



(12) 发明专利

(10) 授权公告号 CN 110169031 B

(45) 授权公告日 2023. 09. 19

(21) 申请号 201780082854.0

(22) 申请日 2017.12.12

(65) 同一申请的已公布的文献号
申请公布号 CN 110169031 A

(43) 申请公布日 2019.08.23

(30) 优先权数据
62/444017 2017.01.09 US

(85) PCT国际申请进入国家阶段日
2019.07.09

(86) PCT国际申请的申请数据
PCT/US2017/065682 2017.12.12

(87) PCT国际申请的公布数据
W02018/128754 EN 2018.07.12

(73) 专利权人 开利公司
地址 美国佛罗里达州

(72) 发明人 A. 屈恩齐

(74) 专利代理机构 中国专利代理(香港)有限公
司 72001
专利代理师 李啸 张金金

(51) Int.Cl.
H04L 9/40 (2022.01)

H04W 12/63 (2021.01)

H04W 12/30 (2021.01)

H04W 12/04 (2021.01)

H04W 12/47 (2021.01)

G07C 9/00 (2020.01)

H04W 4/80 (2018.01)

H04W 4/02 (2018.01)

H04W 76/14 (2018.01)

H04L 9/08 (2006.01)

G06Q 50/12 (2012.01)

(56) 对比文件

US 2003208386 A1, 2003.11.06

US 2013060689 A1, 2013.03.07

CN 103503408 A, 2014.01.08

US 2011282785 A1, 2011.11.17

CN 103475623 A, 2013.12.25

CN 104700479 A, 2015.06.10

CN 101246607 A, 2008.08.20

CN 105103174 A, 2015.11.25

CN 106097492 A, 2016.11.09

CN 105069876 A, 2015.11.18

CN 103248484 A, 2013.08.14

审查员 陈露

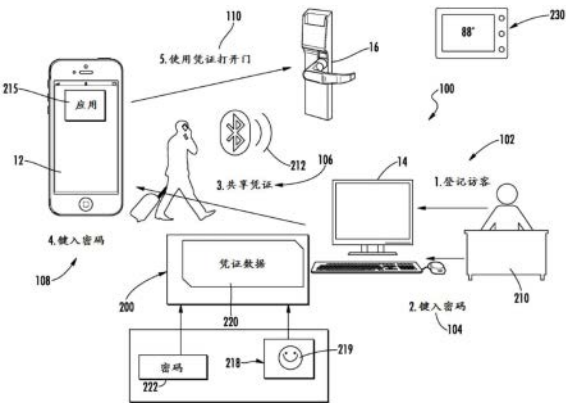
权利要求书1页 说明书8页 附图5页

(54) 发明名称

具有本地移动密钥分配的门禁控制系统

(57) 摘要

一种系统包括在移动装置上的可操作以与本地门户通信的应用,所述应用可操作以从所述本地门户接收移动密钥并且根据所述移动密钥来检索用于授权用户访问门禁控制的移动凭证。一种本地密钥分配方法能够包括:将预共享密码键入到本地门户以对移动凭证加密;将所述加密的移动凭证传达到所述移动装置上的应用;以及将所述预共享密码键入到所述移动装置上的所述应用以解密所述移动凭证。



CN 110169031 B

1. 一种具有本地密钥分配的系统,所述系统包括:

门禁控制的移动密钥卡,所述移动密钥卡可操作以编码有移动密钥并且将所述移动密钥传达到所述门禁控制;以及

在移动装置上的可操作以与所述门禁控制通信的应用,所述应用可操作以从所述门禁控制接收所述移动密钥并且响应于将预共享密码键入到所述应用中而根据所述移动密钥解密移动凭证使得所述应用上的所述移动凭证可操作以访问所述门禁控制;

其中所述移动密钥是通过键入所述预共享密码以在生成所述移动凭证之后对所述移动凭证加密而形成的。

2. 如权利要求1所述的系统,其中生成所述移动凭证是利用加密密钥的本地数据库来执行。

3. 如权利要求1所述的系统,其中生成所述移动凭证是利用本地门户能够访问的集中式云服务来执行。

4. 如权利要求1所述的系统,其中所述移动凭证可操作以访问服务。

5. 如权利要求4所述的系统,其中所述服务是恒温器。

6. 如权利要求1所述的系统,其中所述移动密钥可操作以使所述应用换肤。

7. 如权利要求1所述的系统,其中在所述移动装置上的所述应用可操作以经由蓝牙、NFC、电子邮件和SMS文本消息传递中的至少一者与本地门户通信。

8. 如权利要求1所述的系统,所述系统还包括显示器,所述显示器可操作以呈现待通过所述移动装置扫描的图像,其中所述图像是基于所述移动密钥生成。

9. 一种本地密钥分配方法,所述方法包括:

键入预共享密码以在生成移动凭证之后对所述移动凭证加密以形成移动密钥;

利用所述移动密钥对移动密钥卡进行编码;

将所述移动密钥首先从所述移动密钥卡传达到门禁控制,然后从所述门禁控制传达到移动装置上的应用;以及

将所述预共享密码键入到所述移动装置上的所述应用以解密所述移动凭证使得所述应用上的所述移动凭证可操作以访问所述门禁控制。

10. 如权利要求9所述的方法,其中键入所述预共享密码包括键入驾照号码。

11. 如权利要求9所述的方法,其中键入所述预共享密码包括键入确认码。

12. 如权利要求9所述的方法,其中传达所述加密的移动凭证包括经由蓝牙进行通信。

13. 如权利要求9所述的方法,其中传达所述加密的移动凭证包括经由SMS文本消息传递进行通信。

14. 如权利要求9所述的方法,其中传达所述加密的移动凭证包括经由电子邮件进行通信。

15. 如权利要求9所述的方法,其中将所述预共享密码键入到本地门户在登记时发生。

16. 如权利要求9所述的方法,所述方法还包括响应于将所述加密的移动凭证传达到所述移动装置而与本地门户通信以指示访客偏好。

具有本地移动密钥分配的门禁控制系统

技术领域

[0001] 本公开通常涉及门禁控制系统,并且更特别地,涉及本地移动密钥分配的方法。

背景技术

[0002] 凭证服务通常在云或场外位置中代管,凭证服务能够将移动凭证(对访问权限编码的安全加密的可验证数据)发出到移动装置以用于打开电子锁。有时候,前台或预约系统或本地门户能够将移动凭证发出到移动装置。凭证是在利用访客的账户识别访客之后发出。通常,访客经由旅馆忠诚计划来创建并且管理关联到凭证服务的账号。

