(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104468113 B
(45)授权公告日 2019.09.27

(21)申请号 201410470037.0

(22)申请日 2014.09.15

(65)同一申请的已公布的文献号
申请公布号 CN 104468113 A

(43)申请公布日 2015.03.25

(30)优先权数据
14/028,208 2013.09.16 US

(73)专利权人 安讯士有限公司
地址 瑞典隆德

(72)发明人 马西亚斯·布鲁斯
妮可拉斯·汉森

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 林斯凯

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 103036894 A,2013.04.10,
WO 2010038923 A1,2010.04.08,
CN 102404314 A,2012.04.04,
CN 102004888 A,2011.04.06,

审查员 田雨润

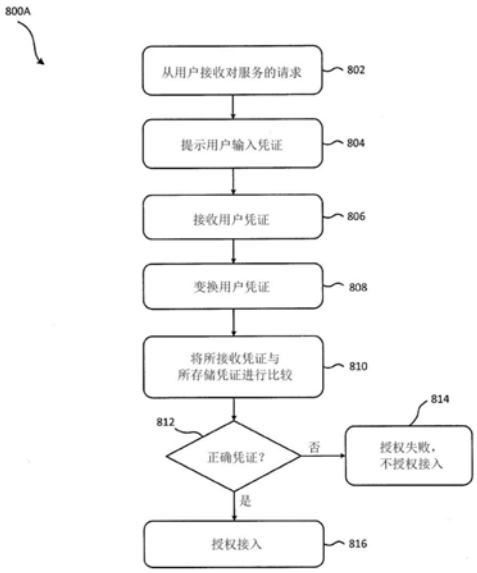
权利要求书3页 说明书18页 附图15页

(54)发明名称

用于分布用户凭证的装置和方法

(57)摘要

本申请案涉及用户凭证的分布。一种方法涉及在分布式物理进入控制系统中分布用户凭证，且更一般来说涉及在分布式系统中分布用户凭证。一种方法可包含存储用户凭证数据库DB(360)、用于验证用户是否可接入由装置(115)提供的第一服务(332)及第二服务(334)的第一经变换凭证DB(356)及第二经变换凭证DB(358)。所述方法可包含基于所述用户凭证DB(360)而产生所述第一经变换凭证DB(356)及所述第二经变换凭证DB(358)，及将从用户接收的凭证与所述第一经变换凭证DB(356)或所述第二经变换凭证DB(358)进行比较以确定是否准予对所述第一服务(332)或所述第二服务(334)的接入。所述方法可包含将所述用户凭证DB(360)分布到以一网络连接的多个其它装置(115/210)以供所述其它装置产生用于验证用户是否可接入服务的经变换凭证DB。



CN 104468113 B

1.一种用于分布用户凭证的装置(115/210),其包含:

存储器(350),其用以存储用户凭证数据库DB(360)、用于验证用户是否可接入由所述装置(115/210)提供的第一服务(332)的第一经变换凭证DB(356)及用于验证用户是否可接入由所述装置(115/210)提供的第二服务(334)的第二经变换凭证DB(358);

通信接口(218),其用于接收未变换的凭证;

处理器(214),其用以:

基于所述用户凭证DB(360)而更新所述第一经变换凭证DB(356)及所述第二经变换凭证DB(358),及

将所接收的未变换的凭证与存储于所述第一经变换凭证DB(356)中的第一经变换凭证进行比较,以确定所述所接收的未变换的凭证对于验证用户是否可接入所述第一服务(332)是正确还是不正确的,或将所述所接收的未变换的凭证与存储于所述第二经变换凭证DB(358)中的第二经变换凭证进行比较以确定所述所接收的未变换的凭证对于验证所述用户是否可接入所述第二服务(334)是正确还是不正确的;

以及

所述通信接口,其用以:

将所述用户凭证DB(360)分布到以对等网络连接的多个其它装置(115/210)以供所述其它装置产生用于验证用户是否可接入由所述其它装置提供的服务的其它经变换凭证DB;以及

从所述对等网络中的所述其它装置接收所述用户凭证DB(360)。

2.根据权利要求1所述的装置,

其中所述用户凭证DB为经加密用户凭证DB,且其中所述处理器经配置以解密所述经加密用户凭证DB且基于经解密用户凭证DB而产生所述第一及第二经变换凭证DB;且

其中所述通信接口经配置以将所述经加密用户凭证DB分布到所述其它装置以供所述其它装置产生用于验证用户是否可接入由所述其它装置提供的服务的所述其它经变换凭证DB。

3.根据权利要求1或权利要求2所述的装置,

其中所述第一服务包含以下各项中的一者:安全壳层SSH服务器、文件传送协议FTP服务器、远程桌面协议ROP服务器、虚拟专用网络VPN服务器或虚拟网络信道VNC服务器,且

其中所述第二服务不同于所述第一服务且包含以下各项中的一者:安全壳层SSH服务器、文件传送协议FTP服务器、远程桌面协议ROP服务器、虚拟专用网络VPN服务器或虚拟网络信道VNC服务器。

4.根据权利要求2所述的装置,

其中所述处理器经配置以通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第一经变换凭证DB;且

其中所述处理器经配置以通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第二经变换凭证DB。

5.根据权利要求1到2中任一权利要求所述的装置,其中所述第一经变换凭证DB及所述第二经变换凭证DB各自经配置以借助同一凭证验证同一用户。

6.根据权利要求1或2所述的装置,

其中所述处理器经配置以从管理员接收经更新用户凭证、更新所述用户凭证DB，

基于所述经更新用户凭证DB而产生所述第一经变换凭证DB及所述第二经变换凭证DB，且

其中所述通信接口经配置以将所述经更新用户凭证DB分布到所述其它装置以供所述其它装置产生用于验证用户是否可接入由所述其它装置提供的服务的所述其它经变换凭证DB。

7.根据权利要求2所述的装置，其中所述处理器经配置以：

基于通过所述通信接口从管理员接收的口令而解密经加密密钥以产生密钥；

基于所述密钥而解密所述经加密用户凭证DB；

基于所述密钥而解密经加密管理员口令以产生经解密管理员口令；以及

当从所述管理员接收的所述口令等同于所述经解密管理员口令时授权接入。

8.一种包含多个根据权利要求1或2所述的装置的系统，所述装置经由对等网络通信以分布用户凭证DB。

9.一种用于分布用户凭证的方法，其包含：

存储用户凭证数据库DB以存储未变换的凭证、用于验证用户是否可接入由装置提供的第一服务的第一经变换凭证DB及用于验证用户是否可接入由所述装置提供的第二服务的第二经变换凭证DB；

基于所述用户凭证DB而产生所述第一经变换凭证DB及所述第二经变换凭证DB；

在所述装置中接收未变换的凭证并将所述未变换的凭证变换以产生变换的所接收的凭证；

将经变换的所述所接收的凭证与存储于所述第一经变换凭证DB中的第一经变换凭证进行比较，以确定所述所接收的未变换的凭证对于验证用户是否可接入所述第一服务是正确还是不正确的，或将经变换的所述所接收的凭证与存储于所述第二经变换凭证DB中的第二经变换凭证进行比较，以确定所述所接收的未变换的凭证对于验证所述用户是否可接入所述第二服务是正确还是不正确的；

将所述用户凭证DB分布到以对等网络连接的多个其它装置以供所述其它装置产生用于验证用户是否可接入由所述其它装置提供的服务的其它经变换凭证DB；以及

从所述对等网络中的所述其它装置接收所述用户凭证DB。

10.根据权利要求9所述的方法，其中所述用户凭证DB为经加密用户凭证DB，所述方法进一步包括：

解密所述经加密用户凭证DB且基于经解密用户凭证DB而产生所述第一及第二经变换凭证DB；以及

将所述经加密用户凭证DB分布到所述其它装置以供所述其它装置中的每一者产生用于验证用户是否可接入由对应的装置提供的服务的对应的经变换凭证DB。

11.根据权利要求10所述的方法，其进一步包括：

通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第一经变换凭证DB；以及

通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第二经变换凭证DB。

12.根据权利要求9、10或11所述的方法，其中所述第一经变换凭证DB及所述第二经变换凭证DB各自经配置以借助同一凭证验证同一用户。

13.根据权利要求9、10或11所述的方法，其进一步包括：

从管理员接收经更新用户凭证，且更新所述用户凭证DB；

基于所述经更新用户凭证DB而产生所述第一经变换凭证DB及所述第二经变换凭证DB；以及

将所述经更新用户凭证DB分布到所述其它装置以供所述其它装置中的每一者产生用于验证用户是否可接入由对应的装置提供的服务的对应的经变换凭证DB。

14.根据权利要求10或11所述的方法，其进一步包括基于从管理员接收的口令而解密所述经加密用户凭证DB。

15.根据权利要求14所述的方法，

其中基于从所述管理员接收的所述口令而解密所述经加密用户凭证DB包括：

基于从所述管理员接收的所述口令而解密经加密密钥以产生密钥，及

基于所述密钥而解密所述经加密用户凭证DB，且

其中所述方法进一步包括：

基于所述密钥而解密经加密管理员口令以产生经解密管理员口令；以及

当从所述管理员接收的所述口令等同于所述经解密管理员口令时授权接入。

用于分布用户凭证的装置和方法

技术领域

[0001] 本发明涉及在物理进入控制系统中分布用户凭证，且更一般来说涉及分布用户凭证。

背景技术

[0002] 进入控制系统可用于控制对设施的物理进入。进入控制系统(以及其它类型的控制系统)可具有众多控制器，每一控制器为用户提供各种服务。每一控制器上的每一服务可需要用于验证用户以授权对所述服务的接入的凭证。因此，可需要用户记住其用于每一装置上的每一服务的凭证。

发明内容

[0003] 在一个实施例中，一种装置可包含存储器，其用以存储用户凭证数据库(DB)、用于验证用户是否可接入由所述装置提供的第一服务的第一经变换凭证DB及用于验证用户是否可接入由所述装置提供的第二服务的第二经变换凭证DB。所述装置可包含处理器，其用以基于所述用户凭证DB而更新所述第一经变换凭证DB及所述第二经变换凭证DB，及将从用户接收的凭证与所述第一经变换凭证DB进行比较以验证所述用户是否可接入所述第一服务或将从所述用户接收的所述凭证与所述第二经变换凭证DB进行比较以验证所述用户是否可接入所述第二服务。所述装置可包含通信接口，其用以将所述用户凭证DB分布到以对等网络连接的多个其它装置以供所述其它装置产生用于验证用户是否可接入由对应其它装置提供的服务的经变换凭证DB。所述处理器可从所述对等网络中的所述其它装置接收所述用户凭证DB。

[0004] 在一个实施例中，所述用户凭证DB可为经加密用户凭证DB，且所述处理器可解密所述经加密用户凭证DB且基于所述经解密用户凭证DB而产生所述第一及第二经变换凭证DB。所述通信接口可将所述经加密用户凭证DB分布到所述其它装置以供所述其它装置产生用于验证用户是否可接入由所述装置提供的服务的对应经变换凭证DB。

