



(12)发明专利申请

(10)申请公布号 CN 110178160 A

(43)申请公布日 2019.08.27

(21)申请号 201880008079.9

(22)申请日 2018.01.19

(30)优先权数据

62/449393 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/US2018/014429 2018.01.19

(87)PCT国际申请的公布数据

W02018/136740 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.肯尼迪-福斯特 B.霍姆

(74)专利代理机构 中国专利代理(香港)有限公司 72001

代理人 姜冰 张金金

(51)Int.Cl.

G07C 9/00(2006.01)

G06F 21/35(2006.01)

H04W 12/06(2006.01)

H04W 12/08(2006.01)

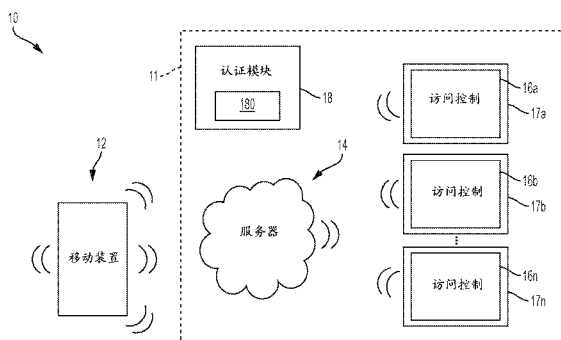
权利要求书2页 说明书6页 附图6页

(54)发明名称

可信第三方的访问控制系统

(57)摘要

提供了一种访问控制系统,并且所述访问控制系统包括被布置成限制对受保护资源的访问的控制装置以及被布置为与所述控制装置进行信号通信的连网装置。所述连网装置响应于在对所述受保护资源的访问的请求中向所述控制装置呈现凭证,而从可信装置请求对用户的认证,所述凭证与所述用户的访问权限相关联,所述连网装置接收所述认证,以及所述控制装置在所述认证的所述接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。



1. 一种访问控制系统,包括:

控制装置,所述控制装置被布置成限制对受保护资源的访问;以及

连网装置,所述连网装置被布置为与所述控制装置进行信号通信,

其中:

所述连网装置响应于在对所述受保护资源的访问的请求中向所述控制装置呈现凭证,而向可信装置请求对用户的认证,

所述凭证与所述用户的访问权限相关联,

所述连网装置接收所述认证,以及

所述控制装置在所述认证的所述接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。

2. 根据权利要求1所述的访问控制系统,其中,所述控制装置包括门锁。

3. 根据权利要求1所述的访问控制系统,其中,所述连网装置包括服务器。

4. 根据权利要求1所述的访问控制系统,其中,所述可信装置包括便携式计算装置。

5. 根据权利要求1所述的访问控制系统,其中,所述可信装置包括智能电话。

6. 根据权利要求1所述的访问控制系统,其中,所述凭证可呈现为卡或标记卡。

7. 根据权利要求1所述的访问控制系统,其中,所述认证是字母数字的或生物测定的。

8. 根据权利要求1所述的访问控制系统,其中,与所述控制装置和所述连网装置远程地存储与对所述用户的认证有关的数据。

9. 一种访问控制系统,包括:

控制装置,所述控制装置被布置成限制对受保护资源的访问;以及

连网装置,所述连网装置被布置为与所述控制装置进行信号通信,并被配置成将认证应用分发给用户的可信装置,访问权限的凭证被准予给所述用户,

其中:

所述连网装置响应于在对所述受保护资源的访问的请求中向所述控制装置呈现所述凭证,而请求所述可信装置通过执行所述认证应用来认证所述用户,

所述连网装置接收来自所述可信装置的对所述用户的所述认证的肯定或否定指示,以及

所述控制装置在由所述连网装置所进行的所述认证的所述肯定指示的所述接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。

10. 根据权利要求9所述的访问控制系统,其中,所述控制装置包括门锁。

11. 根据权利要求9所述的访问控制系统,其中,所述连网装置包括服务器。

12. 根据权利要求9所述的访问控制系统,其中,所述可信装置包括便携式计算装置。

13. 根据权利要求9所述的访问控制系统,其中,所述可信装置包括智能电话。

14. 根据权利要求9所述的访问控制系统,其中,所述凭证可呈现为卡或标记卡。

15. 根据权利要求9所述的访问控制系统,其中,所述认证应用需要字母数字认证或生物测定认证。

16. 根据权利要求15所述的访问控制系统,其中,与所述控制装置和所述连网装置远程地存储与所述字母数字认证或生物测定认证有关的数据。

17. 一种操作访问控制系统的方法,所述方法包括:

在被布置成限制对受保护资源的访问的控制装置处接收对所述受保护资源的访问的请求中的凭证的呈现；

识别所述凭证与用户的访问权限相关联；

向可信装置请求对所述用户的认证；以及

在所述认证的接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。

18. 根据权利要求17所述的方法，还包括将所述凭证发给所述用户。

19. 根据权利要求17所述的方法，还包括将认证应用分发给所述可信装置。

20. 根据权利要求19所述的方法，其中：

所述认证应用需要字母数字认证或生物测定认证，以及

与所述访问控制系统远程地存储与所述字母数字认证或生物测定认证有关的数据。

可信第三方的访问控制系统

技术领域

[0001] 以下描述涉及访问控制系统,并且更具体地,涉及具有用于基于读取器或无读取器的访问控制装置的可信第三方的访问控制系统。

背景技术

[0002] 访问控制系统通常通过在物理密钥卡上编码数据进行操作,所述数据指示由该密钥卡的经授权持有者所持有的某些访问权限。一些访问控制系统通常以在线模式来操作,其中读取器经由网络而与访问控制系统的集中式服务器进行通信,以确定是否对呈现此类密钥卡的用户准予(grant)访问。在此类在线系统中,访问权限通常是参考标识符或某一其它类似元素。其它访问控制系统是离线的,其具有被编码为数据的访问权限,所述数据可由离线锁来解码和解译以在用户呈现密钥卡时检索访问权限。一个示例是旅馆锁系统,在其中前台工作人员对客人卡进行编码,并且当客人接近他的被指派的客房门并将客人卡呈现给门锁上的读取器时,客房门上离线的、电池提供动力的锁对密钥卡进行解码。这里,门锁上的读取器读取被编码在客人卡上的数据、解码所述数据、并基于与所解码的数据相关联的权限而准许或拒绝访问。

[0003] 诸如上述示例性旅馆系统之类的访问控制系统可能具有个人找到客人卡或密钥卡并然后冒充经授权的客人以获得对在旅馆内他们正常将不能访问的区域的访问(例如,经授权的客人的被指派的客房)的问题。因此,已经提出了当前的解决方案,其中访问控制系统采用双因素认证或生物测定验证特征。这些特征要求在准予对受保护资源的访问之前认证将客人卡或密钥卡呈现给读取器的客人卡或密钥卡持有者作为客人卡或密钥卡的用户或经授权的持有者。因此,除了用于敏感信息的数据存储以及将敏感信息作为数据而捕获、审计和维护的商业工作流程系统之外,所述特征还需要硬件和软件,诸如虚拟专用网络(VPN)令牌或指纹/视网膜扫描仪。这在许多市场中引起了隐私和责任关注,并且与相当大的构建和维护成本相关联。

发明内容

[0004] 根据本公开的一个方面,提供了一种访问控制系统,并且所述访问控制系统包括被布置成限制对受保护资源的访问的控制装置以及被布置为与所述控制装置进行信号通信的连网装置。所述连网装置响应于在对所述受保护资源的访问的请求中向所述控制装置呈现凭证,而向可信装置请求对用户的认证,所述凭证与所述用户的访问权限相关联,所述连网装置接收所述认证,以及所述控制装置在所述认证的所述接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。

[0005] 根据附加或备选实施例,所述控制装置包括门锁。

[0006] 根据附加或备选实施例,所述连网装置包括服务器。

[0007] 根据附加或备选实施例,所述可信装置包括便携式计算装置。

[0008] 根据附加或备选实施例,所述可信装置包括智能电话。

- [0009] 根据附加或备选实施例,所述凭证可呈现为卡或标记卡。
- [0010] 根据附加或备选实施例,所述认证是字母数字的或生物测定的。
- [0011] 根据附加或备选实施例,与所述控制装置和所述连网装置远程地存储与所述用户的认证有关的数据。
- [0012] 根据本公开的另一方面,提供了一种访问控制系统。所述访问控制系统包括控制装置,所述控制装置被布置成限制对受保护资源的访问;以及连网装置。所述连网装置被布置为与所述控制装置进行信号通信,并被配置成将认证应用分发给用户的可信装置,访问权限的凭证被准予给所述用户。所述连网装置响应于在对所述受保护资源的访问的请求中向所述控制装置呈现所述凭证,而请求所述可信装置通过执行所述认证应用来认证所述用户,并且接收来自所述可信装置的对所述用户的所述认证的肯定或否定指示。所述控制装置在由所述连网装置所进行的所述认证的所述肯定指示的所述接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。
- [0013] 根据附加或备选实施例,所述控制装置包括门锁。
- [0014] 根据附加或备选实施例,所述连网装置包括服务器。
- [0015] 根据附加或备选实施例,所述可信装置包括便携式计算装置。
- [0016] 根据附加或备选实施例,所述可信装置包括智能电话。
- [0017] 根据附加或备选实施例,所述凭证可呈现为卡或标记卡。
- [0018] 根据附加或备选实施例,所述认证应用需要字母数字认证或生物测定认证。
- [0019] 根据附加或备选实施例,与所述控制装置和所述连网装置远程地存储与所述字母数字认证或生物测定认证有关的数据。
- [0020] 根据本公开的又一方面,提供了一种操作访问控制系统的方法。所述方法包括在被布置成限制对受保护资源的访问的控制装置处接收对所述受保护资源的访问的请求中的凭证的呈现、识别与用户的访问权限相关联的所述凭证、向可信装置请求对所述用户的认证、以及在所述认证的接收时根据所述访问权限而准许对所述受保护资源的某种程度的访问。
- [0021] 根据附加或备选实施例,所述方法还包括将所述凭证发给所述用户。
- [0022] 根据附加或备选实施例,所述方法还包括将认证应用分发给所述可信装置。
- [0023] 根据附加或备选实施例,所述认证应用需要字母数字认证或生物测定认证,并且与所述访问控制系统远程地存储与所述字母数字认证或生物测定认证有关的数据。
- [0024] 根据结合附图的以下描述,这些和其它优点及特征将变得更显而易见。

