(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113536277 A
(43)申请公布日 2021.10.22

(21)申请号 202010290427.5

(22)申请日 2020.04.14

(71)申请人 中移动信息技术有限公司
地址 100000 北京市昌平区未来科学城英才北三街16号院16号楼1006室
申请人 中国移动通信集团有限公司

(72)发明人 王阳 谢军 田峰 何欣 韩志峰 曲大林 张德春 卞淑 王鸿元

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 彭琼

(51)Int.Cl.
G06F 21/34(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)

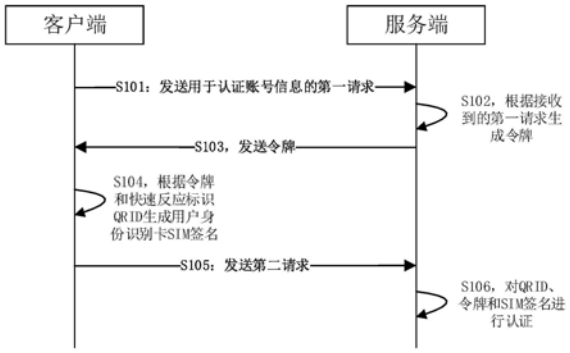
权利要求书3页 说明书9页 附图4页

(54)发明名称

认证的方法、系统、服务端、客户端及存储介质

(57)摘要

本发明实施例公开了一种认证的方法、系统、服务端、客户端及存储介质。该方法包括：根据接收到的第一请求生成令牌，第一请求是客户端发送的用于认证账号信息的请求；向客户端发送令牌，以用于客户端根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名；接收客户端发送的第二请求，第二请求包括令牌、QRID和SIM签名；对QRID、令牌和SIM签名进行认证，以用于当QRID、令牌和SIM签名认证通过时，客户端访问服务端。本发明实施例的认证的方法、系统、服务端、客户端及存储介质，可以实现登录设备安全登录4A管理平台。



CN 113536277 A

1.一种认证的方法,其特征在于,应用于服务端,所述方法包括:

根据接收到的第一请求生成令牌,所述第一请求是客户端发送的用于认证账号信息的请求;

向所述客户端发送所述令牌,以用于所述客户端根据所述令牌和快速反应标识QRID生成用户身份识别卡SIM签名;

接收所述客户端发送的第二请求,所述第二请求包括所述令牌、所述QRID和所述SIM签名;

对所述QRID、所述令牌和所述SIM签名进行认证,以用于当所述QRID、所述令牌和所述SIM签名认证通过时,所述客户端访问所述服务端。

2.根据权利要求1所述的方法,其特征在于,所述服务端包括第一模块、第二模块和第三模块;所述对所述QRID、所述令牌和所述SIM签名进行认证,包括:

所述第一模块对所述QRID进行认证;

当所述第一模块对所述QRID的认证通过时,所述第一模块向所述第二模块发送所述令牌和所述SIM签名;

当所述第二模块对所述令牌的认证通过时,所述第二模块向所述第三模块发送所述SIM签名;

所述第三模块对所述SIM签名进行认证,得到认证结果,并将所述认证结果通过所述第二模块发送给所述第一模块。

3.一种认证的方法,其特征在于,所述方法应用于客户端,所述方法包括:

向服务端发送用于认证账号信息的第一请求,以用于所述服务端根据所述第一请求生成令牌;

根据所述令牌和从所述服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名;

向所述服务端发送第二请求,所述第二请求包括所述令牌、所述QRID和所述SIM签名,所述第二请求用于所述服务端对所述QRID、所述令牌和所述SIM签名进行认证,以使所述服务端对所述QRID、所述令牌和所述SIM签名认证通过时,允许所述客户端访问所述服务端。

4.根据权利要求3所述的方法,其特征在于,从所述服务端获取快速反应标识QRID,包括:

扫描所述服务端提供的二维码信息,从所述二维码信息中获取所述QRID。

5.根据权利要求3或4所述的方法,其特征在于,在所述向服务端发送用于认证账号信息的第一请求之前,所述方法还包括:

显示提示信息,用于提示用户输入SIM盾口令;

接收用户输入的SIM盾口令;

对所述SIM盾口令进行认证,以使所述SIM盾口令认证通过后,向服务端发送所述第一请求。

6.一种认证的系统,其特征在于,所述系统包括:

客户端,用于向服务端发送用于认证账号信息的请求,以用于服务端对客户端进行认证;

服务端,用于对客户端进行认证,并在认证通过时,允许客户端访问服务端。

7.根据权利要求6所述的系统,其特征在于,所述请求包括第一请求和第二请求;

所述客户端,还用于向服务端发送用于认证账号信息的第一请求,以用于所述服务端根据所述第一请求生成令牌;

所述客户端,还用于根据所述令牌和从所述服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名;

所述客户端,还用于向所述服务端发送第二请求,所述第二请求包括所述令牌、所述QRID和所述SIM签名,所述第二请求用于所述服务端对所述QRID、所述令牌和所述SIM签名进行认证,以使所述服务端对所述QRID、所述令牌和所述SIM签名认证通过时,允许所述客户端访问所述服务端。

8.根据权利要求7所述的系统,其特征在于,

所述服务端,还用于根据接收到的第一请求生成令牌,所述第一请求是客户端发送的用于认证账号信息的请求;

所述服务端,还用于向所述客户端发送所述令牌,以用于所述客户端根据所述令牌和快速反应标识QRID生成用户身份识别卡SIM签名;

所述服务端,还用于接收所述客户端发送的第二请求,所述第二请求包括所述令牌、所述QRID和所述SIM签名;