[0003] 需要账号创建,使得前台能够在系统中识别访客,然后将移动凭证发出到访客的账户。举例来说,在凭证服务中利用唯一识别符、利用电话号码或利用电子邮件地址来识别访客。访客识别所需的这种账号设置与管理过程还需要相对复杂的交互作用,以管理每个访客账号。复杂的账号设置与管理过程包括初始的账号设置、账号管理、密码管理(密码改变、密码过期、忘记密码)、账号恢复和账号删除。

发明内容

[0004] 根据本公开的一个公开的非限制性实施方案的系统能够包括在移动装置上的可操作以与本地门户通信的应用,所述应用可操作以从所述本地门户接收移动密钥并且根据所述移动密钥来检索用于授权用户访问门禁控制的移动凭证。

[0005] 本公开的又一实施方案可以包括所述本地门户可操作以接收预共享密码以在生成所述移动凭证之后对所述移动凭证加密以形成移动密钥。

[0006] 本公开的又一实施方案可以包括所述应用可操作以响应于将所述预共享密码键入到所述应用中而根据移动密钥来解密所述移动凭证。

[0007] 本公开的又一实施方案可以包括生成所述移动凭证是利用加密密钥的本地数据库来执行。

[0008] 本公开的又一实施方案可以包括生成所述移动凭证是利用所述本地门户能够访问的集中式云服务来执行。

[0009] 本公开的又一实施方案可以包括所述移动凭证可操作以操作门禁控制。

[0010] 本公开的又一实施方案可以包括所述移动凭证可操作以访问服务。

[0011] 本公开的又一实施方案可以包括所述服务是恒温器。

[0012] 本公开的又一实施方案可以包括所述移动密钥可操作以使所述移动应用换肤。

[0013] 本公开的又一实施方案可以包括在所述移动装置上的所述应用可操作以经由蓝牙、NFC、电子邮件和SMS文本消息传递中的至少一者与所述本地门户通信。

[0014] 本公开的又一实施方案可以包括移动密钥卡,所述移动密钥从所述移动密钥卡传达到所述移动应用。

[0015] 本公开的又一实施方案可以包括所述移动密钥首先从所述移动密钥卡传达到门禁控制,然后从所述门禁控制传达到所述移动应用。

[0016] 本公开的又一实施方案可以包括显示器,所述显示器可操作以呈现待通过所述移动装置扫描的图像,所述图像是基于所述移动密钥生成。

[0017] 根据本公开的一个公开的非限制性实施方案的本地密钥分配方法能够包括:将预共享密码键入到本地门户以对移动凭证加密;将所述加密的移动凭证传达到所述移动装置上的应用;以及将所述预共享密码键入到所述移动装置上的所述应用以解密所述移动凭证。

[0018] 本公开的又一实施方案可以包括键入所述预共享密码包括键入驾照号码。

[0019] 本公开的又一实施方案可以包括键入所述预共享密码包括键入确认码。

[0020] 本公开的又一实施方案可以包括传达所述加密的移动凭证包括经由蓝牙进行通信。

[0021] 本公开的又一实施方案可以包括传达所述加密的移动凭证包括经由SMS文本消息传递进行通信。

[0022] 本公开的又一实施方案可以包括传达所述加密的移动凭证包括经由电子邮件进行通信。

[0023] 先前特征和要素可以以各种组合非排他性地组合,除非另有明确指示。这些特征和要素以及其操作将根据以下描述和附图变得更明显。然而,应当理解,以下描述和图式意图在本质上是示例性的,并且是非限制性的。

附图说明

[0024] 所属领域的技术人员将从公开的非限制性实施方案的以下详细描述了解各种特征。伴随详细描述的图式能够简要地描述如下:

[0025] 图1是用户鉴别系统的一般示意性系统图;

[0026] 图2是电子锁系统的框图;

[0027] 图3是根据一个实施方案的凭证方法的本地通信的流程图;

[0028] 图4是根据另一实施方案的凭证方法的本地通信的流程图;

[0029] 图5是根据另一实施方案的凭证方法的本地通信的流程图;以及

[0030] 图6是根据另一实施方案的凭证方法的本地通信的流程图。

具体实施方式

[0031] 图1示意性地图示用户鉴别系统10。系统10通常包括移动装置12、本地门户14和示意性地图示为16a、16b、……、16n的多个门禁控制16。应当了解,尽管在示意性框图中单独地定义了特定系统,但是所述系统中的每一个或任何一个可以经由硬件和/或软件以其他方式组合或分开。

[0032] 移动装置12是具无线能力的手持装置,例如可操作以经由应用“app”与本地门户14和门禁控制16通信的智能电话装置,所述应用在智能电话装置(在本文中也被称为移动装置12)上运行。本地门户14可以向移动装置12提供移动凭证和其他数据,例如固件或软件更新,从而传达到门禁控制16中的一个或多个。尽管本地门户14在本文中被描绘为单个装置(例如供人使用以使用、生成移动密钥200的计算机、平板、电话,或一般地,具有输入端和输出端的单个计算装置等,如本文中所描述),但是应当了解,本地门户14可以替代地体现

为许多系统,移动装置12从所述系统接收凭证和其他数据。

[0033] 每个门禁控制16是具无线能力、访问受限或使用受限的装置,例如无线锁、用于建筑物入口的门禁控制读取器、电子银行控制件、数据传送装置、密钥分配器装置、工具分配装置、汽车点火系统、车门锁或车厢锁以及其他使用受限的机器。移动装置12将凭证提交到门禁控制16,由此选择性地准许用户访问或激活门禁控制16的功能。用户可以例如将凭证提交到机电锁以打开所述锁,并且由此能够进入限制区。在另一实例中,用户可以将凭证提交到电子银行控制件以取款。在更另外实例中,用户可以将凭证提交到分配具有与凭证相关联的数据或从凭证检索的数据的密钥卡的单元。在又一另外实例中,用户可以将凭证提交到能够访问计算机系统的单元。移动装置12可以存储用于上文所提及的实例中的一个或全部或其他的凭证,并且另外可以同时存储用于每个类型的应用的多个凭证。一些凭证可以用于多个门禁控制16。举例来说,设施中的多个电子锁可以响应同一凭证。其他凭证可以特定于单个门禁控制16。

