

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2014 年 7 月 10 日 (10.07.2014)



(10) 国际公布号
WO 2014/106372 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2013/078879
- (22) 国际申请日: 2013 年 7 月 5 日 (05.07.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310004998.8 2013 年 1 月 7 日 (07.01.2013) CN
- (71) 申请人: 广州广电运通金融电子股份有限公司 (GRG BANKING EQUIPMENT CO., LTD.) [CN/CN]; 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。
- (72) 发明人: 徐俊 (XU, Jun); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 熊飞 (XIONG, Fei); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 雷正生 (LEI, Zhengsheng); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 宁群伟 (NING, Qunwei); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。 王庆华 (WANG, Qinghua); 中国广东省广州市萝岗区科学城科林路 9 号, Guangdong 510663 (CN)。
- (74) 代理人: 北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街 22 号赛特广场 7 层, Beijing 100004 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV,

[见续页]

(54) Title: AUTHENTICATION METHOD AND APPARATUS BASED ON FINANCIAL SELF-SERVICE EQUIPMENT

(54) 发明名称: 一种基于金融自助设备的认证方法及装置

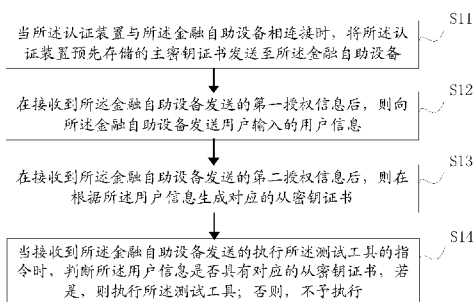


图 1 / FIG. 1

- S11 A MASTER KEY CERTIFICATE PRE-STORED IN THE AUTHENTICATION APPARATUS IS SENT TO THE FINANCIAL SELF-SERVICE EQUIPMENT WHEN THE AUTHENTICATION APPARATUS IS CONNECTED WITH THE FINANCIAL SELF-SERVICE EQUIPMENT
- S12 USER INFORMATION INPUT BY A USER IS SENT TO THE FINANCIAL SELF-SERVICE EQUIPMENT AFTER FIRST AUTHORIZATION INFORMATION SENT BY THE FINANCIAL SELF-SERVICE EQUIPMENT IS RECEIVED
- S13 A CORRESPONDING SLAVE KEY CERTIFICATE IS GENERATED ACCORDING TO THE USER INFORMATION AFTER SECOND AUTHORIZATION INFORMATION SENT BY THE FINANCIAL SELF-SERVICE EQUIPMENT IS RECEIVED
- S14 WHEN A COMMAND OF EXECUTING THE TEST TOOL SENT BY THE FINANCIAL SELF-SERVICE EQUIPMENT IS RECEIVED, WHETHER THE SLAVE KEY CERTIFICATE CORRESPONDING TO THE USER INFORMATION EXISTS IS JUDGED, IF SO, THE TEST TOOL IS EXECUTED; AND IF NOT, THE TEST TOOL IS NOT EXECUTED

(57) Abstract: Disclosed is an authentication method based on financial self-service equipment, comprising: sending a master key certificate pre-stored in an authentication apparatus to the financial self-service equipment when the authentication apparatus is connected with the financial self-service equipment; sending user information input by a user to the financial self-service equipment after first authorization information sent by the financial self-service equipment is received, and the first authorization information being the information sent after the master key certificate is judged to be legal by the financial self-service equipment; generating a corresponding slave key certificate according to the user information after second authorization information sent by the financial self-service equipment is received, and the second authorization information being the information sent after the user information is judged to be legal by the financial self-service equipment; and when a command of executing a test tool sent by the financial self-service equipment is received, judging whether the slave key certificate corresponding to the user information exists, if so, executing the test tool; and if not, not executing the test tool. The double authentication mode provided in the present invention can improve the safety of the financial self-service equipment.

(57) 摘要:

[见续页]



WO 2014/106372 A1



SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, ZA, ZM, ZW。

IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD,
TG)。

- (84) **指定国** (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种基于金融自助设备的认证方法, 包括: 当认证装置与金融自助设备相连接时, 将认证装置预先存储的主密钥证书发送至金融自助设备; 在接收到金融自助设备发送的第一授权信息后, 则向金融自助设备发送用户输入的用户信息, 第一授权信息为金融自助设备判断主密钥证书为合法证书后发送的信息; 在接收到金融自助设备发送的第二授权信息后, 则在根据用户信息生成对应的从密钥证书, 第二授权信息为金融自助设备判断用户信息为合法信息后发送的信息; 当接收到金融自助设备发送的执行测试工具的指令时, 判断用户信息是否具有对应的从密钥证书, 若是则执行测试工具; 否则不予执行。本发明提供的双重认证的方式可以提高了金融自助设备的安全性。