[0005] 在一个实施例中，所述第一服务可包含安全壳层服务器、文件传送协议服务器、远程桌面协议服务器、虚拟专用网络服务器或虚拟网络信道服务器。在此实施例中，所述第二服务可不同于所述第一服务且可包含安全壳层服务器、文件传送协议服务器、远程桌面协议服务器、虚拟专用网络服务器或虚拟网络信道服务器。

[0006] 在一个实施例中，所述处理器可通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第一经变换凭证DB。所述处理器还可通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第二经变换凭证DB。

[0007] 在一个实施例中，所述第一经变换凭证DB及所述第二经变换凭证DB可各自经配置以借助同一凭证验证同一用户。在一个实施例中，所述处理器可从管理员接收经更新用户凭证、更新所述用户凭证DB，基于所述经更新用户凭证DB而产生所述第一经变换凭证DB及所述第二经变换凭证DB。所述通信接口可将所述经更新用户凭证DB分布到所述其它装置以

供所述其它装置产生用于验证用户是否可接入由对应装置提供的服务的对应经变换凭证DB。

[0008] 在一个实施例中，所述处理器可基于通过所述通信接口从管理员接收的口令而解密所述经加密用户凭证DB。在一个实施例中，所述处理器可基于通过所述通信接口从所述管理员接收的所述口令而解密经加密密钥以产生密钥。所述处理器还可基于所述密钥而解密所述经加密用户凭证DB。

[0009] 在一个实施例中，所述处理器可基于所述密钥而解密经加密管理员口令以产生经解密管理员口令。所述处理器还可当从所述管理员接收的所述口令等同于所述经解密管理员口令时授权接入。

[0010] 一个实施例包含一种方法。所述方法可存储用户凭证数据库(DB)、用于验证用户是否可接入由装置提供的第一服务的第一经变换凭证DB及用于验证用户是否可接入由所述装置提供的第二服务的第二经变换凭证DB。所述方法可基于所述用户凭证DB而产生所述第一经变换凭证DB及所述第二经变换凭证DB。所述方法可将从用户接收的凭证与所述第一经变换凭证DB进行比较以验证所述用户是否可接入所述第一服务或将从所述用户接收的所述凭证与所述第二经变换凭证DB进行比较以验证所述用户是否可接入所述第二服务。所述方法还可将所述用户凭证DB分布到以对等网络连接的多个其它装置以供所述其它装置产生用于验证用户是否可接入由所述其它装置提供的服务的经变换凭证DB。所述方法还可从所述对等网络中的所述其它装置接收所述用户凭证DB。

[0011] 在一个实施例中，所述用户凭证DB可为经加密用户凭证DB，且所述方法可解密所述经加密用户凭证DB且基于所述经解密用户凭证DB而产生所述第一及第二经变换凭证DB。所述方法还可将所述经加密用户凭证DB分布到所述其它装置以供所述其它装置中的每一者产生用于验证用户是否可接入由所述对应装置提供的服务的对应经变换凭证DB。

[0012] 在一个实施例中，所述方法可包含通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第一经变换凭证DB。所述方法可通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第二经变换凭证DB。

[0013] 在一个实施例中，所述第一经变换凭证DB及所述第二经变换凭证DB各自经配置以借助同一凭证验证同一用户。在一个实施例中，所述方法可包含从管理员接收经更新用户凭证、更新所述用户凭证DB，及基于所述经更新用户凭证DB而更新所述第一经变换凭证DB及所述第二经变换凭证DB。所述方法还可包含将所述经更新用户凭证DB分布到所述其它装置以供所述其它装置中的每一者产生用于验证用户是否可接入由所述对应装置提供的服务的对应经变换凭证DB。

[0014] 在一个实施例中，所述方法可包含基于从管理员接收的口令而解密所述经加密用户凭证DB。在一个实施例中，所述方法可包含基于从所述管理员接收的所述口令而解密经加密密钥以产生密钥，及基于所述密钥而解密所述经加密用户凭证DB。

[0015] 在一个实施例中，所述方法可包含基于所述密钥而解密经加密管理员口令以产生经解密管理员口令。所述方法可包含当从所述管理员接收的所述口令等同于所述经解密管理员口令时授权接入。

[0016] 一个实施例可包含一种系统。所述系统可包含经由网络通信的多个装置。每一装置可包含存储器，其用以存储用户凭证数据库(DB)、用于验证用户是否可接入由对应装置

提供的第一服务的第一经变换凭证DB及用于验证用户是否可接入由对应装置提供的第二服务的第二经变换凭证DB。每一装置可包含处理器，其用以基于所述用户凭证DB而更新所述第一经变换凭证DB及所述第二经变换凭证DB。所述处理器可将从用户接收的凭证与所述第一经变换凭证DB或所述第二经变换凭证DB进行比较以确定是否准予对所述第一服务或所述第二服务的接入。每一装置可包含通信接口，其用以将所述用户凭证DB分布到所述其它装置以供所述其它装置中的每一者产生用于验证用户是否可接入由所述对应装置提供的服务的对应经变换凭证DB。所述通信接口可从所述其它装置接收所述用户凭证DB。

[0017] 在所述系统的一个实施例中，所述装置以对等网络连接且在所述对等网络中的所述装置当中分布所述用户凭证DB。在一个实施例中，所述用户凭证DB为经加密用户凭证DB，且所述处理器经配置以解密所述经加密用户凭证DB且基于所述经解密用户凭证DB而产生所述第一及第二经变换凭证DB。在所述系统的一个实施例中，所述通信接口可将所述经加密用户凭证DB分布到所述其它装置以供所述其它装置中的每一者产生用于验证用户是否可接入由所述对应装置提供的服务的对应经变换凭证DB。

[0018] 在所述系统的一个实施例中，所述处理器可通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第一经变换凭证DB，且可通过使用密码单向函数变换来自所述经解密用户凭证DB的凭证而产生所述第二经变换凭证DB。

[0019] 下文描述其它实施例。也就是说，上文所描述的实施例仅作为实例而提供。

附图说明

[0020] 图1是图解说明根据本文中所描述的实施例的示范性环境的框图；

[0021] 图2A及2B是图解说明图1的系统单元的示范性组件的框图；

[0022] 图3A及3B是图解说明在一个实施例中图1的系统单元的功能组件的框图；

[0023] 图3C是图解说明在一个实施例中图3B的控制器中的管理逻辑的功能组件的框图；

[0024] 图4是图解说明在一个实施例中图1的系统单元的示范性物理布局的平面布置图；

[0025] 图5是图解说明图1的分布式控制系统的示范性物理布局的平面布置图；

[0026] 图6是图解说明图1的管理装置的示范性组件的框图；

[0027] 图7A是在一个实施例中的示范性管理员凭证数据库的框图；

[0028] 图7B及7C是在一个实施例中的示范性用户凭证数据库的框图；

[0029] 图7D到7G是在一个实施例中的示范性服务凭证数据库的框图；

[0030] 图8A是用于验证经授权接入控制单元中的服务的用户的示范性过程的流程图；

[0031] 图8B是供管理员更新图7B及7C的用户凭证数据库以及图7D到7G的服务凭证数据库的示范性过程的流程图；且

[0032] 图8C是在一个实施例中用于验证管理员的示范性过程的流程图。

具体实施方式

[0033] 以下详细描述参考附图。不同图式中的相同参考编号识别相同或类似元件。

[0034] 下文所描述的一个实施例涉及物理进入控制系统(PACS)中的控制器。其它实施例可包含不同于PACS的环境，例如用于控制建筑物管理、监视及安全系统内的不同应用的系统中的控制器。举例来说，一个实施例可包含家庭自动化系统中的控制器。

[0035] 如上文所提及，可需要用户记住用于由每一控制器提供的每一服务的凭证。这对于用户来说可为烦累的。在下文所描述的一个实施例中，管理员可将用户凭证管理为在多个控制器上针对多个服务相同。在另一实施例中，举例来说，管理员还可从另一控制器管理存储于一个控制器中的用户凭证。下文的一或多个实施例涉及在特定环境中于物理进入控制系统(例如，分布式物理进入控制系统)中分布用户凭证。如所描述，其它实施例可涉及在其它类型的系统(例如，不同于物理进入控制系统)中分布用户凭证。一个实施例可涉及一种将用户凭证存储于一装置上而不将那些凭证分布到其它装置的方法及装置。

[0036] 图1是可在其中实施下文所描述的系统及方法的示范性环境100的框图。如图1中所展示，环境100可包含分布式控制系统110(例如，分布式物理进入控制系统)、网络120及管理装置130。

[0037] 分布式控制系统110可包含分布式计算系统，所述分布式计算系统包含系统单元115-A到115-N(统称为“系统单元115”或“单元115”且个别地称为“单元115”)。在一个实施例中，系统单元115包含物理进入控制装置。举例来说，系统单元115可包含控制对安全区域(例如一房间或一房间群组)的进入的控制器。系统单元115可经由读取器装置接收凭证(例如，进入卡凭证)且确定所述凭证是否为真实的且与进入所述安全区域的授权相关联。如果是，那么所述控制器可发出打开门上的锁或执行与准予进入所述安全区域相关联的其它操作的命令。

[0038] 分布式控制系统110可包含一或多个分布式数据集。分布式数据集包含以分布式(及潜在地冗余)方式存储于与所述分布式数据集相关联的系统单元115中的数据。在一个实施例中，分布式数据集复制于一个以上装置上。举例来说，整个分布式数据集可存储于所有单元115中。在另一实施例中，一或多个单元115可存储分布式数据集的子集。而且，分布式数据集可与所有系统单元115相关联或可与系统单元115的子集相关联。

[0039] 在一个实施例中，在单元115当中达成共识以便对分布式数据集(例如，基于共识的分布式数据库)做出改变。系统单元115可提议对基于共识的分布式数据集的改变。如果与分布式数据集相关联的法定数目的单元115接受了改变，那么可达成共识，且可将改变传播到每一相关联单元115中的分布式数据集的每一局部副本。因此，如果法定数目的相关联单元115投票赞成分布式数据集的改变，那么可达成关于所述改变的共识。法定数目可对应于相关联单元115的最小大多数。因此，如果分布式数据集与N个单元115相关联，那么在N/2+1个相关联单元115投票赞成改变的情况下(如果N为偶数)或在(N-1)/2+1个相关联单元115投票赞成改变的情况下(如果N为奇数)，可达到法定数目。需要最小大多数达到法定数目可确保在考虑两个冲突提议时，至少一个系统单元115接收到两个提议且选择所述提议中的一者以达成共识。

[0040] 基于共识的分布式数据集可确保与分布式数据集相关联的任何系统单元115均包含由所述分布式数据集管理的信息(例如，在一个实施例中，所有信息)。举例来说，分布式数据集可包含进入规则，且所述进入规则可用于与所述分布式数据集相关联的任何系统单元115。因此，由于一或多个分布式数据集，在一个实施例中，控制系统110可对应于不具有中央控制装置(例如服务器装置)的分散式系统。在其它实施例中，控制系统110可包含分散式系统及中央控制装置(例如服务器装置)两者。对控制系统110的改变可在任何系统单元115处配置，且如果改变与分布式数据集相关联，那么可将所述改变传播到与所述分布式数