[0034] 参考图2,示例电子锁系统20的框图包括门禁控制16a、移动装置12和本地门户14。门禁控制16a通常包括锁致动器22、锁控制器24、锁天线26、锁收发器28、锁处理器30、锁存储器32、锁电源34、锁读卡器90和凭证模块36。门禁控制16a对来自移动装置12的凭证作出响应,并且可以例如是锁盒的锁、门锁或锁芯。尽管本公开主要关注用于门禁控制的凭证,但是应当了解,其他系统(其中凭证从移动装置传输到门禁控制,以便向线上系统证明用户或在离线系统中验证用户访问权限或许可)将自本公开获益。这些系统包括虚拟或电子银行系统、机器操作系统、分配系统、数据访问系统和计算机访问系统。

[0035] 在从移动装置12接收适当凭证并且使用凭证模块36进行鉴别之后,或在从锁读卡器90接收到卡数据之后,锁控制器24命令锁致动器22锁上或打开机械或电子锁。锁控制器24和锁致动器22可以是单个电子或机电锁单元的部分,或可以是单独售卖或安装的部件。

[0036] 锁收发器28能够将数据传输到至少移动装置12和从至少移动装置12接收数据。锁收发器28可以是例如近场通信(near field communication;NFC)、蓝牙或Wi-Fi收发器,或另一适当的无线收发器。锁天线26是适合锁收发器28的任何通信。锁处理器30和锁存储器32分别是数据处理装置和存储装置。锁处理器30可以是例如微处理器,微处理器能够处理指令以验证卡数据并且确定卡数据中所含的访问权限,或将消息从收发器传递到凭证模块36,并且接收从凭证模块36返回的具有卡数据的响应指示。锁存储器32可以是RAM、EEPROM或其他存储介质,其中锁处理器30能够读取和写入包括但不限于锁配置选项和锁审计踪迹的数据。锁审计踪迹可以是包括通过经由锁读卡器90或移动装置12访问锁来起始的事件的统一审计踪迹。锁电源34是为锁控制器24供电的电源,例如电力线连接件、电力清除系统或电池。在其他实施方案中,在锁致动器22主要或全部由例如用户工作(例如转动螺栓)的另一源供电的情况下,锁电源34只可以为锁控制器24供电。

[0037] 凭证模块36与锁处理器30通信,并且可操作以解密并且验证凭证,以提取传达到锁控制器24中的虚拟卡数据作为“虚拟卡读数”。就是说,门禁控制16a基本上具有两个读取器,一个读取器90用于读取物理密钥卡92和凭证模块36,以经由锁处理器30和收发器28和天线26与移动装置12通信。

[0038] 移动装置12通常包括密钥天线40、密钥收发器42、密钥处理器44、密钥存储器46、GPS接收器48、输入装置50、输出装置52和密钥电源54。密钥收发器42是对应于锁收发器28

的收发器类型,并且密钥天线40是对应天线。在一些实施方案中,关键收发器42和关键天线40还可以用于与本地门户14通信。在其他实施方案中,可以包括一个或多个单独的收发器和天线以与本地门户14通信。密钥存储器46是用于在移动装置12上在本地存储多个凭证的类型。

[0039] 参考图3,从功能框图方面公开方法100。应当了解,这些功能可以在能够在各种基于微处理器的电子设备控制实施方案中执行的专属硬件电路或程序软件例程中进行。

[0040] 方法100不要求本地门户14识别访客,但是会局部地(例如在物业前台210处)将移动密钥200分配给移动装置12,而不需要复杂相互作用以管理访客账号。方法100准许本地门户14对移动密钥200“编码”并且将移动密钥200安全地传递到移动装置12,所述传递通过例如直接到移动装置的应用215的蓝牙212;通过到移动装置12可访问的电子邮件地址,使得相关的移动密钥数据200能够通过拷贝从电子邮件传送并且粘贴到应用215中;和/或通过SMS文本消息发送到移动装置12,再次从文本消息拷贝并且粘贴到应用215中。在电子邮件或SMS的情况下,移动密钥数据200还可以利用专门链接传送到应用215中,当“点击”或访问所述专门链接时,移动装置启动应用215并且将数据200传送到所述应用中。或者,数据200能够渲染到例如QR码、图像、图片等的图像219中,并且应用215能够利用移动装置12扫描图像219,所述图像在例如靠近前台210的服务亭或屏幕或显示器218和作为本地门户14或具有本地门户14的部分中呈现。应用215接着能够处理图像219以获得移动密钥数据200。

[0041] 为了安全地传送移动凭证数据220,用预共享密码222对数据220加密(例如,如同加密ZIP文件或其他加密文件格式),所述预共享密码例如驾照号码、物业确认码、图像、(例如用于支付旅馆停留的)信用卡号码、电话号码、电子邮件地址、其他片段的预共享数据,或这些数据中的任一者的组合。理想地,在访客到达之前基于与物价共享的信息来确定密码222,使得当访客出现在前台210时和当移动密钥200从本地门户14发送到移动装置12时,所述密码不被共享。这个加密的移动凭证数据220也被称作移动密钥200。通过将预共享密码222键入到应用215中,能够根据移动密钥数据200解密凭证数据220,并且能够接着利用所述凭证数据。

[0042] 最初,访客登记(步骤102)准许物业管理员(即旅馆前台接待员)经由包括集中式预约系统、物业管理系统等标准物业工具/方法将访客登记。就是说,物业人员将使用例如人工检查驾照或其他证件的标准方法来验证访客的真实身份。

