

(12) 实用新型专利

(10) 授权公告号 CN 202771546 U

(45) 授权公告日 2013. 03. 06

(21) 申请号 201220296399. 9

(ESM) 同样的发明创造已同日申请发明专利

(22) 申请日 2012. 06. 19

(73) 专利权人 中国工商银行股份有限公司  
地址 100140 北京市西城区复兴门内大街  
55 号

(72) 发明人 靳如森 张颖 李兴双 嵇津湘  
骆伯俊 罗伟

(74) 专利代理机构 北京三友知识产权代理有限  
公司 11127  
代理人 任默闻

(51) Int. Cl.  
G07F 19/00(2006. 01)  
G07F 9/00(2006. 01)

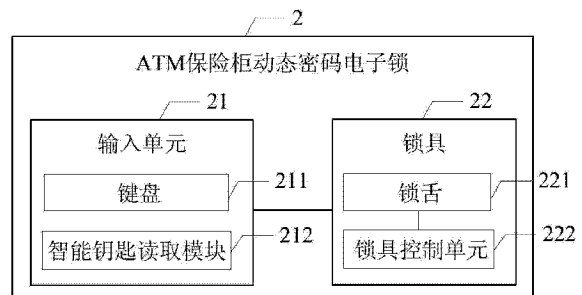
权利要求书 1 页 说明书 10 页 附图 9 页

(54) 实用新型名称

ATM 及 ATM 的安全认证系统

(57) 摘要

本实用新型提供一种 ATM 及 ATM 的安全认证系统, 其中, 该 ATM 包括 ATM 本体、用户身份认证单元和 ATM 保险柜动态密码电子锁, 其中, 用户身份认证单元包括: 用户信息接收模块, 用于接收外部输入的用户 ID 和密码; 用户信息发送模块, 用于将用户 ID 和密码发送给后台服务器, 以使后台服务器在对用户 ID 和密码认证成功时, 生成一次性开锁密码; ATM 保险柜动态密码电子锁包括: 输入单元, 包括键盘, 用于接收外部输入的一次性开锁密码; 智能钥匙读取模块, 用于读取智能钥匙信息; 锁具, 与输入单元连接, 包括: 锁舌; 锁具控制单元, 用于在对一次性开锁密码、和智能钥匙信息认证成功时, 控制锁舌活动以开启 ATM 保险柜动态密码电子锁。通过本实用新型, 可以提高 ATM 保险柜锁的安全性。



1. 一种 ATM,所述 ATM 包括 ATM 本体,其特征在于,所述的 ATM 还包括 ATM 保险柜动态密码电子锁,其中,

所述的 ATM 保险柜动态密码电子锁包括:

输入单元,包括:

输入一次性开锁密码的键盘;

读取智能钥匙信息的智能钥匙读写器;

锁具,与所述的输入单元连接,包括:

锁舌;

控制所述锁舌活动以开启所述 ATM 保险柜动态密码电子锁的电路控制部件,与所述的锁舌连接。

2. 根据权利要求 1 所述的 ATM,其特征在于,所述的 ATM 保险柜动态密码电子锁还包括:

转盘,

发电机,与所述的转盘连接,

超级电容,与所述的发电机连接,

通过外力转动所述转盘,所述转盘带动所述发电机的线圈旋转,所述发电机的线圈产生电压并提供给所述的超级电容充电,以激活所述的锁具控制单元控制所述锁舌活动。

3. 根据权利要求 1 所述的 ATM,其特征在于,所述的 ATM 保险柜动态密码电子锁还包括:

液晶显示屏,用于显示外部输入的一次性开锁密码以及所述 ATM 保险柜动态密码电子锁的提示信息。

4. 根据权利要求 1 所述的 ATM,其特征在于,所述的 ATM 保险柜动态密码电子锁还包括:

摄像头,连接后台服务器。

5. 一种 ATM 的安全认证系统,其特征在于,所述的系统包括如权利要求 1 至 4 中任一项所述的 ATM、后台服务器、智能钥匙、以及用户终端,所述的 ATM 与所述的后台服务器连接。

## ATM 及 ATM 的安全认证系统

### 技术领域

[0001] 本实用新型涉及银行计算机网络,具体地,涉及一种 ATM 及 ATM 的安全认证系统。

### 背景技术

[0002] 目前业界自动柜员机(简称 ATM,包括自动取款机和存取款一体机,下同)设备保险柜按照《自动柜员机(ATM)通用规范(GB/T 18789-2002)》要求配置了两把锁:一把机械锁和一把机械密码锁,在日常加钞和维护开锁时一人持钥匙、一人持密码,闭锁时操作人员要旋转密码锁上的密码转盘,将密码打乱。

[0003] 近年来,随着银行零售业务的发展,银行自助设备数量不断增长。但是,现有 ATM 保险柜锁在使用过程中存在以下缺陷:

[0004] 1、密码和钥匙分别专人保管,管理成本较高,并存在失窃风险;

[0005] 2、尽管银行针对保险柜锁的钥匙和密码制定了管理办法,但现有制度的落实仅依靠人工控制,使得操作制度落实不到位,比如保险柜门关闭没有打乱密码,密码不能定期更换、人员变动没有及时更换密码等,从而导致安全隐患。近年来,随着设备数量的增长,针对 ATM 保险柜的安全案件也有所增多。

[0006] 3、缺乏保险柜开关记录,不具备实时监控锁开关状态的条件,不能验证开锁人的身份,没有安全核查和审计功能;

[0007] 因此,现有 ATM 保险柜锁存在潜在的安全隐患,并且运行管理成本较高,随着设备数量的增加,管理的难度和风险逐步增大,不能很好地满足实际应用的需要。

### 实用新型内容

[0008] 本实用新型实施例的主要目的在于提供一种 ATM 及 ATM 的安全认证系统,以解决现有技术中的 ATM 保险柜锁存在的安全性较低的问题。

[0009] 为了实现上述目的,本实用新型实施例提供一种 ATM,所述 ATM 包括 ATM 本体,所述的 ATM 还包括用户身份认证单元和 ATM 保险柜动态密码电子锁,其中,所述的用户身份认证单元包括:用户信息接收模块,用于接收外部输入的用户 ID 和密码;用户信息发送模块,与所述的用户信息发送模块连接,用于将所述的用户 ID 和密码发送给后台服务器,以使所述后台服务器在对所述的用户 ID 和密码认证成功时,生成一次性开锁密码;所述的 ATM 保险柜动态密码电子锁包括:输入单元,包括键盘,用于接收外部输入的所述一次性开锁密码;智能钥匙读取模块,用于读取智能钥匙信息;锁具,与所述的输入单元连接,包括:锁舌;锁具控制单元,与所述的锁舌连接,用于在对所述一次性开锁密码、和所述智能钥匙信息认证成功时,控制所述锁舌活动以开启所述 ATM 保险柜动态密码电子锁。

[0010] 所述的 ATM 保险柜动态密码电子锁还包括:转盘,发电机,与所述的转盘连接,超级电容,与所述的发电机连接,通过外力转动所述转盘,所述转盘带动所述发电机的线圈旋转,所述发电机的线圈产生电压并提供给所述的超级电容充电,以激活所述的锁具控制单元控制所述锁舌活动。

[0011] 所述的 ATM 保险柜动态密码电子锁还包括：液晶显示屏，用于显示外部输入的一次性开锁密码以及所述 ATM 保险柜动态密码电子锁的提示信息。

[0012] 所述的锁具控制单元控制所述锁舌在预定时间内活动。

[0013] 所述的 ATM 保险柜动态密码电子锁还包括：锁具状态信息获取单元，与所述的锁舌和保险柜门连接，用于获取所述的 ATM 保险柜动态密码电子锁的锁舌状态信息和保险柜门状态信息；锁具状态信息发送单元，与所述的锁具状态信息获取单元连接，用于将所述的 ATM 保险柜动态密码电子锁的锁舌状态信息和保险柜门状态信息发送给所述后台服务器。

[0014] 所述的 ATM 保险柜动态密码电子锁还包括：摄像头，用于对所述 ATM 周围的情况进行摄像；视频传送单元，与所述的摄像头连接，用于将所述摄像头拍摄的视频传送给所述后台服务器。

[0015] 所述的 ATM 保险柜动态密码电子锁还包括：预警单元，用于在所述 ATM 周围存在安全问题时，启动预警流程。

[0016] 本实用新型实施例还提供一种 ATM 的安全认证系统，该系统包括：上述的 ATM、后台服务器、智能钥匙、以及用户终端，所述的 ATM 与所述的后台服务器连接，所述的 ATM 接收用户输入的用户 ID 和密码并发送给所述后台服务器，所述后台服务器在对所述的用户 ID 和密码认证成功时，生成一次性开锁密码并发送给所述用户终端，所述 ATM 保险柜动态密码电子锁接收用户输入的所述一次性开锁密码和读取所述智能钥匙的信息，在对所述一次性开锁密码、和所述智能钥匙信息认证成功时，控制所述锁舌活动以开启所述 ATM 保险柜动态密码电子锁。

