



(12) 发明专利

(10) 授权公告号 CN 103400434 B

(45) 授权公告日 2016. 02. 03

(21) 申请号 201310342110. 1

US 2007/0271112 A1, 2007. 11. 22,

(22) 申请日 2013. 08. 07

王刚 . ATM 动态密码电子锁管理系统的设计与实现 .《河南科技》. 2013, (第 5 期), 25-26+70.

(73) 专利权人 珠海汇金科技股份有限公司

毛淑平 . ATM 动态密码电子锁使用研究 .《金融科技时代》. 2012, (第 3 期), 65-69.

地址 519085 广东省珠海市软件园路 1 号会展中心 3# 第三层

审查员 黄煜

(72) 发明人 马铮

(74) 专利代理机构 珠海智专专利商标代理有限公司 44262

代理人 林永协

(51) Int. Cl.

G07C 9/00(2006. 01)

(56) 对比文件

CN 201886484 U, 2011. 06. 29,

CN 202771546 U, 2013. 03. 06,

CN 101793115 A, 2010. 08. 04,

CN 1710974 A, 2005. 12. 21,

CN 101798889 A, 2010. 08. 11,

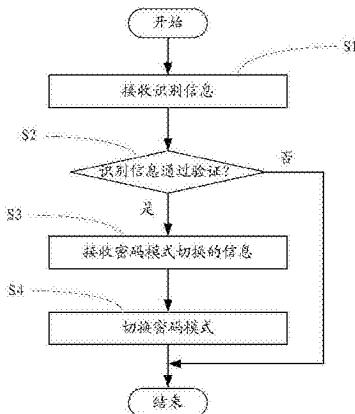
权利要求书2页 说明书7页 附图7页

(54) 发明名称

动静态密码锁的控制方法及控制装置

(57) 摘要

本发明提供一种动静态密码锁的控制方法及控制装置，该方法包括动静态密码锁接收密码模式切换的识别信息，在通过对识别信息的验证后，根据输入的信息切换动静态密码锁的密码模式，密码模式包括静态密码模式与动态密码模式，动静态密码锁工作在静态密码模式下，每次开锁时接收并验证固定的密码，动静态密码锁工作在动态密码模式下，每次开锁时接收并验证变化的密码。该控制装置是应用上述方法对动静态密码锁进行控制。本发明能方便地实现动静态密码锁在动态密码工作模式与静态密码工作模式之间的切换。



1. 动静态密码锁的控制方法,该动静态密码锁用于银行的 ATM 设备上,该控制方法为加钞前开启所述动静态密码锁的方法,其特征在于:该控制方法包括

动静态密码锁接收密码模式切换的识别信息,在通过对所述识别信息的验证后,根据输入的信息切换所述动静态密码锁的密码模式,所述密码模式包括静态密码模式与动态密码模式;

所述动静态密码锁工作在所述静态密码模式下,每次开锁时接收并验证固定的密码;

所述动静态密码锁工作在所述动态密码模式下,每次开锁时接收并验证变化的密码。

2. 根据权利要求 1 所述的动静态密码锁的控制方法,其特征在于:

所述识别信息至少包括模式切换密码、指纹信息或信息纽扣信息中的一种。

3. 根据权利要求 1 或 2 所述的动静态密码锁的控制方法,其特征在于:

所述动静态密码锁工作在所述动态密码模式下的开锁步骤包括:

所述动静态密码锁在开锁人员的身份信息通过验证后,生成一随机数,所述随机数被传输至后台的管理服务器,所述管理服务器应用所述随机数生成开锁密码,所述开锁密码被传输至所述动静态密码锁;

所述动静态密码锁对所述开锁密码解密,并在判断所述开锁密码解密后的数据与所述随机数一致时开启所述动静态密码锁。

4. 根据权利要求 3 所述的动静态密码锁的控制方法,其特征在于:

所述动静态密码锁生成所述随机数后将所述随机数发送至手持设备,由所述手持设备将所述随机数发送至所述管理服务器。

5. 根据权利要求 3 所述的动静态密码锁的控制方法,其特征在于:

所述动静态密码锁生成所述随机数后,将所述随机数显示在显示屏上,开锁人员通过短信或电话通知管理人员,所述管理人员将所述随机数输入至所述管理服务器。

6. 根据权利要求 3 所述的动静态密码锁的控制方法,其特征在于:

所述动静态密码锁生成所述随机数后,通过 ATM 专用网络将所述随机数至传输所述管理服务器。

7. 根据权利要求 3 所述的动静态密码锁的控制方法,其特征在于:

所述管理服务器接收所述随机数前如接收到报警信息,则延迟所述开锁密码的生成;

所述动静态密码锁开锁前如接收到所述报警信息后,延迟开启操作。

8. 动静态密码锁的控制装置,该动静态密码锁用于银行的 ATM 设备上,该控制装置为加钞前开启所述动静态密码锁的装置,其特征在于:该控制装置包括

识别信息验证模块,用于接收并验证密码模式切换的识别信息;

密码模式切换模块,用于根据输入的信息切换所述动静态密码锁的密码模式,所述密码模式包括静态密码模式与动态密码模式;

静态密码工作模块,用于在开锁时接收并验证固定的密码;

动态密码工作模块,用于在开锁时接收并验证变化的密码。

9. 根据权利要求 8 所述的动静态密码锁的控制装置,其特征在于:

所述识别信息至少包括模式切换密码、指纹信息或信息纽扣信息中的一种。

10. 根据权利要求 8 或 9 所述的动静态密码锁的控制装置,其特征在于:

所述动态密码工作模块还包括:

随机数生成模块,用于生成随机数;

开锁密码验证模块,用于接收开锁密码,对开锁密码进行解密并判断所述开锁密码解密后的数据与所述随机数的一致性。

动静态密码锁的控制方法及控制装置

技术领域

[0001] 本发明涉及一种锁具，具体地，是一种用于银行自动柜员机上的动静态密码锁的控制方法以及这种密码锁的控制装置。

背景技术

[0002] 目前，银行的 ATM(Automated Teller Machine，自助存取款机)设备柜体内设有钞箱，柜体的柜门上设有密码锁。银行的工作人员对钞箱进行加钞工作前，需要开启密码锁，并在加钞工作完毕后，关闭该密码锁。