所述服务端,还用于对所述QRID、所述令牌和所述SIM签名进行认证,以用于当所述QRID、所述令牌认证和所述SIM签名认证通过时,所述客户端访问所述服务端。

9.根据权利要求8所述的系统,其特征在于,所述服务端包括第一模块、第二模块和第三模块;

所述第一模块,用于对所述QRID进行认证;

所述第一模块,还用于当所述第一模块对所述QRID的认证通过时,向所述第二模块发送所述令牌和所述SIM签名;

所述第二模块,用于当所述第二模块对所述令牌的认证通过时,向所述第三模块发送所述SIM签名;

所述第三模块,用于对所述SIM签名进行认证,得到认证结果,并将所述认证结果通过所述第二模块发送给所述第一模块。

10.一种服务端,其特征在于,所述服务端包括:

处理模块,用于根据接收到的第一请求生成令牌,所述第一请求是客户端发送的用于认证账号信息的请求;

发送模块,用于向所述客户端发送所述令牌,以用于所述客户端根据所述令牌和快速反应标识QRID生成用户身份识别卡SIM签名;

接收模块,用于接收所述客户端发送的第二请求,所述第二请求包括所述令牌、所述QRID和所述SIM签名;

所述处理模块,还用于对所述QRID、所述令牌和所述SIM签名进行认证,以用于当所述QRID、所述令牌认证和所述SIM签名认证通过时,所述客户端访问所述服务端。

11.一种客户端,其特征在于,所述客户端包括:

发送模块,用于向服务端发送用于认证账号信息的第一请求,以用于所述服务端根据所述第一请求生成令牌;

处理模块，用于根据所述令牌和从所述服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名；

所述发送模块，还用于向所述服务端发送第二请求，所述第二请求包括所述令牌、所述QRID和所述SIM签名，所述第二请求用于所述服务端对所述QRID、所述令牌和所述SIM签名进行认证，以使所述服务端对所述QRID、所述令牌和所述SIM签名认证通过时，允许所述客户端访问所述服务端。

12.一种计算机存储介质，其特征在于，所述计算机存储介质上存储有计算机程序指令，所述计算机程序指令被处理器执行时实现如权利要求1-2任意一项所述的认证的方法，或，所述计算机程序指令被处理器执行时实现如权利要求3-5任意一项所述的认证的方法。

认证的方法、系统、服务端、客户端及存储介质

技术领域

[0001] 本发明涉及数据安全领域，尤其涉及一种认证的方法、系统、服务端、客户端及存储介质。

背景技术

[0002] 目前，记账(Account)，授权(Authentication)，认证(Authorization)，审计(Audit)简称4A，管理平台作为目前生产系统的安全服务屏障，安全重要性不言而喻，现有4A管理平台的登录方式主要为帐号密码登录、短信验证码登录，或基于此的二维码扫码登录。

[0003] 但是在日常的使用过程中，帐号密码登录方式往往存在密码泄露、密码窃取的问题，短信验证码登录又会存在短信被嗅探拦截，他人冒用及非法登录操作的风险，而基于帐号密码或短信验证码的二维码扫码登录方式同样也具有数据泄露的问题。

[0004] 所以现有4A管理平台的登录方式存在安全问题，且容易造成用户数据泄露。

发明内容

[0005] 本发明实施例提供了一种认证方法、系统、服务端、客户端及存储介质，解决了现有的4A管理平台登录方式中存在的安全问题和用户数据泄露的问题，能够实现安全登录4A管理平台。

[0006] 第一方面，提供了一种应用于服务端的认证的方法，该方法包括：

[0007] 根据接收到的第一请求生成令牌，第一请求是客户端发送的用于认证账号信息的请求；

[0008] 向客户端发送令牌，以用于客户端根据令牌和快速反应标识(Quick ResponseIdentity Document，QRID)生成用户身份识别卡(SubscriberIdentification Module，SIM)签名；

[0009] 接收客户端发送的第二请求，第二请求包括令牌、QRID和SIM签名；

[0010] 对QRID、令牌和SIM签名进行认证，以用于当QRID、令牌和SIM签名认证通过时，客户端访问服务端。

[0011] 在第一方面的一些实现方式中，服务端包括第一模块、第二模块和第三模块；对QRID、令牌和SIM签名进行认证，包括：

[0012] 第一模块对QRID进行认证；

[0013] 当第一模块对QRID的认证通过时，第一模块向第二模块发送令牌和SIM签名；

[0014] 当第二模块对令牌的认证通过时，第二模块向第三模块发送SIM签名；

[0015] 第三模块对SIM签名进行认证，得到认证结果，并将认证结果通过第二模块给第一模块。

[0016] 第二方面，提供了一种应用于客户端的认证的方法，该方法包括：

[0017] 向服务端发送用于认证账号信息的第一请求，以用于服务端根据第一请求生成令

牌；

[0018] 根据令牌和从服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名；

[0019] 向服务端发送第二请求，第二请求包括令牌、QRID和SIM签名，第二请求用于服务端对QRID、令牌和SIM签名进行认证，以使服务端对QRID、令牌和SIM签名认证通过时，允许客户端访问服务端。

[0020] 在第二方面的一些实现方式中，从服务端获取的快速反应标识QRID，包括：

[0021] 客户端扫描服务端提供的二维码信息，从二维码信息中获取QRID。

[0022] 在第二方面的一些实现方式中，向服务端发送用于认证账号信息的第一请求之前，还包括：

[0023] 显示提示信息，用于提示用户输入SIM盾口令；

[0024] 接收用户输入的SIM盾口令；

[0025] 对SIM盾口令进行认证，以使SIM盾口令认证通过后，向服务端发送第一请求。

[0026] 第三方面，提供了一种认证的系统，系统包括：

[0027] 客户端，用于向服务端发送用于认证账号信息的请求，以用于服务端对客户端进行认证；

[0028] 服务端，用于对客户端进行认证，并在认证通过时，允许客户端访问服务端。

[0029] 在第三方面的一些实现方式中，请求包括第一请求和第二请求；

[0030] 客户端，还用于向服务端发送用于认证账号信息的第一请求，以用于服务端根据第一请求生成令牌；

[0031] 客户端，还用于根据令牌和从服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名；

[0032] 客户端，还用于向服务端发送第二请求，第二请求包括令牌、QRID和SIM签名，第二请求用于服务端对QRID、令牌和SIM签名进行认证，以使服务端对QRID、令牌和SIM签名认证通过时，允许客户端访问服务端。