一种基于金融自助设备的认证方法及装置

本申请要求于 2013 年 1 月 7 日提交中国专利局、申请号为 201310004998.8、发明名称为“一种基于金融自助设备的认证方法及装置”的中国专利申请 5 的优先权，其全部内容引用在本申请中。

技术领域

本发明涉及程序测试领域，更具体的说，涉及基于金融自助设备的认证方法及装置。

10

背景技术

随着金融自助服务的普及，金融自助设备凭借便利、快捷的服务已经成为了金融机构与客户接触的最主要的支付渠道，其中，金融自助设备包括 ATM 自动取款机和自助信息查询机等。金融自助设备的系统性能的测试、故障排除 15 和维护也成为各厂商及维护人员非常关注的问题。

现有的金融自助设备的测试工具通常存储在普通的 U 盘或移动存储介质中，当维护人员需要对金融自助设备进行测试或维护时，需要将 U 盘插入到金融自助设备上，并使用 U 盘内部的测试工具对金融自助设备进行测试或维护。

20 但是现有的测试 U 盘或移动存储介质不存在任何的安全防护机制或授权处理。在工作人员通过 U 盘对金融自助设备的日常维护过程中，如果出现移动存储介质丢失或被盗等情况，都会给金融自助设备带来相当大的安全隐患。

因此，如何提供一种基于金融自助设备的安全性高的认证方法及装置，成为目前最需要解决的问题。

25

发明内容

有鉴于此，本发明的设计目的在于，提供一种基于金融自助设备的认证方法及装置，以提高金融自助设备的安全性。

一种基于金融自助设备的认证方法，应用于可与所述金融自助设备相连接

的认证装置, 所述认证装置内存储有测试工具, 包括:

当所述认证装置与所述金融自助设备相连接时, 将所述认证装置预先存储的主密钥证书发送至所述金融自助设备;

5 在接收到所述金融自助设备发送的第一授权信息后, 则向所述金融自助设备发送用户输入的用户信息, 所述第一授权信息为所述金融自助设备判断所述主密钥证书为合法证书后发送的信息;

在接收到所述金融自助设备发送的第二授权信息后, 则在根据所述用户信息生成对应的从密钥证书, 所述第二授权信息为所述金融自助设备判断所述用户信息为合法信息后发送的信息;

10 当接收到所述金融自助设备发送的执行所述测试工具的指令时, 判断所述用户信息是否具有对应的从密钥证书, 若是, 则执行所述测试工具; 否则, 不予执行。

优选地, 所述主密钥证书包括有效期限、厂商信息、银行信息和使用权限。

优选地, 当所述认证装置与所述金融自助设备相连接时, 还包括:

15 清除所述认证装置内预先存储的第一授权信息、第二授权信息和从密钥证书。

优选地, 在执行所述测试工具时, 还包括:

记录执行所述测试工具的整个过程。

优选地, 在根据所述用户信息生成对应的从密钥证书的步骤后, 还包括:

20 将所述从密钥证书进行加密;

将加密后的从密钥证书保存在所述认证装置内部的隐藏区域。

优选地, 当所述主密钥证书的使用权限为普通用户时, 则所述普通用户可使用所述测试工具。

25 优选地, 当所述主密钥证书的使用权限为高级用户时, 则所述高级用户可使用或修改所述测试工具。

一种基于金融自助设备的认证方法, 应用于可与认证装置相连接的所述金融自助设备, 所述认证装置内存储有测试工具, 包括:

当所述认证装置与所述金融自助设备相连接时, 获取所述认证装置预先存储的主密钥证书;

30 当判断出所述主密钥证书为合法证书时, 则向所述认证装置发送第一授权

信息，并获取用户输入的用户信息；

当判断出所述用户信息为合法信息时，则向所述认证装置发送第二授权信息；

向所述认证装置发送执行所述测试工具的指令。

5 一种基于金融自助设备的认证装置，所述认证装置可与所述金融自助设备相连接，所述认证装置内存储有测试工具，包括：

第一发送模块，用于当所述认证装置与所述金融自助设备相连接时，将所述认证装置预先存储的主密钥证书发送至所述金融自助设备；

10 第一接收模块，用于接收所述金融自助设备发送的第一授权信息，所述第一授权信息为所述金融自助设备判断所述主密钥证书为合法证书后发送的信息；

第二发送模块，用于在所述第一接收模块接收到所述第一授权信息后，则向所述金融自助设备发送用户信息；

15 第二接收模块，用于接收到所述金融自助设备发送的第二授权信息，所述第二授权信息为所述金融自助设备判断所述用户信息为合法信息后发送的信息；

从密钥证书生成模块，用于在所述第二接收模块接收到第二授权信息后，则在根据所述用户信息生成对应的从密钥证书；

20 第三接收模块，用于接收所述金融自助设备发送的执行所述测试工具的指令；

从密钥证书检测模块，用于在所述第三接收模块接收到执行所述测试工具的指令时，判断所述用户信息是否具有对应的从密钥证书，若是，则执行所述测试工具；否则，不予执行。

与现有技术相比，本实施例提供的技术方案具有以下优点和特点：

25 在本发明提供的方案中，需要分别对主密钥证书和用户信息的正确性进行判断，以便对认证装置的权限和维护人员的身份进行双重认证，如果认证装置丢失或被盗，只要输入的用户信息不正确，那么就无法使用该认证装置内部的测试工具；如果输入的用户信息正确，但是认证装置无法提供正确的主密钥证书，那么也无法使用该认证装置内部的测试工具，因此，本发明提供的双重认证的方式提高了金融自助设备的安全性。