附图说明

[0025] 在说明书结尾的权利要求中特别指出并清楚地要求保护被视为本公开内容的主題。根据结合附图的以下具体实施方式,本公开的前述和其它特征及优点是显而易见的,在附图中:

- 图1是根据实施例的访问控制系统的示意图示;
- 图2是图1的访问控制系统的组件的示意图示;
- 图3是根据实施例的图示访问控制系统的操作的流程图;
- 图4是以不同方式来图示图3的操作的流程图;

图5是根据实施例的图示访问控制系统的操作的流程图;以及图6是以不同方式来图示图5的操作的流程图。

具体实施方式

[0026] 如下面将描述的,提供了一种访问控制系统,在其中用户使用他们的便携式计算装置或电话来认证他们自己的标识,以便获得对具有凭证的受保护资源的访问。访问控制系统的管理员可以选择信任特定的第三方认证器或生物测定验证应用,这两者在便携式计算装置或电话上通常是可用的。访问控制系统可以补充具有诸如门读取器和其它类似访问控制装置的特征的传统访问控制系统。也就是说,当请求对受保护资源的访问的人将他们的标记卡(badge)呈现给正常阻止这种访问的门锁的读取器时,访问控制系统向经授权的标记卡持有者的便携式计算装置或电话(无论哪个都已被预先标识为值得信任)发送对于认证的请求。如果经授权的标记卡持有者是请求访问的人,则他/她使用存储在便携式计算装置或电话上的经认证或经生物测定地锁定的应用来确认他们刚刚已请求对门的访问(即,认证他们自己),以便验证呈现标记卡的人也是便携式计算装置或电话的所有者,并且也是经授权的标记卡持有者。另一方面,如果经授权的标记卡持有者不是请求访问的人,则将相对容易确定请求访问的人可能正不正确地这样做。

[0027] 参考图1,提供了访问控制系统10,并且访问控制系统10可以被部署在建筑物11中(诸如旅馆或办公楼)以用于与移动装置12进行交互。访问控制系统10包括服务器14,多个访问控制装置16a、16b、...、16n,对应的多个受保护资源17a、17b、...、17n,并且在一些情况下包括认证模块18。

[0028] 移动装置12可以是具有无线能力的手持装置(诸如便携式计算装置、平板计算机或智能电话)其可操作以与服务器14、访问控制装置16a、16b、...、16n和/或认证模块18进行通信。

[0029] 服务器14可以提供访问凭证和其它编码或非编码数据的生成,所述访问凭证和其它编码或非编码数据可以被传递或呈现给访问控制装置16a、16b、...、16n中的一个或多个,以便获得对受保护资源17a、17b、...、17n中的一个或多个的访问。尽管服务器14被描绘为单个装置,但服务器14可以被实施为多个系统。访问控制装置16a、16b、...、16n中的每个可以是具有无线能力的、访问受限或使用受限的装置,诸如无线锁、用于建筑物或房间入口的访问控制读取器、电子银行业务控制、数据转移装置、密钥分配器装置、工具分配装置、电梯亭(elevator kiosk)、交通工具控制系统和/或另一使用受限的机器。如此,访问控制装置16a、16b、...、16n中的每个可以被布置成限制对受保护资源17a、17b、...、17n中的对应一个受保护资源的访问。也就是说,访问控制装置16a可以被设置为门锁,并且受保护资源17a可以被设置为客房。认证模块18可以被设置为Bluetooth™模块180。

[0030] 参考图2,提供了用于与移动装置12进行交互的访问控制系统20的框图。如图2中所示,访问控制系统20包括访问控制装置16a、服务器14和认证模块18,访问控制装置16a在这种情况下是门锁。访问控制装置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34和锁卡读取器90,并且可进一步包括凭证模块36。访问控制装置16a能够通过解锁到客房的门来响应于正确凭证的呈现。