[0033] 在第三方面的一些实现方式中，

[0034] 服务端，还用于根据接收到的第一请求生成令牌，第一请求是客户端发送的用于认证账号信息的请求；

[0035] 服务端，还用于向客户端发送令牌，以用于客户端根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名；

[0036] 服务端，还用于接收客户端发送的第二请求，第二请求包括令牌、QRID和SIM签名；

[0037] 服务端，还用于对QRID、令牌和SIM签名进行认证，以用于当QRID、令牌认证和SIM签名认证通过时，客户端访问服务端。

[0038] 在第三方面的一些实现方式中，

[0039] 服务端包括第一模块、第二模块和第三模块；

[0040] 第一模块，用于对QRID进行认证；

[0041] 第一模块，还用于当第一模块对QRID的认证通过时，向第二模块发送令牌和SIM签名；

[0042] 第二模块，用于当第二模块对令牌的认证通过时，向第三模块发送SIM签名；

[0043] 第三模块，用于对SIM签名进行认证，得到认证结果，并将认证结果通过第二模块

发送第一模块。

[0044] 第四方面,提供了一种服务端,服务端包括:

[0045] 处理模块,用于根据接收到的第一请求生成令牌,第一请求是客户端发送的用于认证账号信息的请求;

[0046] 发送模块,用于向客户端发送令牌,以用于客户端根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名;

[0047] 接收模块,用于接收客户端发送的第二请求,第二请求包括令牌、QRID和SIM签名;

[0048] 处理模块,还用于对QRID、令牌和SIM签名进行认证,以用于当QRID、令牌认证和SIM签名认证通过时,客户端访问服务端。

[0049] 在第四方面的一些实现方式中,服务端包括第一模块、第二模块和第三模块;

[0050] 第一模块,用于对QRID进行认证;

[0051] 第一模块,还用于当第一模块对QRID的认证通过时,向第二模块发送令牌和SIM签名;

[0052] 第二模块,用于当第二模块对令牌的认证通过时,向第三模块发送SIM签名;

[0053] 第三模块,用于对SIM签名进行认证,得到认证结果,并将认证结果通过第二模块给第一模块。

[0054] 第五方面,提供了一种客户端,客户端包括:

[0055] 发送模块,用于向服务端发送用于认证账号信息的第一请求,以用于服务端根据第一请求生成令牌;

[0056] 处理模块,用于根据令牌和从服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名;

[0057] 发送模块,还用于向服务端发送第二请求,第二请求包括令牌、QRID和SIM签名,第二请求用于服务端对QRID、令牌和SIM签名进行认证,以使服务端对QRID、令牌和SIM签名认证通过时,允许客户端访问服务端。

[0058] 在第五方面的一些实现方式中,

[0059] 扫描模块,用于客户端扫描服务端提供的二维码信息,从二维码信息中获取QRID。

[0060] 在第五方面的一些实现方式中,

[0061] 显示模块,可以用于显示提示信息,用于提示用户输入SIM盾口令。

[0062] 接收模块,可以用于接收用户输入的SIM盾口令。

[0063] 处理模块,还可以用于对SIM盾口令进行认证,以使SIM盾口令认证通过后,向向服务端发送第一请求。

[0064] 第六方面,提供了一种计算机存储介质,计算机存储介质上存储有计算机程序指令,计算机程序指令被处理器执行时实现第一方面,以及第一方面的一些实现方式中认证的方法,或,计算机程序指令被处理器执行时实现第二方面,以及第二方面的一些实现方式中认证的方法。

[0065] 本发明实施例提供一种认证的方法、系统、服务端、客户端及存储介质,可以通过获取的快速反应标识(Quick ResponseIdentity Document,QRID)与令牌TOKEN生成用户身份识别卡(Subscriber Identification Module,SIM)签名之后,再进行认证,实现登录设备安全登录4A管理平台,解决了4A管理平台的登录方式中存在的安全问题,实现了客户端

登录4A管理平台过程的安全性。

附图说明

[0066] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中所需要使用的附图作简单地介绍，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。

[0067] 图1是本发明实施例提供的一种认证的方法的交互示意图；

[0068] 图2是本发明实施例提供的另一种认证的方法的交互示意图；

[0069] 图3是本发明实施例提供的一种服务端的结构示意图；

[0070] 图4是本发明实施例提供的一种客户端的结构示意图；

[0071] 图5是本发明实施例提供的一种认证的系统的结构示意图；

[0072] 图6是本发明实施例提供的一种计算设备的示例性硬件架构的结构图。

具体实施方式

[0073] 下面将详细描述本发明的各个方面的特征和示例性实施例，为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细描述。应理解，此处所描述的具体实施例仅被配置为解释本发明，并不被配置为限定本发明。对于本领域技术人员来说，本发明可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本发明的示例来提供对本发明更好的理解。

[0074] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0075] 目前，记账(Account)，授权(Authentication)，认证(Authorization)，审计(Audit)简称4A，管理平台作为目前生产系统的安全服务屏障，安全重要性不言而喻，现有4A管理平台的登录方式主要为帐号密码登录、短信验证码登录，或基于此的二维码扫码登录。