据集相关联的其它系统单元115。此外，控制系统110可相对于装置故障展现稳健性，因为可避免单个故障点。举例来说，如果特定系统单元115失效，那么其它单元115可继续操作而不会丢失数据(或使数据丢失最小化)。在另一实施例中，可在无共识的情况下对分布式数据集做出改变。

[0041] 网络120可使得单元115能够彼此通信及/或可使得管理装置130能够与特定单元115通信。网络120可包含一或多个电路交换网络及/或包交换网络。举例来说，网络120可包含局域网(LAN)、广域网(WAN)、城域网(MAN)、公共交换电话网络(PSTN)、特设网络、内联网、因特网、基于光纤的网络、无线网络及/或这些或其它类型网络的组合。

[0042] 管理装置130允许管理员连接到特定单元115以便配置控制系统110、改变控制系统110的配置、从控制系统110接收信息及/或以其它方式管理控制系统110。管理装置130可包含经配置以与单元115中的一或多者通信的任何装置。举例来说，管理装置130可包含便携式通信装置(例如，移动电话、智能电话、平板电话装置、全球定位系统(GPS)装置及/或另一类型的无线装置)；个人计算机或工作站；服务器装置；膝上型计算机；平板计算机或另一类型的便携式计算机；及/或具有通信能力的任何类型的装置。在一个实施例中，管理装置130可为单元115的部分。如此，管理员可从单元115中的一或多者管理控制系统110。

[0043] 虽然图1展示环境100的示范性组件，但在其它实施方案中，环境100相比图1中所描绘的组件可包含更少的组件、不同的组件、不同布置的组件或额外组件。另外或替代地，环境100中的任一装置(或任何装置群组)可执行描述为由环境100中的一或多个其它装置执行的功能。

[0044] 图2A及2B是图解说明单元115的示范性组件的框图。如图2A中所展示，单元115可包含控制器210及一或多个外围装置230。控制器210可控制单元115的操作，可与其它单元115通信、可与管理装置130通信及/或可控制外围装置230。外围装置230可包含将信息提供到控制器210、由控制器210控制及/或以其它方式与控制器210通信的装置。在一个实施例中，外围装置230可包含任何类型的安全装置。举例来说，外围装置230可包含例如读取器装置240、锁装置250、传感器260(例如，摄像机)及/或致动器270等安全装置。

[0045] 如图2B中所展示，控制器210可包含总线212、处理器214、存储器216、网络接口218、外围接口220及外壳222。总线212包含准许控制器210的组件当中的通信的路径。处理器214可包含任何类型的单核心处理器、多核心处理器、微处理器、基于锁存器的处理器及/或解译并执行指令的处理逻辑(或处理器、微处理器及/或处理逻辑的族群)。在其它实施例中，处理器214可包含集成电路及专用集成电路(ASIC)、现场可编程门阵列(FPGA)及/或另一类型的集成电路或处理逻辑。处理器214可包含可各自执行不同功能的多个处理器(例如，在相同或单独芯片中)。举例来说，处理器214可包含专用于加密及解密数据的电路(例如，ASIC)以及微处理器。

[0046] 存储器216存储信息、数据及/或指令。存储器216可包含任何类型的动态、易失性及/或非易失性存储装置。存储器216可存储供由处理器214执行的指令或供由处理器214使用的信息。举例来说，存储器216可包含随机存取存储器(RAM)或另一类型的动态存储装置、只读存储器(ROM)装置或另一类型的静态存储装置、内容可寻址存储器(CAM)、磁性及/或光学记录存储器装置及其对应驱动器(例如，硬盘驱动器、光学驱动器等等)及/或可装卸形式的存储器，例如快闪存储器。

[0047] 网络接口218可包含收发器(例如,发射器及/或接收器),所述收发器使得控制器210能够经由有线通信链路(例如,导电线、双绞线电缆、同轴电缆、传输线、光纤电缆及/或波导等等)、无线通信链路(例如,射频、红外及/或视觉光学器件等等)或无线与有线通信链路的组合与其它装置及/或系统通信(例如,发射及/或接收数据)。网络接口218可包含将基带信号转换为射频(RF)信号的发射器及/或将RF信号转换为基带信号的接收器。网络接口218可耦合到用于发射及接收RF信号的天线。

[0048] 网络接口218可包含逻辑组件,所述逻辑组件包含输入及/或输出端口、输入及/或输出系统及/或促进将数据发射到其它装置的其它输入及输出组件。举例来说,网络接口218可包含用于有线通信的网络接口卡(例如,以太网卡)及/或用于无线通信的无线网络接口(例如,WiFi)卡。网络接口218还可包含用于经由电缆通信的通用串行总线(USB)端口、蓝牙无线接口、射频识别(RFID)接口、近场(NFC)无线接口及/或将数据从一种形式转换为另一形式的任何其它类型的接口。

[0049] 外围接口220可经配置以与一或多个外围装置230通信。举例来说,外围接口220可包含一或多个逻辑组件,所述逻辑组件包含输入及/或输出端口、输入及/或输出系统及/或促进将数据发射到外围装置230的其它输入及输出组件。作为一实例,外围接口220可使用串行外围接口总线协议(例如,韦根(Wiegand)协议及/或RS-485协议)与外围装置230通信。作为另一实例,外围接口220可使用不同类型的协议。在一个实施例中,网络接口218还可充当用于将外围装置230耦合到控制器210的外围接口。

[0050] 外壳222可包封控制器210的组件且可保护控制器210的组件免受环境影响。在一个实施例中,外壳222可包含外围装置230中的一或多者。在另一实施例中,外壳222可包含管理装置130。外壳222可在具有一个以上系统单元115及/或一个以上控制器210的系统中界定一个系统单元115及/或控制器210与其它系统单元115及/或控制器210的边界。

[0051] 如下文所描述,控制器210可执行与分布用于一或多个装置上的一或多个服务的用户凭证有关的操作。控制器210可由于ASIC的硬连线电路而执行这些操作。控制器210还(或替代地)可响应于处理器214执行计算机可读媒体(例如存储器216)中所含有的软件指令而执行这些操作。计算机可读媒体可包含非暂时性存储器装置。存储器216可实施于单个物理存储器装置内或跨越多个物理存储器装置散布。可将软件指令从另一计算机可读媒体或从另一装置读取到存储器216中。存储器216中所含有的软件指令可致使处理器214执行本文中所描述的过程。因此,本文中所描述的实施方案并不限于硬件电路及软件的任何特定组合。

[0052] 返回到外围装置230,读取器装置240可包含从用户读取凭证并将所述凭证提供到控制器210的装置。举例来说,读取器装置240可包含经配置以从用户接收字母数字个人识别号码(PIN)的小键盘;用以配置在磁条或另一类型的存储装置(例如射频识别(RFID)标签)上存储卡代码的卡的读卡器;经配置以读取用户的指纹的指纹读取器;经配置以读取用户的虹膜的虹膜读取器;麦克风及经配置以记录用户的话音特征标志的话音特征标志识别器;NFC读取器;与面部辨识软件相关联的摄像机;及/或另一类型的读取器装置。读取器装置240可包含可提供凭证的任何类型的安全装置,且可包含一或多个传感器装置,例如下文参考传感器260所描述的任何传感器装置。举例来说,读取器装置240可包含用于面部辨识的摄像机及/或用于话音辨识的麦克风。在此情况中,举例来说,用户的话音或面部可为用

户的凭证。

[0053] 锁装置250可包含由控制器210控制的锁。锁装置250可锁住门(例如,防止其打开或关闭)、窗户、HVAC通风孔及/或到安全区域的另一类型的进入开口。举例来说,锁装置250可包含电磁锁;具有由控制器210控制的电动机的机械锁;机电锁;及/或另一类型的锁。

[0054] 传感器260可包含感测装置。作为实例,传感器260可包含:用以感测门打开还是关闭的门传感器;可见光监视装置(例如,摄像机)、红外(IR)光监视装置、热特征标志监视装置、音频监视装置(例如,麦克风)及/或另一类型的监视装置;报警传感器,例如运动传感器、热传感器、压力传感器及/或另一类型的报警传感器;篡改传感器,例如位于单元115内侧的位置传感器;及/或位于与单元115相关联的安全区域内的“退出请求”按钮;及/或另一类型的传感器装置。在以下实例中,传感器260可称为“摄像机260”。

[0055] 致动器270可包含致动器装置。作为一实例,致动器270可控制照明装置。作为其它实例,致动器270可包含:防盗报警激活器;用以播放消息或产生报警信号的扬声器;显示装置;用以移动传感器260(例如,控制摄像机或其它监视装置的视域)的电动机;用于打开/关闭门、窗户、HVAC通风孔及/或与安全区域相关联的另一开口的电动机;用以将锁装置250固定于锁住或未锁位置中的电动机;灭火装置;及/或另一类型的致动器装置。

[0056] 虽然图2A及2B展示单元115的示范性组件,但在其它实施方案中,单元115相比图2A及2B中所描绘的组件可包含更少的组件、不同的组件、额外组件或不同布置的组件。举例来说,虽然在图2A中展示单个读取器装置240、单个锁装置250、单个传感器260及单个致动器270,但实际上,外围装置230可包含多个读取器装置240、多个锁装置250、多个传感器260及/或多个致动器270。外围装置230也可不包含图2A中所展示的装置中的一或多者。另外或替代地,单元115的任何组件(或任何组件群组)可执行描述为由单元115的一或多个其它组件执行的任务。

[0057] 此外,虽然示范性分布式控制系统110包含物理进入分布式控制系统,但其它实施方案可控制不同于物理进入的系统。另一方面,分布式控制系统110可包含任何类型的物理进入控制系统(例如,在操作环境中),例如打开及/或关闭门或控制对建筑物或设施的物理进入的控制系统。分布式控制系统110还可包含用以控制风扇(例如,起动或停止)、用以起始建筑物管理系统中的报警(例如,失败的验证、成功的验证等等)或用以控制工业自动化系统中的机器人臂的系统。

[0058] 图3A是图解说明系统单元115的示范性功能层的框图。如图3A中所展示,单元115可包含应用程序接口(API)层310、应用层320、分布层340及存储层350。

[0059] API层310包含经配置以与(例如)管理装置130通信的API。当管理员使用管理员装置130登录到单元115中时,API层310可与管理员装置130通信以验证管理员。作为另一实例,API层310可与管理员装置130通信以改变单元115的配置。API层310可从管理员装置130接收数据并将所述数据提供到分布层340及/或存储层350。API层310还可与管理员装置130通信以在应用层320中安装应用。API层310可经配置以处置不同管理员类型。举例来说,API层310可包含用以处置Web服务管理员、Linux管理员、开放网络视频接口论坛(ONVIF)管理员的API及/或另一类型的API。

[0060] 应用层320可包含安装于单元115上的一或多个应用。应用可包含控制逻辑应用、用以打开及关闭门的门控制应用、用以接收用户凭证的读取器控制应用以及其它应用。下