[0031] 在典型操作中,认证模块18或凭证模块36确定被呈现给锁卡读取器90的凭证是不

正确的或正确的,据此锁控制器24命令锁致动器22维持被锁定状态或解锁机械锁或电子锁。锁控制器24和锁致动器22可以是单个电子锁或机电锁单元的一部分,或者可以是被单独出售或安装的组件。锁收发器28能够至少向和从移动装置12、服务器14和认证模块18传送和接收数据。锁收发器28例如可以是近场通信(NFC)装置、Bluetooth™模块、Wi-Fi收发器或另一适当的无线收发器。锁天线26可以是被适当耦合到锁收发器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。例如,锁处理器30可以是微处理器,其可以处理指令以证实卡数据并确定卡数据中所包含的访问权限或者将消息从收发器传递到凭证模块36以及从凭证模块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可以读取和写入数据,所述数据包括但不限于锁配置选项和锁审计尾迹(lock audit trail)。锁审计尾迹可以是统一的审计尾迹,其包括通过经由锁卡读取器90或移动装置12来访问锁而发起的事件。锁功率供应34是功率源,诸如线路功率连接、功率提取系统或对锁控制器24提供动力的电池。在其它实施例中,锁功率供应34可以仅对锁控制器24提供动力,其中锁致动器22主要或完全由另一源(例如用户工作(例如,转动螺栓))来提供动力。

[0032] 认证模块18和凭证模块36可以被布置成与锁处理器30进行通信,并且可操作以解密和证实凭证以提取被传送到锁控制器24中的虚拟卡数据作为“虚拟卡读取”。

[0033] 虽然图2示出了被连接到处理器30的收发器28和锁天线26,但这不是限制可以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可以包含作为凭证模块36的一部分的收发器28和天线26,或者凭证模块36可以具有与处理器30分离的收发器28和天线26,处理器30还具有相同类型或不同类型的单独的收发器28和天线26。在一些实施例中,处理器30可以将经由收发器28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可以被实施为在处理器30内完全或部分执行的软件模块。

[0034] 根据实施例,移动装置12可以包括密钥天线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和密钥功率供应54。密钥收发器42是与锁收发器28对应类型的收发器,并且密钥天线40是对应天线。在一些实施例中,密钥收发器42和密钥天线40还可用于与服务器14、认证模块18和凭证模块36进行通信。在其它实施例中,可以包括一个或多个单独的收发器和天线以与服务器14、认证模块18和凭证模块36进行通信。密钥存储器46可以存储各种类型的字母数字数据或生物测定数据。

[0035] 因此,继续参考图1和图2,提供了访问控制系统20,并且访问控制系统20包括访问控制装置16a和连网装置,所述连网装置是诸如服务器14(下文称为“连网装置14”)。例如,访问控制装置16a可以被设置为旅馆中客房的门锁,并且被布置为限制对受保护资源17a的访问。受保护资源17a可被设置为客房本身。连网装置14被布置成与访问控制装置16a进行信号通信,并且被配置成将认证应用分发给用户的可信装置,访问权限的凭证由一个或多个系统(例如,连网装置14)准予给所述用户。可信装置可以被设置为便携式计算装置或被设置为电话(诸如上面讨论的移动装置12),并且在下文中将被称为“可信装置12”。

[0036] 认证应用可被设置为字母数字认证应用或生物测定认证应用,并且可被存储在可信装置12的密钥存储器46或任何其它存储器单元中。因此,虽然与字母数字标识或生物测定标识相关联的数据可能相当大,尤其是在生物测定数据的情况下,但访问控制系统20不需要包括足以独自存储和维持字母数字标识数据或生物测定标识数据的每个实例的存储

器或存储能力。

[0037] 根据实施例,访问控制系统20的管理员可以自己确定什么类型的装置将有资格作为可信装置12。此类资格可以基于在考虑中的装置中的可用安全性级别以及装置的便携性。凭证可以是任何类型的访问权限凭证,并且在用户确实被授权获得对受保护资源17a的访问时在给定时间段内与用户相关联。出于清楚和简洁的目的,将假设凭证是发给用户并且用户必须呈现给锁卡读取器90以便获得对受保护资源17a的访问的密钥卡上的编码数据。备选地,可以假设凭证是被存储在可信装置12上的编码数据,在这种情况下,可信装置12被用于请求和获得对受保护资源17a的访问。

[0038] 在访问控制系统20的操作中,当凭证作为密钥卡被人(这个人可以是被授权使用密钥卡的用户或未被这样授权的另一人)呈现给访问控制装置16a的锁卡读取器90时,连网装置14向可信装置12发出请求以验证该人实际上是用户。可信装置12通过执行认证应用来完成此操作,该认证应用将认证用户或以其它方式证实该人是用户,或者该认证应用将指示正在进行对安全访问的未经授权的尝试。根据实施例,认证应用可以向用户请求字母数字密码或者请求用户将生物测定标识(例如,指纹或声纹)提交到可信装置12中。如果呈现凭证的人是用户,则用户将继续输入字母数字密码或将生物测定标识提交到可信装置12中以便完成并满足认证应用。当这发生时,可信装置将向连网装置14发送肯定标识信号,连网装置14然后将把解锁信号传递到访问控制装置16a。另一方面,如果呈现凭证的人不是用户,则用户可以根据输入字母数字密码或提交生物测定标识的请求而识别对未经授权的访问的请求正被尝试。在这里,用户可能只是拒绝遵从或采取某种程度的适当行动。同时,由于连网装置14将不会接收到肯定标识信号(或者如果接收到否定标识信号),则连网装置14将指示访问控制装置16a维持被锁定状态,并且访问控制装置16a将不准许呈现凭证的人获得所请求的访问。