[0003] 为了确保加钞的安全性，加钞工作通常由两名工作人员进行，一名工作人员负责在密码锁上输入密码，另一名工作人员负责使用钥匙开启密码锁。现在的密码锁通常为静态密码锁，即每次开锁时所使用的密码均为固定的密码。虽然密码锁的密码会定期更换，但仍难以确保密码使用的安全性，一旦密码被泄露，将严重影响 ATM 设备的安全性。另外，由于工作人员需要长期记忆开锁的密码，由于每一台 ATM 设备上的密码锁的密码并不相同，其记忆量大，不利于加钞工作的进行。

[0004] 因此，现有部分 ATM 设备使用动态密码锁，即每一次开锁时，工作人员输入一次性的开锁密码，每一个密码只能一次使用，一旦密码输入后，即不能再次使用。这样，工作人员无需记忆复杂的开锁密码，而是每次开锁前接收一次性的开锁密码，并将开锁密码输入到密码锁上，由密码锁对开锁密码进行验证。使用动态密码锁能够提高 ATM 设备加钞的安全性，也避免工作人员需要记忆开锁密码的麻烦。

[0005] 但是，动态密码的使用需要由银行后台的管理中心服务器通过密码生成主机生成开锁密码，并将开锁密码发送给现场的工作人员，这样导致开锁流程复杂，且需要较长的时间。并且，银行需要为动态密码锁的使用对 ATM 设备、后台管理中心服务器进行升级、改造，这需要花费大量的时间与费用。另外，动态密码锁的使用过程中也需要银行投入大量的费用对其进行维护，造成银行的经营成本增加。

[0006] 然而，对于同一台 ATM 设备在不同的使用时期其安全性能要求不尽相同，在安全性能要求较低的时候，使用静态密码锁即可满足其工作要求，但在安全性能要求较高的时候，则需要使用动态密码锁才能满足其工作要求。若银行根据 ATM 设备在不同时期的安全性能要求频繁地更换密码锁，将给银行带来极大的工作量。

发明内容

[0007] 本发明的主要目的是提供一种可以灵活改变工作状态的动静态密码锁的控制方法。

[0008] 本发明的另一目的是提供一种可方便地更改密码模式的动静态密码锁的控制装置。

[0009] 为了实现上述的主要目的，本发明提供的动静态密码锁的控制方法包括动静态密码锁接收密码模式切换的识别信息，在通过对识别信息的验证后，根据输入的信息切换动

静态密码锁的密码模式，密码模式包括静态密码模式与动态密码模式，动静态密码锁工作在静态密码模式下，每次开锁时接收并验证固定的密码，动静态密码锁工作在动态密码模式下，每次开锁时接收并验证变化的密码。

[0010] 由上述方案可见，动静态密码锁在对识别信息验证后，可以根据输入的信息切换密码模式，即可以在静态密码模式与动态密码模式之间进行切换，切换的过程灵活、方便。银行切换动静态密码锁的工作模式时，只需要执行简单的操作即可，大大减小银行的工作量。

[0011] 一个优选的方案是，识别信息至少包括模式切换密码、指纹信息或信息纽扣信息中的一种。

[0012] 由此可见，使用密码、指纹或信息纽扣等作为识别信息，能够简单且方便地实现识别信息的验证。

[0013] 进一步的方案是，动静态密码锁工作在动态密码模式下的开锁步骤包括：动静态密码锁在开锁人员的身份信息通过验证后，生成一随机数，随机数被传输至后台的管理服务器，管理服务器应用随机数生成开锁密码，开锁密码被传输至动静态密码锁，动静态密码锁对开锁密码解密，并在判断开锁密码解密后的数据与随机数一致时开启动静态密码锁。

[0014] 这样，动静态密码锁工作在动态密码模式下，每次开锁时均生成随机数，管理服务器每次根据随机数生成的开锁密码不会重复，动静态密码锁通过验证开锁密码与随机数来确定能否开锁，确保动静态密码锁工作的安全性。

[0015] 更进一步的方案是，动静态密码锁生成随机数后，通过 ATM 专用网络将随机数至传输管理服务器。

[0016] 可见，由于 ATM 专业网络是银行系统内部的 ATM 设备与后台的管理服务器之间的专用通信网络，其安全很高，能够避免使用普通的通信网络可能出现的开锁密码被盗取的情况，提高 ATM 设备加钞的安全性。

[0017] 更进一步的方案是，管理服务器接收随机数前如接收到报警信息，则延迟开锁密码的生成，动静态密码锁开锁前如接收到报警信息，则延迟开启操作。

[0018] 可见，加钞的工作人员一旦发生异常的情况时，可以向后台的管理服务器发送报警信息，管理服务器在后台报警并延迟生成开锁密码，有利于保障加钞工作人员的人身安全，为保安人员赶到现场争取时间，提高加钞工作的安全性。

[0019] 为实现上述的另一目的，本发明提供的动静态密码锁的控制装置包括识别信息验证模块、密码模式切换模块、静态密码工作模块以及动态密码工作模块，识别信息验证模块用于接收并验证密码模式切换的识别信息，密码模式切换模块用于根据输入的信息切换动静态密码锁的密码模式，密码模式包括静态密码模式与动态密码模式，静态密码工作模块用于在开锁时接收并验证固定的密码，动态密码工作模块用于在开锁时接收并验证变化的密码。

[0020] 由上述方案可见，动静态密码锁可以根据输入的信息切换密码模式，这样，银行可以根据 ATM 设备的工作需要切换动静态密码锁的密码模式，在保障 ATM 设备加钞安全性的同时，也能最大限度地降低银行的维护成本。