[0076] 但是在日常的使用过程中，帐号密码登录方式往往存在密码泄露、密码窃取的问题，短信验证码登录又会存在短信被嗅探拦截，他人冒用及非法登录操作的风险，而基于帐号密码或短信验证码的二维码扫码登录方式同样也具有数据泄露的问题。

[0077] 因此，上述技术方案中4A管理平台的登录方式存在安全问题，容易造成用户数据泄露。

[0078] 为解决上述技术方案中4A管理平台的登录方式中存在的安全问题，因此，本发明实施例提供了一种认证的方法、系统、服务端、客户端及存储介质，通过获取的快速反应标识(Quick ResponseIdentity Document，QRID)与令牌Token，生成用户身份识别卡(Subscriber Identification Module，SIM)签名之后，再进行认证，实现登录设备安全登

录4A管理平台，解决了上述技术方案中4A管理平台的登录方式中存在的安全问题，实现了客户端登录4A管理平台过程的安全性。

[0079] 需要说明的是，在本发明实施例中，服务端可以包括第一模块、第二模块、第三模块和第四模块。4A平台登录服务模块可以称为第一模块，认证服务模块可以称为第二模块，SIM认证模块可以称为第三模块，4A平台端可以称为第四模块。

[0080] 下面结合附图对本发明实施例提供的技术方案进行描述。

[0081] 图1是本发明实施例提供的一种认证的方法的交互示意图。如图1所示，该方法基于两个执行主体，分别是客户端和服务端，该认证的方法可以包括：

[0082] S101:客户端向服务端发送用于认证账号信息的第一请求。

[0083] 具体的，在客户端向服务端发送用于认证账号信息的第一请求之前，客户端可以显示提示信息，以用于提示用户输入SIM盾口令，并接收用户输入的SIM盾口令。可选的，在一个实施例中，客户端可以通过WAP网关向服务端发送第一请求，其中第一请求可以是用于账号信息认证(号码)的请求。

[0084] S102:服务端根据接收到的第一请求生成令牌。

[0085] S103:服务端向客户端发送令牌。

[0086] S104:客户端根据令牌和从服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名。

[0087] 其中，从服务端获取的快速反应标识QRID可以是客户端扫描服务端提供的二维码信息，从二维码信息中获取QRID。其中，服务端提供的二维码信息可以是拨VPN的内网访问地址。

[0088] S105:客户端向服务端发送第二请求。

[0089] 其中，第二请求可以包括令牌、QRID和SIM签名。

[0090] S106:服务端对QRID、令牌和SIM签名进行认证。

[0091] 当服务端对QRID、令牌和SIM签名认证通过时，可以允许客户端访问服务端。

[0092] 其中，服务端可以包括第一模块、第二模块、第三模块和第四模块。4A平台登录服务模块可以称为第一模块，认证服务模块可以称为第二模块，SIM认证模块可以称为第三模块，4A平台端可以称为第四模块。图1中的S101至S105的具体过程可以如图2所示，图2是本发明实施例提供的另一种认证的方法的交互示意图。

[0093] 如图2所示，S101，客户端向认证服务模块发送用于认证账户信息的第一请求；S102，认证服务模块根据第一请求生成令牌；S103，认证服务模块向客户端发送令牌；S104，客户端根据令牌和QRID生成SIM签名；S105，客户端向4A平台登录服务模块发送第二请求；然后执行图1中的S106:服务端对QRID、令牌和SIM签名进行认证。

[0094] 如图2所示，服务端对QRID、令牌和SIM签名进行认证的过程，具体可以包括，4A平台登录服务模块对QRID进行认证，当4A平台登录服务模块对QRID的认证通过时，4A平台登录服务模块向认证服务模块发送令牌和SIM签名。之后认证服务模块对令牌的进行认证，当认证服务模块对令牌的认证通过时，认证服务模块向SIM认证模块发送SIM签名，即，认证服务模块相当于转发SIM签名给SIM认证模块。然后SIM认证模块对SIM签名进行认证，认证通过后，得到认证结果，并将认证结果通过认证服务模块给4A平台登录服务模块，完成服务端的认证流程。其中，认证结果可以包括账号信息。

[0095] 在服务端对QRID、令牌认证和SIM签名认证通过时，服务端的SIM认证模块通过服务端的认证服务模块发送给服务端的4A平台登录服务模块，以允许客户端可以通过4A平台登录服务模块访问第四模块，即，客户端可以通过4A平台登录服务模块访问4A平台端。

[0096] 客户端通过4A平台登录服务模块访问4A平台端，完成了客户端安全登录4A平台的过程。可选的，在一个实施例中，在服务端对QRID、令牌认证和SIM签名认证通过时，因为允许客户端可以通过4A平台登录服务模块访问4A平台端，所以客户端的界面可以重定向至4A平台主页。

[0097] 在本发明实施例提供的认证的方法中，用户可以通过支持SIM盾手机卡的客户端，使用客户端中扫码应用扫描4A平台二维码实现登录4A平台。

[0098] 此外，如图2所示，在S101之前，即，客户端在向服务端发送用于认证账号信息的第一请求之前，可以对SIM盾口令进行认证。以使SIM盾口令认证通过后，向服务端发送第一请求。

[0099] 本发明实施例中提供的认证的方法，可以通过获取的快速反应标识(Quick ResponseIdentity Document，QRID)与令牌TOKEN生成用户身份识别卡(Subscriber Identification Module，SIM)签名之后，再进行认证，实现登录设备安全登录4A管理平台，解决了4A管理平台的登录方式中存在的安全问题，实现了客户端登录4A管理平台过程的安全性。