[0039] 当凭证作为可信装置12呈现给锁卡读取器90时,连网装置14再次向可信装置12发出请求以验证该人实际上是用户。如上,可信装置12通过执行认证应用来完成此操作,该认证应用可以向用户请求字母数字密码或者请求将生物测定标识提交到可信装置12中。如果呈现凭证的人是用户,则用户将继续输入字母数字密码或将生物测定标识提交到可信装置12中,以便完成并满足认证应用,从而产生肯定标识信号和解锁指令。另一方面,如果呈现凭证的人不是用户,则用户将因为他没有拥有他的电话而不知道对未经授权的访问的请求正被尝试,但是呈现凭证的人将不能完成并满足认证应用。因此,将不会接收到肯定标识信号(或将接收到否定标识信号),将指示访问控制装置16a维持被锁定状态并且将不准许呈现凭证的人获得所请求的访问。

[0040] 此时,要理解的是,即使呈现凭证的人被认证或以其它方式验证了他/她的身份,访问控制装置16a也将仅准许呈现凭证的人根据与凭证相关联的访问权限来获得所请求的访问。也就是说,如果呈现他自己的经授权凭证的人被认证但是正尝试获得对旅馆中受限区域(例如,另一人的客房或旅馆经理的办公室)的访问,则对应访问控制装置16a将拒绝准许所请求的访问。

[0041] 根据权利要求15所述的访问控制系统,其中,与所述控制装置和所述连网装置远程地存储与所述字母数字认证或生物测定认证有关的数据。

[0042] 参考图3和图4,示出了访问控制系统20的操作情况,其中凭证作为密钥卡而被呈

现给访问控制装置16a的锁卡读取器90。如图3和图4中所示,行动者向锁卡阅读器90呈现物理标记卡(图3中的301和图4中的401),据此访问控制装置16a向访问控制系统20,或者更具体地向连网装置14请求访问指令(图3中的302和图4中的402)。此时,连网装置14向可信装置12请求身份验证(图3中的303和图4中的403),可信装置12响应地执行认证应用(图3中的304和图3中的404),并且行动者或以字母数字方式或以生物测定方式来确认他的身份或者未能这样做(图3中的305和图4中的405)。如果行动者确认,则可信装置12向连网装置14提供行动者的身份和授权确认(图3中的306和图4中的406)。随后,连网装置14向访问数据库查询行动者的身份(图3中的307和图4中的407),接收访问控制数据(图3中的308和图4中的408),并确定行动者是否具有获得所请求的访问的准许(图3中的309和图4中的409)。如果是的话,则连网装置14指示访问控制装置16a准许所请求的访问,并且访问控制装置16a遵从(图3中的310和图4中的410)。

[0043] 参考图5和图6,示出了访问控制系统20的操作情况,其中使用可信装置12来呈现凭证。如图5和图6中所示,行动者使用可信装置12来请求访问(图5中的501和图6中的601),据此访问控制装置16a向访问控制系统20,或者更具体地向连网装置14请求访问指令(图5中的502和图6中的602)。此时,连网装置14向可信装置12请求身份验证(图5中的503和图6中的603),可信装置12响应地执行认证应用(图5中的504和图5中的604),并且行动者或以字母数字方式或以生物测定方式来确认他的身份或者未能这样做(图5中的505和图6中的605)。如果行动者确认,则可信装置12向连网装置14提供行动者的身份和授权确认(图5中的506和图6中的606)。随后,连网装置14向访问数据库查询行动者的身份(图5中的507和图6中的607),接收访问控制数据(图5中的508和图6中的608),并确定行动者是否具有获得所请求的访问的准许(图5中的509和图6中的609)。如果是的话,则连网装置14指示访问控制装置16a准许所请求的访问,并且访问控制装置16a遵从(图5中的510和图6中的610)。

[0044] 虽然仅结合有限数量的实施例详细地提供了本公开,但是应该容易理解的是,本公开不限于此类公开的实施例。相反,可以修改本公开以结合此前未描述但与本公开的精神和范畴相称的任何数量的变化、变更、替换或等同布置。另外,虽然已经描述了本公开的各种实施例,但要理解的是,(一个或多个)示例性实施例可以仅包括所描述的示例性方面中的一些。因此,本公开要不被视为受前述描述所限制,而是仅受所附权利要求的范畴所限制。