附图说明

- [0021] 图 1 是本发明动静态密码锁控制装置第一实施例的结构框图。
- [0022] 图 2 是本发明动静态密码锁控制方法第一实施例中切换密码模式的流程图。
- [0023] 图 3 是本发明动静态密码锁控制方法第一实施例中的动静态密码锁与管理服务器连接的结构框图。
- [0024] 图 4 是本发明动静态密码锁控制方法第一实施例中应用动态密码开锁的流程图。
- [0025] 图 5 是本发明动静态密码锁控制方法第二实施例中的动静态密码锁与管理服务器连接的结构框图。
- [0026] 图 6 是本发明动静态密码锁控制方法第二实施例中应用动态密码开锁的流程图。
- [0027] 图 7 是本发明动静态密码锁控制方法第三实施例中的动静态密码锁与管理服务器连接的结构框图。
- [0028] 图 8 是本发明动静态密码锁控制方法第三实施例中应用动态密码开锁的流程图。
- [0029] 以下结合附图及实施例对本发明作进一步说明。

具体实施方式

[0030] 本发明的动静态密码锁可以应用在银行的 ATM 设备上, 加钞的工作人员在加钞前启动静态密码锁, 并在加钞完毕后闭合动静态密码锁。本发明的动静态密码锁的控制方法是对动静态密码锁的工作进行控制, 动静态密码锁的控制装置是对动静态密码锁进行控制的装置。

[0031] 第一实施例:

[0032] 参见图 1, 本发明的动静态密码锁控制装置设有识别信息验证模块 11、密码模式切换模块 12、静态密码工作模块 13 以及动态密码工作模块 14, 动态密码工作模块 14 内设有随机数生成模块 15 以及开锁密码验证模块 16。

[0033] 识别信息验证模块 11 用于接收识别信息, 并对识别信息进行验证。本实施例中, 识别信息可以是由工作人员输入的模式切换密码、指纹信息或者信息纽扣(Information Button)的信息。

[0034] 如识别信息为模式切换密码, 则动静态密码锁上设置一个键盘, 由工作人员在键盘上输入密码, 识别信息验证模块 11 对密码进行验证识别。如识别信息为指纹信息, 则动静态密码锁上设置指纹扫描仪, 用于接收工作人员的指纹信息, 识别信息验证模块 11 对指纹信息进行识别验证。如识别信息为信息纽扣信息时, 在动静态密码锁上设置用于读取信息纽扣的信息的读取装置, 识别信息验证模块 11 对信息纽扣的信息进行验证。

[0035] 密码模式切换模块 12 用于根据输入的信息切换密码模式, 如从静态密码工作模式切换至动态密码工作模式, 或者从动态密码工作模式切换至静态密码工作模式。

[0036] 静态密码工作模块 13 工作在静态密码工作模式下, 此时, 动静态密码锁每次开锁时接收固定的密码。当然, 该固定的密码是相对固定的, 并不是绝对固定, 即工作人员可以根据需要定期或不定期修改。

[0037] 动态密码工作模块 14 工作在动态密码工作模式下, 此时, 动静态密码锁每次开锁时将由随机数生成模块 15 生成一个随机数, 并接收开锁密码, 开锁密码验证模块 16 对开锁密码进行解密并验证, 在验证通过后开启动静态密码锁。

[0038] 下面结合图 2 说明动静态密码锁切换密码模式的工作流程。首先, 工作人员在动

静态密码锁上输入识别信息,即执行步骤 S1,识别信息可以是模式切换密码或者指纹信息或者信息纽扣信息。然后,动静态密码锁执行步骤 S2,对识别信息进行验证,如通过验证,则执行步骤 S3,接收密码模式切换的信息。此时,动静态密码锁上可以显示密码模式的选择窗口,由工作人员选择,或者由工作人员输入密码模式的编号。密码模式被选择后,动静态密码锁执行步骤 S4,切换其密码工作模式,即切换到动态密码工作模式或者切换到静态密码工作模式。如步骤 S2 中,识别信息未能通过验证,则结束流程,动静态密码锁的密码模式切换操作失败。

[0039] 通过上述简单的操作,银行能够方便且简单地切换动静态密码锁的密码工作模式,在对 ATM 设备安全性要求较高的时期,选择动态密码工作模式,在对 ATM 设备安全性要求不高时,选择静态密码工作模式,降低维护动静态密码锁的成本。

[0040] 动静态密码锁工作在动态密码工作模式下,可以通过不同的开锁流程执行开锁操作,下面将详细说明三种开锁操作流程。

[0041] 参见图 3,在第一种开锁流程下,需要使用手持设备 25 进行开锁操作。手持设备 25 为 PDA(Personal Digital Assistant,掌上电脑)等可以移动的小型化设备,开锁人员开锁时需要携带手持设备 25。

[0042] 本实施例中,动静态密码锁 10 通过无线射频方式与手持设备 25 进行通信,手持设备 25 可以通过普通的通信网络 23 与后台的管理中心服务器 21 进行通信,管理中心服务器 21 则与密码生成主机 22 进行通信。在银行系统中,管理中心服务器 21 与密码生成主机 22 构成管理服务器,用于对多台 ATM 设备进行管理,包括对 ATM 设备上的动静态密码锁 10 进行管理。

[0043] 加钞工作由两名工作人员同时进行,每一名工作人员均为开锁人员,每一名开锁人员均具有自己的编号。参见图 4,需要开启动静态密码锁时,开锁人员执行步骤 S11,在手持设备上输入身份信息,包括每一名开锁人员的编号以及指纹信息,当然,也可以是其他用于识别身份的信息,如开锁人员持有的密码等。一旦加钞工作发生异常情况,开锁人员需要及时发出报警信息,则可以在手持设备上提示报警,如按下特定的按键或者输入特定的信息。

[0044] 然后,手持设备通过通信网络将开锁人员的身份信息发送至管理中心服务器,即执行步骤 S12。如果开锁人员通过手持设备输入报警的信息,手持设备将报警信息一并发送至管理中心服务器。