30

附图说明

为了更清楚地说明本发明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地介绍，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。

图 1 为本发明所提供的一种基于金融自助设备的认证方法的流程图；

图 2 为本发明所提供的另一种基于金融自助设备的认证方法的流程图；

图 3 为本发明所提供的一种基于金融自助设备的认证装置的模块图；

图 4 为本发明所提供的另一种基于金融自助设备的认证装置的模块图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例提供了一种基于金融自助设备的认证方法及装置，以提高金融自助设备的安全性。由于上述测试驱动程序的方法的具体实现存在多种方式，下面通过具体实施例进行详细说明：

实施例一

请参见图 1 所示，图 1 所示的为一种基于金融自助设备的认证方法，该方法应用于可与所述金融自助设备相连接的认证装置，所述认证装置内存储有测试工具，该方法包括：

步骤 S11、当所述认证装置与所述金融自助设备相连接时，将所述认证装置预先存储的主密钥证书发送至所述金融自助设备；

其中，主密钥证书包括该认证装置的有效期限、厂商信息、银行信息和使用权限。对于认证装置的有效期限而言，如果当前的时间不在有效期限内，那么该主密钥证书就会作废；对于厂商信息而言，指代的为金融自助设备的生产厂商；对于银行信息而言，指代的是使用该金融自助设备的银行；对于使用权

限而言,当所述主密钥证书的使用权限为普通用户时,则所述普通用户可使用所述测试工具,当所述主密钥证书的使用权限为高级用户时,则所述高级用户可使用或修改所述测试工具。

在每次将认证装置与金融自助设备相连接时,还需要清除认证装置内预先存储的第一授权信息、第二授权信息和从密钥证书等认证信息,因为上一次认证装置与金融自助设备连接时,有一些认证信息还存储在认证装置中,所以为了避免上一次的认证信息会干扰到本次的认证操作,所以需要清空认证装置内部的认证信息。

5 步骤 S12、在接收到所述金融自助设备发送的第一授权信息后,则向所述金融自助设备发送用户输入的用户信息,所述第一授权信息为所述金融自助设备判断所述主密钥证书为合法证书后发送的信息;

其中,用户信息可以为用户名和密码,密码具体可以为静态密码和/或动态密码。

15 步骤 S13、在接收到所述金融自助设备发送的第二授权信息后,则在根据所述用户信息生成对应的从密钥证书,所述第二授权信息为所述金融自助设备判断所述用户信息为合法信息后发送的信息;

其中,在生成对应的从密钥证书之后,为了保证从密钥证书的安全,避免对外泄露,还需要将所述从密钥证书进行加密,并将加密后的从密钥证书保存在所述认证装置内部的隐藏区域中。

20 步骤 S14、当接收到所述金融自助设备发送的执行所述测试工具的指令时,判断所述用户信息是否具有对应的从密钥证书,若是,则执行所述测试工具;否则,不予执行。

其中,每一次使用测试工具前,都需要判断该用户信息是否对应有从密钥证书,从而实现了每一次使用测试工具都需要合法授权才能够使用。

25 在图 1 所示的实施例,需要分别对主密钥证书和用户信息的正确性进行判断,以便对认证装置的权限和维护人员的身份进行双重认证,如果认证装置丢失或被盗,只要输入的用户信息不正确,那么就无法使用该认证装置内部的测试工具;如果输入的用户信息正确,但是认证装置无法提供正确的主密钥证书,那么也无法使用该认证装置内部的测试工具,因此,本发明提供的双重认证的方式提高了金融自助设备的安全性。

30

在图 1 所示的实施例中,在本实施例执行的过程中,都需要记录每个过程的执行,这样实现了对所有事件的跟踪。如果工作人员未经授权在内部使用认证装置,或者工作人员将认证装置带出内部环境使用、或者认证装置遭受病毒感染,都会被记录下来,所以便于对认证装置的非法使用进行查询。

5

实施例二

请参见图 2 所示,图 2 所示的为一种基于金融自助设备的认证方法,该方法应用于可与认证装置相连接的所述金融自助设备,所述认证装置内存储有测试工具,该方法包括:

10 步骤 S21、当所述认证装置与所述金融自助设备相连接时,获取所述认证装置预先存储的主密钥证书;