[0100] 与认证的方法的实施例相对应，本发明实施例还提供了一种用于认证的服务端。

[0101] 图3是本发明实施例提供的一种服务端的结构示意图。

[0102] 如图3所示，服务端可以包括：处理模块201，发送模块202，接收模块203。

[0103] 其中，处理模块201，可以用于根据接收到的第一请求生成令牌，第一请求是客户端发送的用于认证账号信息的请求。

[0104] 发送模块202，可以用于向客户端发送令牌，以用于客户端根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名。

[0105] 接收模块203，可以用于接收客户端发送的第二请求，第二请求包括令牌、QRID和SIM签名。

[0106] 处理模块201，还可以用于对QRID、令牌和SIM签名进行认证，以用于当QRID、令牌认证和SIM签名认证通过时，客户端访问服务端。

[0107] 处理模块201，还可以用于使用服务端的第一模块对QRID进行认证。

[0108] 处理模块201，还可以用于当服务端的第一模块对QRID的认证通过时，服务端的第一模块向服务端的第二模块发送令牌和SIM签名。

[0109] 处理模块201，还可以用于当服务端的第二模块对令牌的认证通过时，服务端的第二模块向服务端的第三模块发送SIM签名。

[0110] 处理模块201，还可以用于服务端的第三模块对SIM签名进行认证，得到认证结果，并将认证结果通过服务端的第二模块给服务端的第一模块。

[0111] 本发明实施例中提供的用于认证的服务端，可以通过获取的快速反应标识(Quick ResponseIdentity Document，QRID)与令牌TOKEN生成用户身份识别卡(Subscriber Identification Module，SIM)签名之后，再进行认证，实现登录设备安全登录4A管理平台，解决了4A管理平台的登录方式中存在的安全问题，实现了客户端登录4A管理平台过程的安

全性。

[0112] 与认证的方法的实施例相对应,本发明实施例还提供了一种用于认证的客户端。

[0113] 图4是本发明实施例提供的一种客户端的结构示意图。

[0114] 如图4所示,服务端可以包括:发送模块301,处理模块302,扫描模块303,显示模块304,接收模块305。

[0115] 其中,发送模块301,可以用于向服务端发送用于认证账号信息的第一请求,以用于服务端根据第一请求生成令牌。

[0116] 处理模块302,可以用于根据令牌和从服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名。

[0117] 发送模块301,还可以用于向服务端发送第二请求,第二请求包括令牌、QRID和SIM签名,第二请求用于服务端对QRID、令牌和SIM签名进行认证,以使服务端对QRID、令牌和SIM签名认证通过时,允许客户端访问服务端。

[0118] 扫描模块303,可以用于客户端扫描服务端提供的二维码信息,从二维码信息中获取QRID。

[0119] 显示模块304,可以用于显示提示信息,用于提示用户输入SIM盾口令。

[0120] 接收模块305,可以用于接收用户输入的SIM盾口令。

[0121] 处理模块302,还可以用于对SIM盾口令进行认证,以使SIM盾口令认证通过后,向向服务端发送第一请求。

[0122] 本发明实施例中提供的用于认证的客户端,可以通过获取的快速反应标识(Quick ResponseIdentity Document,QRID)与令牌TOKEN生成用户身份识别卡(Subscriber Identification Module,SIM)签名之后,再进行认证,实现登录设备安全登录4A管理平台,解决了4A管理平台的登录方式中存在的安全问题,实现了客户端登录4A管理平台过程的安全性。

[0123] 与认证的方法的实施例相对应,本发明实施例还提供了一种认证的系统,用于执行认证功能。

[0124] 图5是本发明实施例提供的一种认证的系统的结构示意图。

[0125] 如图5所示,认证的系统可以包括:客户端401,服务端402,服务端402又可以包括第一模块403,第二模块404,第三模块405。

[0126] 其中,客户端401,可以用于向服务端发送用于认证账号信息的请求,以用于服务端对客户端进行认证,其中,请求包括第一请求和第二请求。

[0127] 服务端402,可以用于对客户端进行认证,并在认证通过时,允许客户端访问服务端。客户端401,还可以用于向服务端发送用于认证账号信息的第一请求,以用于服务端根据第一请求生成令牌。

[0128] 客户端401,还可以用于根据令牌和从服务端获取的快速反应标识QRID生成用户身份识别卡SIM签名。

[0129] 客户端401,还可以用于向服务端发送第二请求,第二请求包括令牌、QRID和SIM签名,第二请求用于服务端对QRID、令牌和SIM签名进行认证,以使服务端对QRID、令牌和SIM签名认证通过时,允许客户端访问服务端。

[0130] 服务端402,还可以用于根据接收到的第一请求生成令牌,第一请求是客户端发送

的用于认证账号信息的请求。

[0131] 服务端402,还可以用于向客户端发送令牌,以用于客户端根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名。

[0132] 服务端402,还可以用于接收客户端发送的第二请求,第二请求包括令牌、QRID和SIM签名。

[0133] 服务端402,还可以用于对QRID、令牌和SIM签名进行认证,以用于当QRID、令牌认证和SIM签名认证通过时,客户端访问服务端。

[0134] 服务端的第一模块403,可以用于对QRID进行认证。

[0135] 服务端的第一模块403,还可以用于当第一模块对QRID的认证通过时,向第二模块发送令牌和SIM签名。

[0136] 服务端的第二模块404,可以用于当第二模块对令牌的认证通过时,向第三模块发送SIM签名。

[0137] 服务端的第三模块405,可以用于对SIM签名进行认证,得到认证结果,并将认证结果通过第二模块发送第一模块。

[0138] 本发明实施例中提供的认证的系统,可以通过获取的快速反应标识(Quick ResponseIdentity Document,QRID)与令牌TOKEN生成用户身份识别卡(Subscriber Identification Module,SIM)签名之后,再进行认证,实现登录设备安全登录4A管理平台,解决了4A管理平台的登录方式中存在的安全问题,实现了客户端登录4A管理平台过程的安全性。