[0045] 管理中心服务器接收到手持设备发送的信息后,执行步骤 S13,判断是否接收到报警信息,如是,则执行步骤 S15,延迟执行操作,即延迟生成开锁所需要的开锁密码,并向手持设备发送正等待后台处理的信息。同时,管理中心服务器及时报警。这样,开锁人员可以在不被察觉的情况下实现报警。

[0046] 如管理中心服务器没有接收到报警信息,则执行步骤 S14,对开锁人员的身份信息进行识别,即判断开锁人员是否得到授权开锁、所需要开锁的动静态密码锁是否为需要加钞的 ATM 设备等。管理中心服务器通过对开锁人员的身份识别后,将通过识别验证的信息发送至手持设备。

[0047] 然后,开锁人员按下动静态密码锁任一按键,动静态密码锁执行步骤 S16,动静态密码锁生成一随机数,并通过无线射频方式将随机数发送至手持设备。手持设备接收到随

机数后,执行步骤 S17,将随机数、开锁人员的身份信息通过通信网络发送至管理中心服务器。

[0048] 接着,管理中心服务器执行步骤 S18,对随机数进行验证,即根据该随机数验证生成该随机数的动静态密码锁是否为授权可以开启的动静态密码锁。优选地,动静态密码锁所生成的随机数包含有动静态密码锁自身的编号,一般与管理中心服务器确定随机数由哪一台 ATM 设备的动静态密码锁发出。

[0049] 通过对随机数的验证后,管理中心服务器将随机数以及开锁人员的身份信息发送至密码生成主机。密码生成主机根据随机数、开锁人员的身份信息生成开锁密码,并将开锁密码发送至管理中心服务器。

[0050] 然后,管理中心服务器执行步骤 S19,将开锁密码发送至手持设备,手持设备显示该开锁密码,开锁人员将开锁密码输入至动静态密码锁。动静态密码锁执行步骤 S20,对开锁密码进行解密,并对解密后的数据进行验证,即执行步骤 S21,判断解密后的数据是否与之前生成的随机数一致,如是表示通过验证,则执行步骤 S22,判断开锁人员是否发出了报警信息,如没有,执行步骤 S23,开启动静态密码锁。如开锁人员曾发出报警信息,则执行步骤 S24,延迟执行开锁操作,以争取更多的时间让保安人员赶到现场协助处理。

[0051] 这样,动静态密码锁开锁时生成随机数,后台的管理服务器根据随机数生成一次性的开锁密码,开锁密码一次性使用,确保 ATM 设备的加钞安全性。

[0052] 第二实施例:

[0053] 下面结合图 5 与图 6 说明动静态密码锁在动态密码工作模式下的另一种开锁流程。本实施例中,动静态密码锁不需要通过手持设备发送信息,开锁人员通过短信或电话的方式将随机数发送至后台的管理服务器。

[0054] 本实施例中,开锁人员 31 可以对动静态密码锁 30 进行操作,其通过通信网络 32 以短信或电话的方式与后台的管理人员 33 进行通信,管理人员 33 对管理中心服务器 34 进行操作,管理中心服务器 34 与密码生成主机 35 通信。本实施例中,管理中心服务器 34 与密码生成主机 35 构成管理服务器。

[0055] 执行开锁操作时,两名开锁人员在动静态密码锁上输入身份信息,如其中一名开锁人员将电子钥匙贴近动静态密码锁,另一名开锁人员在动静态密码锁上输入密码,即执行步骤 S31。然后,动静态密码锁执行步骤 S32,对开锁人员的身份信息进行识别验证。当然,一旦开锁人员在加钞现场发生异常情况时,可以在动静态密码锁上输入报警的信息,如按下特定的按键或者输入特定的密码等。

[0056] 动静态密码锁执行步骤 S33,判断是否接收到报警信息,如是,则执行步骤 S35,延迟操作,即延迟生成随机数、延迟对接收的开锁密码进行验证等。并且,可以通过 ATM 设备与管理服务器之间专用的 ATM 专用网络发出报警信息。

[0057] 如动静态密码锁没有接收到报警信息,则执行步骤 S34,生成随机数,并将随机数显示在显示屏上,开锁人员观看到随机数后,通过通信网络以短信或电话等方式将随机数发送至管理人员。管理人员接收到随机数后,执行步骤 S36,将随机数输入到管理中心服务器,由管理中心服务器对随机数进行验证,即判断生成随机数的动静态密码锁所在的 ATM 设备是否得到授权加钞。

[0058] 管理中心服务器通过对随机数的验证后,执行步骤 S37,将随机数以及开锁人员的

身份信息传输至密码生成主机，密码生成主机应用随机数以及开锁人员的身份信息生成一次性使用的开锁密码。然后，管理人员执行步骤 S38，将开锁密码通过通信网络以电话或短信的方式发送至开锁人员，开锁人员执行步骤 S39，将开锁密码输入到动静态密码锁上。

[0059] 接着，动静态密码锁对开锁密码进行解密，并对开锁密码进行验证，即执行步骤 S40，判断对开锁密码解密后的数据是否与生成的随机数一致，如一致，执行步骤 S41，判断开锁人员是否发出了报警信息，如是，则执行步骤 S43，延迟执行开锁操作。如没有接收到开锁人员发出的报警信息，则执行步骤 S42，开启动静态密码锁。

[0060] 第三实施例：

[0061] 参见图 7，本实施例的动静态密码锁 40 通过 ATM 专用网络 41 与 ATM 工控机 42 通信，ATM 工控机 42 通过 ATM 专用网络 43 与后台的管理中心服务器 44 通信，管理中心服务器 44 与密码生成主机 45 通信。管理中心服务器 44 与密码生成主机 45 构成本实施例的管理服务器。

[0062] 由于 ATM 专用网络 41、43 为银行内部实现 ATM 设备与 ATM 工控机 42、后台管理服务器之间通信的专用网络，且为封闭式的网络，安全性能远远高于普通的通信网络。本实施例中，动静态密码锁 40 生成的随机数以及管理服务器生成的开锁密码均通过 ATM 专用网络 41、43 进行传输，从而确保随机数以及开锁密码传动安全性，避免随机数或者开锁密码被窃取。