[0043] 一旦访客经过登记,即从可用信息选择预共享密码222并且将所述预共享密码键入(步骤104)到本地门户14中。就是说,除了选择客房和/或指示标准额外授权(包括但不限于停车场、泳池等)之外,物业人员还可以设定预共享密码222。基于先前已知值(例如物业确认码)或其他信息,预共享密码222能够在当时达成一致(例如使用驾照号码)。本地门户14接着根据所述预共享密码生成移动密钥数据200。这种生成能够例如利用加密密钥的本地数据库和相关联门禁控制16信息来执行,以供物业创建凭证数据220。这些加密密钥可以是对称形式,其中本地门户14和门禁控制16各自具有同一个加密密钥的拷贝,并且移动凭证数据220是通过本地门户14生成并且能够由门禁控制16基于知道相同密钥来验证。或者,加密密钥可以是不对称形式,其中例如,本地门户14可以持有用于建构移动凭证数据220的私人密钥,所述移动凭证数据220可以由门禁控制16基于知道相应的公共密钥来验证。此外,如所属领域的技术人员众所周知的,凭证数据220可以由多个凭证组成,所述多个凭证

还可以包括能够创建信任链的证书,在所述信任链中,本地门户14具有被持有认证私人密钥的认证方宣告值得信任的公共/私人密钥对。如果门禁控制16知道认证公共密钥,则所述门禁控制能够验证宣告本地门户14公共密钥值得信任的证书。验证证书将通过使用加密密钥验证证书的数字签名来进行,其中所述签名将仅在证书的内容未改变的情况下可验证。接着,在验证本地门户14公共密钥值得信任之后,所述门禁控制能够通过使用本地门户14公共密钥来另外验证凭证数据220是有效的。前述实例概述一个保证人可如何为本地门户担保,但是所属领域的技术人员能够创建保证人的链或阶层,其中一个保证人为另一人担保,直到最后,最后一个保证人为本地门户担保。只要门禁控制16具有根公共密钥,整个证书链即能够遍历并且得到验证。或者,替代在本地生成凭证数据200,本地门户14能够访问例如托管在云中或安全网络上的另一服务,以请求生成移动凭证数据220。接着用预共享密码222对凭证数据220加密,从而产生移动密钥数据200,然后能够使所述移动密钥数据可供访客及其恰当指定的门禁控制16获得。凭证数据220能够包括例如数据,例如:

[0044] a. 用于授权访客打开相关联客房门禁控制的凭证数据,包括但不限于可编码到物理塑料磁条或RFID卡上的相同数据。

[0045] b. 用于其他接入点、例如wi-fi网络接入、其他门禁控制系统(例如,徽章id)所需的凭证数据,或供凭证模块36使用的鉴别信息,凭证模块36需要所需鉴别信息以验证、解密并且检索凭证数据以打开相关联的客房门禁控制。

[0046] c. 能够用于例如针对特定物业“换肤”或定制移动应用215在显示于移动装置12上的视觉外观的标志、图片、URL或其他数据。这种“换肤”可以在移动密钥数据200已通过移动应用215接收到并且数据已经用密码222解密之后发生,或“换肤”可以在接收移动密钥数据200时发生,如果“换肤”数据的部分包括在移动密钥数据200内,但是没有用密码222加密。此外,“换肤”可以在结合确定移动装置12的当前位置(例如,GPS坐标)加载移动密钥数据200时发生,确定是移动装置必须在处于那个位置的物业(例如旅馆),并且单独地从公共位置(例如旅馆网站)检索“换肤”数据。

[0047] d. 远程编程数据,所述远程编程数据供例如访客门锁的门禁控制16改变可编程参数(例如改变加密密钥、更新时间表或校正实时时钟,或任何其他典型的门禁控制参数)。这种远程编程数据可以在不知道访客的情况下通过应用215发送到门禁控制16,并且可以是使用“sneaker net”的锁管理系统方法的部分。

[0048] e. 用于鉴别其他服务(例如客房中的恒温器230)的凭证数据。

[0049] 接下来,共享移动密钥数据200(步骤106)。就是说,将移动密钥数据200从本地门户14直接发送到移动装置12,不需要经由云代管的凭证服务路由。另外,访客能够将其移动密钥数据200连同其预共享密码222共享,使得凭证220能够另外传送到另一移动装置12。访客能够发送由本地门户14提供的同一移动密钥数据200和密码222,或者访客能够使用应用215利用不同的密码222将凭证数据220加密到单独的移动密钥数据200中。移动密钥数据200能够使用本地门户14用于本地分配的相同方法从一个移动装置12共享到另一移动装置12。举例来说,访客能够将数据200用电子邮件发送给朋友。或者,访客可以经由SMS发送所述数据。或者,访客的电话可以呈现图片或图像219,访客朋友的移动装置12可利用朋友装置上的相机来查看/接收所述图片或图像。这样提供不需要账号管理或其他云服务而在本地将凭证数据220分配给朋友的有效方式。

[0050] 详细地,存在几种共享移动密钥200的方法:

[0051] a. 蓝牙:在这个实施方案中,本地门户14用于经由蓝牙将移动密钥200发送到直接在移动装置12上的应用215。在应用215中,访客能够选择例如“获得我的密钥”的特征,和/或物业人员可选择本地门户14上的“发送密钥”的特征。一旦激活,本地门户14和移动装置12可以发现彼此,建立蓝牙连接,并且将移动密钥200从本地门户14传送到移动装置12上的应用215。

[0052] b. 电子邮件:在这个实施方案中,本地门户14用于将移动密钥200作为文件附件发送到电子邮件地址。在接收到之后,接着可将文件附件拷贝/粘贴到应用215中。这个过程也能够通过如下操作来执行:将特定文件类型与相关联应用215关联,使得当从移动装置12上的电子邮件客户端“打开”文件时,应用215启动。或者,移动密钥200可以作为预先格式化的链接在电子邮件中发送。访客点击链接会激活链接并且编码在链路中含有移动密钥200,并且移动装置可以利用编码在链接中的识别应用215的信息来识别并且启动应用215。

[0053] c. SMS:在这个实施方案中,本地门户14用于根据电子邮件实施方案将移动密钥200作为文本消息发送到移动装置12。

[0054] d. 图像:在这个实施方案中,移动应用215能够利用移动装置12上的相机或扫描器对呈现在例如邻近前台210的服务亭218的显示器上的图像219扫描,显示器是本地门户14的部分或与本地门户14相关联。扫描图像219允许移动装置12在应用215处理所述图像以检索所述数据之后接收移动密钥200。