[0139] 图6示出了能够实现根据本发明实施例的认证的方法的计算设备的示例性硬件架构的结构图。如图6所示,计算设备500包括输入设备501、输入接口502、中央处理器503、存储器504、输出接口505、以及输出设备506。其中,输入接口502、中央处理器503、存储器504、以及输出接口505通过总线510相互连接,输入设备501和输出设备506分别通过输入接口502和输出接口505与总线510连接,进而与计算设备500的其他组件连接。

[0140] 具体地,输入设备501接收来自外部的输入信息,并通过输入接口502将输入信息传送到中央处理器503;中央处理器503基于存储器504中存储的计算机可执行指令对输入信息进行处理以生成输出信息,将输出信息临时或者永久地存储在存储器504中,然后通过输出接口505将输出信息传送到输出设备506;输出设备506将输出信息输出到计算设备500的外部供用户使用。

[0141] 也就是说,图6所示的计算设备也可以被实现为认证的设备,该认证的设备可以包括:存储有计算机可执行指令的存储器;以及处理器,该处理器在执行计算机可执行指令时可以实现本发明实施例提供的认证的方法。

[0142] 本发明实施例还提供一种计算机可读存储介质,该计算机可读存储介质上存储有计算机程序指令;该计算机程序指令被处理器执行时实现本发明实施例提供的认证的方法。

[0143] 需要明确的是,本发明并不局限于上文所描述并在图中示出的特定配置和处理。为了简明起见,这里省略了对已知方法的详细描述。在上述实施例中,描述和示出了若干具体的步骤作为示例。但是,本发明的方法过程并不限于所描述和示出的具体步骤,本领域的技术人员可以在领会本发明的精神后,作出各种改变、修改和添加,或者改变步骤之间的顺

序。

[0144] 以上所述的结构框图中所示的功能块可以实现为硬件、软件、固件或者它们的组合。当以硬件方式实现时，其可以例如是电子电路、专用集成电路(ASIC)、适当的固件、插件、功能卡等等。当以软件方式实现时，本发明的元素是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。“机器可读介质”可以包括能够存储或传输信息的任何介质。机器可读介质的例子包括电子电路、半导体存储器设备、ROM、闪存、可擦除ROM(EROM)、软盘、CD-ROM、光盘、硬盘、光纤介质、射频(RF)链路，等等。代码段可以经由诸如因特网、内联网等的计算机网络被下载。

[0145] 还需要说明的是，本发明中提及的示例性实施例，基于一系列的步骤或者装置描述一些方法或系统。但是，本发明不局限于上述步骤的顺序，也就是说，可以按照实施例中提及的顺序执行步骤，也可以不同于实施例中的顺序，或者若干步骤同时执行。

[0146] 以上所述，仅为本发明的具体实施方式，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、模块和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。应理解，本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本发明的保护范围之内。

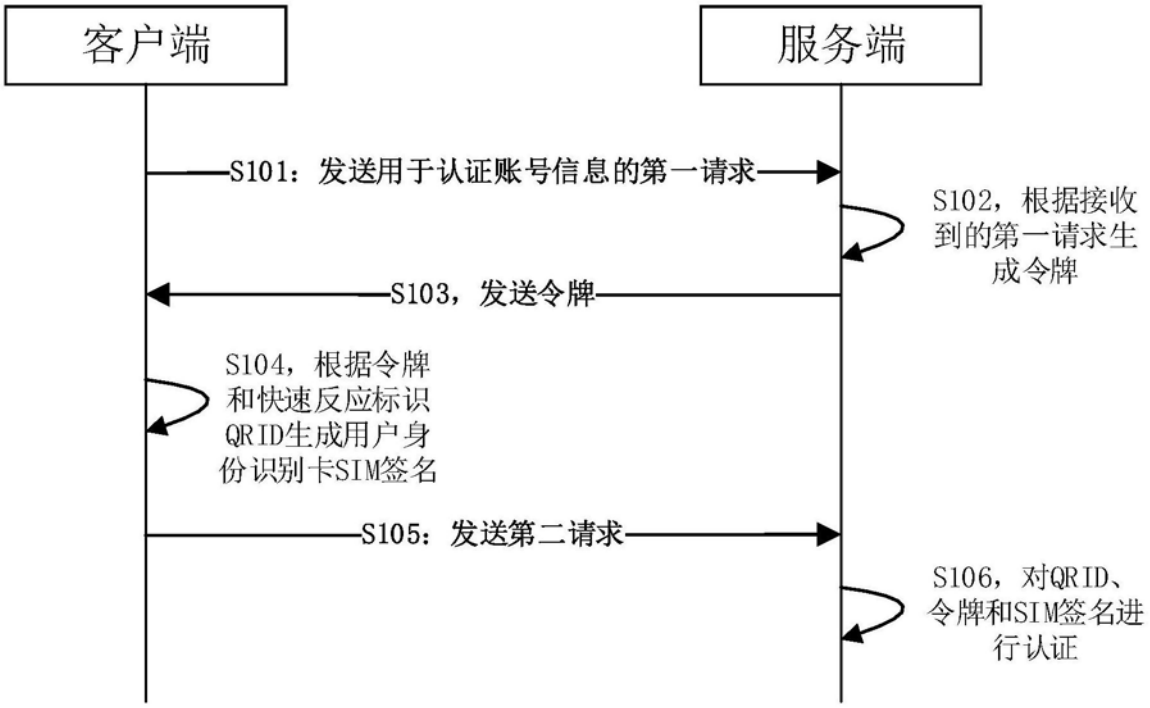

客户端
服务端
S101：发送用于认证账号信息的第一请求
S102，根据接收到的第一请求生成令牌
S103，发送令牌
S104，根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名
S105：发送第二请求
S106，对QRID、令牌和SIM签名进行认证