[0063] 参见图 8，对动静态密码锁开锁时，首先由开锁人员输入身份信息，如两名开锁人员所持有的密码或者指纹信息等，即执行步骤 S51。然后，动静态密码锁将开锁人员的身份信息通过 ATM 专用网络传输至管理中心服务器，即执行步骤 S52。一旦开锁人员遇到异常情况，可以在动静态密码锁上发出报警信息，如输入特定的密码或者按下特定的按键。

[0064] 接着，管理中心服务器执行步骤 S53，判断是否接收到报警信息，如是，则执行步骤 S55，延迟操作，即延迟生成开锁密码，并通过后台进行秘密报警。

[0065] 如管理中心服务器没有接收到报警信息，则执行步骤 S54，管理中心服务器对开锁人员的身份信息进行验证，并通过验证后，将通过验证的信息通过 ATM 专用网络传输至动静态密码锁。随后，动静态密码锁执行步骤 S56，生成一个随机数，并将随机数发送至管理中心服务器。管理中心服务器执行步骤 S57，对随机数进行验证，即判断生成随机数的动静态密码锁是否为授权可以开启的动静态密码锁。

[0066] 然后，管理中心服务器执行步骤 S58，将随机数发送至密码生成主机，密码生成主机应用随机数生成一次性使用的开锁密码，并将开锁密码通过 ATM 专用网络发送至动静态密码锁。动静态密码锁接收到开锁密码后，执行步骤 S59，对开锁密码进行解密，并对解密后的数据进行验证，即执行步骤 S60，判断解密后的数据是否与生成的随机数一致，如一致，则执行步骤 S61，进一步判断开锁人员是否发出报警信息，如是，执行步骤 S63，延迟开锁操作，如没有接收到开锁人员发出的报警信息，则开启动静态密码锁，即执行步骤 S62。

[0067] 本实施例中，动静态密码锁通过 ATM 专用网络与管理中心服务器机械能通信，并通过 ATM 专用网络发送随机数以及开锁密码，大大提高随机数以及开锁密码传输的安全性，保障 ATM 设备的加钞安全。

[0068] 当然，上述的实施例仅是本发明较佳的实施方式，实际应用时，还可以有更多的改变，例如，手持设备不一定通过无线射频信号与动静态密码锁通信，还可以通过诸如 USB 接

口等方式与动静态密码锁通信等,这样的改变也能实现本发明的目的。

[0069] 最后需要强调的是,本发明不限于上述实施方式,如在动态密码工作模式下开锁流程的改变、开锁人员身份信息的改变等变化也应该包括在本发明权利要求的保护范围内。