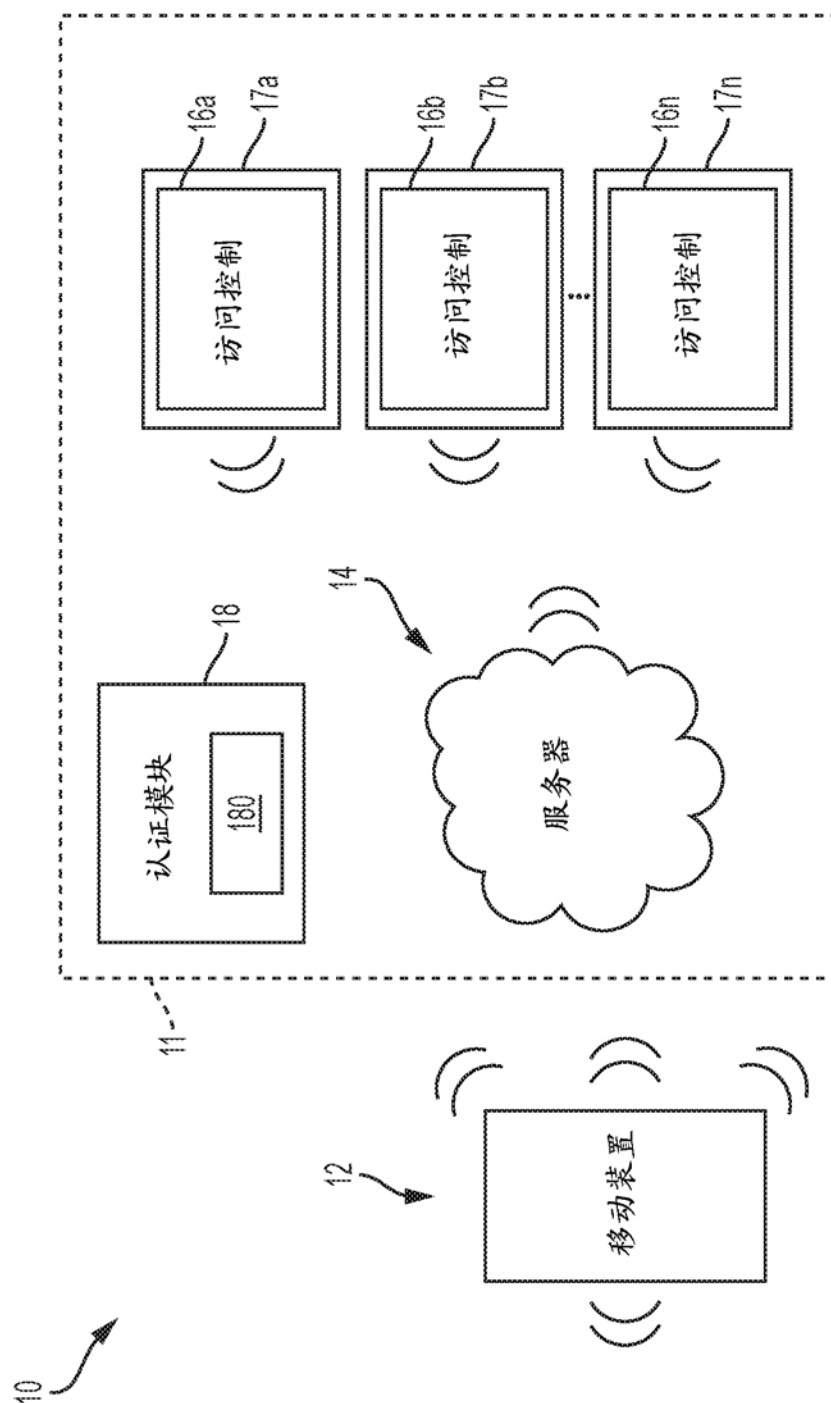


图 1

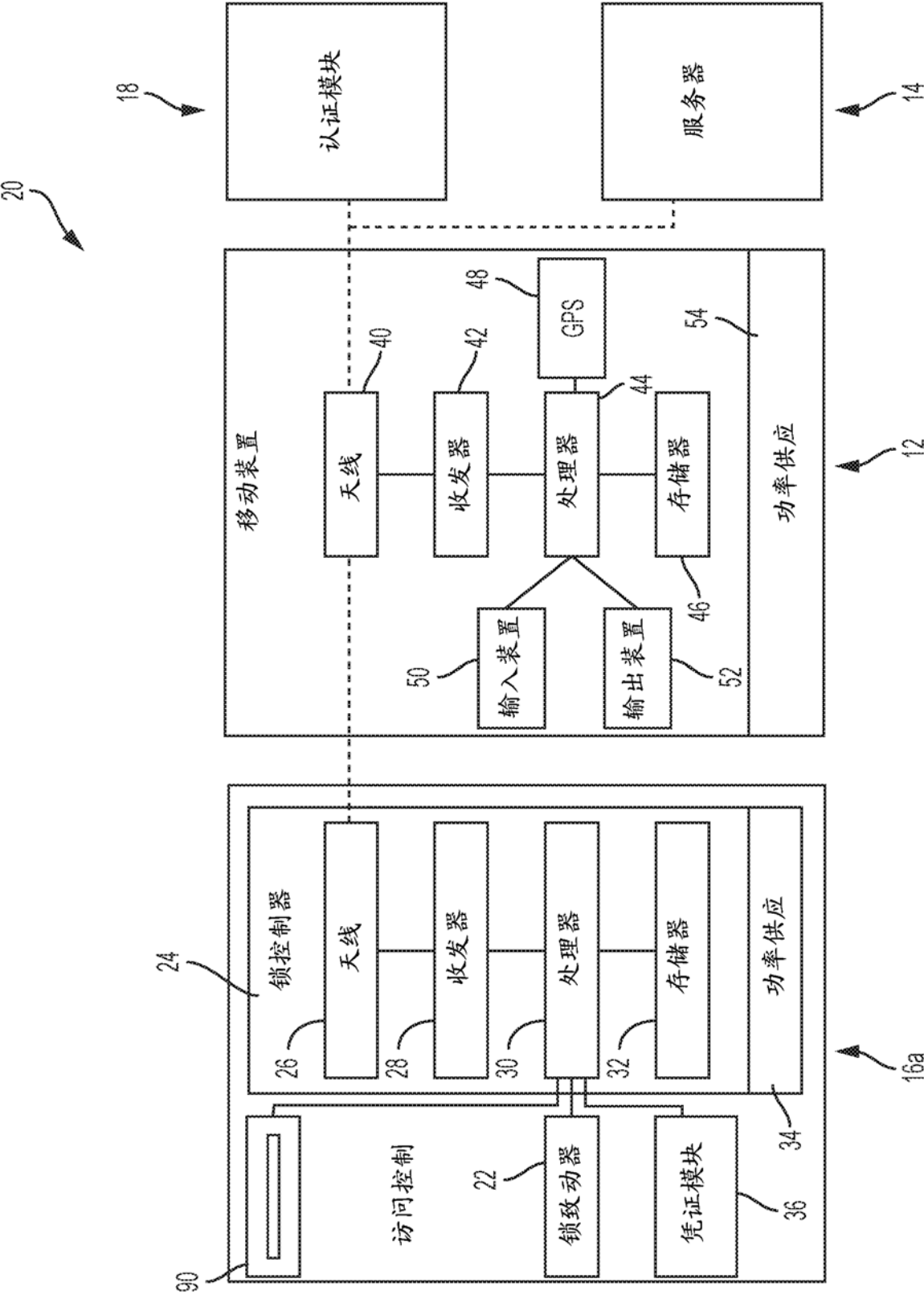


图 2