文关于图3B更详细地论述应用。

[0061] 分布层340可管理与单元115相关联的一或多个分布式数据集。举例来说，分布层340可以对等网络连接控制器210以用于分布数据集。分布层340可使用协议(例如，PAXOS协议)来建立关于特定基于共识的分布式数据集的改变的共识。作为一实例，分布层340可将改变的提议发送到与分布式数据集相关联的其它系统单元115且可从其它系统单元115接收改变的法定数目。作为另一实例，分布层340可投票赞成从另一单元115接收的提议。作为又一实例，分布层340可接收已在未投票赞成改变的情况下达成对所述改变的共识的指示。当接收到对改变的共识的指示时，分布层340可在分布式数据集的局部副本中做出所述改变。分布层340可经由网络120维持与其它单元115的安全连接(例如，输送层安全(TLS)连接)。

[0062] 存储层350可存储与单元115相关联的一或多个数据集。存储于存储层350中的数据集可对应于局部数据集或可对应于分布式数据集。局部数据集可存储与存储所述局部数据集的特定单元115相关联(及/或仅与所述特定单元相关联)的信息。分布式数据集可存储与同所述分布式数据集相关联的其它系统单元115相关联的信息。

[0063] 图3B是控制器210的示范性功能组件的框图，其中为应用层320及存储层350提供了更多细节。如图3B中所展示，应用层320可包含控制逻辑应用322(或“控制逻辑322”)、管理员验证逻辑323、门控制应用324、读取器控制应用326、事件处置应用328、时间表处置应用330、第一服务应用332(或“第一服务332”)及/或第二服务应用334(或“第二服务334”)。举例来说，其它应用可包含报警及控制应用。处置这些功能组件的逻辑可涉及控制器210及/或系统单元115的不同部分。也就是说，例如，处置这些功能组件的逻辑可不连接到单个硬件模块。

[0064] 控制逻辑322可基于所接收凭证且基于所存储进入规则而确定是否准予用户的物理进入。管理员逻辑323可准予管理员的接入(例如，远程接入，例如远程登录)且提供其它管理过程。举例来说，管理逻辑323可基于凭证(例如，用户名及口令)而验证管理员，且授权管理员来存取并更新用户凭证(例如，针对其它管理员及/或针对希望被准予物理进入的用户)等等。在一个实施例中，管理逻辑323可授权经验证管理员来存取并更新用于特定系统单元115的用户凭证或更新用于其它或甚至所有系统单元115的用户凭证。下文关于图3C来描述管理逻辑323的这些功能。

[0065] 门控制应用324可控制一或多个门及/或相关联锁装置250。举例来说，门控制应用324可确定门打开还是关闭及/或锁住还是未锁，且可操作一或多个装置以打开或关闭门及/或将门锁住或开锁。读取器控制应用326可控制一或多个读取器装置240且可获得并处理从一或多个读取器装置240接收的凭证。事件处置应用328可处理由单元115记录的事件，例如门打开事件、报警事件、传感器事件及/或其它类型的所登记事件。事件处置应用328可产生报告及/或报警并将所述报告及/或报警发送到管理员装置130(及/或发送到另一指定装置，例如其它单元115)。时间表处置应用330可管理与单元115相关联的一或多个时间表。举例来说，针对特定用户群组的进入规则可基于一天的特定时间而改变。

[0066] 第一服务应用332及第二服务应用334可将服务提供给经验证管理员。服务的实例包含安全壳层(SSH)服务器、文件传送协议(FTP)服务器、远程桌面协议(RDP)服务器、虚拟专用网络(VPN)服务器、虚拟网络信道(VNC)服务器等等。每一控制器210可包含不同服务应

用集。举例来说，一个控制器210可提供SSH服务器及RDP服务器，而另一控制器210可提供SSH服务器及VPN服务器。

[0067] 如图3B中所展示，存储层350可存储配置数据352、管理员凭证DB 354、第一服务凭证DB 356、第二服务凭证DB 358及/或用户凭证DB 360。

[0068] 配置数据352存储与特定单元115相关联的配置数据，例如控制器210的硬件配置、连接到控制器210的外围装置230、安装于应用层320中的应用或其它类型的配置信息。在一个实施例中，配置数据352并不分布到其它控制器210，因为其是特定控制器210特有的。在其它实施例中，配置数据352可作为备份分布到其它控制器210，而并不在其它控制器210中使用配置数据352。

[0069] 管理员凭证DB 354存储用于验证可管理系统单元115(例如，以远程登录)的用户的凭证(例如，用户名及口令)。下文关于图7A来描述管理员凭证DB 354。在一个实施例中，管理员凭证DB 354分布在其它控制器210当中以允许相同管理员从控制器210或单元115中的任一者管理系统110。

[0070] 第一服务凭证DB 356(或第一经变换凭证DB 356)及第二服务凭证DB 358(或第二经变换凭证DB 358)存储用于验证经授权接入由控制器210提供的服务(例如，第一服务332或第二服务334)的用户(例如，额外管理员)的凭证(例如，用户名及口令)。举例来说，第一服务332可使用第一服务凭证DB 356来验证试图接入第一服务332的用户。同样地，第二服务334可使用第二服务凭证DB 358来验证试图接入第二服务334的用户。

[0071] 在一个实施例中，DB 356及/或358中的凭证可不以明文形式(例如，以未加密格式或可揭露凭证的方式)存储。在此实施例中，凭证DB 356及/或358可存储经变换用户凭证。举例来说，在一个实施方案中，第一服务凭证DB 356可存储已借助密码单向函数(例如，散列)变换的凭证。在此实例中，第一服务凭证DB 356可存储用户名及对应口令的散列。作为另一实例，第一服务凭证DB 356可存储用户名及对应口令的加盐散列。下文关于图7D到7G来描述第一服务凭证DB 356及第二服务凭证DB 358。

[0072] 用户凭证DB 360可存储可接入由系统单元115提供的服务(例如，第一服务332及/或第二服务334)的用户的凭证(例如，用户名及口令)。在一个实施例中，用户凭证DB 360可存储与在服务凭证DB(例如，第一服务凭证DB 356及/或第二服务凭证DB 358)中所存储的相同的用户(或若干用户)的相同凭证(或若干凭证)。在一个实施方案中，用户凭证DB 360以不同于凭证DB 356及358的方式存储凭证。举例来说，用户凭证DB 360可以一方式存储凭证以便自身揭露所述凭证(例如，以明文格式或以未变换格式)，这与存储经变换凭证的服务凭证DB 356及/或358相对。在一个实施例中，可从用户凭证DB 360变换出或导出服务凭证DB 356及358。

[0073] 图3C是管理逻辑323的示范性组件的框图，所述组件可包含管理员验证器382、用户凭证更新逻辑384、经变换凭证产生器386及/或凭证变换规则DB 388。管理员验证器382接收尝试登录到控制器210中的管理员的凭证，确定所述凭证是否为真实的，且可授权对控制器210的接入(例如，包含编辑及改变用户凭证DB 360的能力)。用户凭证更新逻辑384可(例如，从管理员)接收对与控制器210的服务的用户相关联的凭证的改变及/或更新(供存储在用户凭证DB 360中)。经变换凭证产生器386可基于对用户凭证DB 360的改变及/或更新而产生或更新服务凭证DB(例如，第一服务凭证DB 356及第二服务凭证DB 358)。经变换

凭证产生器386可基于存储于凭证变换规则DB 388中的信息(例如,规则及装置特有信息)而变换凭证。举例来说,规则DB 388可指示针对SSH服务,应使用SHA-224算法借助局部机器的硬件地址(例如,装置特有信息或MAC地址)来对口令进行散列运算。此外,在一个实施例中,规则DB 388可为控制系统110中的其它控制器210存储规则及装置特有信息。

[0074] 虽然图3A、3B及3C展示单元115的示范性功能组件,但在其它实施方案中,单元115相比图3A、3B及3C中所描绘的功能组件可包含更少的功能组件、不同的功能组件、不同布置的功能组件或额外功能组件。另外,单元115的组件(或任何组件群组)中的任一者可执行描述为由单元115的一或多个其它功能组件执行的功能。此外,举例来说,可经由一或多个ASIC的硬连线电路来实施单元115的功能组件。另外或替代地,可由执行来自存储器216的指令的处理器214来实施单元115的功能组件。

[0075] 图4是图解说明单元115的示范性物理布局400的平面布置图。如图4中所展示,物理布局400可包含墙壁410、门420、控制器210、读取器装置240、锁装置250、传感器260及致动器270。

[0076] 墙壁410包封安全区域440,例如建筑物中的房间。门420为用户提供到安全区域440的进入。在此实施例中,控制器210安装在安全区域440内侧。在其它实施例中,控制器210可安装在非安全区域450中。读取器装置240安装在安全区域440外侧且锁装置250在安全区域440内侧安装到墙壁410及门420。在此实例中,传感器260为安装在安全区域440外侧在非安全区域450中的监视装置。在此实例中,致动器270包含用于控制监视装置的视域的电动机。

[0077] 当用户将凭证键入到读取器装置240中(例如,通过键入PIN、扫描进入卡、扫描虹膜等等)时,控制器210可使用所述凭证来验证用户的身份且可在进入规则表中执行查找以基于用户的身份及进入规则而确定是否准予用户的进入。如果控制器210确定应准予进入,那么控制器210激活锁装置250以将门420开锁,因此准予用户进入安全区域440。

[0078] 虽然图4展示物理布局400的示范性组件,但在其它实施方案中,物理布局400相比图4中所描绘的组件可包含更少的组件、不同的组件、额外组件或不同布置的组件。另外或替代地,物理布局400中的任一组件(或组件群组)可执行描述为由物理布局400一或多个其它组件执行的任务。

[0079] 图5是图解说明控制系统110的示范性物理布局500的平面布置图。如图5中所展示,物理布局500可包含具有房间520-A到520-F的建筑物510。局部网络530(例如以太网络)可互连系统单元115-A到115-F。在此实例中,系统单元115-A控制进入到房间520-A中的两个门;系统单元115-B控制进入到房间520-B中的外侧门;系统单元115-C控制从房间520-B到房间520-C的一个门,系统单元115-D控制从房间520-C到房间520-D的一个门;系统单元115-E控制从房间520-D到房间520-E的一个门;且单元520-F控制进入到房间520-F中的外侧门。

[0080] 在此实例中,系统单元115-A到115-F不包含中央控制装置(例如,服务器)且可包含一或多个分布式数据集。举例来说,系统单元115-A到115-F可维持分布式凭证表、分布式进入规则表及/或分布式事件日志。假定管理员使用管理装置130登录到系统单元115-A中以添加用户并添加与用户相关联的凭证。可将那些所添加的凭证分布到控制到所述用户可以进入的房间的门的其它系统单元115。举例来说,如果系统单元115-B失效,那么由系统单