[0017] 借助于上述技术方案至少之一，通过用户身份认证单元接收用户的认证信息后发送给后台服务器，以由后台服务器生成一次性开锁密码并发送给用户，用户根据一次性开锁密码和智能钥匙开启 ATM 保险柜动态密码电子锁，以执行加钞等操作，相比于现有技术中，本实用新型实施例的 ATM 保险柜锁安全性较高。

## 附图说明

[0018] 为了更清楚地说明本实用新型实施例或现有技术中的技术方案，下面将对实施例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实用新型的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0019] 图 1 是根据本实用新型实施例的 ATM 的结构示意图；

[0020] 图 2 是根据本实用新型实施例的用户身份认证单元的结构示意图；

[0021] 图 3a 是根据本实用新型实施例的 ATM 保险柜动态密码电子锁的结构示意图；

[0022] 图 3b 是根据本实用新型实施例的 ATM 保险柜动态密码电子锁的另一结构示意图；

[0023] 图 4 是根据本实用新型实施例的 ATM 的具体结构示意图；

[0024] 图 5 是根据本实用新型实施例的动态密码电子锁的具体结构示意图；

[0025] 图 6 是银行工作人员进行加钞或维修 ATM 保险柜的流程图；

[0026] 图 7 是根据本实用新型实施例的安全认证系统的详细结构示意图；

[0027] 图 8 是根据本实用新型实施例的动态密码认证的自动柜员机的连接示意图；

- [0028] 图 9 是根据本实用新型实施例的智能钥匙读写部件的结构示意图；
- [0029] 图 10 是根据本实用新型实施例的客户端的结构示意图；
- [0030] 图 11 是根据本实用新型实施例的服务提供装置的结构示意图；
- [0031] 图 12 是根据本实用新型实施例的监控和管理部件的结构示意图；
- [0032] 图 13 是根据本实用新型实施例的给 ATM 加钞的具体流程图；
- [0033] 图 14 是根据本实用新型实施例的系统启动预警处理流程的异常情况示意图；
- [0034] 图 15 是根据本实用新型实施例的远程集中授权系统的结构示意图。

### 具体实施方式

[0035] 下面将结合本实用新型实施例中的附图,对本实用新型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实用新型一部分实施例,而不是全部的实施例。基于本实用新型中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本实用新型保护的范围。

[0036] 本实用新型实施例提供一种 ATM 及 ATM 的安全认证系统。以下结合附图对本实用新型进行详细说明。

[0037] 实施例一

[0038] 本实用新型实施例提供一种 ATM,该 ATM 包括:ATM 本体(图中未示出),以及图 1 所示的用户身份认证单元 1 和 ATM 保险柜动态密码电子锁 2,现有的 ATM 为机械密码锁,安全系数较低。

[0039] 以下详细描述用户身份认证单元 1 和 ATM 保险柜动态密码电子锁 2。

[0040] 如图 2 所示,用户身份认证单元 1 包括:

[0041] 用户信息接收模块 11,用于接收外部输入的用户 ID 和密码;

[0042] 用户信息发送模块 12,与用户信息发送模块连接,用于将用户 ID 和密码发送给后台服务器,以使后台服务器在对用户 ID 和密码认证成功时,生成一次性开锁密码;

[0043] 如图 3a 所示,ATM 保险柜动态密码电子锁 2 包括:

[0044] 输入单元 21,包括:

[0045] 键盘 211,用于接收外部输入的一次性开锁密码;

[0046] 智能钥匙读取模块 212,用于读取智能钥匙信息;

[0047] 锁具 22,与输入单元连接,包括:

[0048] 锁舌 221;

[0049] 锁具控制单元 222,与锁舌连接,用于在对一次性开锁密码、和智能钥匙信息认证成功时,控制锁舌活动以开启 ATM 保险柜动态密码电子锁。

[0050] 由以上描述可以看出,通过用户身份认证单元接收用户的认证信息后发送给后台服务器,以由后台服务器生成一次性开锁密码并发送给用户,之后用户根据一次性开锁密码和智能钥匙开启 ATM 保险柜动态密码电子锁,以执行加钞等操作,相比于现有技术中,本实用新型实施例的 ATM 保险柜锁安全性较高。

[0051] 如图 3b 所示,上述的 ATM 保险柜动态密码电子锁还包括:

[0052] 转盘 23,

[0053] 发电机 24,与转盘连接,

[0054] 超级电容 25,与发电机连接,

[0055] 通过外力转动转盘,转盘带动发电机的线圈旋转,发电机的线圈产生电压并提供给超级电容充电,以激活锁具控制单元控制锁舌活动。

[0056] 在具体实施时,ATM 保险柜动态密码电子锁还包括:液晶显示屏,用于显示外部输入的一次性开锁密码以及 ATM 保险柜动态密码电子锁的提示信息,以方便用户的使用。

[0057] 在用户操作 ATM 保险柜的过程中,锁具控制单元可以控制锁舌在预定时间内活动,例如,时间为 5 秒,超过 5 秒如果开启工作还未执行,则锁舌恢复至锁定位置。

[0058] 在操作中,ATM 保险柜动态密码电子锁还可以包括:

[0059] 锁具状态信息获取单元,与锁舌和保险柜门连接,用于获取 ATM 保险柜动态密码电子锁的锁舌状态信息和保险柜门状态信息;

[0060] 锁具状态信息发送单元,与锁具状态信息获取单元连接,用于将 ATM 保险柜动态密码电子锁的锁舌状态信息和保险柜门状态信息发送给后台服务器。

[0061] 通过上述的锁具状态信息获取和发送单元,可以使得后台服务器及时掌握 ATM 保险柜的动态,提高 ATM 保险柜操作的安全性。

[0062] 为了进一步提高 ATM 保险柜操作的安全性,ATM 保险柜动态密码电子锁还可以包括:

[0063] 摄像头,用于对 ATM 周围的情况进行摄像;

[0064] 视频传送单元,与摄像头连接,用于将摄像头拍摄的视频传送给后台服务器。

[0065] 通过摄像头和视频传送单元,使得后台服务器可以清晰的看到 ATM 保险柜周围的情况,为及时发现意外情况提供了保障,从而进一步提高了安全性。

[0066] 相应地,ATM 保险柜动态密码电子锁还包括:预警单元,用于在 ATM 周围存在安全问题时,启动预警流程。

[0067] 以下给出一实例。

[0068] 如图 4 所示,是根据本实用新型实施例的一种 ATM,该 ATM 机是对现有 ATM 机进行了改进,将现有 ATM 机上的机械锁替换为动态密码电子锁。参照图 4,本实用新型实施例的 ATM 包括位于上箱体的工控机 11、显示器 12、密码键盘 13、凭条打印机 14、流水打印机 15、读卡器 16、加密模块 17 等部件,以及位于下箱体的现金处理模块 18、钞箱 19、保险柜 10、动态密码电子锁 1a 等部件组成。

[0069] 如图 5 所示,动态密码电子锁,由输入单元和锁具组成,输入单元安装在 ATM 保险柜外柜门上,锁具安装在 ATM 保险柜门内,输入单元通过一根电缆穿过保险柜门上的锁孔同锁具进行连接。输入单元包括键盘、液晶显示屏、转盘、智能钥匙读写器。键盘由 12 个触控反馈键组成,用于输入一次性开锁口令或执行其他管理功能。液晶显示屏为 3 字符液晶显示(带蜂鸣器)部件,输出用户在通过键盘输入的信息,以及锁的提示、报警信息。转盘用于自发电,旋转转盘带动发电机进行发电并把产生的电流存储进锁具内部的超级电容。钥匙读取器用于读取用户钥匙信息,从而校验开锁钥匙(或人员);同时也是管理钥匙的接口,用于执行管理功能(稽核、激活、时间设置和同步等功能)。锁具包括电路控制部件、发电机、超级电容、锁舌和外部通讯接口。电路控制部件是动态密码电子锁的控制中心,控制其它部件与用户进行交互,并负责一次性开锁口令的验证。发电机与输入单元的转盘相连接,通过转动转盘带动发动机线圈的旋转,线圈的快速旋转使得发电机线圈产生电流,发电机线圈

的输出经过整流,从交流电压变为直流电压,并提供给超级电容。一旦超级电容充电到适当的电压,控制锁具功能的电路控制部件将被激活,从而锁具可以进行操作。锁舌是用来控制保险柜门栓是否可以打开的机械装置。锁具通过外部通讯接口与 ATM 工控机相连或者直接与银行网络相连,提供监控和管理功能。

[0070] 用户通过键盘输入一次性开锁口令,如果开锁口令正确并通过智能钥匙读写器读取了正确的钥匙,电路控制部件的驱动电路将激活锁具内的马达解锁活动锁舌,允许活动锁舌旋转到开启位置,此时就可将保险柜门栓从关闭位置释放到开启位置。开启动作需要在一定时间内(比如 4 秒)执行,否则马达将回位,从而阻止活动锁舌旋转到开启位置。保险柜门栓开启后的一定时间内马达将释放,从而允许活动锁舌自动恢复到锁定位置。当保险柜门栓回到关闭位置,就可以让活动锁舌自动旋转到关闭位置,保险柜门和锁将再次关闭。

