(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 110178161 A
(43)申请公布日 2019.08.27

(21)申请号 201880008136.3

(22)申请日 2018.01.19

(30)优先权数据
62/449399 2017.01.23 US

(85)PCT国际申请进入国家阶段日
2019.07.23

(86)PCT国际申请的申请数据
PCT/US2018/014434 2018.01.19

(87)PCT国际申请的公布数据
WO2018/136744 EN 2018.07.26

(71)申请人 开利公司
地址 美国佛罗里达州

(72)发明人 A.屈恩兹 B.A.斯科维尔

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 郑浩 张金金

(51)Int.Cl.
G07C 9/00(2006.01)

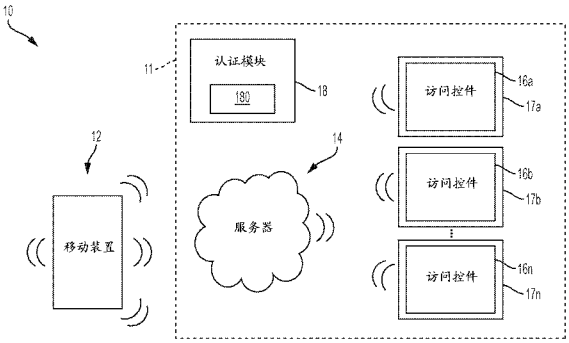
权利要求书2页 说明书8页 附图6页

(54)发明名称

采用安全通过的访问控制系统

(57)摘要

移动装置(12)将凭证发送给认证模块(18)，所述认证模块(18)可以是第一访问控制装置(16a)的凭证模块(36)。如果这些凭证被认证，则所述第一访问控制装置(16a)允许对其关联的第一安全元素(17a)的访问，并且将访问控制装置(16a,16b)放在第二模式中，即，放在安全通过模式中。在所述第二模式中从所述移动装置接收的用来访问第二安全元素(17b)的任何请求被传递并且被当作对第二访问控制装置(16b)的认证请求。所述访问控制装置(16a,16b)基于所请求的访问的类型与凭证的类型是否一致而允许对其关联的安全元素(17a,17b)的访问。



CN 110178161 A

1.一种访问控制系统,包括:

凭证认证器;以及

第一装置和第二装置,所述第一装置和所述第二装置设置用于第一访问限制和第二访问限制,并且可操作在相应第一模式和第二模式中,

所述第一装置响应由移动装置传递于此的用于第一访问的请求,

所述第二装置响应由所述移动装置经由所述第一装置传递于此的用于第二访问的请求,

其中:

在所述相应第一模式中,所述第一装置和所述第二装置分别保持所述第一访问限制和所述第二访问限制,

在所述相应第二模式中,所述第一装置和所述第二装置分别准许所述第一访问和所述第二访问,以及

所述相应第二模式基于凭证从所述移动装置传送给所述凭证认证器并且由所述凭证认证器来认证而实行。

2.如权利要求1所述的访问控制系统,其中所述凭证认证器提供在Bluetooth ™模块内。

3.如权利要求1所述的访问控制系统,其中所述凭证认证器远离所述第一装置和所述第二装置。

4.如权利要求1所述的访问控制系统,其中所述凭证认证器是所述第一装置和所述第二装置其中之一的组件。

5.如权利要求1所述的访问控制系统,其中所述移动装置包括便携计算装置、智能电话和平板中的一个或多个。

6.如权利要求1所述的访问控制系统,其中所述第一装置包括门锁。

7.如权利要求1所述的访问控制系统,其中所述第一装置包括门锁,以及所述第二装置包括Wi-Fi凭证数据库。

8.如权利要求1所述的访问控制系统,其中所述第一装置包括机顶盒,以及所述第二装置包括环境控制器。

9.如权利要求1所述的访问控制系统,其中所述第一装置包括电梯自助服务终端,以及所述第二装置包括电梯分配系统。

10.如权利要求1所述的访问控制系统,其中所述第一装置包括制冷单元。

11.一种访问控制系统,包括:

模块,所述模块具有凭证认证器,由此具有在其上存储的凭证的应用可执行,以建立移动装置与所述模块之间的连接,使得所述凭证可传送于此,以用于由所述凭证认证器所进行的认证;以及

第一装置和第二装置,所述第一装置和所述第二装置分别设置成限制对第一安全元素和第二安全元素的访问,

所述第一装置在第一模式和第二模式中可操作以响应用于对所述第一安全元素的访问的请求,所述请求由所述移动装置来发出,以及

所述第二装置在第一模式和第二模式中可操作以响应用于对所述第二安全元素的访

问的请求,所述请求由所述移动装置经由操作在所述第二模式中的所述第一装置来发出,

其中:

在相应第一模式中,所述第一装置和所述第二装置限制对所述第一安全元素和所述第二安全元素的所述访问,以及

在相应第二模式中,所述第一装置和所述第二装置基于所述凭证由所述凭证认证器来认证以及所述凭证的类型来准许对所述第一安全元素和所述第二安全元素的所述访问。

12.如权利要求11所述的访问控制系统,其中所述模块包括Bluetooth ™模块。

13.如权利要求11所述的访问控制系统,其中所述移动装置包括便携计算装置、智能电话和平板中的一个或多个。

14.如权利要求11所述的访问控制系统,其中所述第一装置包括门锁。

15.如权利要求11所述的访问控制系统,其中所述第一装置包括门锁,以及所述第二装置包括Wi-Fi凭证数据库。

16.如权利要求11所述的访问控制系统,其中所述第一装置包括机顶盒,以及所述第二装置包括环境控制器。

17.如权利要求11所述的访问控制系统,其中所述第一装置包括电梯自助服务终端,以及所述第二装置包括电梯分配系统。

18.如权利要求11所述的访问控制系统,其中所述第一装置包括制冷单元。

19.一种访问控制方法,包括:

在移动装置的应用中存储移动凭证;

识别所述移动装置处于具有凭证认证器的模块的范围之内;

执行所述应用,以建立与所述模块的连接,由此所述移动凭证可传送给所述模块,以用于由所述凭证认证器所进行的认证;以及

在相应安全通过模式中操作第一装置和第二装置,使得所述第一装置和所述第二装置分别响应于下列请求而基于所述凭证由所述凭证认证器来认证以及所述凭证的类型分别准许对第一安全元素和第二安全元素的访问:

由所述移动装置对所述第一装置所发出的用于第一安全元素访问的第一请求,以及

由所述移动装置经由操作在所述安全通过模式中的所述第一装置对所述第二装置所发出的用于第二安全元素访问的第二请求。

20.如权利要求19所述的访问控制方法,其中用于认证的移动凭证传输包括:

将所述移动凭证从所述移动装置发送给所述模块;