元115-B收集的数据可由于包含于其它系统单元中的分布式事件日志而继续为可用的。

[0081] 在图5中，每一单元115与一控制器210相关联。此外，在图5的实施方案中，每一控制器210处于与其它控制器210不同的位置(例如，不同的房间520)中。在其它实施方案中，一些控制器210及单元115可位于与其它控制器及单元115不同的建筑物、不同的地理区域、不同的国家、不同的大洲等等中。尽管其多样的位置，但在一个实施例中，单元115及控制器210可能够发现彼此(或做出最大努力来发现彼此)，形成对等网络并分布数据集。

[0082] 虽然图5展示物理布局500的示范性组件，但在其它实施方案中，物理布局500相比图5中所描绘的组件可包含更少的组件、不同的组件、额外组件或不同布置的组件。举例来说，在另一实施例中，中央控制装置(例如，服务器)可结合一或多个分布式数据集一起使用。另外或替代地，物理布局500的一或多个组件可执行描述为由物理布局500的一或多个其它组件执行的一或多个任务。

[0083] 图6是图解说明管理装置130的示范性组件的框图。如图6中所展示，管理装置130可包含总线610、处理器620、存储器630、输入装置640、输出装置650及通信接口660。

[0084] 总线610包含准许管理装置130的组件当中的通信的路径。处理器620可包含任何类型的单核心处理器、多核心处理器、微处理器、基于锁存器的处理器及/或解译并执行指令的处理逻辑(或处理器、微处理器及/或处理逻辑的族群)。在其它实施例中，处理器620可包含ASIC、FPGA及/或另一类型的集成电路或处理逻辑。

[0085] 存储器630存储信息、数据及/或指令。存储器630可包含动态、易失性及/或非易失性存储装置。存储器630可存储供由处理器620执行的指令或供由处理器620使用的信息。举例来说，存储器620可包含RAM、ROM、CAM、磁性及/或光学记录存储器装置等等。

[0086] 输入装置640允许操作者将信息输入到管理装置130中。举例来说，输入装置640可包含键盘、鼠标、笔、麦克风、触摸屏显示器等等。输出装置650可将信息输出给管理装置130的操作者。输出装置650可包含显示器、打印机、扬声器及/或另一类型的输出装置。

[0087] 通信接口660可包含使得控制器210能够经由有线通信链路、无线通信链路或无线与有线通信链路的组合与其它装置及/或系统通信(例如，发射及/或接收数据)的(例如，发射器及/或接收器)。通信接口660可包含用于有线通信的网络接口卡(例如，以太网卡)及/或用于无线通信的无线网络接口(例如，WiFi)卡。

[0088] 管理装置130可执行与管理系统110中的单元115有关的操作。管理装置130可响应于处理器620执行计算机可读媒体(例如存储器630)中所含有的软件指令而执行这些操作。存储器630中所含有的软件指令可致使处理器620执行这些操作。

[0089] 如上文所提及，控制器210可验证管理员是否可管理单元115。图7A是图解说明在一个实施例中用于此目的的管理员凭证DB 354的框图。管理员凭证DB 354可存储用于解密用户凭证DB 360的主密钥(例如，经加密主密钥)以及用于验证管理员的凭证信息。在一个实施例中，所述主密钥还可用于解密控制系统110中的分布式数据库。术语“主”用于与本文中所描述的其它密钥区分开。

[0090] 如图7A中所展示，管理员凭证DB 354可包含管理员用户名字段702、经加密口令字段704及经加密主密钥字段706。管理员用户名字段702存储管理员的用户名。举例来说，图7A中的管理员凭证DB 354展示两个管理员用户名:admin1及admin2。任何数目个管理员用户名可列示于管理员凭证DB 354中(即，任何数目个记录或行可存在于管理员凭证DB 354

中)。

[0091] 经加密口令字段704存储对应用户名的口令。在此实施例中,字段704中的口令已用存储于经加密主密钥字段706中的主密钥加密。在其它实施例中,口令字段704可存储呈未加密格式或用不同于主密钥的密钥加密的对应口令。并非展示图7A中的经加密口令,字段704展示借以产生经加密口令的函数C(操作数1,操作数2)。函数C使用操作数2作为加密密钥来加密操作数1。函数C可为任何加密函数。举例来说,可使用第一函数C1借助主密钥来加密字段704中的口令。

[0092] 经加密主密钥字段706存储经加密主密钥。在此实施例中,已借助对应管理员的口令加密所述主密钥。因此,管理员凭证DB 354存储管理员的凭证及用于解密用户凭证DB 360的密钥,但每一者是借助另一者加密的。下文关于图8C来论述管理员凭证DB 354。可使用第二函数C2借助口令加密字段706中的主密钥。在一个实施例中,处理器214在可在控制器210中的其它处理器外部的专用电路(例如,ASIC)中执行函数C。

[0093] 管理员凭证DB 354相比图7A中所展示的字段可包含更多、更少或不同的字段。举例来说,在一个实施例中,可省略管理员用户名字段702。在另一实施例中,在管理员凭证DB 354中存储及/或使用的凭证可包含不同于用户名及口令的凭证类型或除其之外还具有其它凭证类型。举例来说,凭证可包含生物计量凭证(例如,指纹或虹膜扫描)等等。

[0094] 如上文所提及,管理员可登录到控制器210中以管理单元115,所述管理可包含更新用户凭证DB 360。用户凭证DB存储供其它用户或管理员接入由控制器210提供的服务的凭证。图7B及7C是一个实施例中的示范性用户凭证DB(例如,在两个不同时间的用户凭证DB 360)的框图。用户凭证DB 360可包含用户名字段742、服务字段744、装置字段746及/或凭证字段748。下文描述这些字段。

[0095] 用户名字段742识别经授权接入控制器210中的服务(例如第一服务332及第二服务334)的用户。在用户凭证DB 360(图7B中所展示)中,用户名包含马格努斯(Magnus)及萨拜娜(Sabina)。任何数目个用户名为可能的(例如,任何数目个条目或记录)。

[0096] 服务字段744识别对应用户名被授权接入的服务(例如,在装置字段746中识别的装置上,使用在凭证字段748中识别的凭证)。在服务字段744中识别的服务包含SSH服务器(“SSH”)及VPN服务器(“VPN”)。任何数目个服务可由控制器210中的任一者提供。

[0097] 装置字段746识别为在对应用户名字段742中识别的用户提供在服务字段744中识别的服务的装置(例如,控制器210)。如上文所提及,并非所有控制器210可提供相同(或甚至任何)服务。此外,举例来说,一些装置的一些服务可不与在凭证字段748中列示的凭证相关联。举例来说,如果凭证字段748中的凭证应与具有对应用户名及对应服务的所有装置相关联,那么装置字段746可识别“全部”。如果存储于凭证字段748中的凭证应不与特定装置(例如,摄像机260)中的对应服务及对应用户名相关联,那么装置字段746可排除一装置(例如,“无摄像机260”)。装置字段746可个别地识别装置,例如读取器240、锁250及致动器270。

[0098] 凭证字段748存储用于针对对应装置(例如,在装置字段746中识别)上的对应服务(例如,在服务字段744中识别)验证对应用户(例如,在用户名字段742中识别)的凭证。

[0099] 在一个实施例中,单个或相同凭证(在凭证字段748中识别)及/或单个或相同用户名(在用户名字段742中识别)可与跨越一或多个装置(在装置字段746中识别)的多个服务(在服务字段744中识别)相关联。在一个实施例中,单个或相同凭证(在凭证字段748中识

别)及/或单个或相同用户名(在用户名字段742中识别)可与跨越一或多个服务(在服务字段744中识别)的多个装置(在装置字段746中识别)相关联。

[0100] 在另一实施例中,凭证(在凭证字段748中界定)(及对应口令)可与网络(例如,分布式物理进入控制系统,例如控制系统110)中的所有装置相关联。或者,凭证(在凭证字段748中界定)(及对应口令)可与网络中的不到所有装置(例如,无摄像机260)相关联。也就是说,可将一些控制器210排除(在凭证字段748中识别)在与跨越多个装置及/或多个服务的凭证相关联之外。

[0101] 凭证字段748可以未变换方式存储凭证。举例来说,如果凭证为口令,那么可在所述口令将由用户键入时存储所述口令。凭证字段748还可以经加密格式存储凭证,但在一个实施例中,以使得可经解密以揭露未变换凭证的格式(例如,双射加密函数)存储。在又一实施例中,举例来说,凭证字段748可以一或多个经变换格式(包含针对由所有控制器210提供的所有服务的所有相关变换)存储凭证。

[0102] 如在以下实例中关于图8B所描述,更新用户凭证DB 360(图7B中所展示)以产生用户凭证DB 360'(图7C中所展示)。以粗体且以箭头来展示对经更新用户凭证DB 360'的改变(与用户凭证DB 360相比)。举例来说,在经更新用户凭证DB 360'中,用户名包含马格努斯、萨拜娜及贡纳尔(Gunnar)。也就是说,将贡纳尔作为用户名添加到了用户凭证DB 360。

[0103] 用户凭证DB 360相比图7B及7C中所展示的字段可包含更多、更少或不同的字段。举例来说,在一个实施例中,可省略用户名字段742,且可使用凭证字段748来识别用户以及验证用户。存储于用户凭证DB 360中的凭证可包含不同于用户名及口令或除其之外的凭证类型。举例来说,用户凭证DB 360可存储生物计量凭证(例如,指纹或虹膜扫描)。

[0104] 如上文所提及,控制器210可验证用户或管理员是否可接入由控制器210提供的服务。控制器210(及对应服务)可使用服务凭证DB来验证这些用户。图7D到7G是图解说明一个实施例中的服务凭证DB(例如,第一服务凭证DB 356及第二服务凭证DB 358,其各自在两个不同时间)的框图。

[0105] 如图7D及7E中所展示,第一服务凭证DB 356可包含用户名字段722及经变换凭证字段724。用户名字段722识别经授权接入第一服务332的用户。举例来说,经变换凭证字段724可包含凭证的密码单向变换,例如与盐并置的口令的散列。在一个实施方案中,变换可为提供第一服务332的装置特有的,例如所述盐为对应装置(例如,控制器210)的硬件地址(例如,媒体接入控制(MAC)地址)。在另一实施方案中,第一服务凭证DB 356不存储经变换凭证,而是原始凭证自身或以使得可获得原始凭证的方式变换(例如,双向散列、加密或双射变换)的凭证。

[0106] 同样地,第二服务凭证DB 358可包含用户名字段732及经变换凭证字段734。用户名字段732可识别经授权接入第二服务334的用户。举例来说,经变换凭证字段734可包含凭证的密码单向变换(例如,与盐并置的口令)。在一个实施方案中,用于产生字段734中的经变换凭证的变换函数不同于用于产生字段724中的经变换凭证的变换函数。也就是说,所述变换函数可为服务特有的(例如,不管所述服务是第一服务332还是第二服务334)。此外,所述变换可为提供第二服务334的装置特有的,例如所述盐为对应控制器210的硬件地址(例如,MAC地址)。在另一实施方案中,第二服务凭证DB 358不存储经变换凭证,而是凭证自身或以使得可获得原始凭证的方式变换(例如,双向散列、加密或双射变换)的凭证。