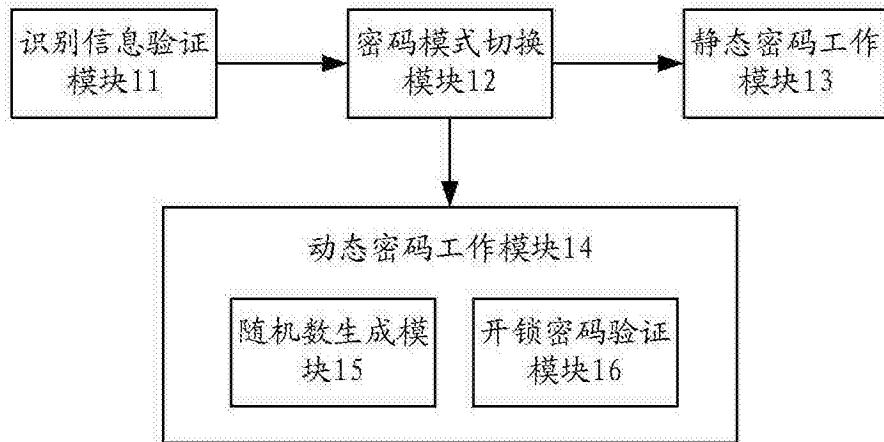


图 1

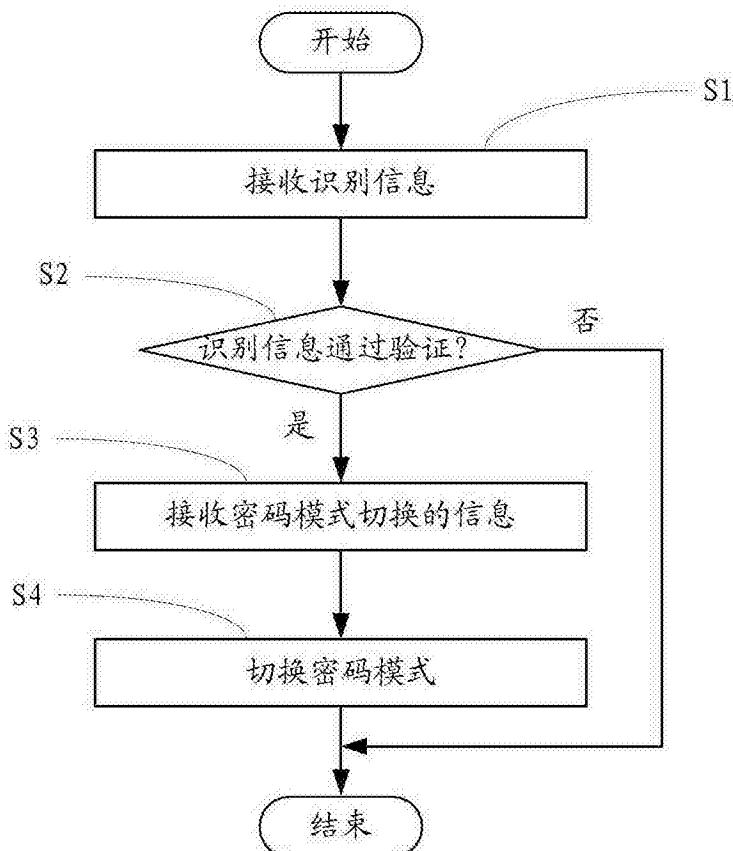


图 2

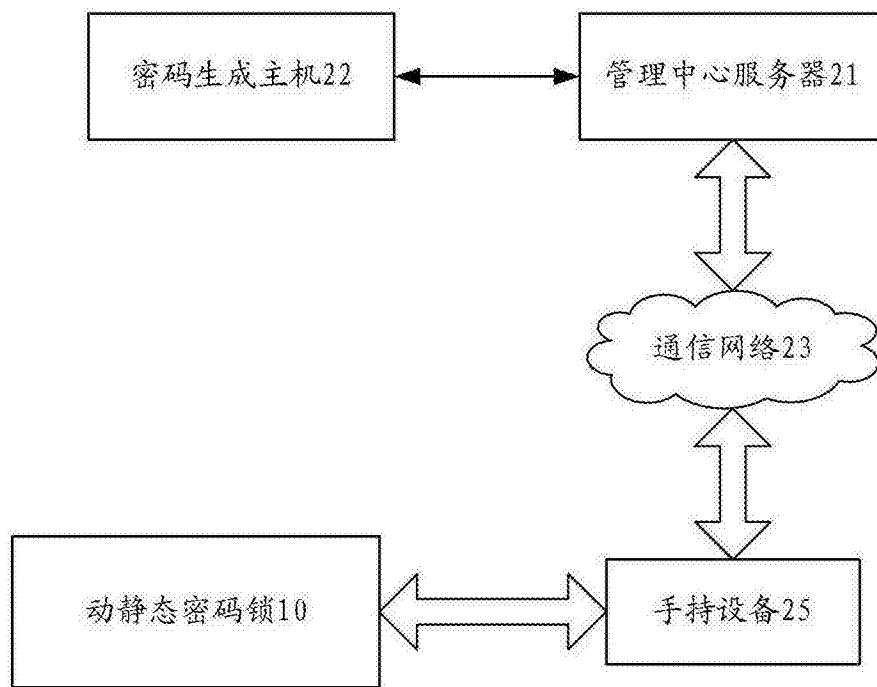