在所述模块处验证所述凭证;以及

建立所述相应安全通过模式。

采用安全通过的访问控制系统

技术领域

[0001] 以下描述涉及访问控制系统,以及更具体来说涉及采用安全通过(secure pass-through)的访问控制系统。

背景技术

[0002] 访问控制系统通过对物理钥匙卡上指示访问权限的数据进行编码来操作。一些访问控制系统通常操作在在线模式中,其中读取器经由网络与访问控制系统的集中服务器进行通信,以确定是否准予访问。在这类在线系统中,访问权限通常是参考标识符或者某一其它类似元素。其它访问控制系统是离线的,其中访问权限被编码为数据,其能够由离线锁来解码和解译以检索访问权限。示例是酒店锁闭系统,其中前台工作人员对客人卡进行编码,以及客房门上的离线电池供电锁对钥匙卡进行解码,并且因此基于所编码的访问权限来准许或拒绝访问。对访问权限进行编码的一些方法包括定序,其中后续访问权限具有序列号,其大于先前访问权限。对访问权限进行编码的一些方法还包括利用移动装置来传递访问凭证。

[0003] 除了用于开门的访问权限之外,到达酒店或办公大楼的客人或访客常常需要Wi-Fi凭证,以安全地接入其房间或办公大楼中的网络。当前,酒店完全没有使用安全性、使用半安全访问代码或者通过要求万维网服务器、防火墙和复杂软件的特殊系统来分发这类凭证。

发明内容

[0004] 按照本公开的一个方面,提供一种访问控制系统,并且所述访问控制系统包括凭证认证器以及第一装置和第二装置。第一装置和第二装置设置用于第一访问限制和第二访问限制,并且可操作在相应第一模式和第二模式中。第一装置响应由移动装置传递于此的用于第一访问的请求,以及第二装置响应由移动装置经由第一装置传递于此的用于第二访问的请求。在相应第一模式中,第一装置和第二装置分别保持第一访问限制和第二访问限制。在相应第二模式中,第一装置和第二装置分别准许第一访问和第二访问。相应第二模式基于凭证从移动装置传送给凭证认证器并且由凭证认证器来认证而实行。

[0005] 按照附加或备选实施例,凭证认证器提供在Bluetooth ™模块内。

[0006] 按照附加或备选实施例,凭证认证器远离第一装置和第二装置。

[0007] 按照附加或备选实施例,凭证认证器是第一装置和第二装置其中之一的组件。

[0008] 按照附加或备选实施例,移动装置包括便携计算装置、智能电话和平板中的一个或多个。

[0009] 按照附加或备选实施例,第一装置包括门锁。

[0010] 按照附加或备选实施例,第一装置包括门锁,以及第二装置包括Wi-Fi凭证数据库。

[0011] 按照附加或备选实施例,第一装置包括机顶盒,以及第二装置包括环境控制器。

[0012] 按照附加或备选实施例，第一装置包括电梯自助服务终端(kiosk)，以及第二装置包括电梯分派系统。

[0013] 按照附加或备选实施例，第一装置包括制冷单元。

[0014] 按照本公开的另一方面，提供一种访问控制系统。所述访问控制系统包括：具有凭证认证器的模块，由此具有在其上存储的凭证的应用可执行，以建立移动装置与所述模块之间的连接，使得凭证可传送于此，以用于由凭证认证器所进行的认证；以及第一装置和第二装置，所述第一装置和所述第二装置分别设置成限制对第一安全元素和第二安全元素的访问。第一装置在第一模式和第二模式中可操作以响应用于对第一安全元素的访问的请求，所述请求由移动装置来发出。第二装置在第一模式和第二模式中可操作以响应用于对第二安全元素的访问的请求，所述请求由移动装置经由操作在第二模式中的第一装置来发出。在相应第一模式中，第一装置和第二装置限制对第一安全元素和第二安全元素的访问。在相应第二模式中，第一装置和第二装置基于凭证由凭证认证器来认证以及凭证的类型来准许对第一安全元素和第二安全元素的访问。

[0015] 按照附加或备选实施例，模块包括Bluetooth ™模块。

[0016] 按照附加或备选实施例，移动装置包括便携计算装置、智能电话和平板中的一个或多个。

[0017] 按照附加或备选实施例，第一装置包括门锁。

[0018] 按照附加或备选实施例，第一装置包括门锁，以及第二装置包括Wi-Fi凭证数据库。

[0019] 按照附加或备选实施例，第一装置包括机顶盒，以及第二装置包括环境控制器。

[0020] 按照附加或备选实施例，第一装置包括电梯自助服务终端，以及第二装置包括电梯分派系统。

[0021] 按照附加或备选实施例，第一装置包括制冷单元。

[0022] 按照本公开的又一方面，提供一种访问控制方法。所述访问控制方法包括：在移动装置的应用中存储移动凭证；识别所述移动装置处于具有凭证认证器的模块的范围之内；执行所述应用以建立与所述模块的连接，由此所述移动凭证可传送给所述模块以用于由凭证认证器所进行的认证；以及在相应安全通过模式中操作第一装置和第二装置，使得第一装置和第二装置分别响应于第一请求和第二请求而基于凭证由凭证认证器来认证以及凭证的类型分别准许对第一安全元素和第二安全元素的访问。第一请求针对由移动装置向第一装置所发出的第一安全元素访问，以及第二请求针对由移动装置经由操作在安全通过模式中的第一装置向第二装置所发出的第二安全元素访问。

[0023] 按照附加或备选实施例，用于认证的移动凭证传输包括：将移动凭证从移动装置发送给所述模块；在所述模块处验证凭证；并且建立安全通过模式。

[0024] 根据结合附图所进行的以下描述，这些以及其它优点和特征将变为更加显而易见。

附图说明

[0025] 在本说明书的结束部分的权利要求书中具体指出并且明确要求保护被看作是本公开的本主题。根据结合附图所进行的以下详细描述，本公开的上述以及其它特征和优点

是显而易见的，其中：

图1是用户认证系统的一般示意系统图；

图2是用户认证系统的框图；

图3是图示用户认证系统的操作的简图；

图4是由用户认证系统所执行的凭证管理方法的流程图；

图5是按照一个所公开的非限制性实施例的由用户认证系统所执行的凭证管理方法的流程图；

图6是按照实施例的图示访问控制方法的流程图。

具体实施方式

[0026] 如下面将描述的，提供一种访问控制系统，其中带有移动装置(又称作移动单元)的人能够通过移动装置与访问控制装置之间的通信的安全“通过”模式来得到经过访问控制装置的对安全元素的访问，所述访问在采用移动凭证的访问权限的认证之后被允许。除了通过访问控制装置来访问安全元素之外，通信的安全“通过”模式还允许移动装置与安全元素进行通信或者交换附加数据。