其中,主密钥证书包括该认证装置的有效期限、厂商信息、银行信息和使用权限。对于认证装置的有效期限而言,如果当前的时间不在有效期限内,那么该主密钥证书就会作废;对于厂商信息而言,指代的为金融自助设备的生产
15 厂商;对于银行信息而言,指代的是使用该金融自助设备的银行;对于使用权限而言,当所述主密钥证书的使用权限为普通用户时,则所述普通用户可使用所述测试工具,当所述主密钥证书的使用权限为高级用户时,则所述高级用户可使用或修改所述测试工具。

20 步骤 S22、当判断出所述主密钥证书为合法证书时,则向所述认证装置发送第一授权信息,并获取用户输入的用户信息;

其中,用户信息可以为用户名和密码,密码具体可以为静态密码和/或动态密码。

步骤 S23、当判断出所述用户信息为合法信息时,则向所述认证装置发送第二授权信息;

25 步骤 S24、向所述认证装置发送执行所述测试工具的指令。

在图 2 所示的实施例中,需要分别对主密钥证书和用户信息的正确性进行判断,以便对认证装置的权限和维护人员的身份进行双重认证,如果认证装置丢失或被盗,只要输入的用户信息不正确,那么就无法使用该认证装置内部的测试工具;如果输入的用户信息正确,但是认证装置无法提供正确的主密钥证
30 书,那么也无法使用该认证装置内部的测试工具,因此,本发明提供的双重认

证的方式提高了金融自助设备的安全性。

实施例三

请参见图 3 所示，图 3 所示的为一种基于金融自助设备的认证装置 1，该
5 认证装置包括第一发送模块 11，用于当所述认证装置 1 与所述金融自助设备 2
相连接时，将所述认证装置 1 预先存储的主密钥证书发送至所述金融自助设备
2；第一接收模块 12，用于接收所述金融自助设备 2 发送的第一授权信息，所
述第一授权信息为所述金融自助设备 2 判断所述主密钥证书为合法证书后发
送的信息；第二发送模块 13，用于在所述第一接收模块 12 接收到所述第一授
10 权信息后，则向所述金融自助设备 2 发送用户信息；第二接收模块 14，用于
接收到所述金融自助设备 2 发送的第二授权信息，所述第二授权信息为所述金
融自助设备 2 判断所述用户信息为合法信息后发送的信息；从密钥证书生成模
块 15，用于在所述第二接收模块 14 接收到第二授权信息后，则在根据所述用
户信息生成对应的从密钥证书；第三接收模块 16，用于接收所述金融自助设
15 备 2 发送的执行所述测试工具的指令；从密钥证书检测模块 17，用于在所述
第三接收模块 16 接收到执行所述测试工具的指令时，判断所述用户信息是否
具有对应的从密钥证书，若是，则执行所述测试工具；否则，不予执行。

在图 3 所示的实施例中，由于本实施例与实施例一所述的方法相对应，所
以关于实施例三的模块的功能请参见实施例一对应的部分，在此不再赘述。

20

实施例四

请参见图 4 所示，图 4 所示的为另一种基于金融自助设备的认证装置 3，
该认证装置 3 包括 5 个功能模块，分别为登陆模块 31、测试工具模块 32、用
户证书授权模块 33、事件跟踪模块 34 和安全初始化模块 35；其中，将认证装
25 置 3 的硬件存储区域划分为 4 个区域，分别为 CDROM 区域、工作区域、备
份区域、隐藏区域，这几个区域分别承载着上述的功能模块，这 4 个分区域用
途与功能分别如下：CDROM 区域为存放维护登陆程序并加密禁用设置；工作
区域为存放常用的测试程序并为普通授权的用户提供使用；备份区域是存放工
作区域的安装工作的安装包为高级用户权限访问区域；隐藏区域又分为：授权
30 证书区与事件跟踪区，为隐藏状态不对外公开作为后台管理类使用，其中的授

权区存放的是所有授权信息，也事件跟踪区存放的是日志系统信息。具体的：

登陆模块 31 设置在 CDROM 区域中。管理维护者使用认证装置 3 时，通过登陆金融自助设备的系统提供用户身份验证机制，合法的用户登录金融自助设备的系统将调用用户授权模块 33，对该用户进行授权，并生成从密钥证书，
5 否则不予授权并结束，同时调用事件跟踪模块 34 对登录过程的事件进行记录与跟踪。

测试工具模块 32 设置在工作区域中。金融自助设备执行认证装置 3 内的测试工具时，首先调用用户授权模块 33 检测是否经过了合法授权认证，授权合法给予其执行，否则不予其执行，同时调用事件跟踪模块 34 对登录过程的事件进行记录与跟踪。
10