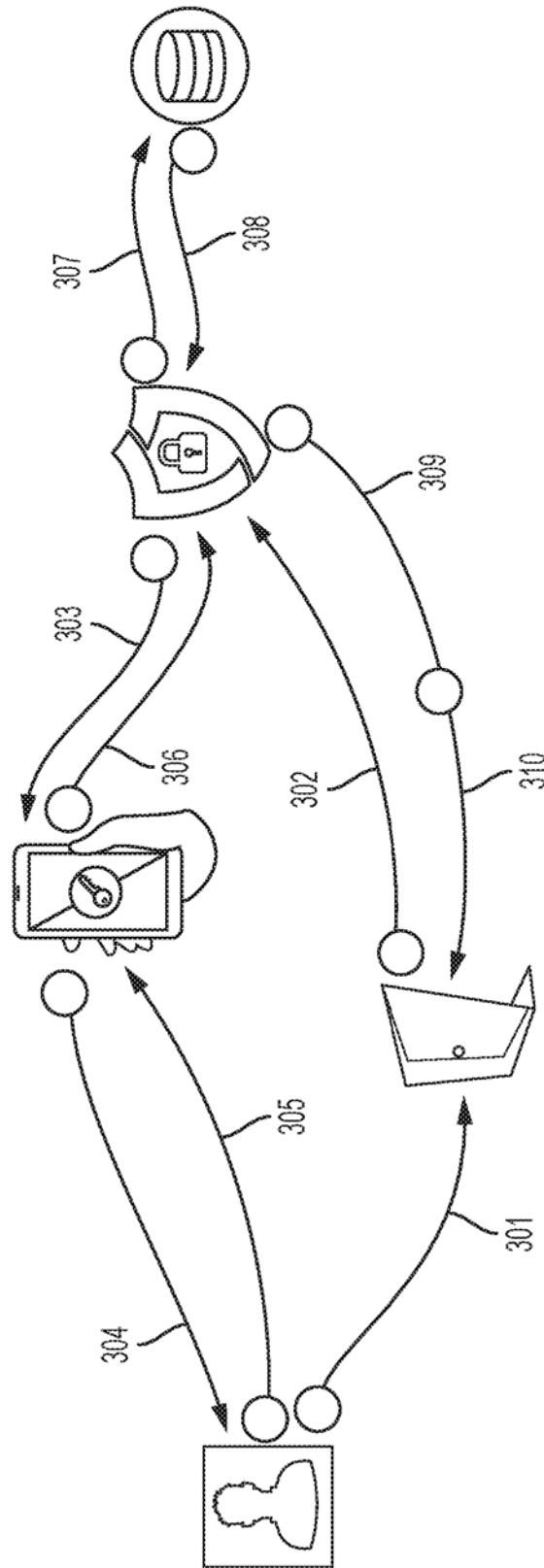


图 3

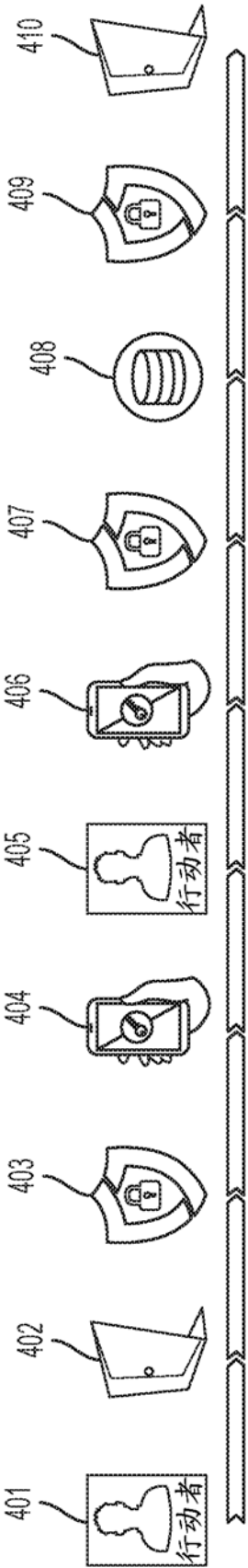


图 4