[0027] 在访问控制系统的操作中，通常与访问控制装置进行通信并且对其进行访问，以开锁并且进入安全房间或空间，开启橱柜，实现设备的使用，或者更一般地访问安全元素。可按照各种方式使用安全元素的附加数据，各种方式包括读取数据、写入数据或者它们的组合。该系统能够部署在如下用例中，例如，其中电话对客房门进行认证并且请求/接收客人Wi-Fi网络的Wi-Fi凭证，其中电话通过进口门对读取器进行认证并且请求/接收用于建筑物Wi-Fi网络的Wi-Fi凭证，其中电话利用移动凭证对客房中的机顶盒或媒体盒进行认证并且请求/接收netflix id/密码(其与他们的暂居处(stay)联接，并且能够立即准许他们在移动装置上观看内容)，其中电话使用移动凭证对电梯控制自助服务终端进行认证并且请求/接收所请求目标楼层的电梯指配(其在移动装置上显示)，其中电话对交通工具进行认证以开门或启动交通工具并且请求/接收远程信息处理数据(例如燃油液面、里程表设定等)，或者其中电话对装置进行认证并且读取/写入配置数据(例如操作时间、温度水平或者装置中的任何可配置参数)。实际上，所述访问控制系统提供对带有移动装置的用户的认证和验证以访问安全元素，并且还提供对安全元素的附加访问，所述安全元素原本要求完全独立认证和验证以进行访问。

[0028] 参照图1，提供访问控制系统10，并且所述访问控制系统10可部署在诸如酒店或办公大楼之类的建筑物11中。访问控制系统10包括移动装置12、服务器14、多个访问控件16a、16b、...、16n以及可作为Bluetooth ™模块180来提供的认证模块18。移动装置12可以是具有无线能力的手持装置，例如智能电话或平板，其可操作以便与服务器14、访问控件16a、16b、...、16n以及认证模块18进行通信。服务器14可向移动装置12提供移动凭证和其它数据，例如将传递给访问控件16a、16b、...、16n中的一个或多个的固件或软件更新。虽然服务器14在本文中描绘为单个装置，但是应当领会，服务器14备选地可体现为多个系统，移动装置12从其中接收移动凭证和其它数据。访问控件16a、16b、...16n中的每个是具有无线能力、受限访问或受限使用的装置，例如无线锁、用于建筑物入口的访问控制读取器、电子银行控件、数据传递装置、钥匙分配器装置、工具分配装置、电梯自助服务终端、交通工具控制

系统和其它受限使用机器。因此，访问控件16a、16b、...、16n中的每个设置成限制对于对应的安全元素17a、17b、...、17n的访问。

[0029] 也就是说，访问控件16a可作为第一装置(例如门锁)来提供，其中安全元素17a因而作为客房来提供，以及访问控件16b可作为第二装置(例如包括用于安全元素17a中的Wi-Fi接入的Wi-Fi密码的数据库)来提供，其中安全元素17b作为用于客房的密码来提供。

[0030] 在典型访问控制系统中，移动装置12可配置成向访问控件16a、16b、...、16n提交凭证，以便由此为用户获得访问。例如，用户可使用移动装置12向机电锁提交凭证，以便对它开锁，以便因而获得对其客房的访问。移动装置12可存储多种类型的凭证，并且一些凭证可用于多个访问控件16a、16b、...、16n。

[0031] 参照图2，示例电子锁系统20的框图包括访问控件16a、移动装置12、服务器14和认证模块18。访问控件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、锁功率供应装置(lock power supply)34以及锁卡读取器90和凭证模块36。访问控件16a响应来自移动装置12的凭证，并且例如可以是锁箱的锁、门锁或锁芯。虽然本公开主要集中于用于访问控件的凭证，但是应当领会，其中凭证从移动装置传送给访问控件以便向在线系统识别用户或者在离线系统中验证用户访问权限或准许的其它系统将从其中获益。这类系统包括虚拟或电子银行系统、机器操作系统、分配系统、人类运送系统(例如电梯、十字转门、地铁、列车等)和数据访问系统。

[0032] 在使用凭证模块36来接收和认证来自移动装置12的适当凭证时或者在接收来自锁卡读取器90的卡数据之后，锁控制器24命令锁致动器22对机械或电子锁进行锁定或开锁。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组成部分，或者可以是单独销售或安装的组件。

[0033] 锁收发器28能够来往于至少移动装置12传送和接收数据。锁收发器28例如可以是近场通信(NFC)、蓝牙或Wi-Fi收发器或者另一个适当无线收发器。锁天线26是适合锁收发器28的任何天线。锁处理器30和锁存储器32分别是数据处理装置和数据存储装置。锁处理器30例如可以是微处理器，其能够处理指令，以验证卡数据，并且确定卡数据中包含的访问权限，或者将消息从收发器传递给凭证模块36，并且从凭证模块36接收回对卡数据的响应指示。锁存储器32可以是RAM、EEPROM或其它存储介质，其中锁处理器30能够读取和写入数据，其包括但不限于锁配置选项和锁审计跟踪。锁审计跟踪可以是统一审计跟踪，其包括通过经由锁卡读取器90或移动装置12来访问锁所发起的事件。锁功率供应装置34是功率源，例如线路功率连接、功率提取系统(power scavenging system)或者向锁控制器24供电的电池。在其它实施例中，锁功率供应装置34可以仅向锁控制器24供电，其中锁致动器22主要或完全由诸如用户工作(例如转动螺栓)之类的另一个源来供电。

[0034] 凭证模块36与锁处理器30进行通信，并且可操作以便对凭证进行解密和验证，以提取传递到锁控制器24中的虚拟卡数据以作为“虚拟卡读取”。也就是说，访问控件16a具有基本上两个读取器，用来读取物理钥匙卡92的一个读取器90，和凭证模块36，其用来经由锁处理器30以及收发器28和天线26与移动装置12进行通信。

[0035] 虽然图2示出连接到处理器30的锁天线26和收发器28，但这并不是要限制可具有直接连接到凭证模块36的附加天线26和收发器28的其它实施例。凭证模块36可包含作为凭证模块36的组成部分的收发器28和天线26，或者凭证模块36可具有与处理器30分开的收发

器28和天线26，处理器30也具有相同或不同类型的独立收发器28和天线26。在一些实施例中，处理器30可将经由收发器28所接收的通信路由到凭证模块36。在其它实施例中，凭证模块36可经过收发器28与移动装置12直接通信。在其它实施例中，凭证模块可以是完全在处理器30内执行的软件模块。

[0036] 移动装置12通常包括钥匙天线40、钥匙收发器42、钥匙处理器44、钥匙存储器46、GPS接收器48、输入装置50、输出装置52和钥匙功率供应装置54。钥匙收发器42是与锁收发器28对应类型的收发器，以及钥匙天线40是对应天线。在一些实施例中，钥匙收发器42和钥匙天线40还可用来与服务器14、访问控件16a、16b、...、16n以及认证模块18进行通信。在其它实施例中，可包含一个或多个独立收发器和天线，以便与服务器14、访问控件16a、16b、...、16n以及认证模块18进行通信。钥匙存储器46具有用来在移动装置12上本地存储多个凭证的类型。在其它实施例中，移动装置12在它与访问控件16a进行通信的同时与服务器14进行通信。这是在线配置，以及在这个实施例中，移动凭证实时地被检索并且传递给凭证模块36，而无需首先存储在移动装置12上的钥匙存储器46中。