用户授权模块 33 设置在隐藏区域的授权证书区中。用户授权模块 33 包括用户从密钥证书授权单元程序和授权证书检测单元程序两个部分，本模块用户不可替代。更进一步说，其中从密钥证书授权单元程序，通过调用登陆模块来对用户身份验证后再通过该模块生成从密钥授权证书，并通过其授权证书检测
15 单元程序对授权证书进行监测。

事件跟踪模块 34 设置在隐藏区域的事件跟踪区中，提供维护管理用户登陆、授权、执行期测试工具等事件的记录与追踪。

安全初始化模块 35 设置在认证装置 3 中。当认证装置 3 插入金融自助设备后，对认证装置 3 进行初始化设置，并清除历史授权信息记录。

20 在图 4 所示的实施例 4 中，实现了以下技术效果：1、测试自助设备均做到维护人员身份认证；2、每一次测试实现合法授权测试；3、测试内容实现了事件跟踪。因此，本发明提供的实施例在每次使用测试工具进行测试之前都需要安全授权与双重证书的认证，从而提升了自助设备测试过程中的安全性，有效控制测试期间金融自助设备内的客户资金安全的风险。

25 需要说明的是，图 1 至图 4 所示的实施例只是本发明所介绍的优选实施例，本领域技术人员在此基础上，完全可以设计出更多的实施例，因此不在此处赘述。

对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它
30 实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要

符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求

1、一种基于金融自助设备的认证方法，应用于可与所述金融自助设备相连接的认证装置，所述认证装置内存储有测试工具，其特征在于，包括：

当所述认证装置与所述金融自助设备相连接时，将所述认证装置预先存储的主密钥证书发送至所述金融自助设备；

在接收到所述金融自助设备发送的第一授权信息后，则向所述金融自助设备发送用户输入的用户信息，所述第一授权信息为所述金融自助设备判断所述主密钥证书为合法证书后发送的信息；

在接收到所述金融自助设备发送的第二授权信息后，则在根据所述用户信息生成对应的从密钥证书，所述第二授权信息为所述金融自助设备判断所述用户信息为合法信息后发送的信息；

当接收到所述金融自助设备发送的执行所述测试工具的指令时，判断所述用户信息是否具有对应的从密钥证书，若是，则执行所述测试工具；否则，不予执行。

2、根据权利要求 1 所述的基于金融自助设备的认证方法，其特征在于，所述主密钥证书包括有效期限、厂商信息、银行信息和使用权限。

3、根据权利要求 1 所述的基于金融自助设备的认证方法，其特征在于，当所述认证装置与所述金融自助设备相连接时，还包括：

清除所述认证装置内预先存储的第一授权信息、第二授权信息和从密钥证书。

4、根据权利要求 1 所述的基于金融自助设备的认证方法，其特征在于，在执行所述测试工具时，还包括：

记录执行所述测试工具的整个过程。

5、根据权利要求 1 所述的基于金融自助设备的认证方法，其特征在于，

在根据所述用户信息生成对应的从密钥证书的步骤后，还包括：

将所述从密钥证书进行加密；

将加密后的从密钥证书保存在所述认证装置内部的隐藏区域。

5 6、根据权利要求 2 所述的基于金融自助设备的认证方法，其特征在于，
当所述主密钥证书的使用权限为普通用户时，则所述普通用户可使用所述测试工具。

7、根据权利要求 2 所述的基于金融自助设备的认证方法，其特征在于，
当所述主密钥证书的使用权限为高级用户时，则所述高级用户可使用或修改所述测试工具。

10 8、一种基于金融自助设备的认证方法，应用于可与认证装置相连接的所述金融自助设备，所述认证装置内存储有测试工具，其特征在于，包括：

当所述认证装置与所述金融自助设备相连接时，获取所述认证装置预先存储的主密钥证书；

15 当判断出所述主密钥证书为合法证书时，则向所述认证装置发送第一授权信息，并获取用户输入的用户信息；

当判断出所述用户信息为合法信息时，则向所述认证装置发送第二授权信息；

向所述认证装置发送执行所述测试工具的指令。

20 9、一种基于金融自助设备的认证装置，所述认证装置可与所述金融自助设备相连接，所述认证装置内存储有测试工具，其特征在于，包括：

第一发送模块，用于当所述认证装置与所述金融自助设备相连接时，将所述认证装置预先存储的主密钥证书发送至所述金融自助设备；

第一接收模块，用于接收所述金融自助设备发送的第一授权信息，所述第一授权信息为所述金融自助设备判断所述主密钥证书为合法证书后发送的信

息;

第二发送模块,用于在所述第一接收模块接收到所述第一授权信息后,则向所述金融自助设备发送用户信息;

第二接收模块,用于接收到所述金融自助设备发送的第二授权信息,所述

5 第二授权信息为所述金融自助设备判断所述用户信息为合法信息后发送的信息;

从密钥证书生成模块,用于在所述第二接收模块接收到第二授权信息后,则在根据所述用户信息生成对应的从密钥证书;