[0071] 本实用新型实施例提供的动态密码电子锁相对于现有技术中的机械密码锁,采用了“一次一密”的动态密码开锁模式,每个密码仅能使用一次,避免静态密码泄露导致的安全隐患;不需要外部电源(如电池等)供电,在转动转盘时的摩擦能提供自我供电,也可由 ATM 通过 USB 接口供电;开锁人员只要关闭保险柜门,通过保险柜门上安装的门磁感应器触发自动落锁。当保险柜门关闭后,门磁感应器感应并将信号输入到密码锁,密码锁的马达启动并带动锁舌伸出实现落锁动作,避免了保险柜门关闭但没有落锁的情况发生;锁通过银行内部网络与后台系统相连,可联机把锁和保险柜门开闭的实时状态上报后台系统,也可提供后台远程管理功能(激活、停用、稽核),为后台管理人员远程监控和管理提供了技术条件。

[0072] 图 6 是银行工作人员进行加钞或维修 ATM 保险柜的流程图,如图 6 所示,该流程包括:

[0073] 步骤 601:开锁申请人员输入开锁人员 ID 和密码,发起开锁请求。

[0074] 步骤 602:后台系统验证申请人身份。

[0075] 步骤 603(可选):授权人员查看现场视频确认申请人身份后,授权开锁请求。

[0076] 步骤 604:后台系统生成一次性开锁口令,通过短信将一次性开锁口令发送开锁申请人员预留手机上。

[0077] 步骤 605:开锁申请人员在动态密码电子锁上输入一次性开锁口令,贴上智能钥匙开锁。动态密码电子锁使用与后台系统相同的算法校验一次性开锁口令,校验通过后锁自动开启。

[0078] 步骤 606:开锁申请人员打开保险柜。

[0079] 步骤 607:动态密码电子锁将锁和保险柜门的实时状态(打开)上报监控系统。

[0080] 步骤 608:开锁申请人员进行正常的业务处理(加钞或者维修)。

[0081] 步骤 609:开锁申请人员关闭保险柜门,动态密码电子锁自动落锁。

[0082] 步骤 610:动态密码电子锁将锁和保险柜门的实时状态(关闭)上报监控系统。

[0083] 对开锁操作人员(或开锁申请人员)的认证方法包括两种:一是后台管理员预先采集开锁操作人员身份信息和预留信息存入服务提供装置的数据库中,操作人员申请开锁时在 ATM 端机输入自己的身份 ID 和预留密码,通过 ATM 和内部网络传送后台,由服务提供装置自动对开锁人员身份进行联机验证的方法;另一个远程集中授权的身份验证方法,就是后台授权人员可通过视频监控系统远程查看开锁人员实时视频图像和 ATM 周边环境图像,

与预先采集的开锁操作人员图像比对,对开锁人员身份进行再次验证,并可确保开锁人员没有被劫持或绑架。方法二作为方法一的辅助手段,实际业务营运过程中可根据需要选择使用。

[0084] 为了保证 ATM 的安全,可以对 ATM 保险柜、保险柜锁开闭状态进行实时监控,具体主要是通过以下方案来实现:使用具备联机功能的动态密码电子锁、保险柜门传感器将保险柜门和锁开闭状态实时上传给后台系统,或后台管理人员联机查询远程 ATM 设备保险柜门、锁的实时开闭状态,如遇异常情况系统自动启动预警处理流程的手段和措施。

[0085] 通过本实用新型实施例,可以确保开锁人员身份合法,后台监控人员可远程监控 ATM 保险柜门和动态密码电子锁的开闭状态,同时系统自动对各种异常情况进行监控并可触发预警流程,降低系统运行的风险,进一步提升 ATM 保险柜锁的安全管理水平。

[0086] 实施例二

[0087] 本实用新型实施例还提供一种 ATM 的安全认证系统,该系统包括上述实施例一中 ATM、以及、后台服务器、智能钥匙、以及用户终端,ATM 与后台服务器连接。其中,ATM 接收用户输入的用户 ID 和密码并发送给后台服务器,后台服务器在对用户 ID 和密码认证成功时,生成一次性开锁密码并发送给用户终端,ATM 保险柜动态密码电子锁接收用户输入的一次性开锁密码和读取智能钥匙的信息,在对一次性开锁密码、和智能钥匙信息认证成功时,控制锁舌活动以开启 ATM 保险柜动态密码电子锁。

[0088] 通过该系统,后台服务器在认证用户身份后生成一次性开锁密码并发送给用户,之后用户根据一次性开锁密码和智能钥匙开启 ATM 保险柜动态密码电子锁,以执行加钞等操作,相比于现有技术中,本实用新型实施例的 ATM 保险柜锁安全性较高。

[0089] 上述 ATM 保险柜动态密码电子锁,使用特定的智能钥匙,也可用固定的静态密码开启。该动态密码电子锁可以以电子的方式记录开锁时间、开锁使用的智能钥匙 ID、开锁使用的动态密码、闭锁时间、闭锁使用的智能钥匙 ID、闭锁代码等信息,为审查稽核锁的操作提供依据。

[0090] 图 7 是根据本实用新型实施例的安全认证系统的详细结构示意图,该系统可实现开锁用户身份联机认证,以及对保险柜锁、保险柜门开闭状态的实时监控。

[0091] 如图 7 所示,该系统包括:动态密码认证的自动柜员机 1、智能钥匙 2、智能钥匙读写部件 3、客户端 4 (包括标准客户端 41 和智能钥匙管理客户端 42)、服务提供装置 5、内部网络 6、监控和管理部件 7。自动柜员机 1 通过内部网络 6 连接服务提供装置 5。智能钥匙读写部件 3 通过 IP 网络端口或通过 USB 口连接服务提供装置 5 所在服务器,主要生成一次性开锁动态密码,或者智能钥匙读写部件 3 通过 USB 口连接智能钥匙管理客户端 42 完成智能钥匙 2 的管理功能。系统客户端 4 通过内部网络 6 以 B/S (浏览器 / 服务器) 的方式访问服务提供装置 5,为用户提供系统的各种服务。

[0092] 以下详细描述各部分。

[0093] 如图 8 所示,动态密码认证的自动柜员机 1 的动态密码电子锁使用 USB 连接线通过网络盒与自动柜员机中的工控机 USB 口相连,也可使用 IP 网络端口直连银行内部网络 6。

[0094] 智能钥匙 2 是一种具备特定电子信息的硬件载体,每条智能钥匙都有唯一的 ID。系统使用智能钥匙读写部件对其电子信息进行读写,并可设置每条钥匙在规定时间内允许打开的动态密码电子锁。开锁人员必须同时使用动态密码和智能钥匙才能开锁。智能钥匙



以电子的方式记录了开锁时间、动态密码电子锁 ID、闭锁时间等信息，便于进行审查稽核。

[0095] 如图 9 所示，智能钥匙读写部件 3 是一种可以对智能钥匙进行管理(包括稽核、激活、删除、修改、时间设置和同步等功能)、并可生成一次性动态密码的硬件设备，由电路控制部件以及与其相连的加密部件、电源、通讯接口、读写接口构成。电路控制部件是整个设备的核心，控制其它部件与外部设备进行交互以及内部逻辑处理。加密部件主要完成一次性动态密码的生成以及读写钥匙电子信息时的加密处理。读写接口是智能钥匙读写部件作为智能钥匙读写设备使用时与智能钥匙的通讯装置。通讯接口是智能钥匙读写部件作为生成一次性动态密码设备使用时与服务提供装置相连的装置，可以是串口、USB 端口、IP 端口的任一种方式。

[0096] 如图 10 所示，系统客户端 4 包括：标准客户端 41 和智能钥匙管理客户端 42，其中：标准客户端 41 是一个安装浏览器的 PC 机，用户使用此客户端可完成两种功能：一是保险柜门、锁开闭状态的实时监控，二是管理功能，包括远程锁管理、稽核查看系统审计信息、加钞/维护任务的管理，系统用户的管理；智能钥匙管理客户端 42 是安装了智能钥匙读写部件设备驱动的 PC 机，使用 USB 接口与智能钥匙读写部件连接实现对钥匙的管理。

[0097] 服务提供装置 5 为一台 PC 服务器(也可以由多台组成，进行负载均衡)，为客户提供 http 应用服务，动态生成 Web 页面文件，提供给标准客户终端和智能钥匙客户端进行交互。

[0098] 如图 11 所示，服务提供装置 5 主要由以下五部分功能构成：

[0099] 用户管理模块 51 主要用于定义用户账号和用户角色，其中：用户账号包括用户 ID、姓名、密码、角色、预留手机号码、照片等；用户角色包括系统管理员、后台授权员色(授权、密码分发)、后台监控员(监控、审计)、后台设备管理员(钥匙、锁)、前台操作员(加钞、维护)的五种基本角色，并按角色分配不同权限。