[0037] 在一些实施例中，认证模块18在访问控件16a、16b、...、16n中的一个或多个中用作凭证模块36。在其它实施例中，认证模块18用来连接到其它设备(未示出)，例如安全元素，其由认证模块18来保护。

[0038] 参照图3，在电子锁系统20的操作期间，移动装置12的用户在钥匙存储器46中存储应用，并且登记以暂居其中部署电子锁系统20的酒店中。在可通过应用来完成这种登记时，或者在另一时刻(at another point)，生成用于用户的一组移动凭证，其在用户暂居时期期间授予用户对酒店的某些安全元素(例如用户的房间、健身房和温泉、用户房间中的Wi-Fi接入等)的访问权限。这些移动凭证被转发到移动装置12并且存储在钥匙存储器46中。如图3中所示，在用户预定时，以及一旦他接近酒店财产邻近并且因而进入认证模块18(其再次可作为Bluetooth ™模块180或者作为具有集成收发器28和天线26的凭证模块36来提供)的范围中，应用就向钥匙存储器46发信号通知关于意向，并且由此使移动装置12建立与认证模块18的连接。通过建立的这个连接，移动凭证从钥匙存储器46传送给认证模块18，它们在其上或者被验证或者被作废。如果移动凭证被作废，则不授予或者不能授予用户对安全元素的访问。另一方面，如果移动凭证被验证，则认证模块18和电子锁系统20实际上生成移动装置12和用户的安全通过状态。

[0039] 认证模块18将接收加密移动凭证，并且然后对移动凭证进行验证和解密，以检索虚拟卡数据。解密和验证可包括但不限于：验证数字签名；验证移动凭证的类型；验证移动凭证标识符匹配锁存储器32中的标识符；验证移动凭证的起始日期和到期日期；验证移动凭证的来源，等等。一旦移动凭证被验证和解密，提取虚拟卡数据。

[0040] 另外，对于采取访问控件16a中的凭证模块36的形式的认证模块18，一旦移动凭证被验证和解密，虚拟卡数据能够被提取并且发送给锁处理器30以用于附加验证。一旦移动装置12上的应用已成功经过如上所述的采用移动认证向认证模块18的认证，认证模块18就将允许附加消息通过该连接被发送。

[0041] 在所生成的安全通过状态的情况下，应用能够进一步被执行，以使移动装置12向访问控件16a、16b、...、16n中的第一访问控件(例如访问控件16a)发出用于对安全元素17a的访问的第一请求，以及经由第一访问控件16a向访问控件16b、...、16n中的第二访问控件

(例如访问控件16b)发出用于对第二安全元素17b的访问的第二安全请求。在这种情况下，如果访问控件16a是用户的客房门并且用户的移动凭证已经由认证模块18验证，则认证模块18将与访问控件16a进行通信，以指示访问控件16a关于用户的移动凭证已经被验证，使得访问控件16a响应于第一请求而准许用户访问该客房，并且使得访问控件16b能够经由访问控件16a采用安全响应来响应第二安全请求。

[0042] 按照实施例，访问控件16a例如可作为用作酒店中的客房的门锁的第一装置来提供，以及第一安全元素17a可作为客房或者作为交通工具中的制冷单元来提供，并且第一安全元素17a可作为那个交通工具的环境控制系统来提供。按照另外的实施例，访问控件16a可作为用作门锁的第一装置来提供，第一安全元素17a可作为客房来提供，访问控件16b可作为用作Wi-Fi凭证数据库的第二装置来提供，以及第二安全元素17b可作为酒店中的每个客房的Wi-Fi登录和密码组合的集合来提供。按照备选和另外的实施例，访问控件16a可作为用作机顶盒的第一装置来提供，第一安全元素17a可作为客房中的电视机来提供，访问控件16b可作为用作环境控制器的第二装置来提供，以及第二安全元素17b可作为酒店中的每个客房的环境控件来提供。按照其它备选和另外的实施例，访问控件16a可作为用作电梯自助服务终端的第一装置来提供，第一安全元素17a可作为电梯控件来提供，访问控件16b可作为用作电梯分配系统的第二装置来提供，以及第二安全元素17b可作为酒店中的电梯轿厢来提供。

[0043] 参照图4，提供用来促进代表将会在钥匙卡92(参见图5)上正常物理编码的数据的凭证的传递的方法100。该方法包括：检索采取数字形式的卡数据(框110)；将卡数据封装在加密移动凭证中(框112)；并且将移动凭证下载到移动装置12(框114)。该方法还包括当用户和移动装置12处于认证模块18的范围之内(即，在酒店的财产上)时向认证模块18安全地传递(框116)。认证模块18然后对移动凭证进行解密和验证(框118)，提取卡数据(框120)，并且将卡数据传递到锁控制器24中以作为“虚拟卡读取”(框122)。

[0044] 这例如准许用户绕过酒店的前台并且直接去其房间。加密移动凭证可通过服务器14使用采用密码算法(例如AES、ECC、RSA等)的数字证书创建和加密的众所周知技术来生成。例如，移动凭证可以包含但不限于包含移动凭证标识符、唯一访问控件标识符、唯一凭证模块标识符、与多个访问控件共享的标识符、指示凭证的类型或格式的参数，它可包含加密数据(例如虚拟卡数据)，并且它可包含数字签名。加密数据可采用能够是认证模块18已知的AES-128加密密钥来加密，或者它可采用能够从移动凭证中包含的信息所确定的推导加密密钥来加密。此外，数字签名可以是基于例如能够是由认证模块18已知的AES-128加密密钥的CBC-MAC类型签名，或者它可能是基于服务器14已知的私有密钥的数字签名并且能够通过认证模块18已知的公有密钥来验证。

[0045] 参照图5，在示范情况下，用户首先经过由酒店所支持的任何过程(例如移动预定、网站、旅行代理等)来预定酒店房间(框210)，并且然后完成登记入住手续以确认其暂居处(框212)。然后在酒店财产管理系统60中基于在登记入住时客人偏好和房间可用性来指配房间(框214)。酒店财产管理系统60可使用由前台应用62所提供的软件到软件应用编程接口(API)来请求采取数字形式的卡数据(框216)。前台应用62的范围可从独立编码器64到云中运行的完整软件封装(其可操作以对于所选择的房间的虚拟卡进行编码并且将虚拟卡数据返回给酒店系统)(框218)。随后，酒店财产管理系统60将在酒店系统已经分配房间之后

对凭证服务70进行另一个软件到软件API调用(框220)。有关信息被传递给凭证服务70，其中有关信息具有用来包括例如哪一个酒店财产、哪一个房间、哪一位客人(例如用户ID)、什么日期以及还有用于暂居处的虚拟卡数据的指示。酒店财产管理服务60还可向用户传递(再次经过任何常规方法)关于确认登记入住并且指配房间的指示(框222)。