10 第三接收模块,用于接收所述金融自助设备发送的执行所述测试工具的指令;

从密钥证书检测模块,用于在所述第三接收模块接收到执行所述测试工具的指令时,判断所述用户信息是否具有对应的从密钥证书,若是,则执行所述测试工具;否则,不予执行。

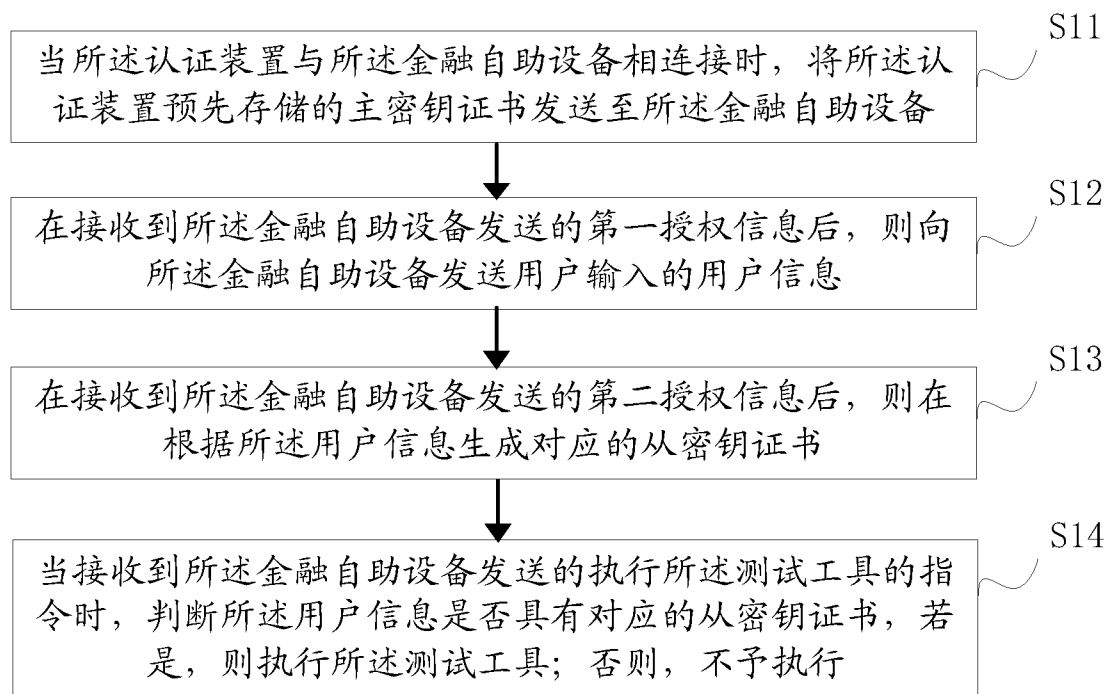


图 1

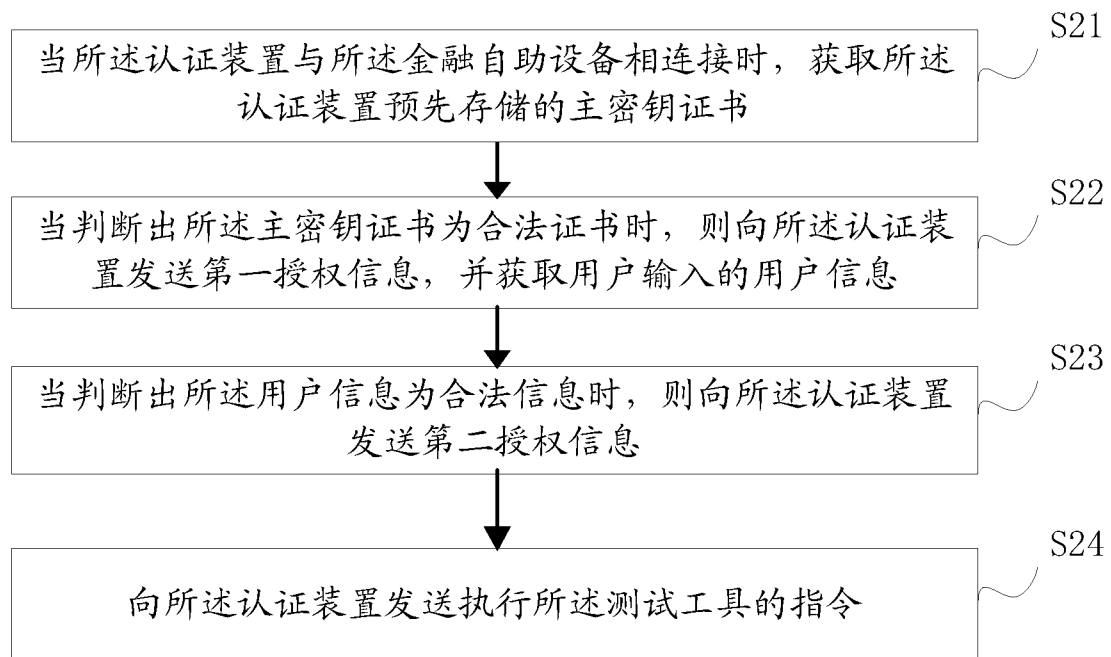


图 2

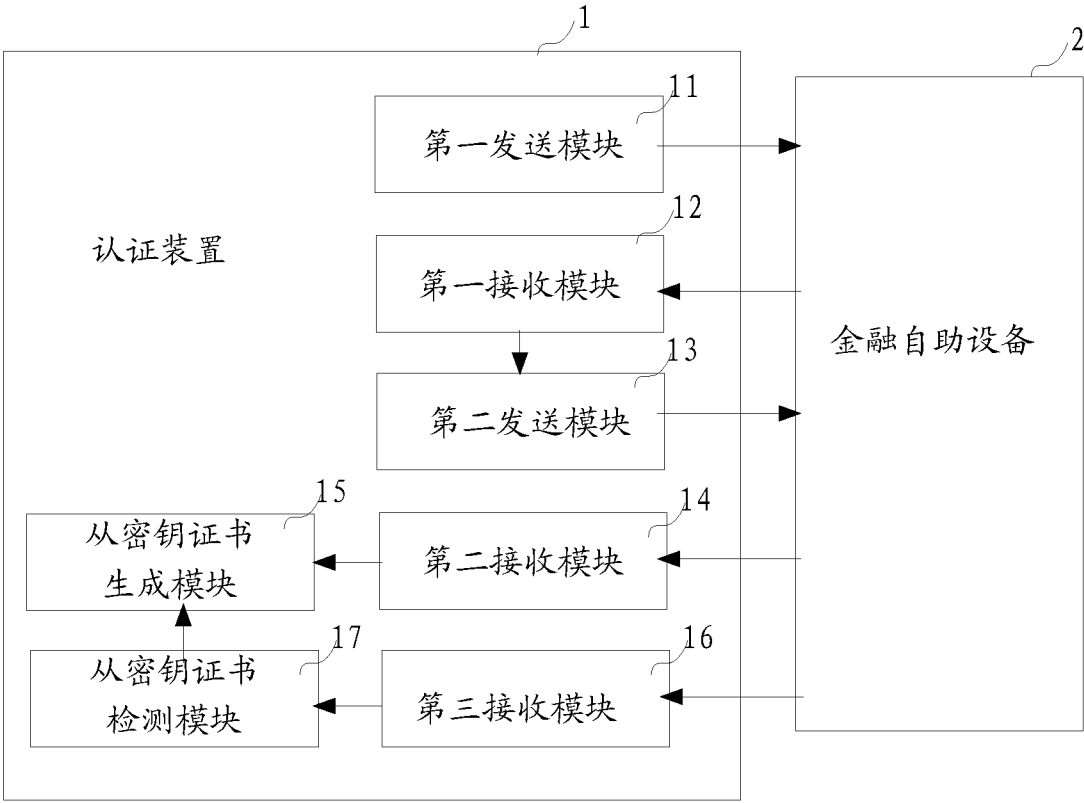


图 3

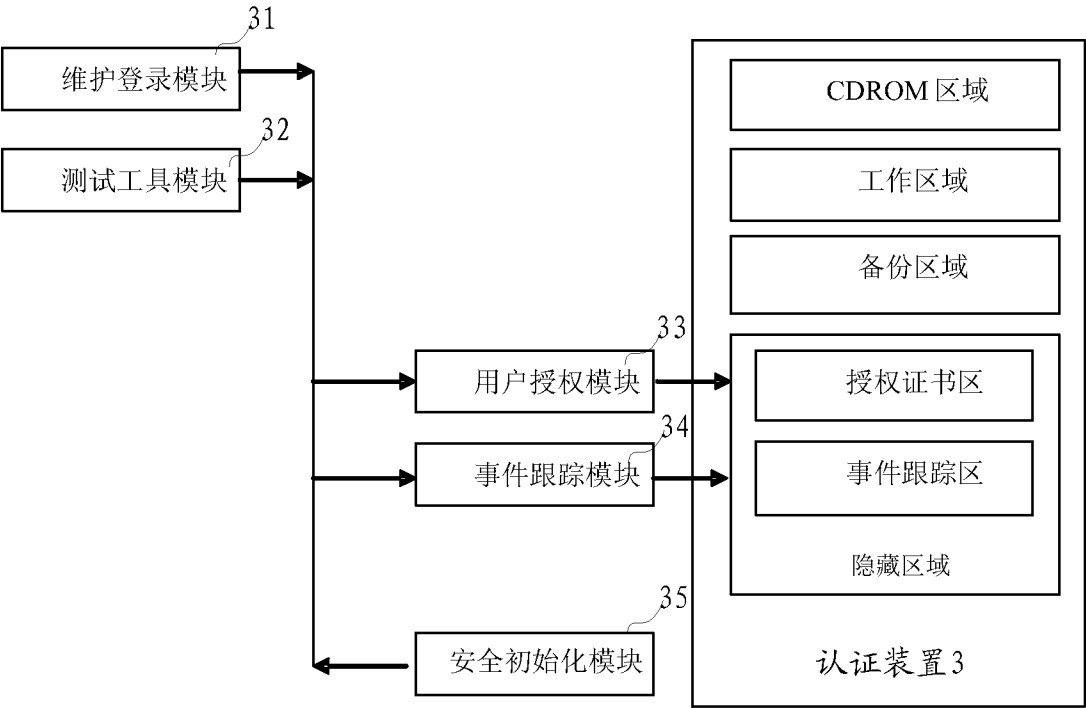


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/078879

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L 9/-; G06F 21/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, GOOGLE, financial, bank, equipment, apparatus, ATM, test, user information, authenticate, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102404112 A (ANCHORTECH (BEIJING) TECHNOLOGY CO.,LTD) 04 April 2012 (04.04.2012) description, pages 2 and 3 and figure 3	1-9
PX	CN 103107884 A (GRG BANKING EQUIPMENT CO., LTD) 15 May 2013 (15.05.2013) claims 1-9	1-9
A	CN 101145903 A (ZTE CORPORATION) 19 March 2008 (19.03.2008) the whole document	1-9
A	CN 101350723 A (BEIJING ITRUSCHINA CO., LTD) 21 January 2009 (21.01.2009) the whole document	1-9
A	US 2007061871 A1 (SIMPKINS, Ryan et al.) 15 March 2007 (15.03.2007) the whole document	1-9
A	US 2001017584 A1 (SHINZAKI, Takashi) 30 October 2001 (30.08.2001) the whole document	1-9

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	