图1

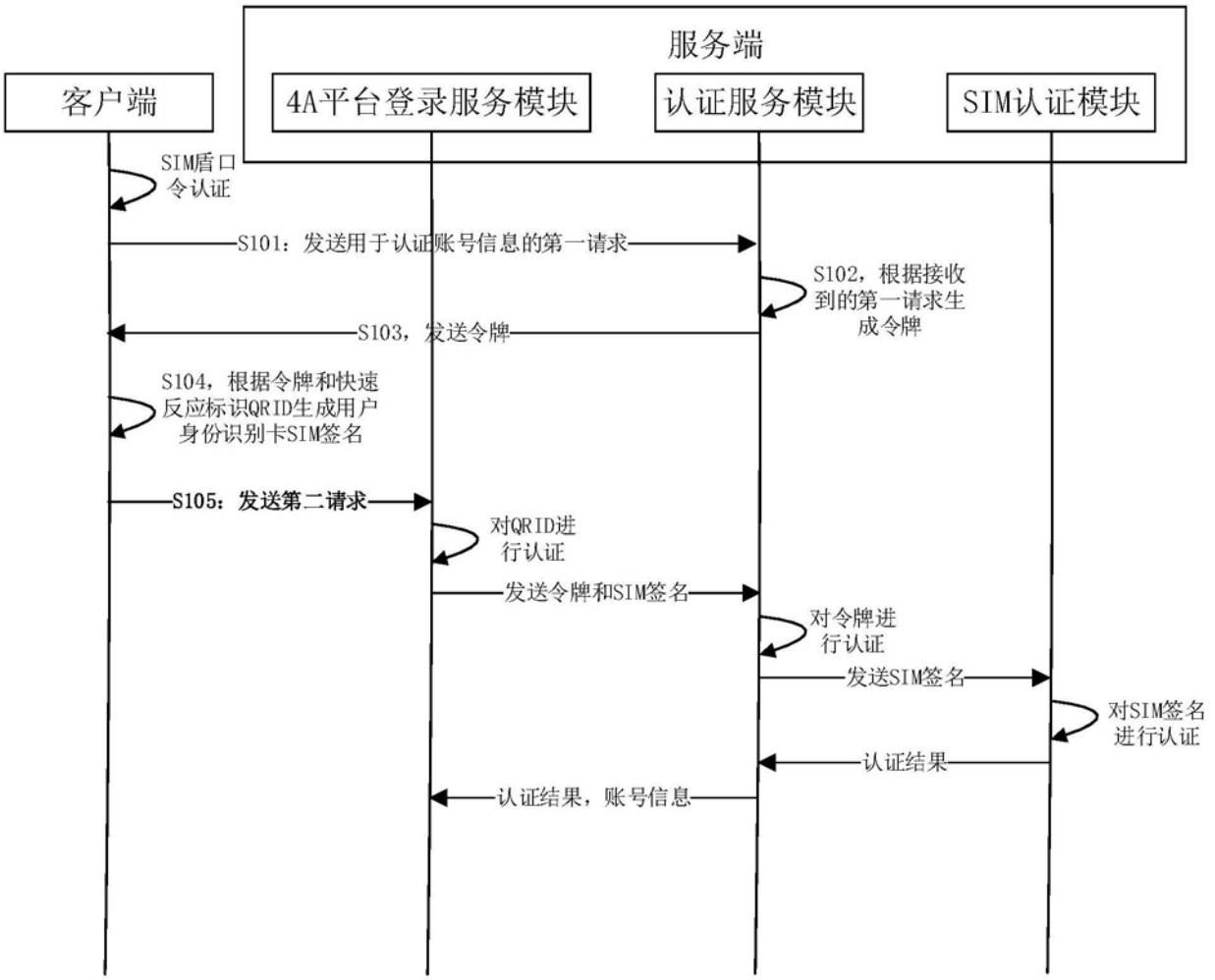

服务端
客户端
4A平台登录服务模块
认证服务模块
SIM认证模块
SIM盾口令认证
S101：发送用于认证账号信息的第一请求
S102，根据接收到的第一请求生成令牌
S103，发送令牌
S104，根据令牌和快速反应标识QRID生成用户身份识别卡SIM签名
S105：发送第二请求
对QRID进行认证
发送令牌和SIM签名
对令牌进行认证
发送SIM签名
对SIM签名进行认证
认证结果
认证结果，账号信息