[0107] 虽然第一服务凭证DB 356中针对萨拜娜的经变换凭证(图7D中针对SSH的UYDAG)不同于第二服务凭证DB 358中针对萨拜娜的经变换凭证(图7G中针对VPN的UHYRV),但此对应于两个服务的相同未变换凭证(例如,口令LETMEIN)。因此,萨拜娜可使用相同凭证(例如,用户名及口令)登录到特定控制器210-A上的SSH服务器及VPN服务器中。此外,即使第一服务凭证DB 356及第二服务凭证DB 358中的经变换凭证在其它控制器210(例如,控制器210-B到210-F)上可不同,但这些经变换凭证还可对应于相同未变换凭证(例如,用户名及口令)。因此,萨拜娜可使用相同凭证(例如,用户名及口令)登录到其它控制器210-B到210-F上的SSH服务器及VPN服务器中。

[0108] 如在以下实例中关于图8B所描述,更新第一服务凭证DB 356(图7D中所展示)以创建经更新第一服务凭证DB 356'(图7E中所展示)。此外,更新第二服务凭证DB 358(图7F中所展示)以创建(经更新)第二服务凭证DB 358'(图7G中所展示)。以粗体且以箭头来展示对经更新第一服务凭证DB 356'及第二服务凭证DB 358'的改变(与第一服务凭证DB 356及第二服务凭证DB 358相比)。

[0109] 第一服务凭证DB 356及第二服务凭证DB 358相比图7D到7G中所展示的字段可包含更多、更少或不同的字段。举例来说,在一个实施例中,可省略用户名字段722或734,且可使用经变换凭证字段724或734来识别用户以及验证用户。在另一实施例中,存储于凭证DB 356及/或358中的凭证可包含不同于用户名及(经变换)口令或除其之外的凭证类型。举例来说,凭证DB 356及358可存储生物计量凭证(例如,指纹或虹膜扫描)。

[0110] 如上文所提及,一个实施例允许用户在使用相同凭证(例如,相同用户名及口令)的同时接入跨越多个装置的多个服务。此外,一个实施例允许在分布式网络中的装置(例如控制系统110的单元115中的控制器210)当中传播对凭证的改变。图8A是用于验证经授权接入控制器210中的服务的用户的示范性过程800A的流程图。举例来说,过程800可由在控制器210中运行的服务(例如,第一服务332及/或第二服务334)执行。每一服务可执行其自身的过程800版本来验证一或多个用户是否可接入所述特定服务。在以下实例中,第一服务332为SSH服务器且第二服务334为VPN服务器。此外,特定控制器210包含如图7B中所展示的用户凭证DB 360、如图7D中所展示的第一服务(SSH)凭证DB 356及如图7F中所展示的第二服务(VPN)凭证DB 358。

[0111] 在此实例中,过程800A以从用户接收对服务的请求开始(框802)。假定所请求服务为需要用户名及口令来进行验证的SSH服务器,且用户希望使用在管理装置130中运行的SSH客户端登录到控制器210中(其中用户远程地定位)。在此情况中,所述服务(SSH服务器)提示用户输入凭证(框804),例如,用户名及口令。所述服务(SSH服务器)接收用户凭证(框806),且在一个实施例中,变换所述用户凭证(框808)。上文关于经变换凭证产生器386论述了凭证的变换的实例。

[0112] 为了验证用户,所述服务(SSH服务器)将所接收凭证(例如,经变换)与所存储凭证进行比较(框810)。将所接收凭证与所存储凭证进行比较可包含变换所接收凭证。如上文所描述,用于服务的凭证存储于控制器210的存储层350中的第一服务(第一经变换)凭证DB 356中。如果所述凭证不等同(例如,所接收凭证不正确)(框812:否),那么授权失败且不授权对服务(SSH服务器)的接入(框814)。如果所接收凭证(其可能已经变换)为正确的(例如,匹配)(框812:是),那么验证成功且授权对服务(SSH服务器)的接入(框816)。

[0113] 举例来说，用户萨拜娜可使用管理装置130借助SSH客户端试图登录到单元115-A(见图5)的控制器210-A中。她被提示键入她的用户名(萨拜娜)及口令(LETMEIN)，她如此进行操作。假定控制器210-A存储如图7D中所展示的第一服务(SSH)凭证DB 356。控制器210-A的服务332(SSH)将口令“LETMEIN”变换为UYDAG，其匹配存储于凭证DB 356中的经变换凭证，且用户萨拜娜被成功地验证且经授权接入控制器210-A中的SSH服务。在此实例中，萨拜娜还可能够以相同用户名及口令(萨拜娜，LETMEIN)登录到控制器210-B上的SSH服务器中，因为控制器210-B中的SSH凭证DB 356是以此方式配置的。事实上，萨拜娜可能够以相同用户名及口令(萨拜娜，LETMEIN)登录到多个控制器210上的VPN服务器中，因为存储于每一控制器210中的VPN凭证DB 358是以此方式配置的。举例来说，SSH凭证表(第一服务凭证DB 356)中的经变换凭证对应于与VPN凭证表(第二服务凭证DB 358)中的经变换凭证相同的口令。然而，萨拜娜希望针对控制系统110中的所有服务(SSH及VPN)及所有控制器210-A到210-F将她的口令从“LETMEIN”改变为“GOTLAND”。然而，如果管理员(或萨拜娜)不得不针对每一装置及每一服务改变所述口令，那么萨拜娜的希望潜在地造成负担。

[0114] 本文中所揭示的实施例可允许萨拜娜(或管理员)在一个控制器210上针对服务改变她在用户凭证DB 360中的口令并已将所述改变传播到其它控制器210。在此情况中，管理员验证器逻辑382可以用于多个服务及/或用于多个装置上的多个服务的相同凭证验证相同用户(例如，萨拜娜)。图8B是供管理员更新用户凭证DB 360及服务凭证DB(例如，DB 356及358)的示范性过程800B的流程图。在以下实例中，管理员使用管理装置130登录到控制器210中。在一个实施例中，管理员可登录到控制器210中的任一者中，因为可视需要将对用户凭证数据库的改变分布到其它控制器210(及其它服务凭证DB)。在此实例中，管理员登录到控制器210-A中，且过程800B由单元115-A的控制器210-A中的用户凭证更新逻辑384执行。

[0115] 过程800B以从登录到控制器210中的管理员接收凭证并验证管理员开始(框822)。举例来说，管理员出于更新萨拜娜的口令(例如，在存储于控制器210-A中的用户凭证DB 360中)的目的而登录到控制器210-A中。下文关于图8C来论述用于验证管理员的方法及过程。在此实例中，假定管理员已被成功地验证且过程800B继续进行到框824。如果用户凭证DB 360经加密，那么将其解密(框824)。在一个实施例中，如关于图8C所描述，用于解密用户凭证DB 360的密钥仅在管理员被成功地验证时可用。解密用户凭证DB 360允许管理员编辑及改变所述DB中的条目。在其它实施例中，用于解密用户凭证DB 360的密钥在不加密的情况下存储于控制器210中。

[0116] 一旦经验证，管理员便可编辑及改变用户凭证DB 360中的信息，包含字段748中的凭证、用户名字段742中的用户名、服务字段744中的服务及/或装置字段746中的装置。这些新的及/或经更新凭证(其可包含用户名)由控制器210-A接收(框826)。还接收对应于所述凭证的经识别服务及经识别装置(框828)，且更新控制器210-A中的用户凭证DB 360(框830)。举例来说，管理员可添加或删除经授权接入由控制器210-A提供的特定服务或由其它控制器210-B到210-F中的一者提供的服务的用户。举例来说，管理员可改变存储于凭证字段748中的凭证(例如，口令)。此外，管理员可改变对应凭证适用于的控制器210。

[0117] 举例来说，如图7A及7B中所展示，管理员将用户名贡纳尔添加到用户凭证DB 360(图7A)以产生用户凭证DB 360’(图7B)。经更新用户凭证DB 360’指示贡纳尔可以接入控制器210-A、210-B及210-C上但非摄像机260(在此实例中，其包含控制器)(如在装置字段746

中所界定)中的VPN服务。对于由这些经识别控制器(在装置字段746中)提供的VPN服务,贡纳尔可使用用户名“贡纳尔”及口令“MUNKKALLAREN”来进行验证。而且,管理员将用户名萨拜娜针对控制系统110中的所有装置(控制器210-F除外)的SSH及VPN服务的凭证(即,口令)从“LETMEIN”改变为“GOTLAND”。

[0118] 如果存在对用户凭证DB 360的改变,那么产生经变换用户凭证(例如,基于经更新及/或未加密用户凭证),且更新服务凭证DB(例如,第一服务凭证DB 356及/或第二服务凭证DB 358)(框832)。针对服务及装置适当地变换存储于用户凭证DB 360中的凭证。如上文所描述,经变换凭证产生器386可基于存储于凭证变换规则DB 388中的规则(及其它信息)而变换凭证。举例来说,产生器386可使用用于SSH服务的密码单向函数(例如,借助局部装置的以太网MAC地址加盐的SHA-224密码散列函数)来产生经变换凭证。在此情况中,过程800B(例如,控制器210执行采用经变换凭证产生器386的凭证更新逻辑384)产生用于装置上的SSH服务器的经更新或新的经变换凭证。

[0119] 在一个实施例中,加密用户凭证DB 360(框834)(例如,在更新服务凭证DB之后,当管理员注销时等等)并将其存储于控制器210-A的存储层350中。还可将用户凭证DB 360分布到其它控制器210(框836),例如控制器210-B到210-F(例如,以对等网络连接)。如下文所描述,可将用户凭证DB 360分布到其它装置的其它控制器210以产生用于验证用户是否可接入由对应其它装置提供的服务的经变换凭证DB。在此情况中,分布层340可将用户凭证DB 360分布到其它装置,如上文所描述。在一个实施例中,举例来说,如果控制器210中的一者位于非安全区域中,那么将用户凭证DB 360分布到不足所有控制器210。

[0120] 在一个实施例中,以经加密格式分布用户凭证DB 360。在此情况中,还可在其它控制器210上存储及使用用于加密用户凭证DB 360的密钥(“主密钥”)。在此情况中,其它控制器210可使用用户凭证DB 360,即使其是以经加密格式分布的。在替代实施例中,用户凭证DB 360是以未加密格式分布的(但控制器210之间的链路可经加密)。

[0121] 控制器210-A中的用户凭证DB 360的改变还可导致对其它控制器210(例如,控制器210-B到210-F)中的服务凭证DB的改变。举例来说,控制器210-B可接收由控制器210-A分布的对用户凭证DB 360的更新。也就是说,可产生额外经变换用户凭证且可更新其它控制器210中的服务凭证DB(框838)。这可以众多方式来完成,如下文所描述。同样地,在不同实例中,控制器210-A可接收(框836)由其它控制器210(例如,对等网络中的控制器210-B到210-F)分布的对用户凭证DB 360的更新,且可产生经变换用户凭证并更新控制器210-A中的服务凭证DB(框838)。在此后一实例中,管理员可登录到控制器210-B中以更新用户凭证DB 360。