[0055] e. NFC:在这个实施方案中,移动应用215利用移动装置12的近场通信(NFC)能力从本地门户14传送移动密钥200。NFC能够在几种模式下操作,并且这个实施方案可与3种模式中的任一者一起使用。移动装置12和本地门户14可在对等模式下传送移动密钥200。或者,移动装置12和本地门户14可通过移动装置12从附接到本地门户14的读取器装置读取“虚拟卡”来传送移动密钥200,所述虚拟卡模拟~在移动装置12看来是实物卡的ISO14443数据卡。或者,本地门户14可在“读写器”模式下操作,并且利用模拟ISO14443数据卡将ISO14443卡图像写入到移动装置。在所有情况下,数据是使用NFC从本地门户14传送到移动装置12和移动应用215。

[0056] 通过包括将数据从应用215发送回到本地门户14,这种局部内疚可以提供访客偏好或控制数据到前台210的传达。这样增强访客体验,例如,传达访客对软枕头的偏好、不需要叫醒等。就是说,移动装置12上的应用215可以包括经由本地门户14传达回到前台210的偏好选择。此类偏好数据的如此发送可以是回到本地门户14的确认移动密钥数据200的接收的响应的部分。或者,这种偏好数据可以应前台210的要求和通过访客激活移动应用215中的特征在任何时间发送,以实现将偏好数据发送回到前台的过程。

[0057] 一旦在应用215中接收到移动密钥200,访客接着键入预各项密码222以对移动密钥200解密(步骤108)。如此将凭证数据220解密并且存储至应用215中,使得所述凭证数据能够用于操作适当的门禁控制16。

[0058] 最后,通过移动装置12来利用凭证数据220以提供对相关门禁控制16的访问(步骤110)。凭证数据220因而驻留在移动装置12上,并且用户能够接着在任何稍后时间在离线模式下操作适当的门禁控制16。

[0059] 参考图4,在方法100A的另一实施方案中,居住家用访问受利用房主的移动装置12

打开居住门锁16影响。将密钥传递到电话的方法与门禁控制16的原始购买和安装相关联。就是说,这个实施方案中的预共享密码222可以与在销售收据上提供的门禁控制的印刷包装相关联,和/或以其他方式传达到房主。居住门锁16本身可以(例如,经由蓝牙)发送用这个预共享密码加密的移动密钥200。房主接着能够将预共享密码222键入到应用215中并且激活移动密钥200。移动密钥200的发送只可以房主能够激活的方式进行,例如通过在将锁的“安全”侧上的按钮从门卸载时推动所述按钮,并且在某种意义上,这导致门锁16随本地门户14立刻打开并且发送移动密钥200。

[0060] 参考图5,在方法100B的另一实施方案中,能够将门禁控制16与入侵系统配对,所述入侵系统是移动密钥的发送方。在这种情况下,所述入侵系统充当本地门户14。接着将预共享密码222键入到所述入侵系统中,或从所述入侵系统检索预共享密码222。或者,在入侵面板显示器上显示预共享密码222,然后将所述预共享密码键入到应用215中。

[0061] 参考图5,在方法100C的另一实施方案中,在前台向访客分发移动密钥卡,所述移动密钥卡与供特定门禁控制16使用的预共享密码相关联。所述预共享密码可在利用移动密钥200对所述移动密钥卡编码时键入。在将所述移动密钥卡插入至门禁控制16中之后,移动密钥200将从所述卡加载,然后从门禁控制16发送(例如,通过蓝牙)到访客的移动装置12上的应用215中。接着将在所述移动密钥卡上编码的所述预共享密码键入到应用215中以解密凭证220。或者,如果移动装置12支持所述能力,则所述移动密钥卡能够通过移动装置12直接读取以检索移动密钥数据200,例如如果移动装置12支持使用NFC读取RFID。

[0062] 本地凭证分配不要求集中式服务将通过移动装置12使用而不需要复杂的账号管理或云服务。移动密钥200将通过预共享密码222担保,并且用户不必管理又一账号和相关联的密码。物业也不需要云服务,或被要求支付订阅费用以提供更流畅的操作。在本文中、包括在图式中的流程图和框图中所描述和描绘的元件暗示元件之间的逻辑边界。然而,根据软件或硬件工程实践,所描绘的元件及其功能可以经由具有处理器的计算机可执行介质在机器上实现,所述处理器能够执行存储在介质上的程序指令以作为单片软件结构、作为独立软件模块或作为使用外部例程、代码、服务等或这些的任何组合的模块,并且所有这些实现方式可以在本公开的范围。

[0063] 术语“一”、“所述”和类似参考在说明书的背景中(尤其在权利要求的背景中)的使用应解释为覆盖单数和复数两者,除非本文中另有指示或尤其与上下文相矛盾。结合量使用的修饰语“约”包括规定值,并且具有通过上下文决定的意义(例如,所述修饰语包括与特定量的测量结果相关联的误差度)。本文中公开的所有范围包括端点,并且所述端点彼此独立地可组合。

[0064] 尽管不同的非限制性实施方案具有特定说明的部件,但是本发明的实施方案不限于那些特定组合。有可能结合来自其他非限制性实施方案中的任一者的特征或部件使用来自所述非限制性实施方案中的任一者的部件或特征中的一些。

[0065] 应当了解,类似图例编号识别几个图中的对应或类似元件。还应当了解,尽管在所说明的实施方案中公开了特定部件排列,但是其他排列将从所述实施方案获益。

[0066] 尽管示出、描述并且要求了特定的步骤顺序,但是应当理解,除非另有指示,否则步骤可以任何次序执行、分离或组合,并且仍将从本公开获益。

[0067] 先前描述是示例性的,而不是由描述内的限制限定。本文中公开了各种非限制性

实施方案,然而,所属领域的普通技术人员会认识到,根据以上教示内容的各种修改和变化将在所附权利要求的范围内。因此将理解,在所附权利要求的范围内,除了特定描述的以外,可以实践本公开。出于这个原因,应研究所附权利要求以确定真正的范围和内容。