图2

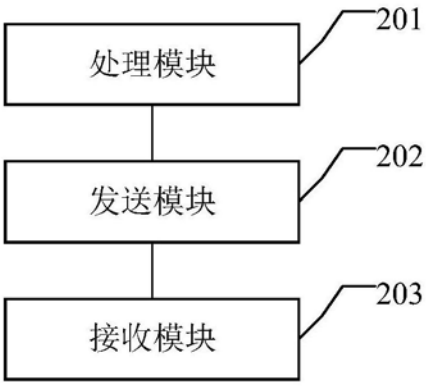

处理模块
201
发送模块
202
接收模块
203

图3

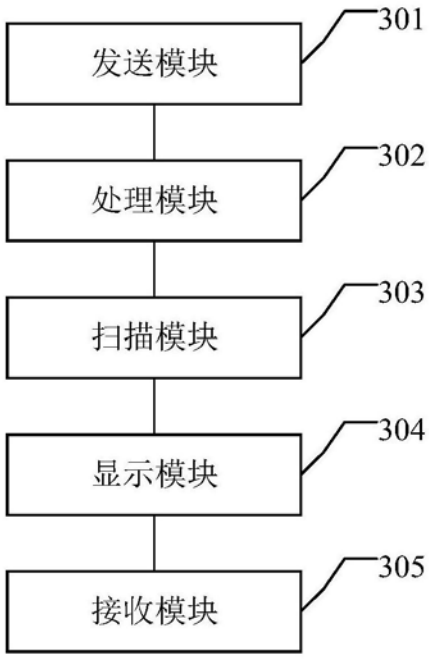

301
发送模块
302
处理模块
303
扫描模块
304
显示模块
305
接收模块

图4

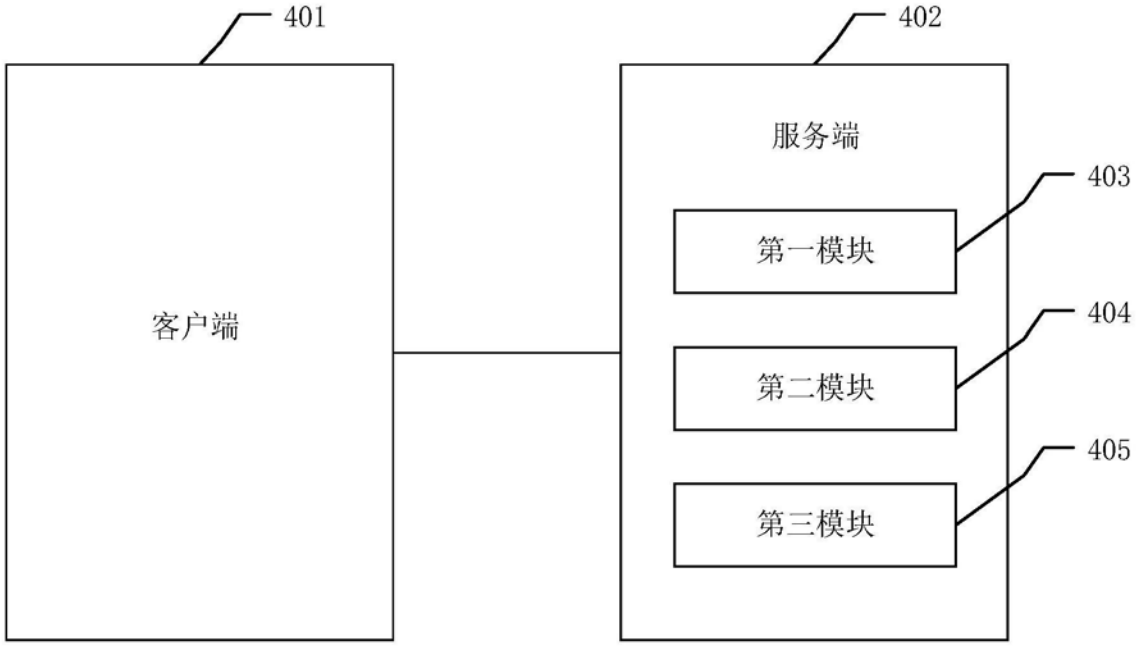

401
客户端
402
服务端
403
第一模块
404
第二模块
405
第三模块

图5

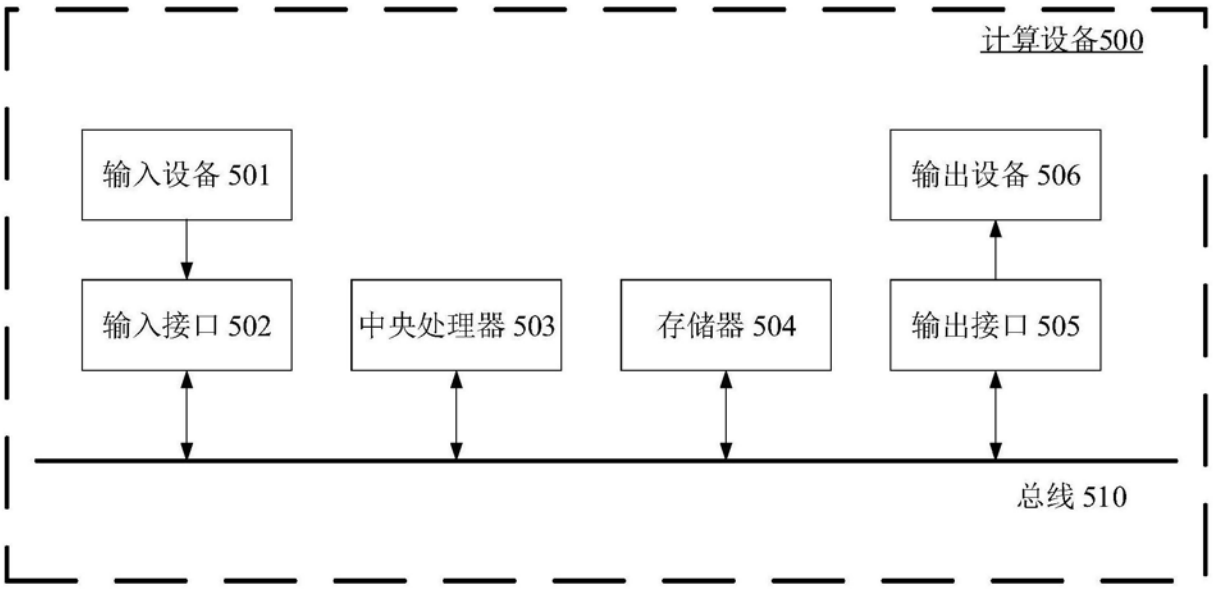

计算设备500
输入设备 501
输出设备 506
输入接口 502
中央处理器 503
存储器 504
输出接口 505
总线 510

图6