[0046] 基于移动装置12的酒店忠诚度移动应用80将利用移动资料库82中的软件到软件API(框224)从凭证服务70下载移动凭证(框226)。移动资料库82将采用先前建立的共享秘密对凭证服务70进行安全认证，所述秘密可能对每一个成功连接发生变化。

[0047] 一旦被认证，凭证服务70在来自移动资料库82的通信时生成用户的移动凭证，并且将在框220中所接收的用于与移动资料库82的这个实例关联的客人的虚拟卡数据加密到移动凭证中。一个凭证可对每个访问控件16a、16b、...、16n来生成，并且虚拟卡数据将在这些独立移动凭证的每个中是相同的，但是可对每个采用唯一密钥来加密。该加密方法可以是AES、3DES或其它这种加密方法。所使用的凭证的方法和类型可以是压缩数字证书或基于标准的证书(例如X.509)或者本领域已知的证书格式。也就是说，例如采用由认证模块18已知以及由凭证服务70已知或者可确定的唯一密钥将虚拟卡数据加密到移动凭证中。移动资料库82将下载移动凭证的列表并且使用采用装置特定信息(例如UDID、IMEI、IMSI、MAC地址等)的数据的本机OS保护和附加加密在移动装置12上存储移动凭证的列表。

[0048] 一旦移动凭证由认证模块18来验证(框227)，用户就将能够操作他被授权在以后任何时间在不要求移动装置12连接到凭证服务70的情况下在离线模式中操作的访问控件16a、16b、...、16n。因此，当用户希望访问其房间时(框228)，用户可经过手势、按钮的点击、屏幕上的轻敲(tap)、指纹读取、密码、与锁的邻近、触摸锁等指示这种意向。响应于这个意向，酒店忠诚度移动应用80再次调用移动资料库82中的软件到软件API，以便向对应的访问控件16a指示安全移动装置/单元请求(框230)。

[0049] 更具体来说，参照图6，提供一种访问控制方法。如图6中所示，该访问控制方法包括在移动装置的应用中存储移动凭证(框601)，并且识别该移动装置处于具有凭证认证器的模块的范围之内(框602)。此时，如果移动装置处于该模块的范围之内，则该访问控制方法还包括执行应用以建立移动装置与该模块之间的连接，由此在该应用中存储的移动凭证可从移动装置传送给该模块以用于由凭证认证器所进行的认证(框603)。

[0050] 随后，确定移动凭证是否被认证(框604)。在移动凭证未被认证的情况下，该访问控制方法结束，并且将不准许响应于任何请求而将被授予的访问(框605)。另一方面，在移动凭证被认证的情况下，该访问控制方法包括在相应安全通过模式中操作第一装置和第二装置(框606)。因此，第一装置将基于凭证由凭证认证器来认证以及凭证的类型被确定为与响应于用于第一安全元素访问的第一请求(其由移动装置向第一装置发出)所请求的访问的类型一致来准许对第一安全元素的访问。同时，第二装置将基于凭证由凭证认证器来认证以及凭证的类型被确定为与响应于用于第二安全元素访问的第二请求(其由移动装置在第一装置操作在安全通过模式的同时经由第一装置向第二装置发出)所请求的访问的类型一致来准许对第二安全元素的访问。

[0051] 也就是说，在其中访问控件16a是第一装置并且用作门锁以及访问控件16b是Wi-Fi凭证数据库的情况下，其智能电话已经使智能电话的移动凭证被认证的客人可通过使其智能电话向门锁发出第一请求来请求对他的被指配的客房的访问。此时，门锁将准许用户

进入该客房。另外，如果用户将要从Wi-Fi凭证数据库来请求其客房的Wi-Fi登录和密码组合，则这种请求可作为第二安全请求由移动装置向门锁发出，该第二安全请求通过Wi-Fi凭证数据库经由门锁来响应。

[0052] 虽然仅结合有限数量的实施例详细提供本公开，但是应当易于理解，本公开并不局限于这类所公开实施例。本公开而是能够修改为结合此前没有描述的但与本公开的精神和范围相称的任何数量的变化、变更、替换或等效布置。另外，虽然描述了本公开的各个实施例，但是要理解，(一个或多个)示范实施例可以仅包含所述示范方面的一些。相应地，本公开不要被看作受到前面描述的限制，而仅通过所附权利要求书的范围来限制。