[0100] 设备(钥匙、锁)管理模块 52 用于锁和钥匙的维护。

[0101] 监控模块 53 用于处理锁和保险柜门上报的实时开闭状态以及后台监控人员远程查看门和锁实时状态命令。

[0102] 业务审批处理模块 54 用于处理业务流程定义、任务的维护、开锁申请审批、动态密码生成、预警事件处理、审计信息调阅、统计分析报表等。在实际操作中，服务提供装置 5 至少得安装有一组业务功能处理模块。

[0103] 外部接口 55 提供与外围系统对接的功能接口，比如与自动语音电话、或人工坐席电话系统对接提供开锁申请的处理，与手机短信通知系统对接提供动态密码以短信的方式发送开锁人员预先绑定的手机，与邮件系统对接可把开锁动态密码以邮件的形式向申请人发送邮件通知等。

[0104] 如图 12 所示，监控和管理部件 7 包括：用于探测保险柜门开闭状态的保险柜门传感器 71、负责协议转换的网络盒 72、USB 连接线 73、用于激活锁和修改开锁静态密码的激活改密插头 74。

[0105] 以下给出一工作流程实例。

[0106] 1、后台管理人员使用标准客户端预先统一采集加钞、维护人员信息，包括身份证号、照片等关键信息，存入服务提供装置数据库。

[0107] 2、后台管理员使用智能钥匙管理客户端，通过智能钥匙读取部件为每一个加钞

组、维护组各配备一把加钞 / 维护钥匙, 初始状态下, 该钥匙无法对开启任何设备保险柜。钥匙平时无需领用和交回, 仅在每次使用时通过后台进行授权。

[0108] 3、后台管理人员根据加钞 / 维修计划, 指定加钞 / 维修人员, 使用标准客户端对人员、钥匙和 ATM 设备进行关联授权, 确保指定人员、指定钥匙在指定的时间内对指定的设备锁具进行开关操作。

[0109] 4、加钞 / 维护人员到达现场后, 在 ATM 后操作面板上输入用户 ID 和口令, 通过内部网路发送到服务提供装置申请一次性开锁密码。

[0110] 5、服务提供装置验证开锁人员身份后, 使用智能钥匙读取部件生成一次性开锁口令。也可以在验证开锁人员身份后, 发送开锁事件信息给远程授权人员操作终端, 后台授权人员通过视频监控系统查看现场情况后, 再授权服务提供装置生成一次性开锁口令。

[0111] 6、开锁口令以短信的方式通知系统预先绑定的开锁人员的手机号码, 或采用邮件、电话等方式通知系统预先绑定的开锁人员的邮箱、电话号码。

[0112] 7、开锁人员收到短信通知(或其它方式的通知)后, 在规定时间内在动态密码电子锁上使用键盘输入一次性开锁口令, 并把智能钥匙与智能钥匙读写部件的读写接口相接, 如果开锁口令正确并且智能钥匙正确, 则动态密码电子锁内部的马达解锁活动锁舌, 此时可将保险柜门栓从关闭位置开释放到开启位置。

[0113] 8、锁舌或者保险柜门的状态一旦发生变化(由关闭变为开启、或者由开启变为关闭), 则在锁具内部的电路控制部件、监控和管理部件共同作用下, 立即将锁舌和保险柜门的状态报送服务提供装置。

[0114] 9、加钞 / 维修工作完成后, 关闭保险柜门, 锁具自动落锁, 并自动上报保险柜关闭、落锁事件到服务提供装置, 流程结束。

[0115] 10、对于身份验证次数超限、一次性密码输入错误次数超限、规定时间内没有收到闭锁信息等特殊情况, 服务提供装置自动启动预警流程。

[0116] 图 13 是给 ATM 加钞的具体流程图, 如图 13 所示, 该流程包括:

[0117] 步骤 1301 : 后台管理人员预先设置开锁人员身份 ID, 建立其个人信息(姓名、身份证号、手机号等), 设定初始密码。

[0118] 步骤 1302 (可选): 后台管理人员预先采集开锁人员的图像信息存入系统, 并与其 ID 建立关联关系。

[0119] 步骤 1303 : 后台管理人员预先为每一个加钞 / 维护组配备智能钥匙, 登记智能钥匙与领用人的绑定关系。

[0120] 步骤 1304 : 后台管理人员根据加钞维护计划, 创建工作任务, 并建立任务与人员, 锁 ID、钥匙 ID、开锁时间段的绑定关系。

[0121] 步骤 1305 : 开锁人员如果是首次处理业务, 使用 ID 和初始密码登录系统, 修改自己的密码。

[0122] 步骤 1306 : 开锁人员现场申请开锁时, 系统先验证其输入密码是否与预留密码一致。

[0123] 步骤 1307 : 后台系统验证开锁事件在计划内(开锁事件所对应的任务、开锁时间、开锁人员 ID、锁 ID 是否匹配)。

[0124] 步骤 1308 : 生成一次性开锁动态密码, 并通知开锁人员。

[0125] 如图 14 所示,当不可避免地发生以下异常的情形时,系统启动预警处理流程:

[0126] (1) 非计划内的锁和保险柜门打开。后台管理人员预先在业务功能处理模块中制定 ATM 加钞和维修的时间计划,如果系统监控发现锁和保险柜门打开事件未在计划之内,则启动预警处理流程。

[0127] (2) 锁和保险柜门超时未上报。后台管理人员预先在业务功能处理模块中定义锁和保险柜门状态上报的时间间隔,如果系统监控发现超过规定时间没有上报,则启动预警处理流程。

[0128] (3) 授权人员查看现场视频后,设备周边环境异常。开锁申请人员到达现场申请开锁时,后台授权人员远程查看现场视频发现周边环境异常(比如开锁人员被劫持、现场出现可疑人员等),则启动预警处理流程。

[0129] (4) 开锁申请人员身份验证次数超限。系统预先定义开锁申请人员密码错误最大次数参数,如果开锁申请人员密码错误超过这个参数值,则启动预警处理流程。

[0130] (5) 授权人员查看现场视频发现申请人身份非法。开锁申请人员到达现场申请开锁时,后台授权人员远程查看现场视频发现申请人与预留的照片不一致或者可疑,则系统根据不同情况启动相应的预警处理流程。

[0131] (6) 系统定义的其它异常事件。

[0132] 以下再给出一远程监控实例。

[0133] 如图 15 所示,基于图 7 所示的远程集中授权系统总体结构包括:安装于 ATM 周边用于对周边环境以及现场人员进行摄像的视频监控设备 7、标准客户端 41,视频监控设备 7 和授权客户端 41 经过内部网络 6 通过流媒体服务部件 8 连接后台视频集中监控服务提供装置 9。其中:

[0134] 授权客户端 41 是一个安装了视频播放软件的 PC 机,通过内部网络同时与服务提供装置 5 和视频集中监控服务提供装置 9 相连接,当前台开锁用户申请开锁时,服务提供装置中业务功能处理模块验证用户身份验证后,将开锁所在的 ATM ID 和开锁人员所对应的预留照片信息发送给授权客户端,将照片显示于屏幕的一角,授权人员远程查看现 ATM ID 对应的场开锁人员和周边环境视频,并与回显在屏幕上图像进行比对,通过后回应业务功能处理模块授权开锁。

[0135] 视频监控设备 7 是安装于 ATM 周边的视频信息采集、录像处理和存储的硬件设备,具备网络远程集中监控、远程报警、远程录像查阅等功能。

[0136] 流媒体服务部件 8 是一台或者多台安装有流媒体数据处理软件的 PC 服务器,其作用是将实时视频录像同时提供多个用户查看,减少网络资源和设备资源的占用。

[0137] 视频集中监控服务提供装置 9 是一台或者多台安装有专用软件的 PC 服务器,该装置为客户提供远程查看视频录像、远程监控视频监控设备 7 运行状态服务。

[0138] 本实用新型实施例通过动态密码电子锁、开锁人员的身份认证以及对保险柜门、锁实时状态的监控,克服了现有的自动柜员机保险柜门和锁状态不支持联机监控的问题,同时解决了传统自动柜员机钥匙和密码管理过程中存在的风险和开闭锁事件无法审计的问题,本实用新型实施例主要有如下几方面效果与优点:

[0139] (1) 通过引入动态密码电子锁,实现了保险柜门关闭后锁具自动落锁,解决了人工操作锁具没有落锁的问题,进一步降低运营风险,保证现金安全。

[0140] (2) 实现了 ATM 保险柜锁开闭的系统控制, 实现 ATM 保险柜开锁远程集中授权, 通过前后台相配合的授权和开锁机制, 进一步优化业务流程, 提高运营效率。

[0141] (3) 实现了 ATM 保险柜锁具的智能化管理, 实时监控锁具状态, 实现开锁超时报警、优化现有钥匙和密码的管理方式, 进一步提升安全管理水平。

[0142] (4) 实现了 ATM 保险柜锁管理与运营流程的统一, 建立加钞、维护任务与钥匙、密码和操作人员的动态关联, 并可对开闭锁事件进行设计追踪, 降低了风险。

[0143] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤可以通过程序来指令相关的硬件来完成, 该程序可以存储于一计算机可读取存储介质中, 比如 ROM/RAM、磁碟、光盘等。