图 3

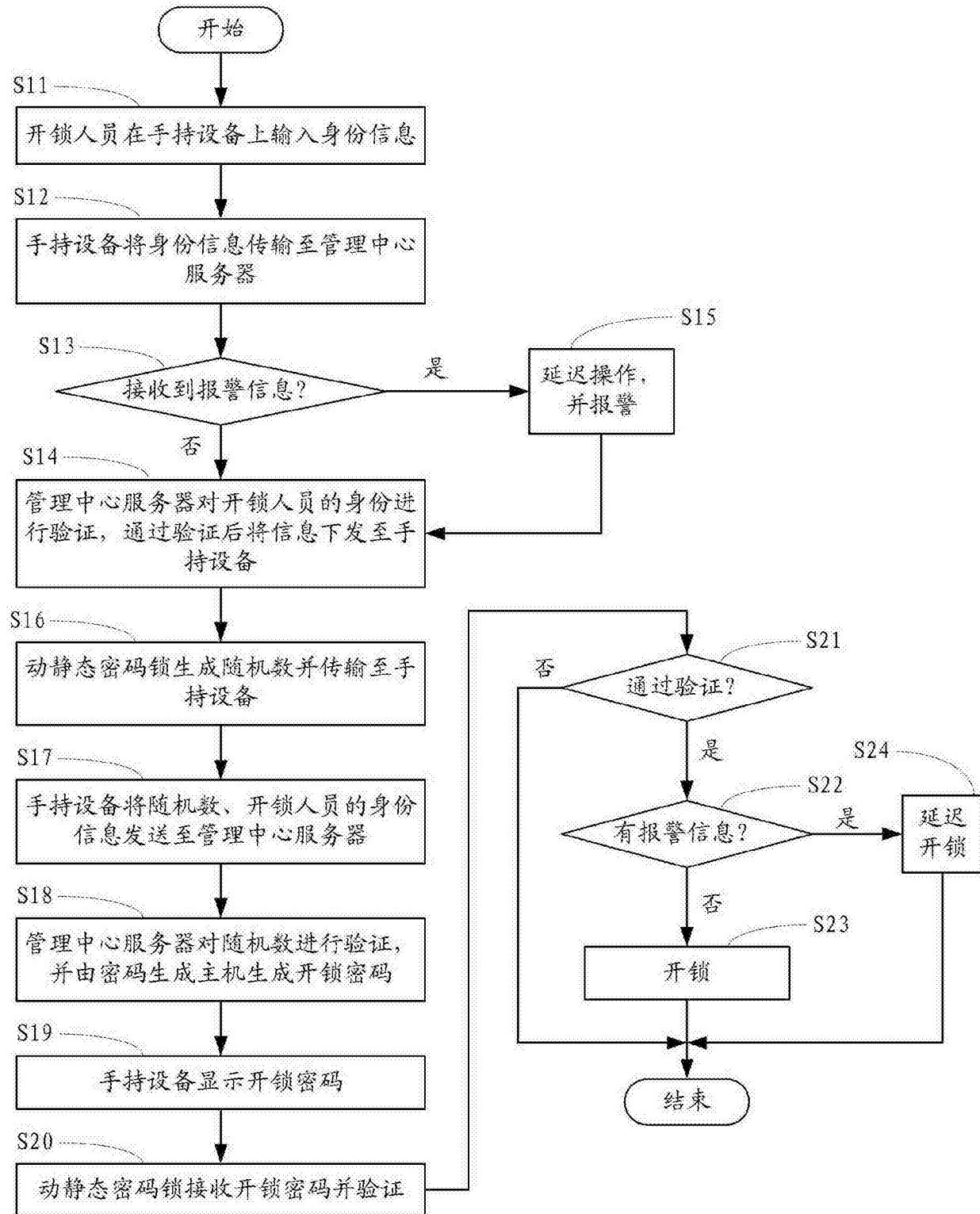


图 4

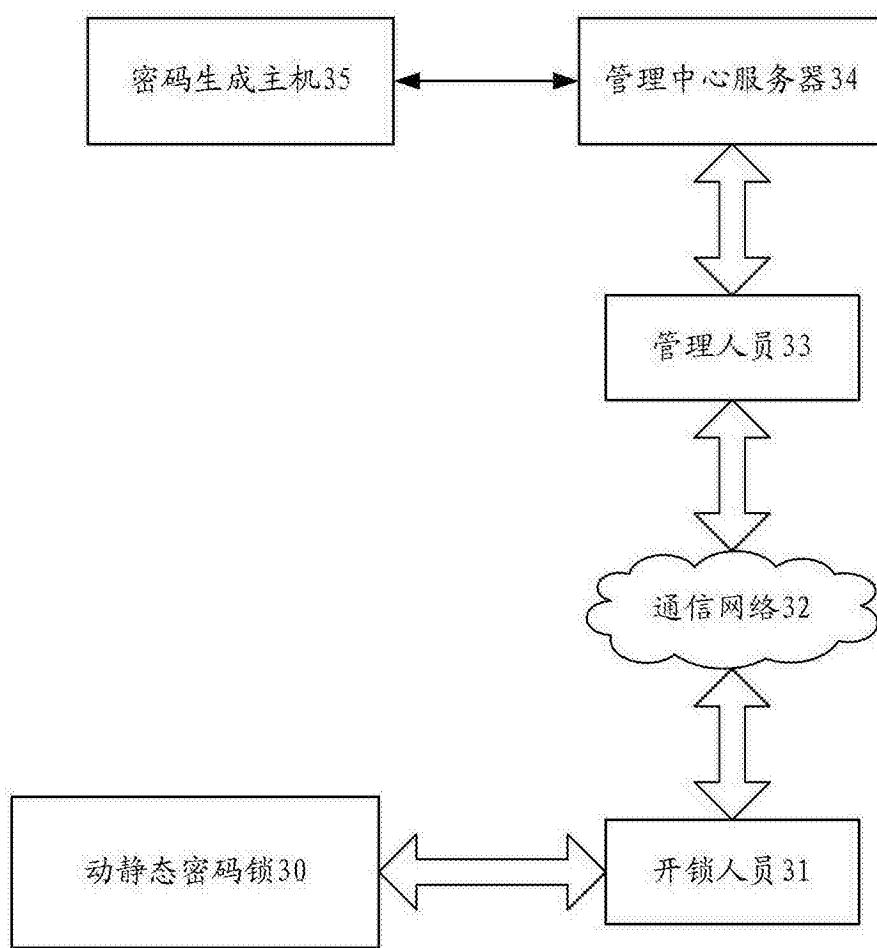


图 5