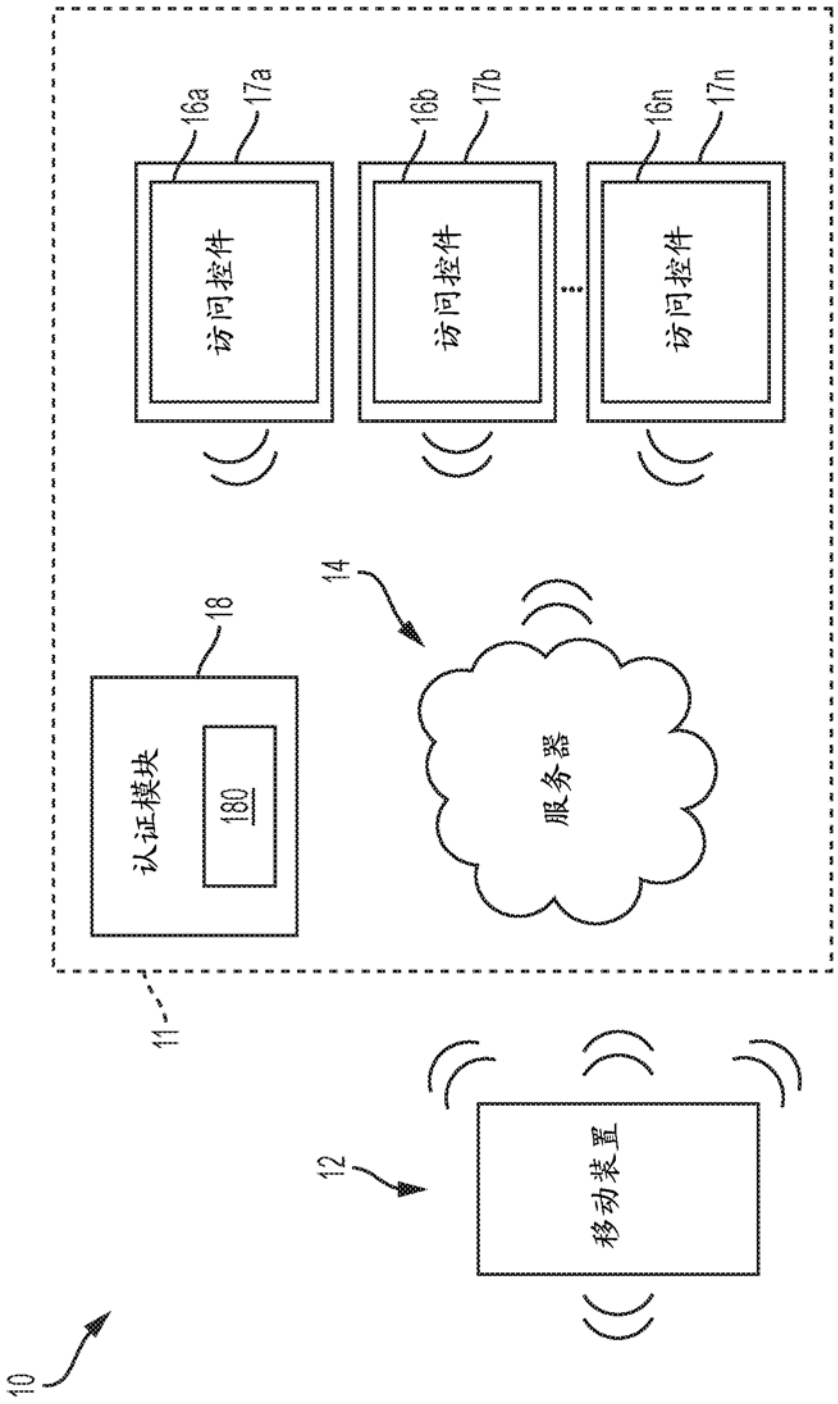

16a
17a
访问控件
16b
17b
访问控件
16n
17n
访问控件
14
18
认证模块
180
服务器
11
12
移动装置
10

图 1

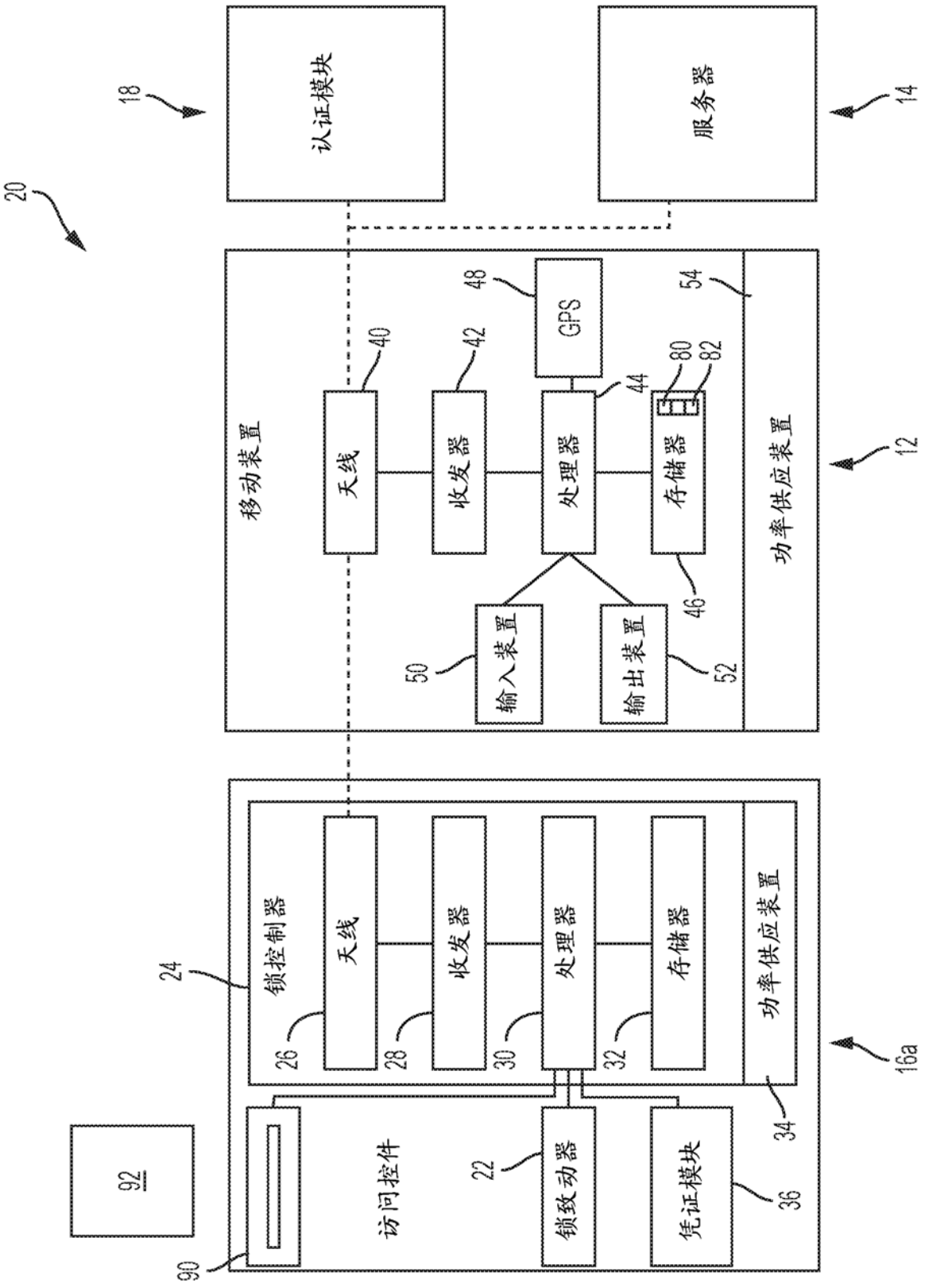

20
18
认证模块
服务器
14
移动装置
天线
收发器
处理器
GPS
存储器
输入装置
输出装置
功率供应装置
12
40
42
44
48
50
52
54
46
80
82
24
锁控制器
26
28
30
32
34
16a
访问控件
22
锁致动器
凭证模块
36
92
90