[0144] 以上所述的具体实施例, 对本实用新型的目的、技术方案和有益效果进行了进一步详细说明, 所应理解的是, 以上所述仅为本实用新型的具体实施例而已, 并不用于限定本实用新型的保护范围, 凡在本实用新型的精神和原则之内, 所做的任何修改、等同替换、改进等, 均应包含在本实用新型的保护范围之内。

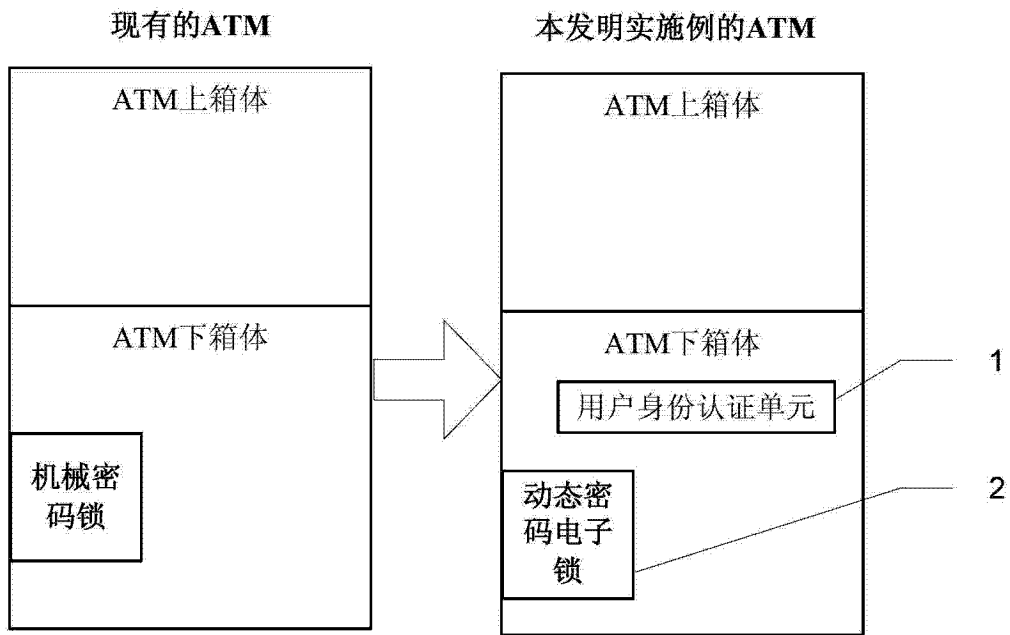


图 1

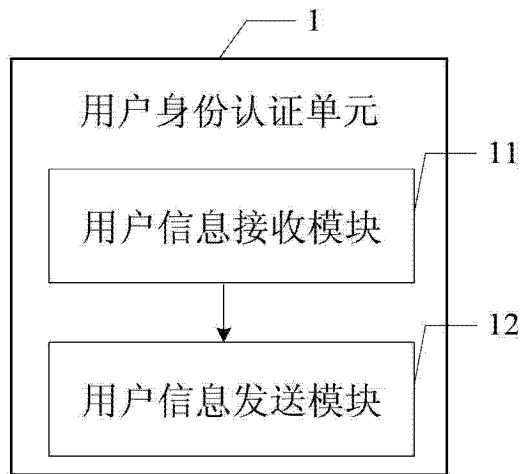