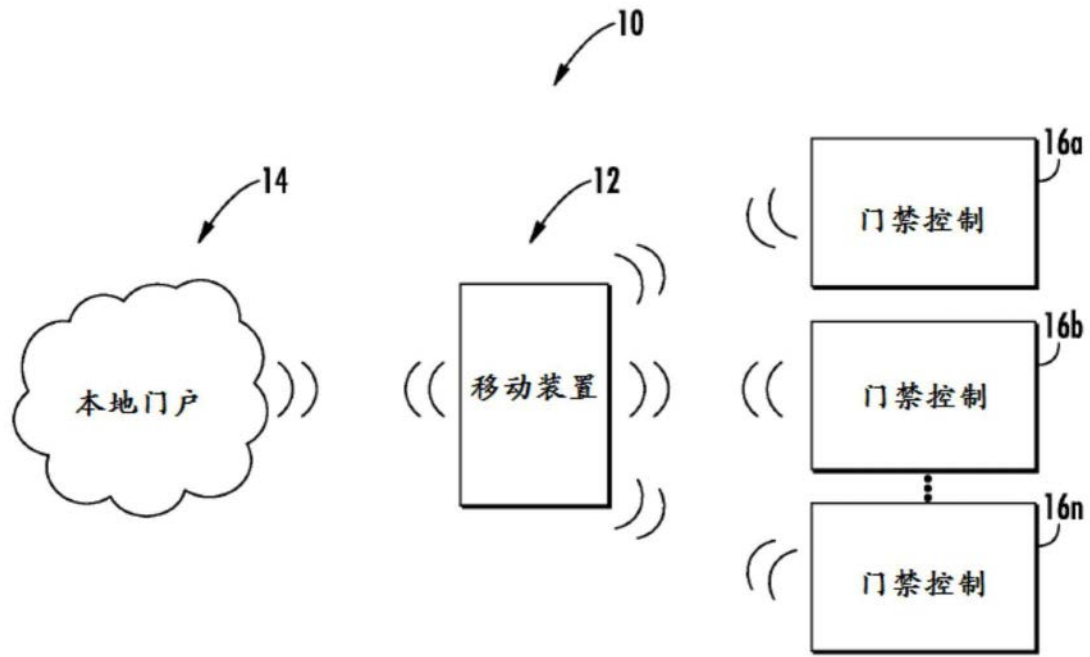


图1

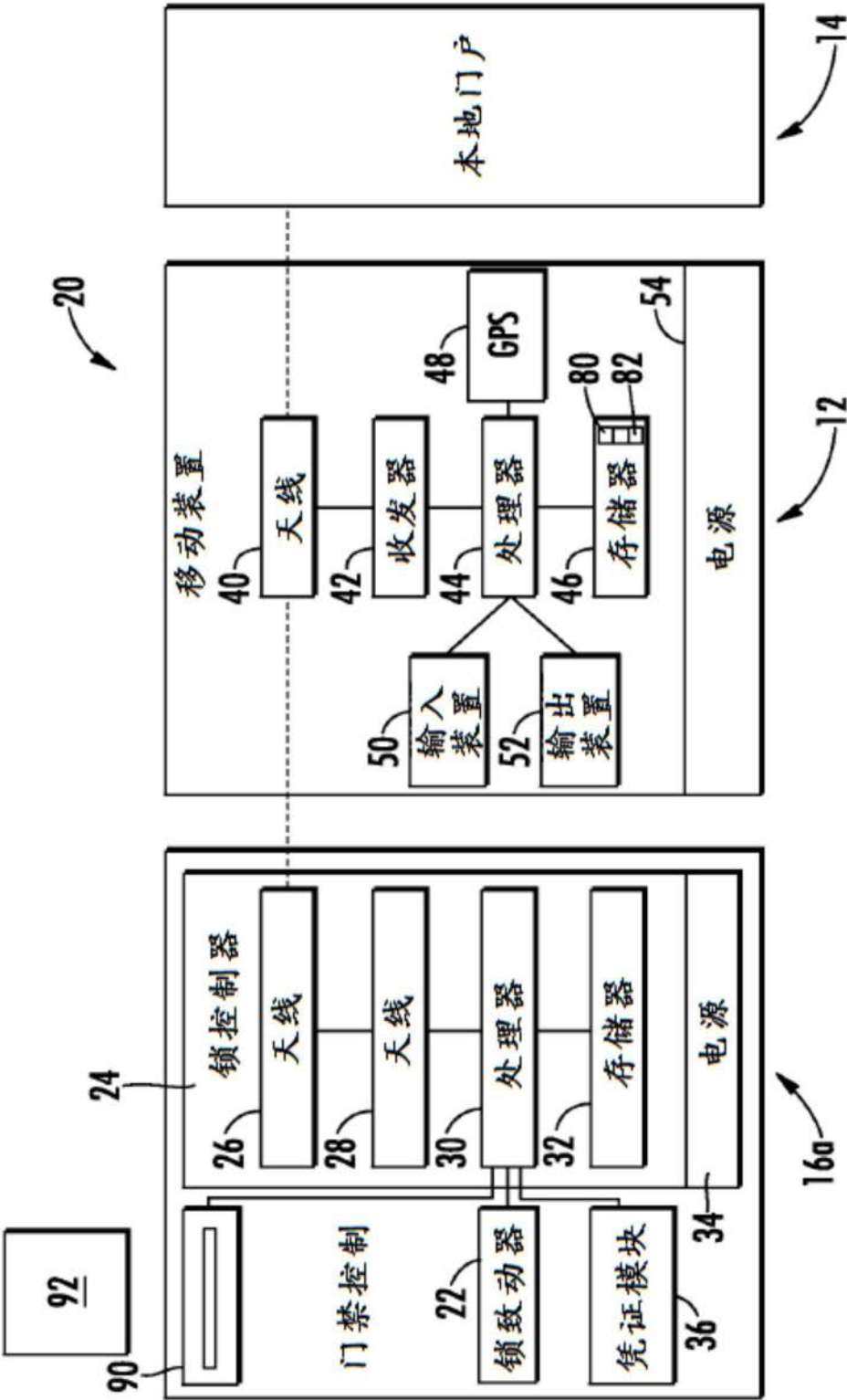


图2