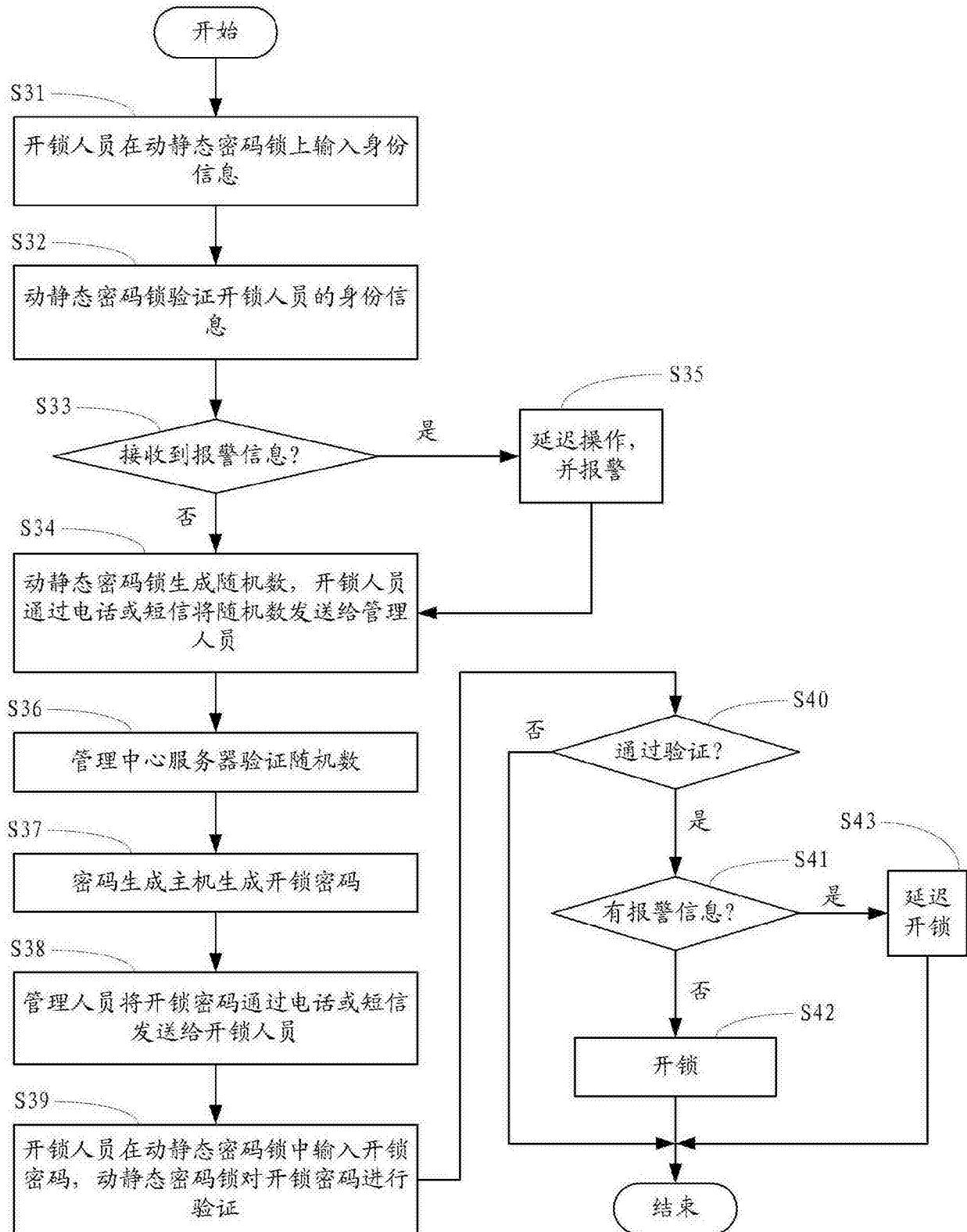


图 6

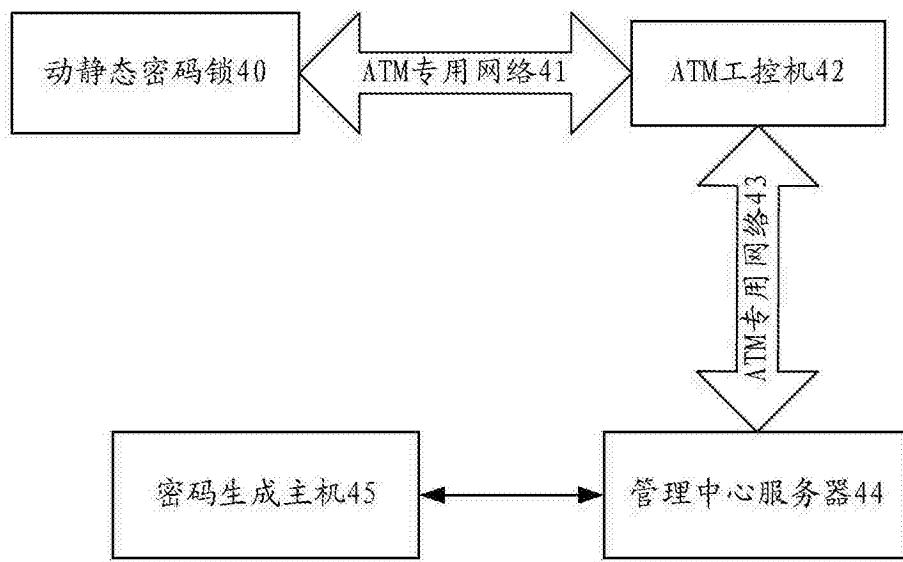


图 7

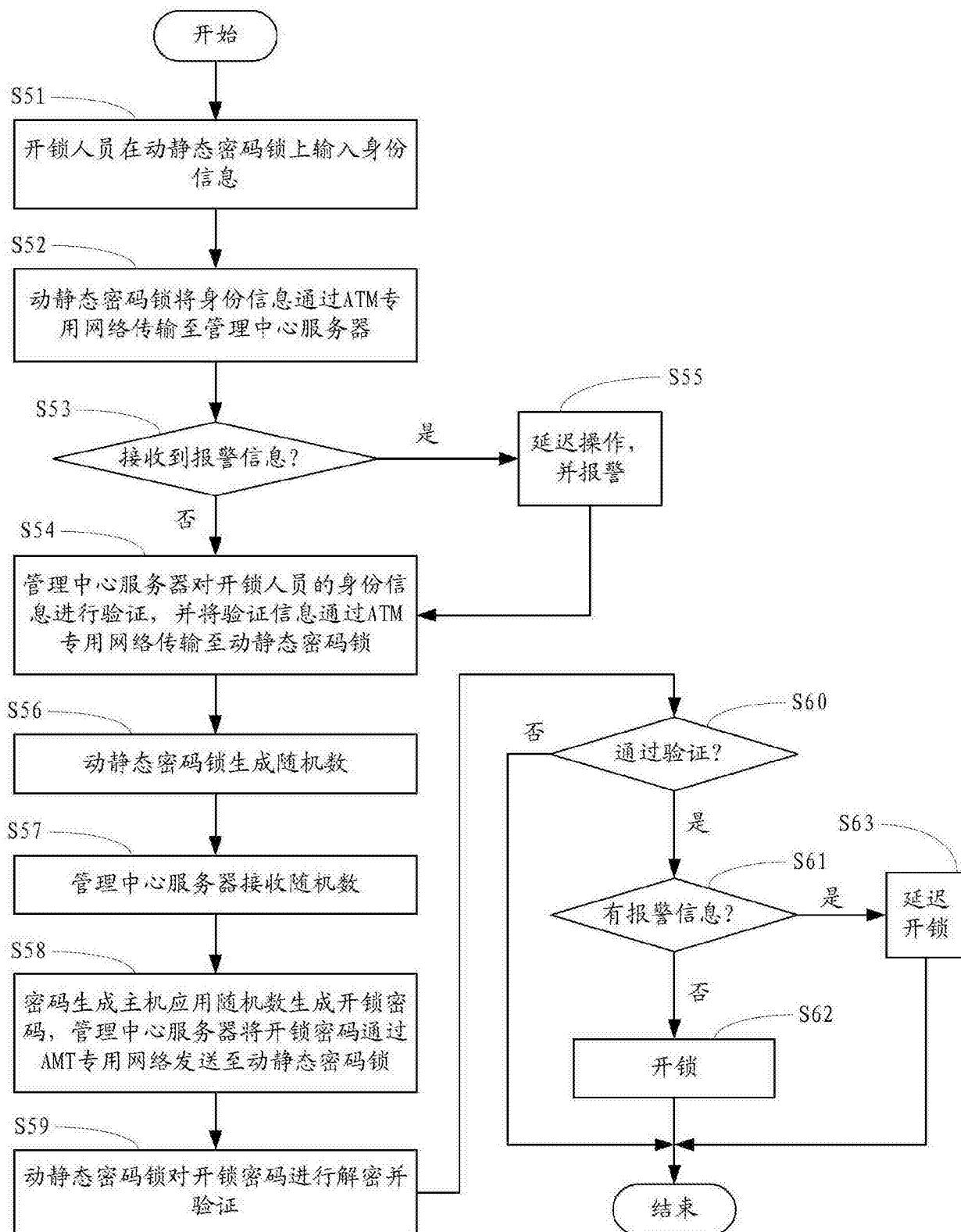


图 8