图 2

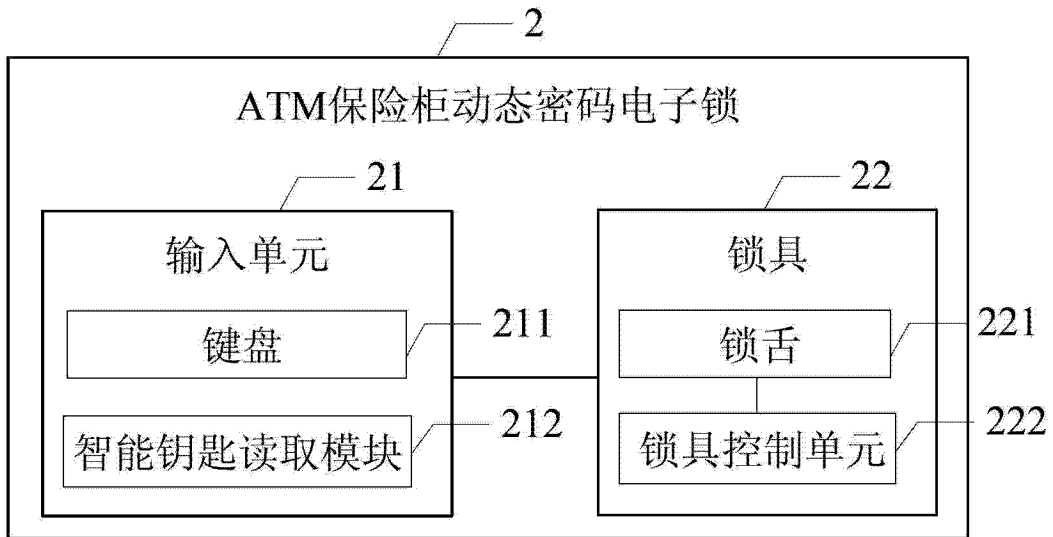


图 3a

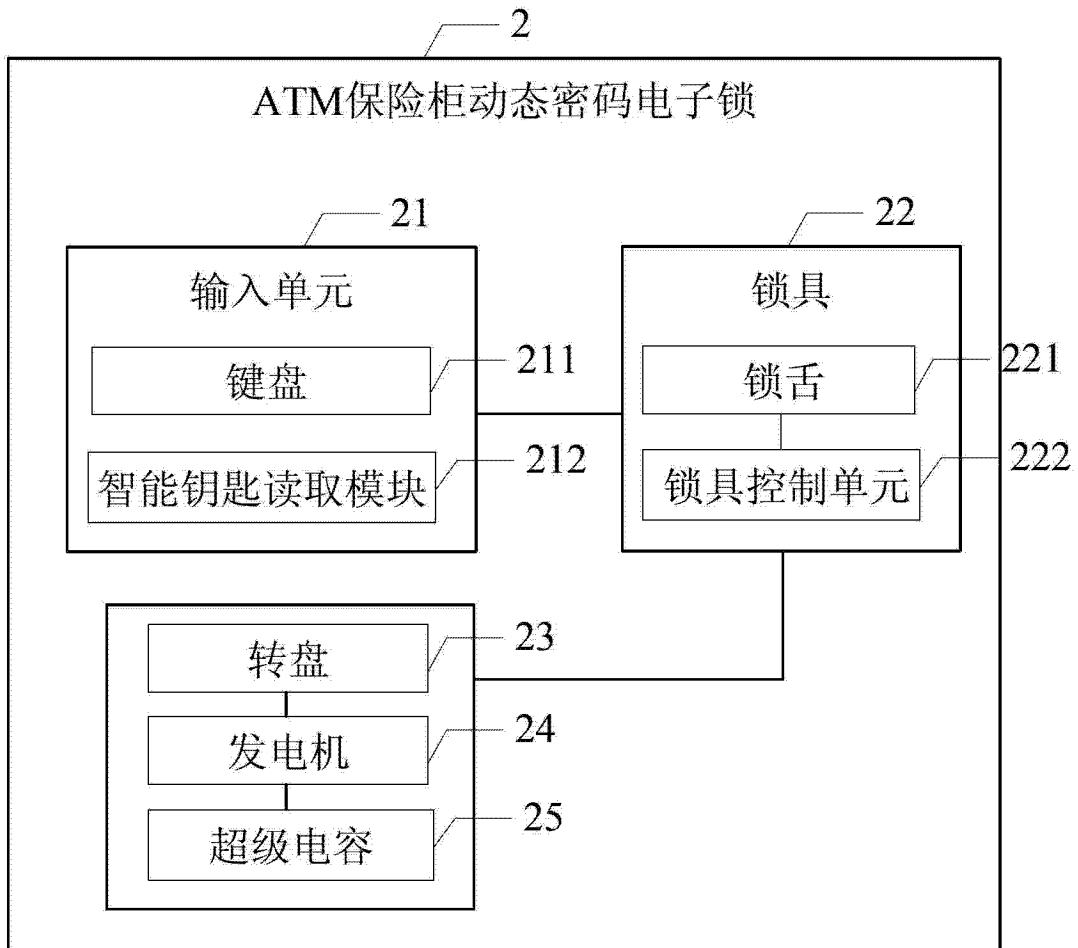


图 3b

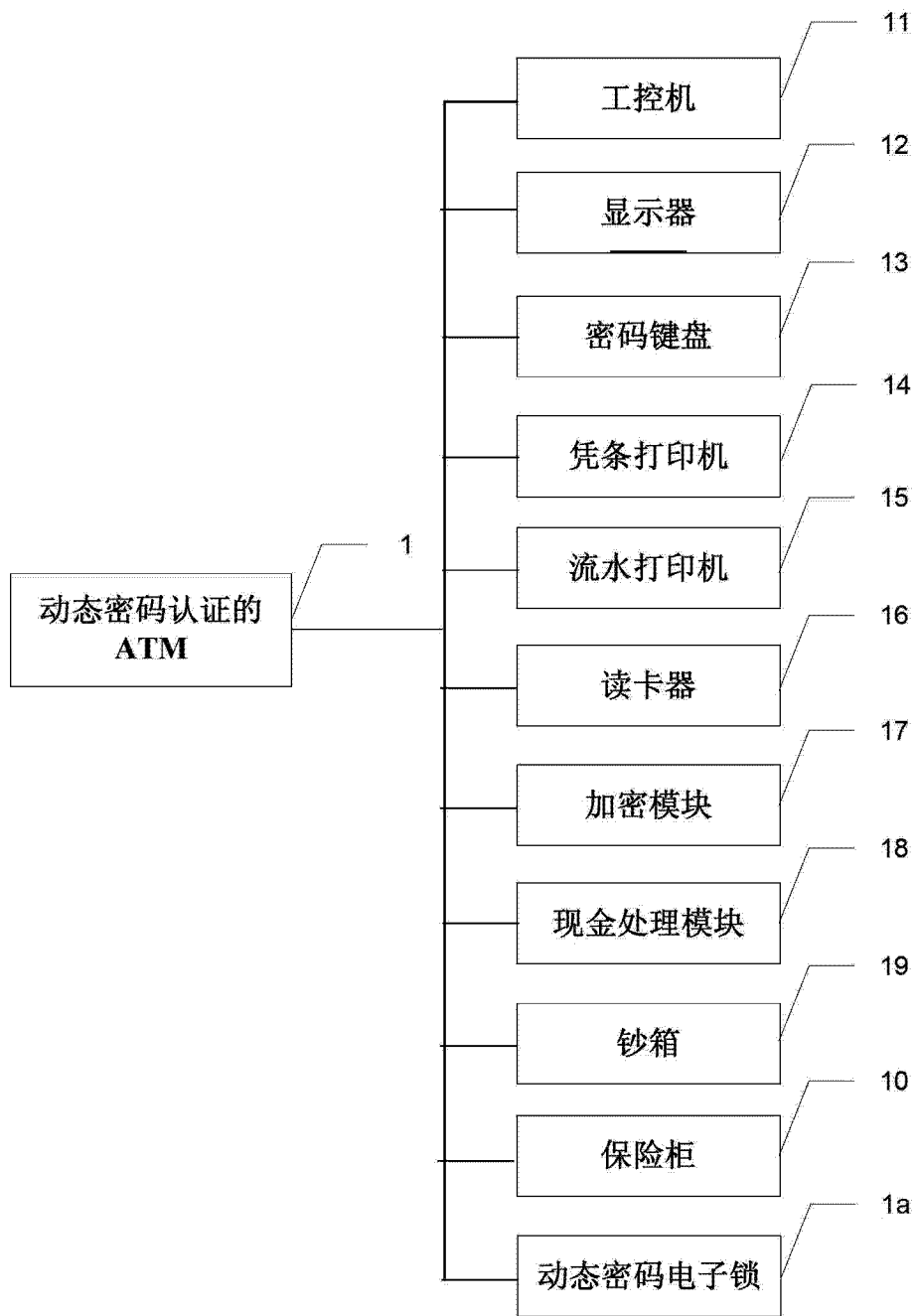


图 4

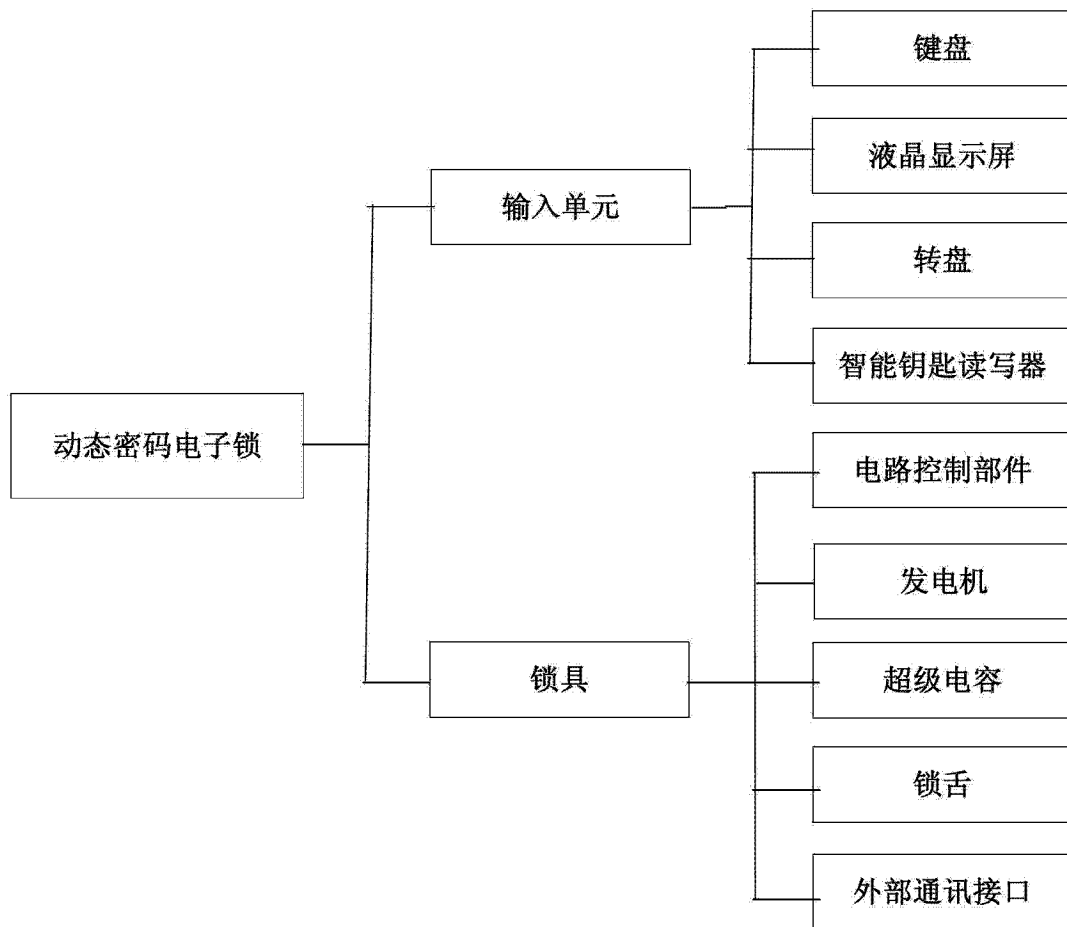


图 5