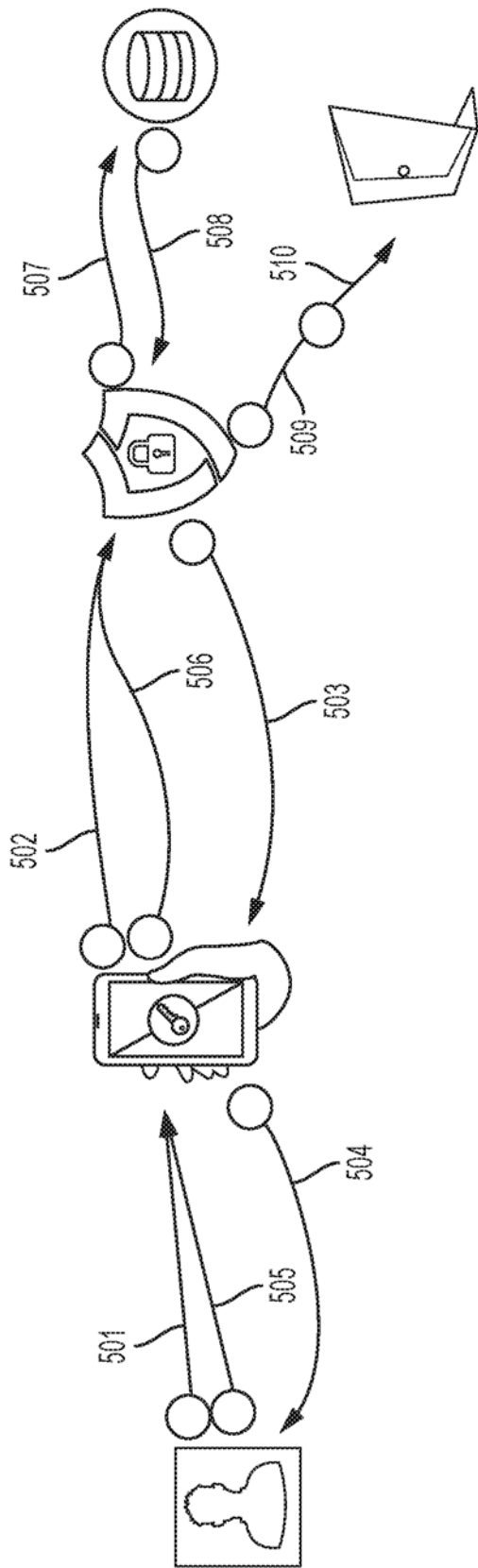


图 5

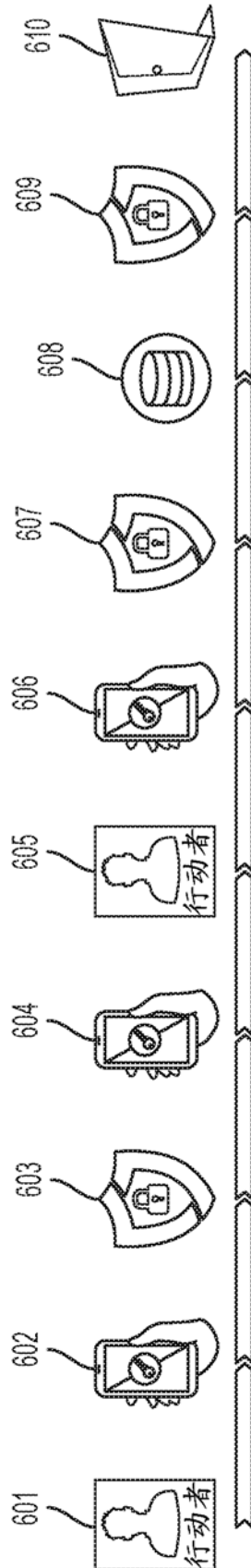


图 6