图 2

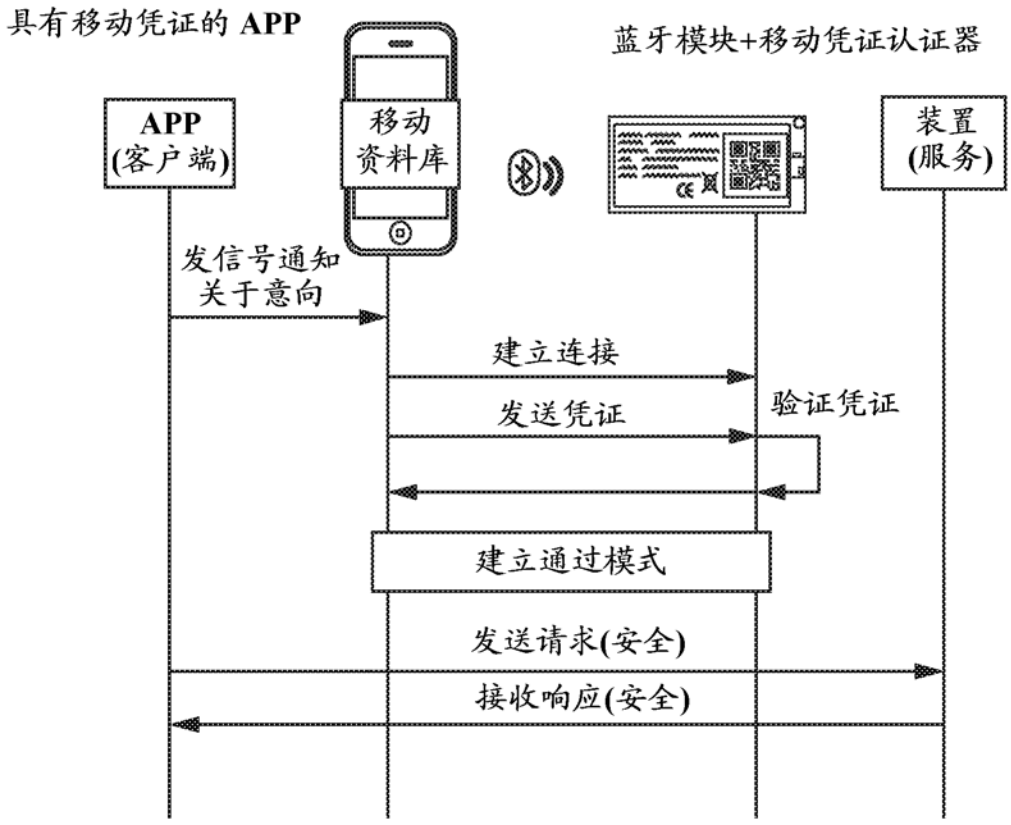

具有移动凭证的 APP
蓝牙模块+移动凭证认证器
APP
(客户端)
移动
资料库
装置
(服务)
发信号通知
关于意向
建立连接
发送凭证
验证凭证
建立通过模式
发送请求(安全)
接收响应(安全)

图 3

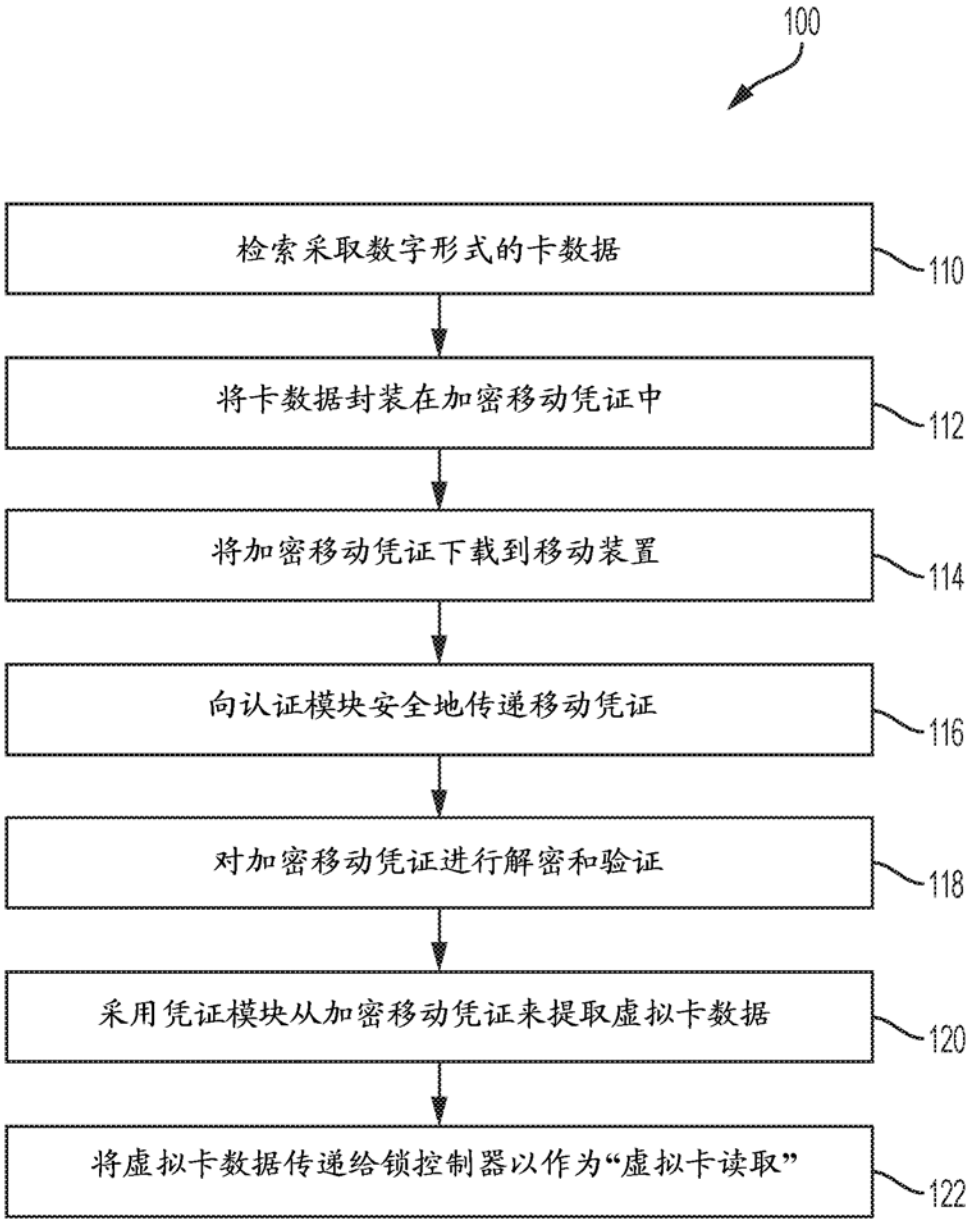

100
检索采取数字形式的卡数据
110
将卡数据封装在加密移动凭证中
112
将加密移动凭证下载到移动装置
114
向认证模块安全地传递移动凭证
116
对加密移动凭证进行解密和验证
118
采用凭证模块从加密移动凭证来提取虚拟卡数据
120
将虚拟卡数据传递给锁控制器以作为“虚拟卡读取”
122