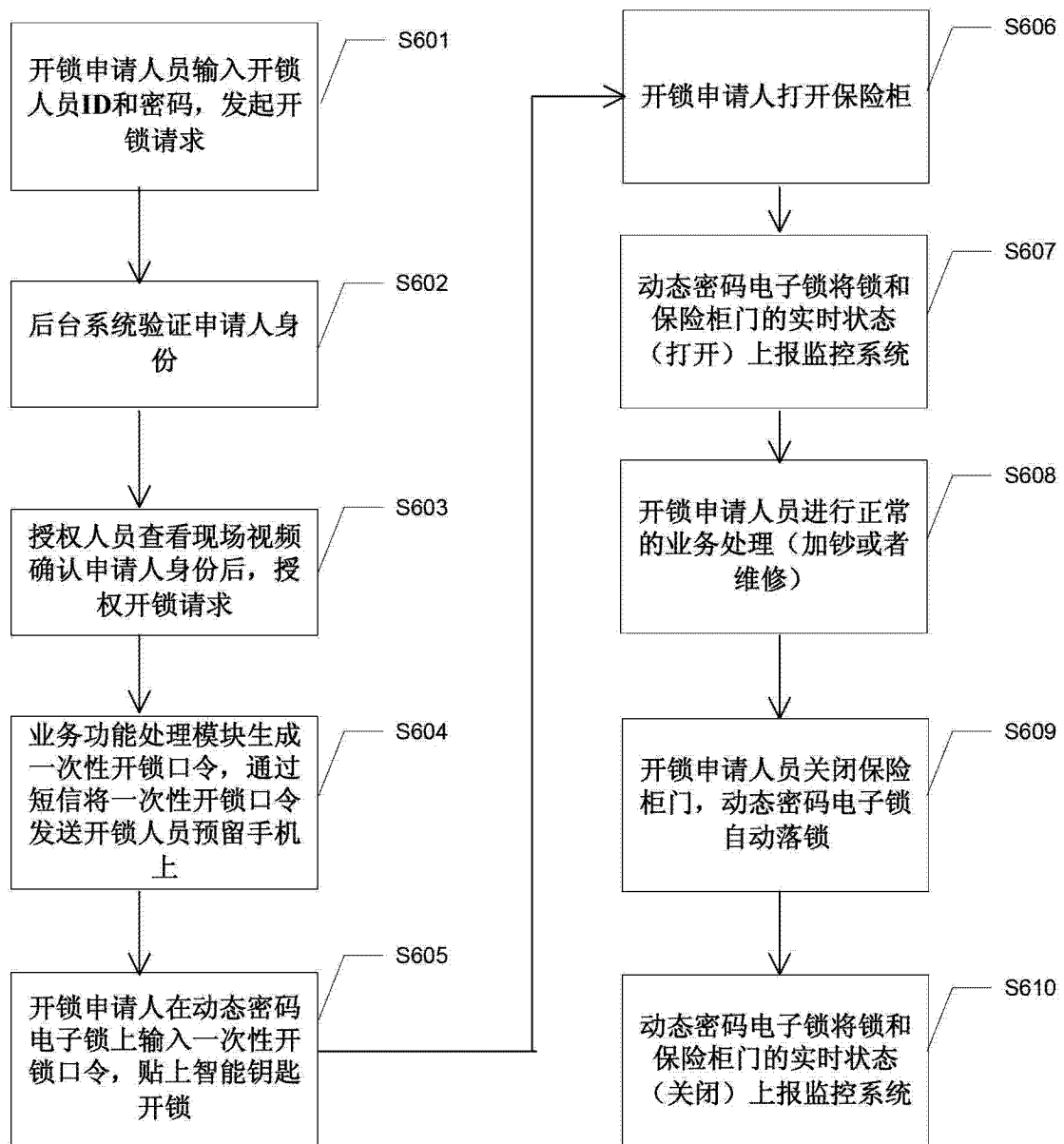


图 6

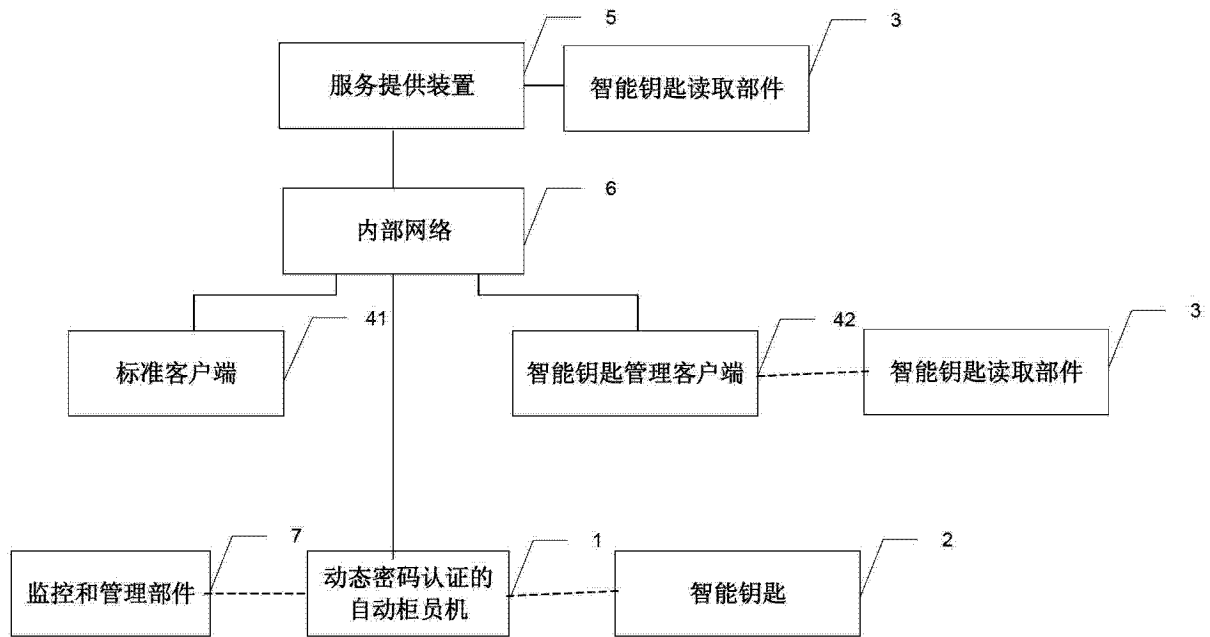


图 7

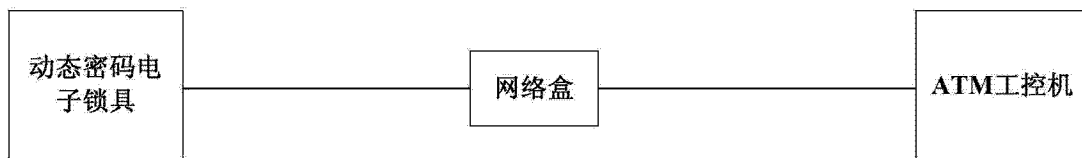


图 8

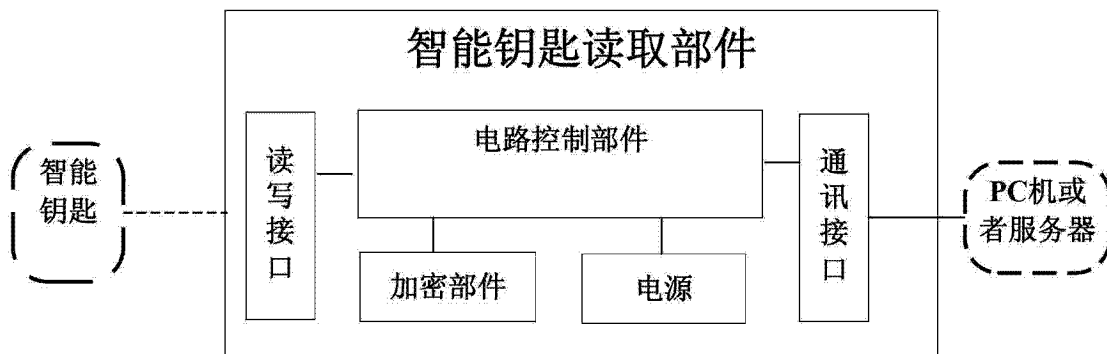


图 9

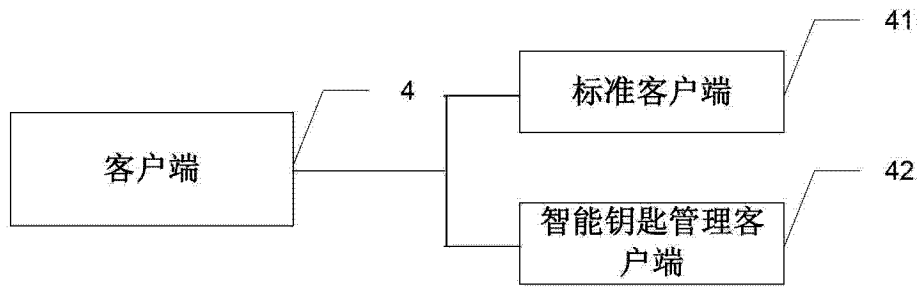


图 10

