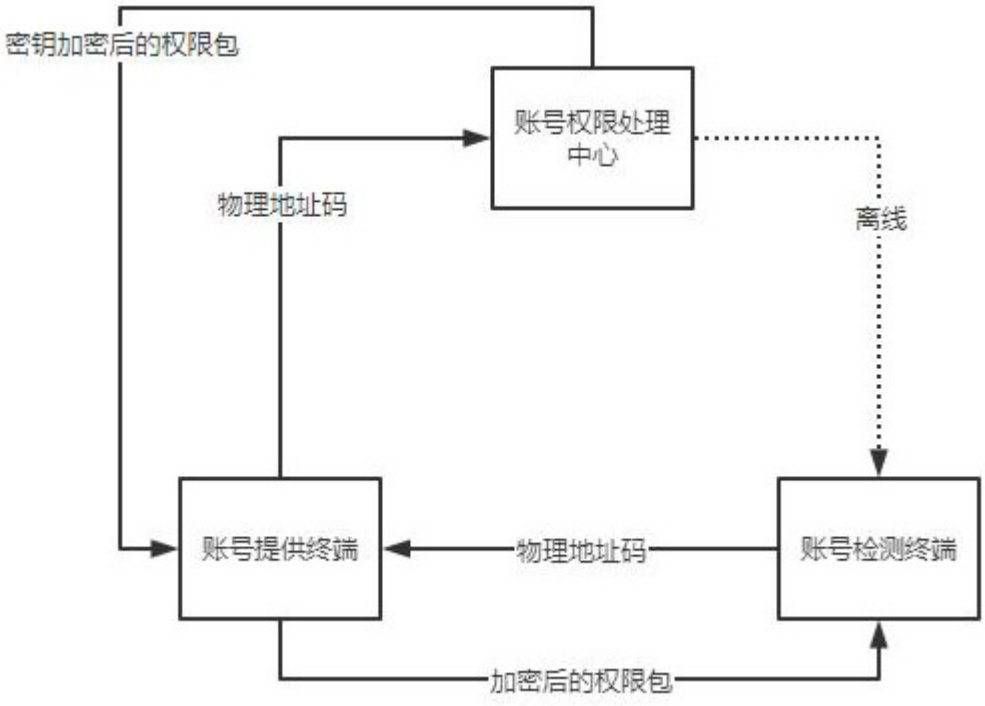

密钥加密后的权限包
账号权限处理中心
物理地址码
离线
账号提供终端
物理地址码
账号检测终端
加密后的权限包

图4

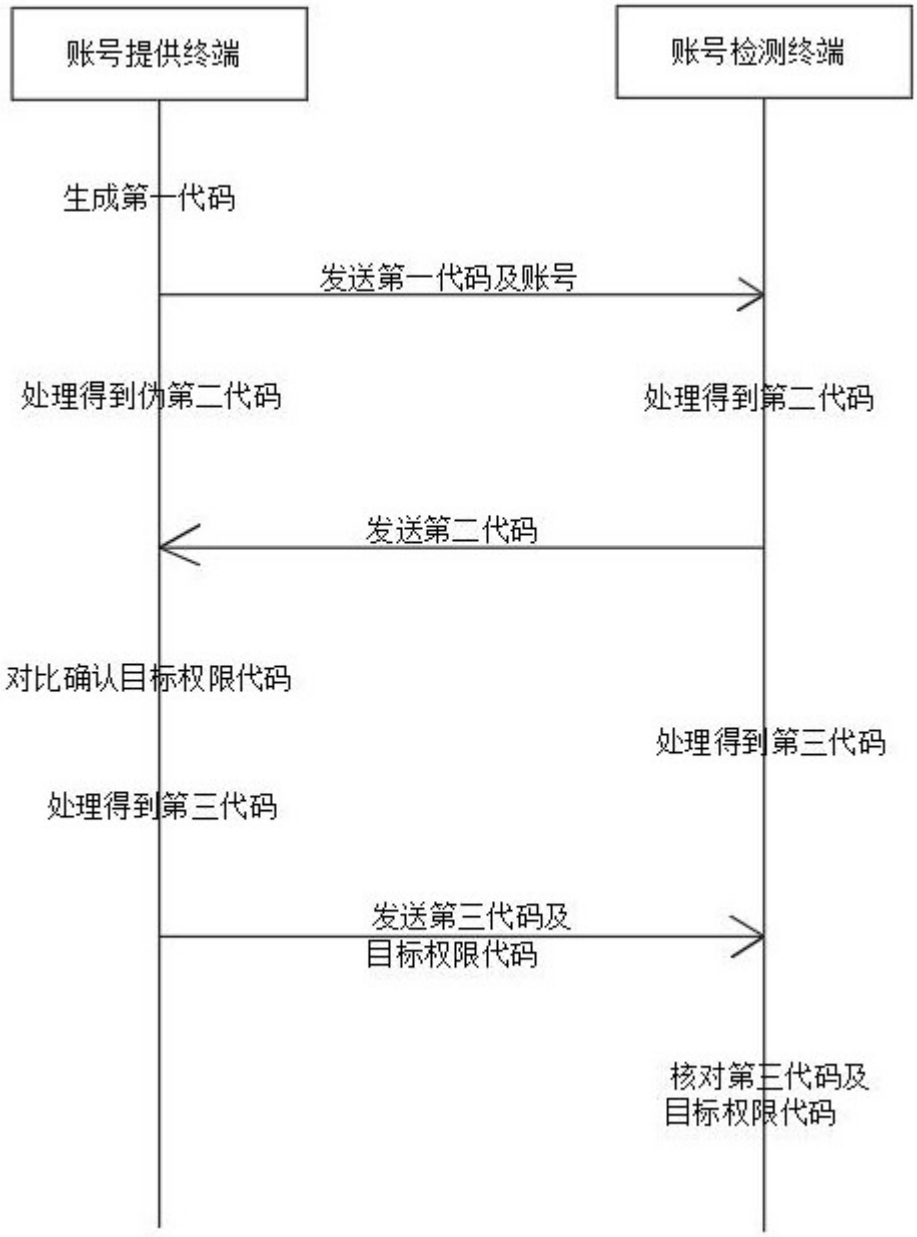

账号提供终端
账号检测终端
生成第一代码
发送第一代码及账号
处理得到伪第二代码
处理得到第二代码
发送第二代码
对比确认目标权限代码
处理得到第三代码
处理得到第三代码
发送第三代码及
目标权限代码
核对第三代码及
目标权限代码

图5