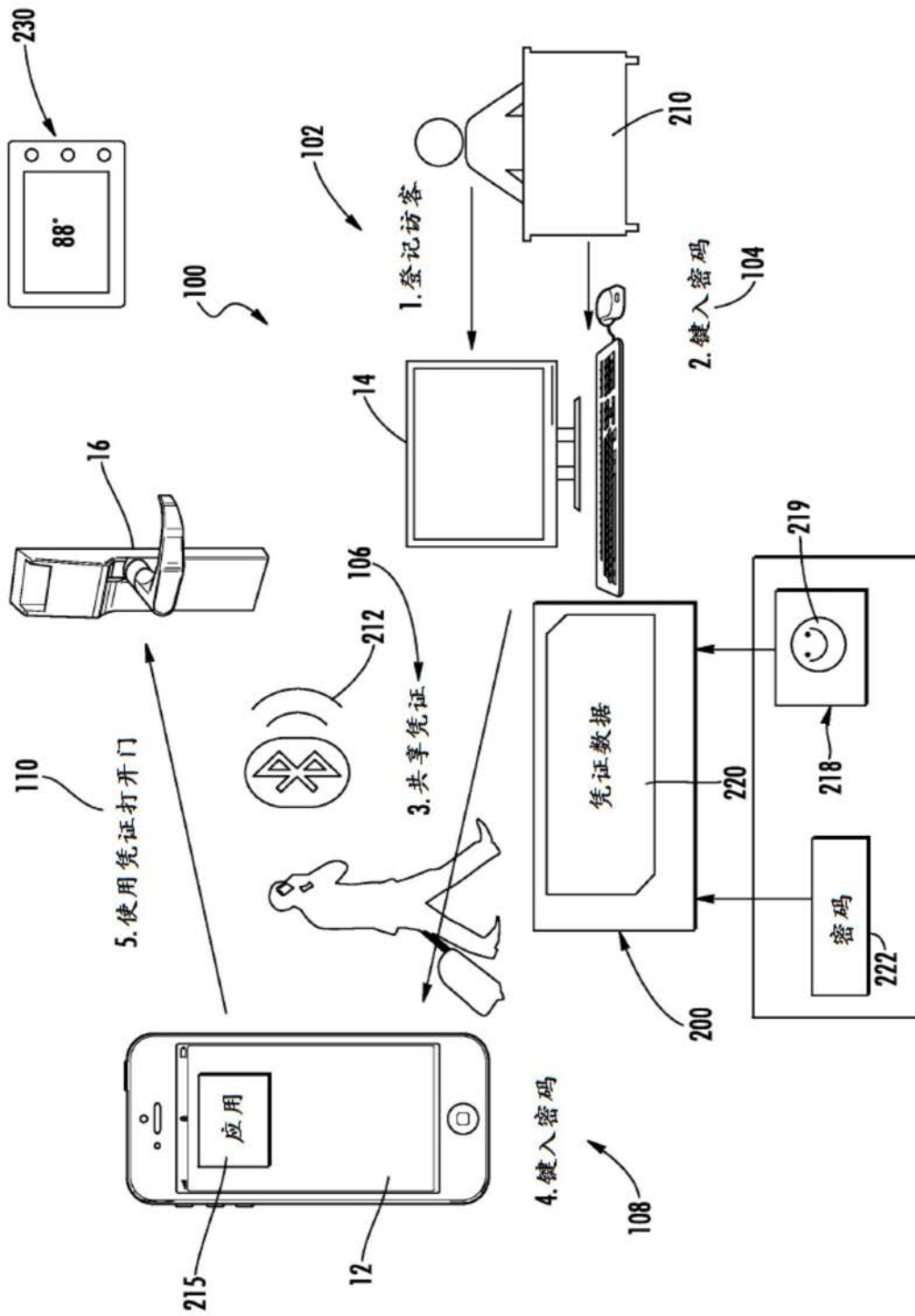


图3

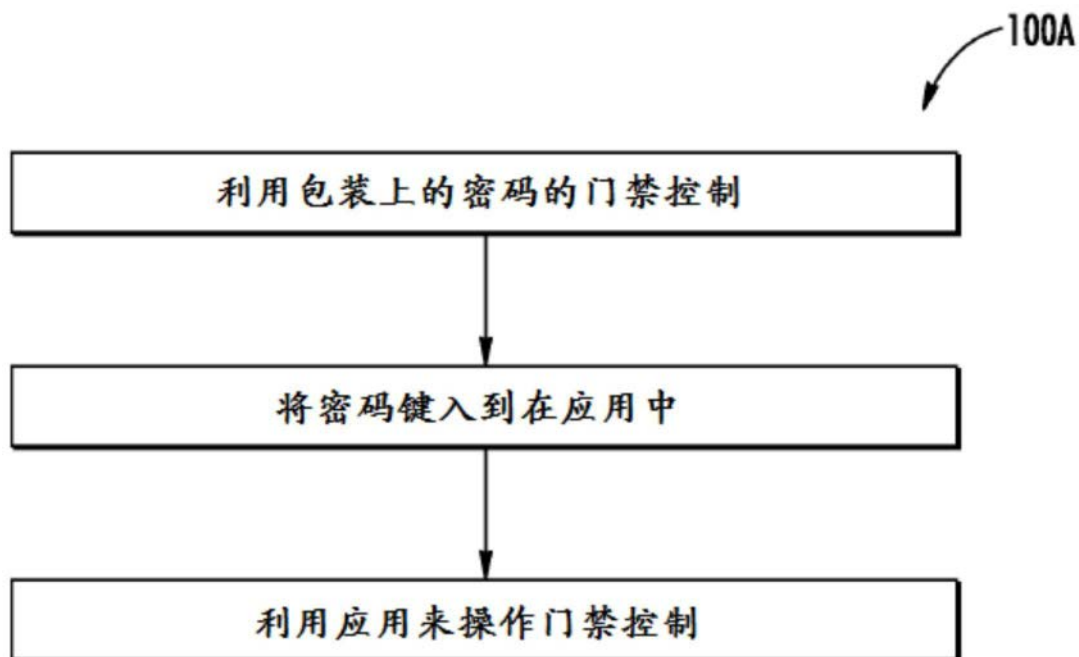


图4