[0122] 在一个实施例中,凭证变换规则DB 388(例如,存储于控制器210-A中)可存储用于其它控制器210(例如,控制器210-B到210-F)以及自身上的服务的规则及信息(例如,装置特有信息)。因此,控制器210-A中的经变换凭证产生器386可产生用于其它控制器210(例如,控制器210-A到210-F)以及自身上的其它服务的经变换凭证。在此情况中,可将服务凭证DB从管理员登录于其中的控制器分布到适当控制器210。此外,服务凭证DB可以未加密方式分布,因为凭证可能已经变换。不过,即使服务凭证DB可以未加密方式分布,控制器210之间的通信链路仍可经加密(例如,通过SSL/TLS)。

[0123] 在另一实施例中,每一控制器210可负责产生其自身的服务凭证DB。在此情况中,

经变换凭证产生器386(在不同于控制器210-A的控制器上)可检测到用户凭证DB 360已改变,且可更新其自身的局部服务凭证DB。在此情况中,如果用户凭证DB 360及主密钥被加密,那么控制器210(例如,控制器210-B到210-F)在无主密钥的情况下便无法接入凭证DB 360。在一个实施例中,当管理员登录到控制器210-A中时,将足以供其它控制器210(例如,控制器210-B到210-F)确定或解密主密钥的信息传递到其它控制器210(例如,使用经加密链路)。因此,其它控制器210(例如,控制器210-B到210-F)可解密从管理员登录到其中的控制器210(例如,控制器210-A)接收的对凭证DB 360的经分布更新。在一个实施例中,主密钥从不存储于任何控制器210中的非易失性存储器中。在其它实施例中,主密钥可存储于非易失性存储器中。或者,可需要管理员登录到每一控制器210中以使得可更新对应局部服务凭证DB。在另一实施例中,举例来说,在于控制器210-A(管理员登录于其中)中更新用户凭证DB 360之后且在已将用户凭证DB 360分布到其它控制器210-B之后,控制器210-A可使用由管理员提供的口令使管理员登录到其它控制器210-B中。以此方式,从管理员接收到对用户凭证DB 360的更新的控制器210-A可确保其它控制器210-B到210-F更新其相应服务凭证DB。

[0124] 如上文关于图8B所论述,管理员可使用管理装置130登录到控制器210中。图8C是在一个实施例中用于验证管理员的过程822的流程图。虽然可使用过程822来验证管理员是否可更新用户凭证DB 360,但也可使用验证过程822来验证管理员是否可相对于控制器210执行其它任务。

[0125] 过程822以从登录到单元115的控制器210中的管理员接收管理员用户名及口令(即,凭证)开始(框842)。过程822查询管理员凭证DB 354以确定是否存在匹配所键入用户名的用户名。如果未在管理员凭证DB 354中找到匹配的用户名(框844:否),那么验证失败且不授权对控制器210的接入(框846)。如果在管理员凭证DB 354中找到匹配的用户名(框844:是),那么过程822继续到框848以确定验证是否成功。

[0126] 基于所接收管理员口令而解密所存储的经加密主密钥(存储于经加密主密钥字段706中)以产生称为“可能主密钥”的密钥(框848),前提是仅假定所接收管理员口令暂时可能为正确的。接着基于可能主密钥而解密所存储管理员口令以产生称为“可能管理员口令”的口令(框850)。如果所接收管理员口令不等同于可能管理员口令(框852:否),那么验证失败且不授权对控制器210的接入(框846)。如果所接收管理员口令与可能管理员口令相同(框852:是),那么验证成功且授权对控制器210的接入(框854)。在此情况中(框854:是),返回到图8B(框824),如果用户凭证DB 360经加密,那么管理逻辑323可基于主密钥(在此情况中,其与可能主密钥相同)而解密用户凭证DB 360。由于经加密主密钥是基于管理员口令而解密的,因此在此实施例中,管理逻辑323也基于所键入管理员口令(在此情况中,其与可能管理员口令相同)而解密用户凭证DB 360。

[0127] 过程822的变化形式是可能的。举例来说,在一个实施例中,不使用由管理员键入的口令。而是,管理员可通过其它手段(例如通过具有密钥或口令管理系统的管理装置130中的客户端软件)提供机密。此外,在一个实施例中,管理员不提供用户名。在此情况中,举例来说,可针对管理员凭证DB 354中的每一条目或记录执行过程822,以确定验证是否成功。

[0128] 在前述说明书中,已参考附图描述了各种实施例。然而,将显而易见,可对本发明

做出各种修改及改变且可实施额外实施例，此并不背离如所附权利要求书中所陈述的本发明的较宽广范围。因此，应将本说明书及图式视为具有说明性意义而非限制性意义。举例来说，尽管已关于图8A到8C描述了若干系列的框，但在其它实施方案中可修改框及/或信号流的次序。此外，可并行地执行非相依框及/或信号流。

[0129] 将明了，在图中所图解说明的实施方案中，可以许多不同形式的软件、固件及硬件来实施如上文所描述的系统及/或方法。用于实施这些系统及方法的实际软件代码或专门化控制硬件并不限于所述实施例。因此，在不参考特定软件代码的情况下来描述所述系统及方法的操作及行为--应理解，软件及控制硬件可经设计以基于本文中的描述而实施所述系统及方法。

[0130] 此外，可将上文所描述的某些部分描述为执行一或多个功能的组件。如本文中所使用，组件可包含硬件(例如处理器、ASIC或FPGA)或硬件与软件的组合(例如，执行软件的处理器)。

[0131] 如本文中所使用的术语“包括(comprises及/或comprising)”规定所陈述特征、整数、步骤或组件的存在，但并不排除一或多个其它特征、整数、步骤、组件或其群组的存在或添加。此外，术语“示范性”(例如，“示范性实施例”、“示范性配置”等等)意指“作为实例”且并不意指“优选”、“最佳”或类似词语。

[0132] 本申请案中所使用的元件、动作及指令不应理解为对所述实施例至关重要或必不可少，除非明确如此描述。而且，如本文中所使用，冠词“一”打算包含一或多个项目。举例来说，“一处理器”可包含一或多个处理器(例如，微处理器及专用于加密及/或解密的电路)。另外，如果将多个装置“中的每一者”描述为包含一特征，那么并非所有装置必定包含所述特征。也就是说，其它装置(除界定为具有所述特征的多个装置之外)可不包含所述特征。此外，短语“基于”打算意指“至少部分地基于”，除非另有明确陈述。