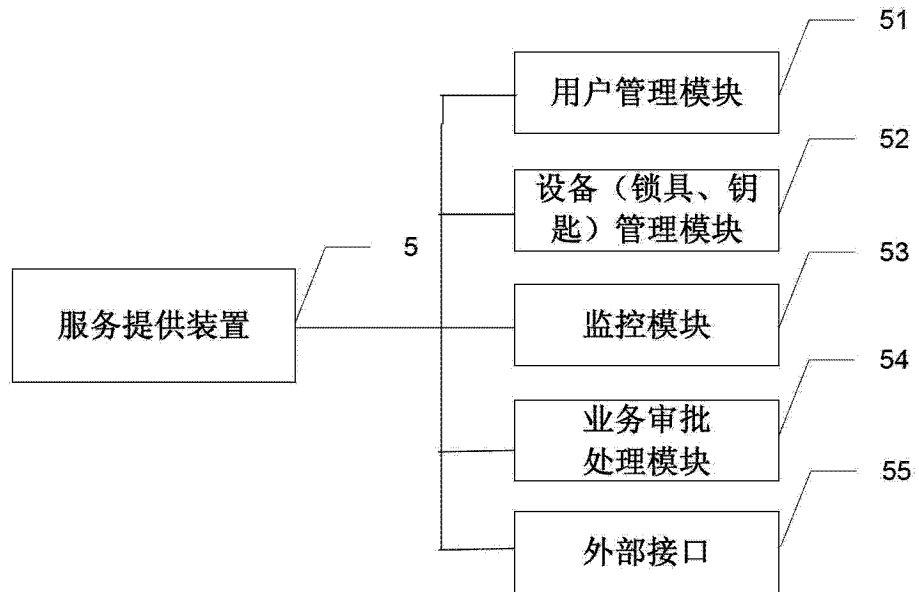


图 11

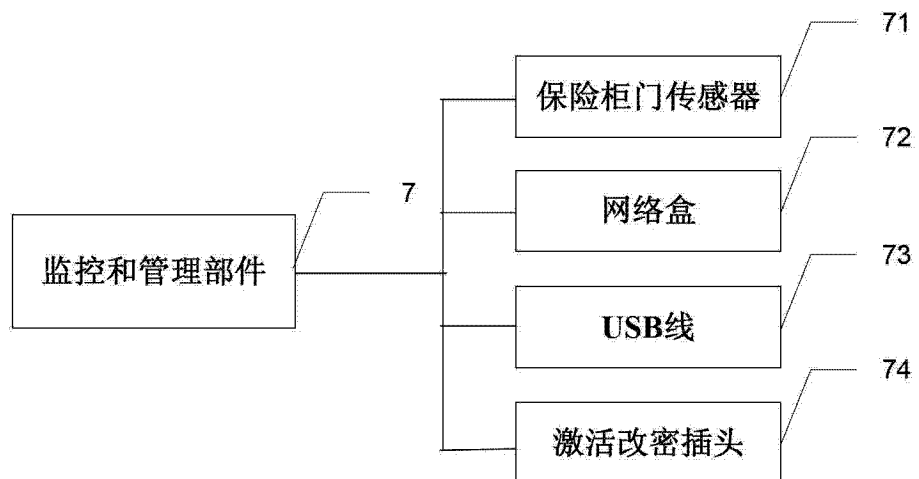


图 12

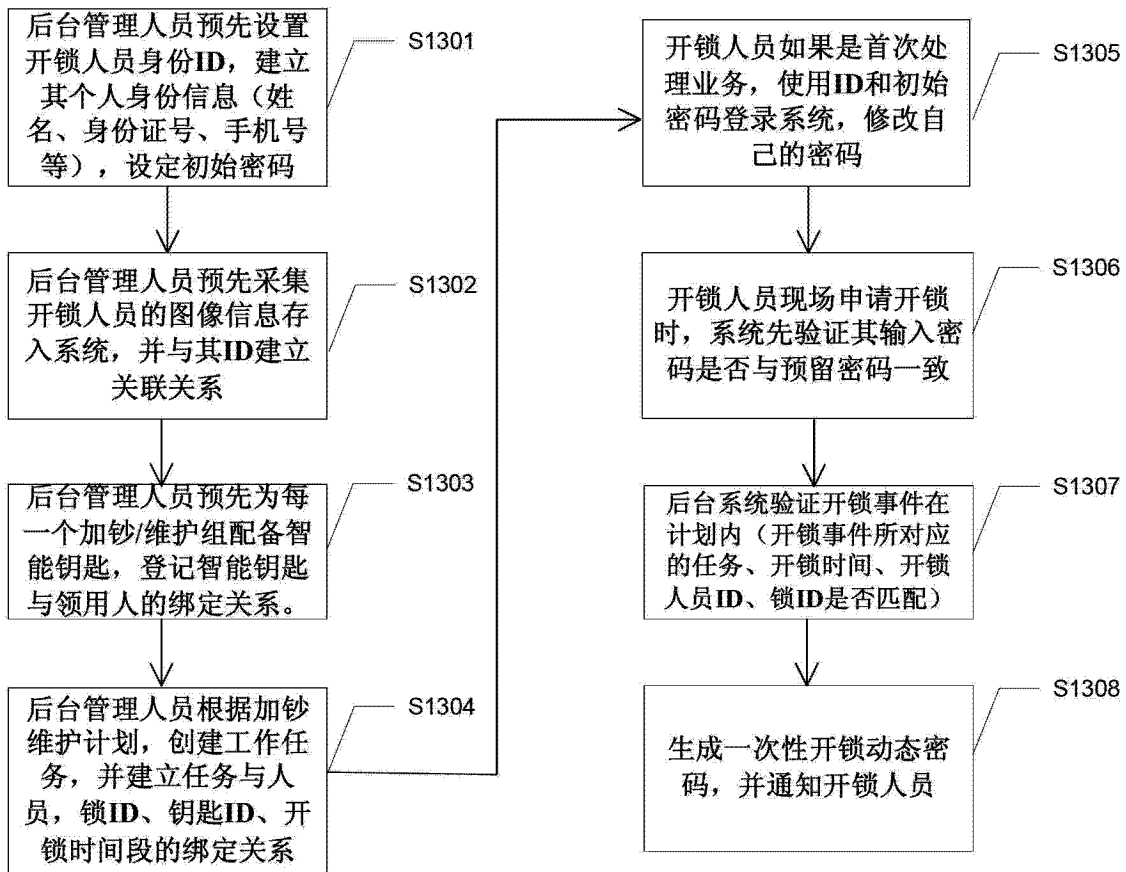


图 13

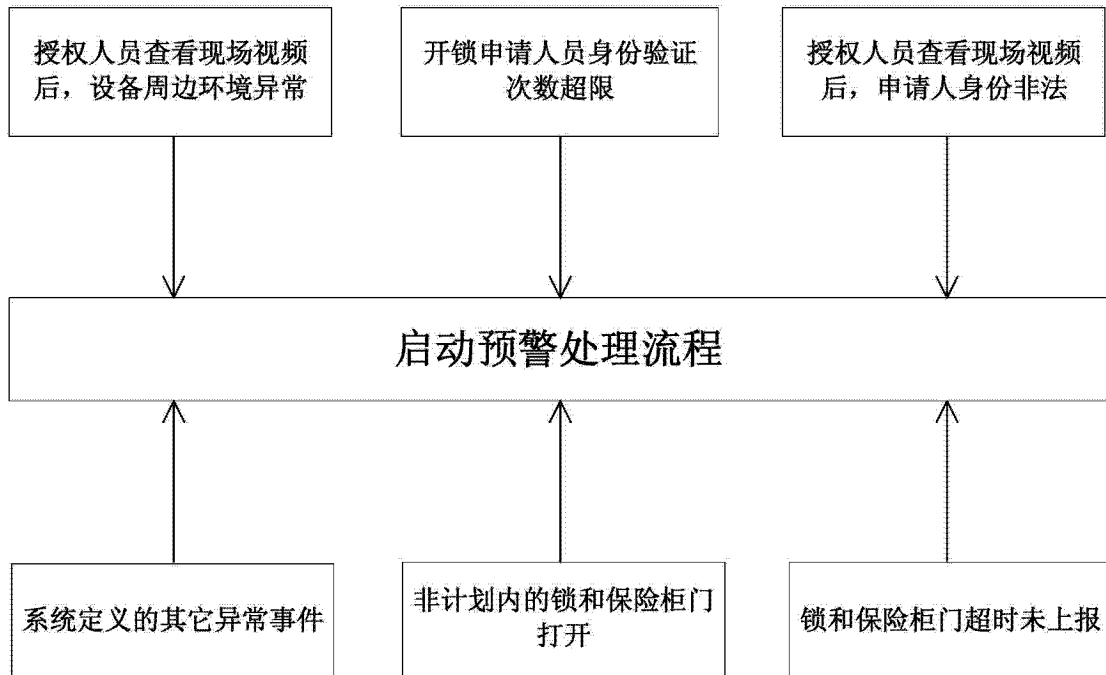


图 14

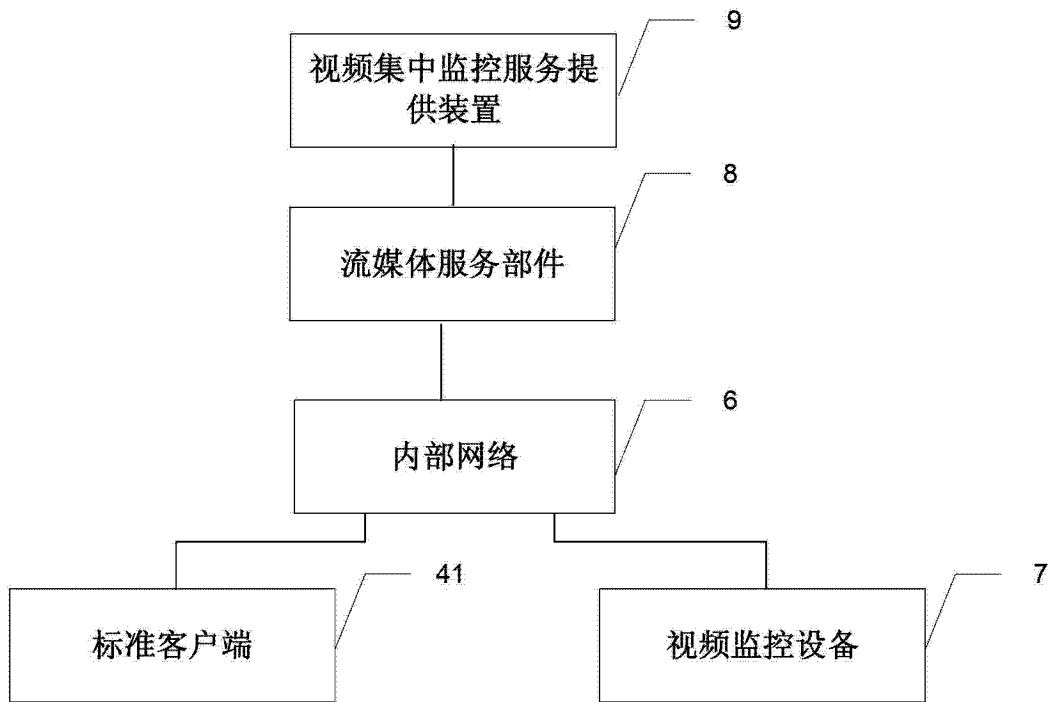


图 15