“A” document defining the general state of the art which is not considered to be of particular relevance	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E” earlier application or patent but published on or after the international filing date	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	“&”document member of the same patent family

Date of the actual completion of the international search 25 September 2013 (25.09.2013)	Date of mailing of the international search report 17 October 2013 (17.10.2013)
---	--

Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer DONG, Libo Telephone No. (86-10) 61648110
---	--

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/078879

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102404112 A	04.04.2012	None	
CN 103107884 A	15.05.2013	None	
CN 101350723 A	21.01.2009	None	
CN 101145903 A	19.03.2008	WO 2009052676A1	30.04.2009
US 2007061871 A1	15.03.2007	None	
US 2001017584 A1	30.08.2001	JP 2001236324 A	31.08.2001
		DE 10105396 A1	20.09.2001

国际检索报告

 国际申请号
PCT/CN2013/078879
A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L 9/-, G06F21/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

数据库: CNPAT,CNKI,WPI,EPODOC,GOOGLE

 检索词: 金融,银行,设备,装置,测试,用户身份,柜员机,取款机,认证,验证,鉴权,financial, bank, equipment,
 apparatus, ATM, test, user information, authenticate, verify
C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN102404112A (清大安科(北京)科技有限公司) 04.4 月 2012 (04.04.2012) 说明书第 2-3 页,附图 3	1-9
PX	CN103107884A (广州广电运通金融电子股份有限公司) 15.5 月 2013 (15.05.2013) 权利要求 1-9	1-9
A	CN101145903A (中兴通讯股份有限公司) 19.3 月 2008 (19.03.2008) 全文	1-9
A	CN101350723A (北京天威诚信电子商务服务有限公司) 21.1 月 2009 (21.01.2009) 全文	1-9
A	US2007061871A1 (SIMPKINS, Ryan et al.) 15.3 月 2007 (15.03.2007) 全文	1-9
A	US2001017584A1 (SHINZAKI, Takashi) 30.8 月 2001 (30.08.2001) 全文	1-9

☐ 其余文件在 C 栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇
 引用文件的公布日而引用的或者因其他特殊理由而引
 用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了
理解发明之理论或原理的在后文件
 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的
 发明不是新颖的或不具有创造性

 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件
 结合并且这种结合对于本领域技术人员为显而易见时,
 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

25.9 月 2013 (25.09.2013)

国际检索报告邮寄日期

17.10 月 2013 (17.10.2013)

ISA/CN 的名称和邮寄地址:

 中华人民共和国国家知识产权局
 中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

董立波电话号码: (86-10) **61648110**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/078879

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN102404112A	04.04.2012	无	
CN103107884A	15.05.2013	无	
CN101350723A	21.01.2009	无	
CN101145903A	19.03.2008	WO2009052676A1	30.04.2009
US2007061871A1	15.03.2007	无	
US2001017584A1	30.08.2001	JP2001236324A	31.08.2001
		DE10105396A1	20.09.2001