图 4

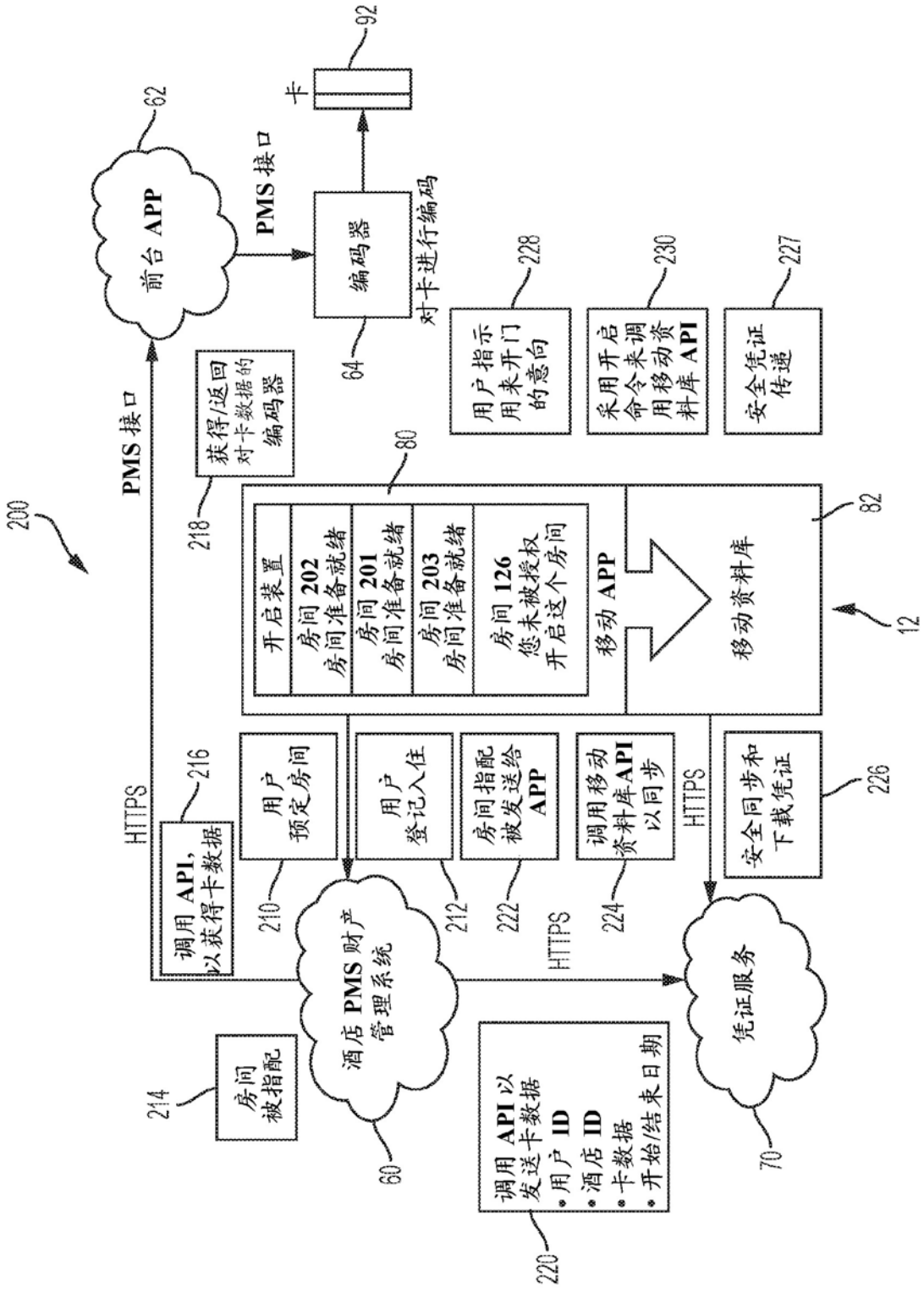

200
前台 APP
62
PMS 接口
卡
92
编码器
对卡进行编码
64
PMS 接口
获得/返回对卡数据的编码器
218
用户指示用来开门的意向
228
采用开启命令来调用移动资料库 API
230
安全凭证传递
227
80
开启装置
房间 202 房间准备就绪
房间 201 房间准备就绪
房间 203 房间准备就绪
房间 126 您未被授权开启这个房间
移动 APP
移动资料库
82
12
HTTPS
调用 API，以获得卡数据
216
用户预定房间
210
用户登记入住
212
房间指配被发送给 APP
222
调用移动资料库 API 以同步
224
HTTPS
安全同步和下载凭证
226
酒店 PMS 财产管理系统
60
凭证服务
70
房间被指配
214
调用 API 以发送卡数据
• 用户 ID
• 酒店 ID
• 卡数据
• 开始/结束日期
220

图 5

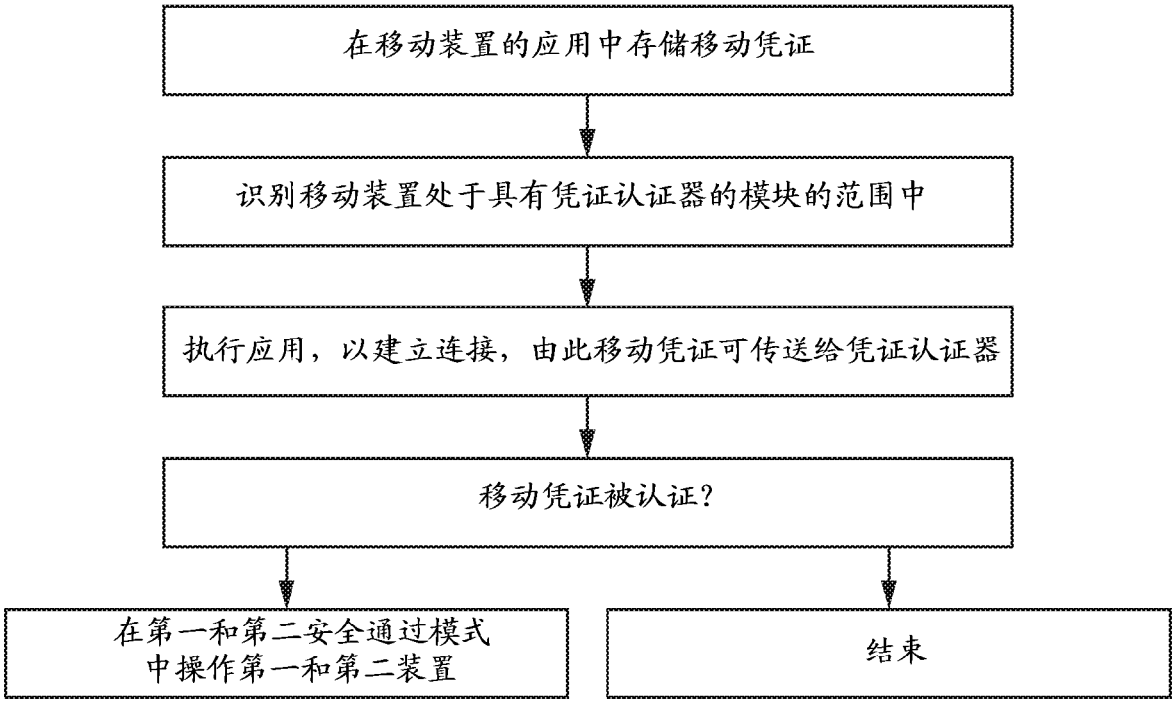

在移动装置的应用中存储移动凭证
识别移动装置处于具有凭证认证器的模块的范围中
执行应用，以建立连接，由此移动凭证可传送给凭证认证器
移动凭证被认证？
在第一和第二安全通过模式中操作第一和第二装置
结束

图 6