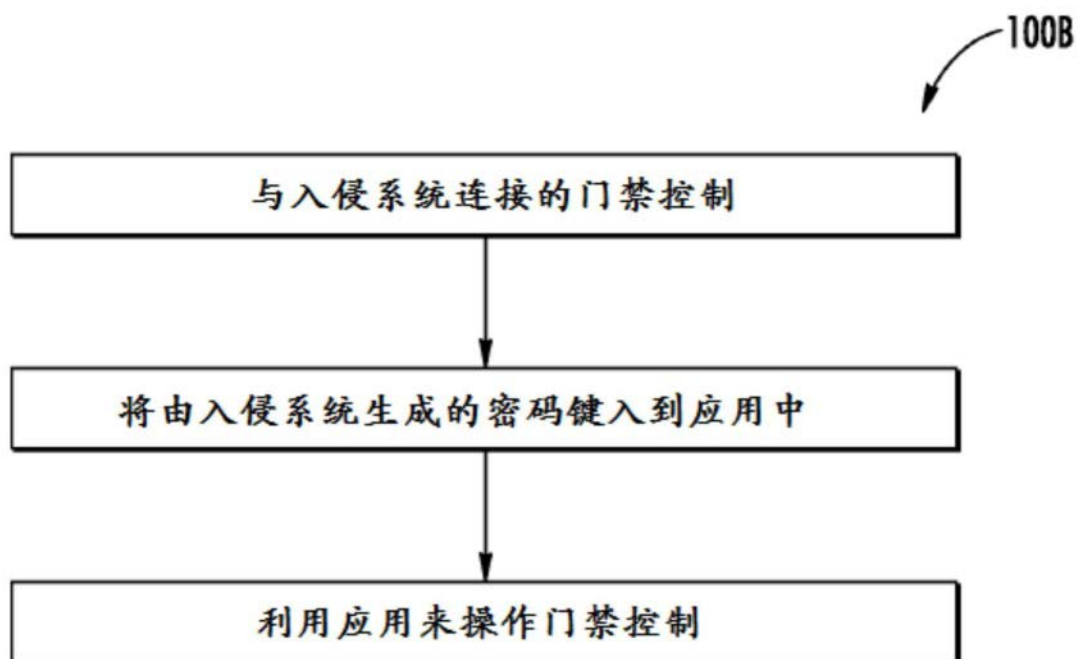


图5

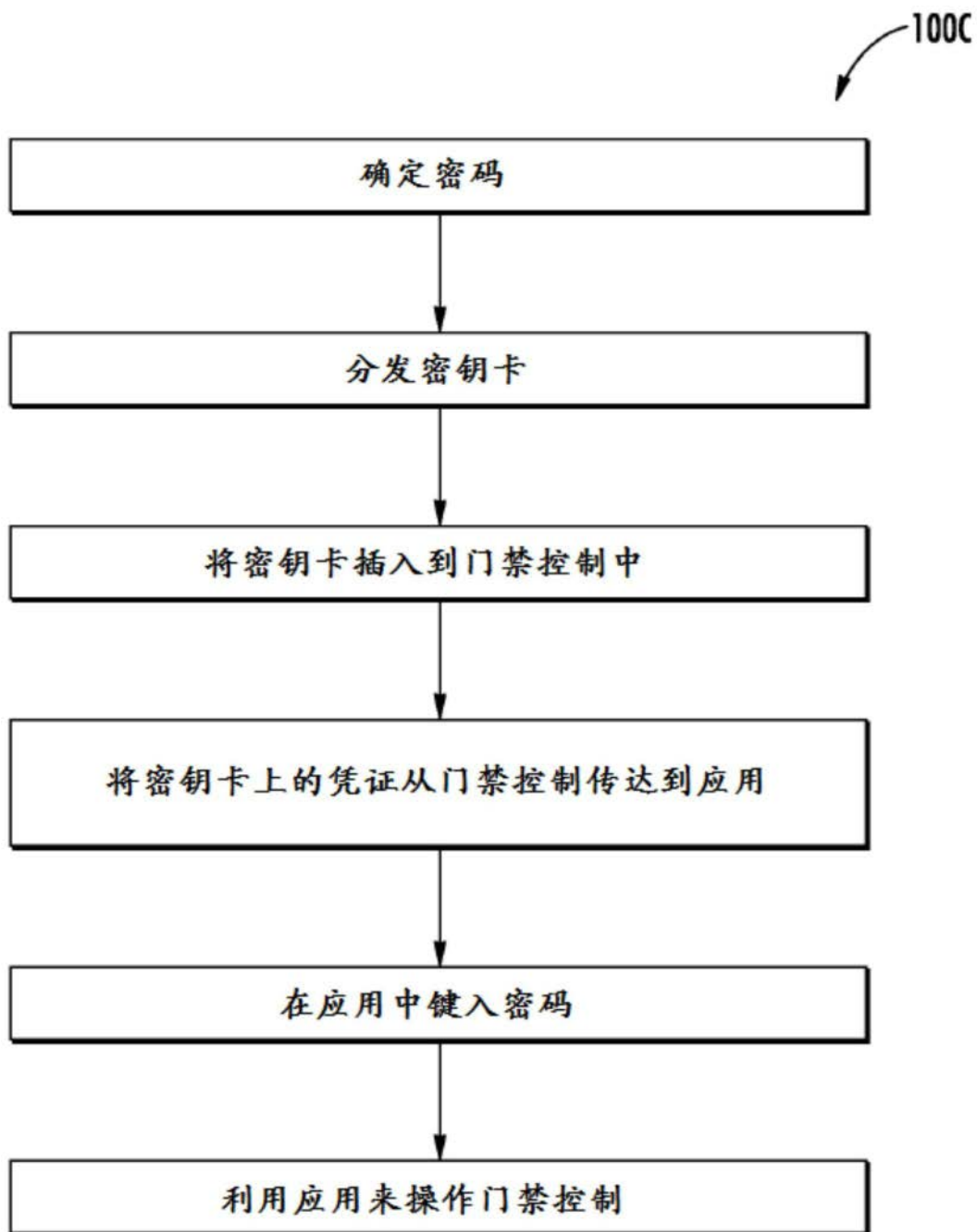


图6