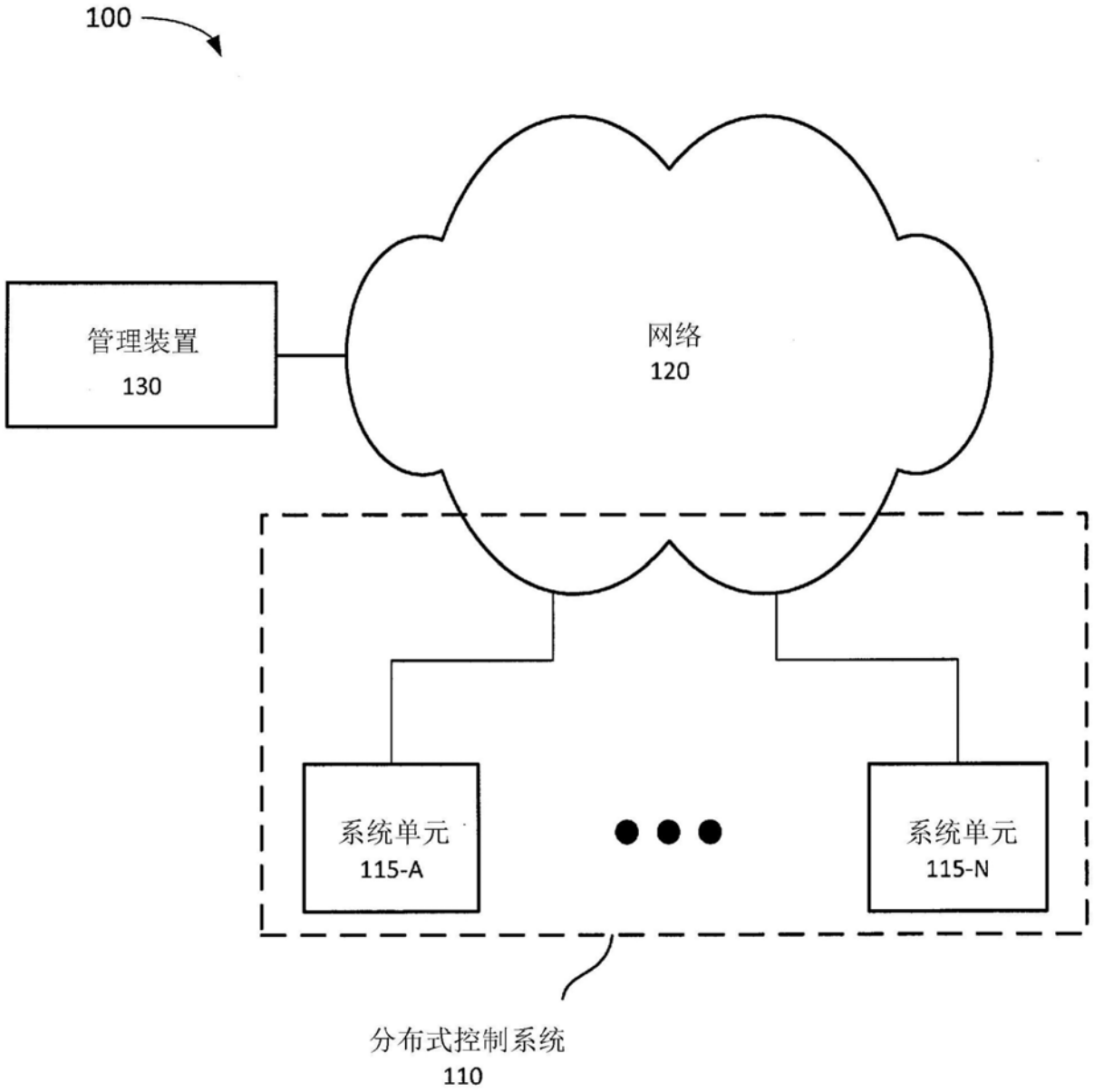


图1

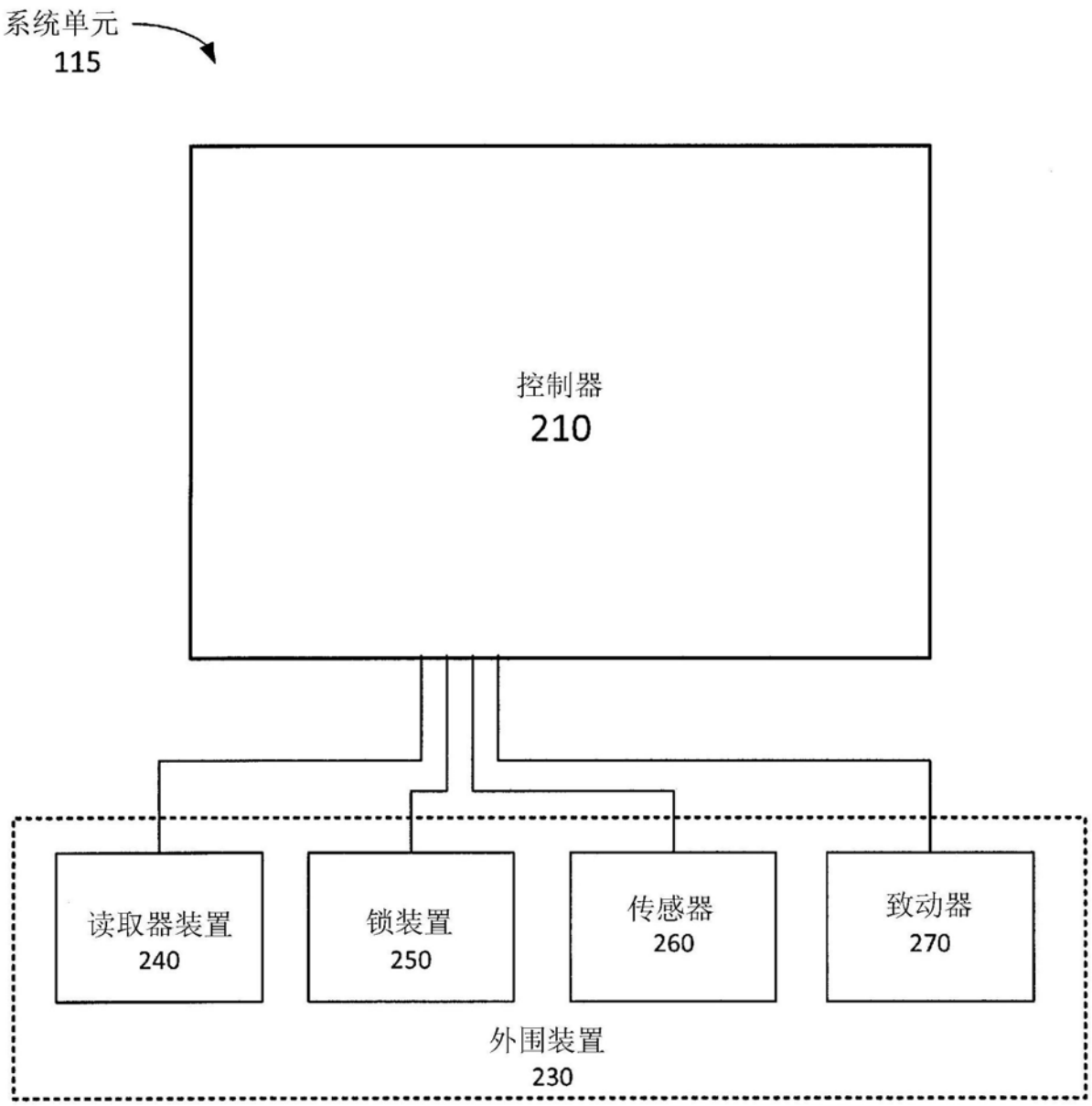


图2A

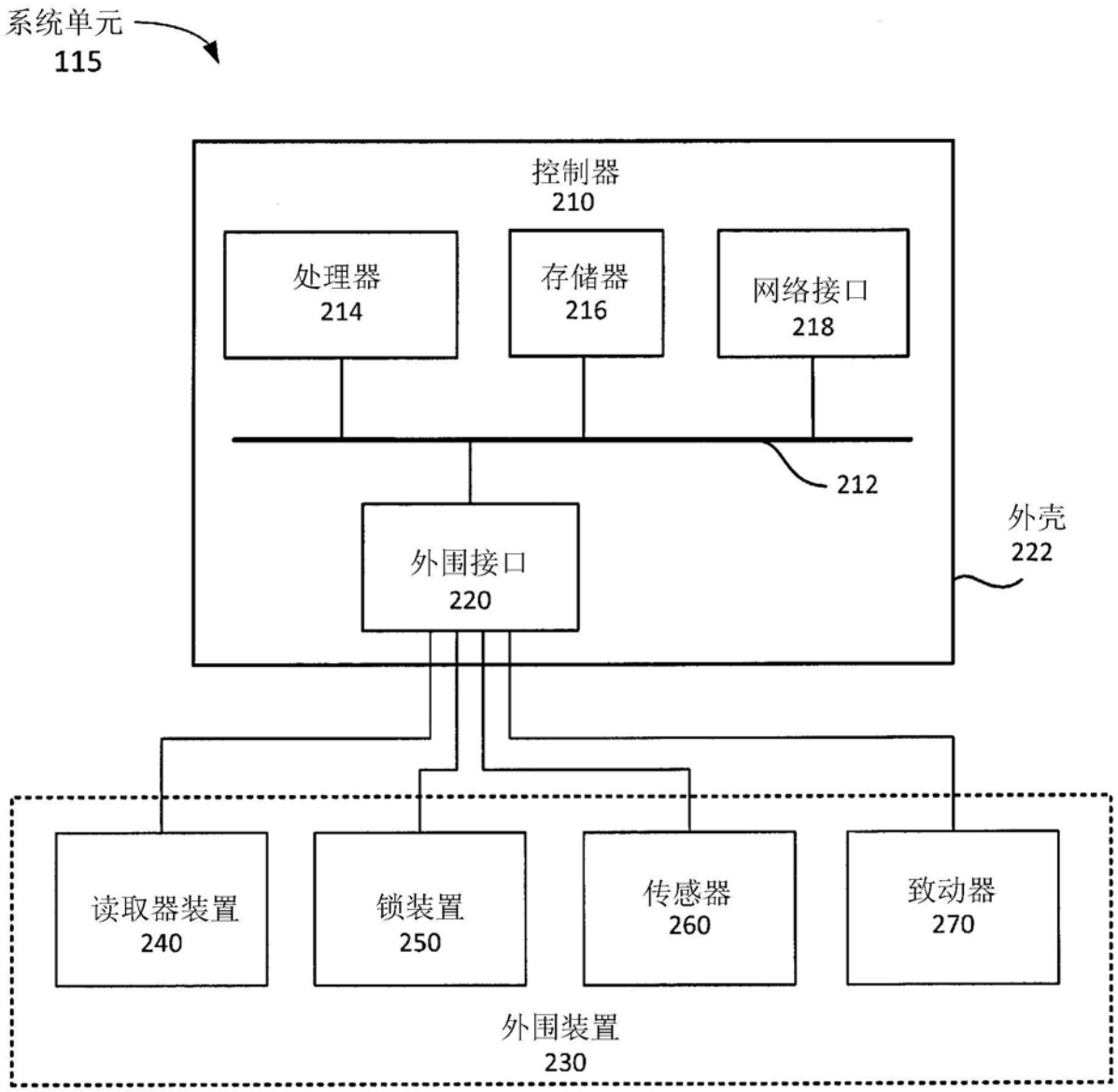

系统单元
115
控制器
210
处理器
214
存储器
216
网络接口
218
212
外围接口
220
外壳
222
读取器装置
240
锁装置
250
传感器
260
致动器
270
外围装置
230

图2B

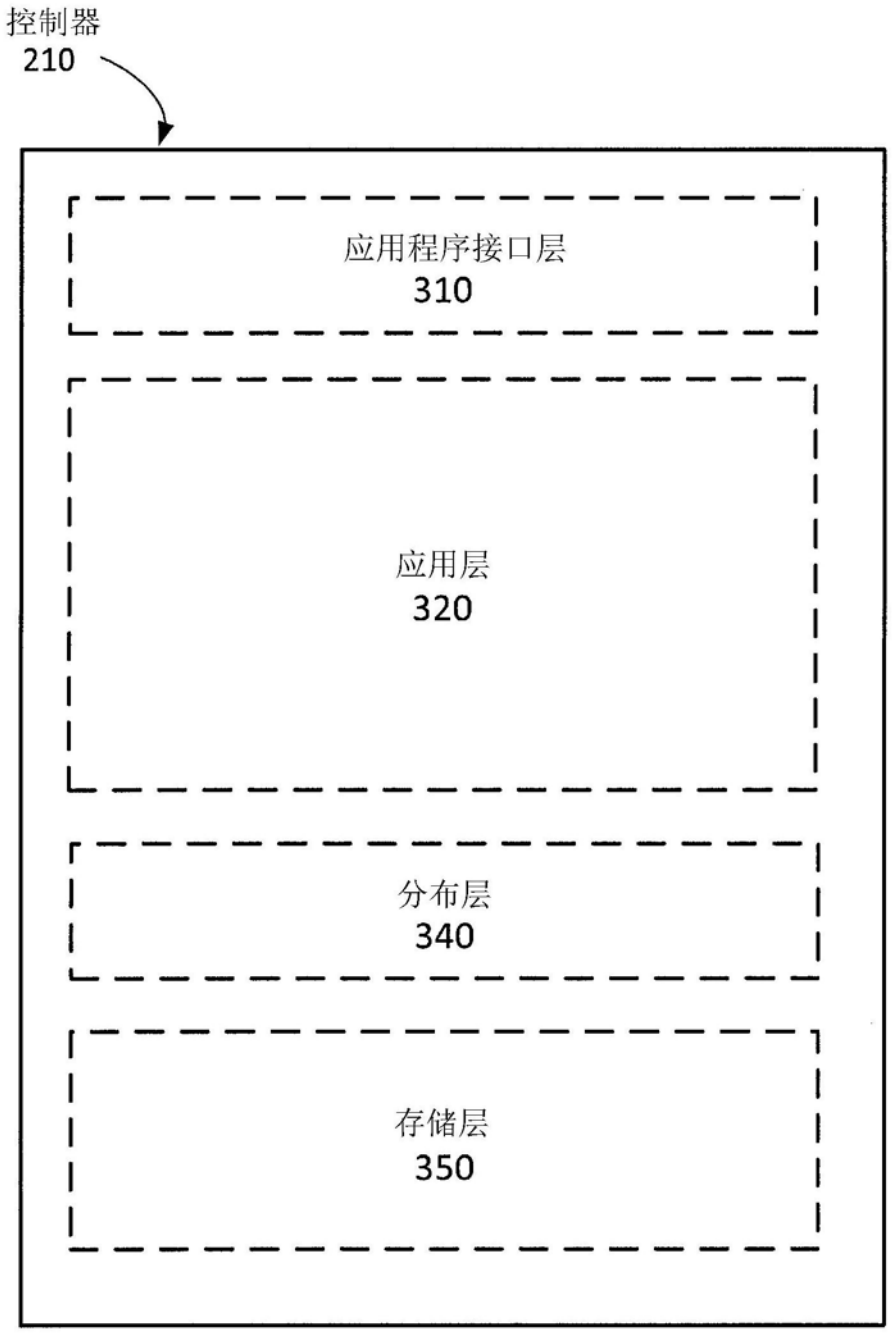


图3A

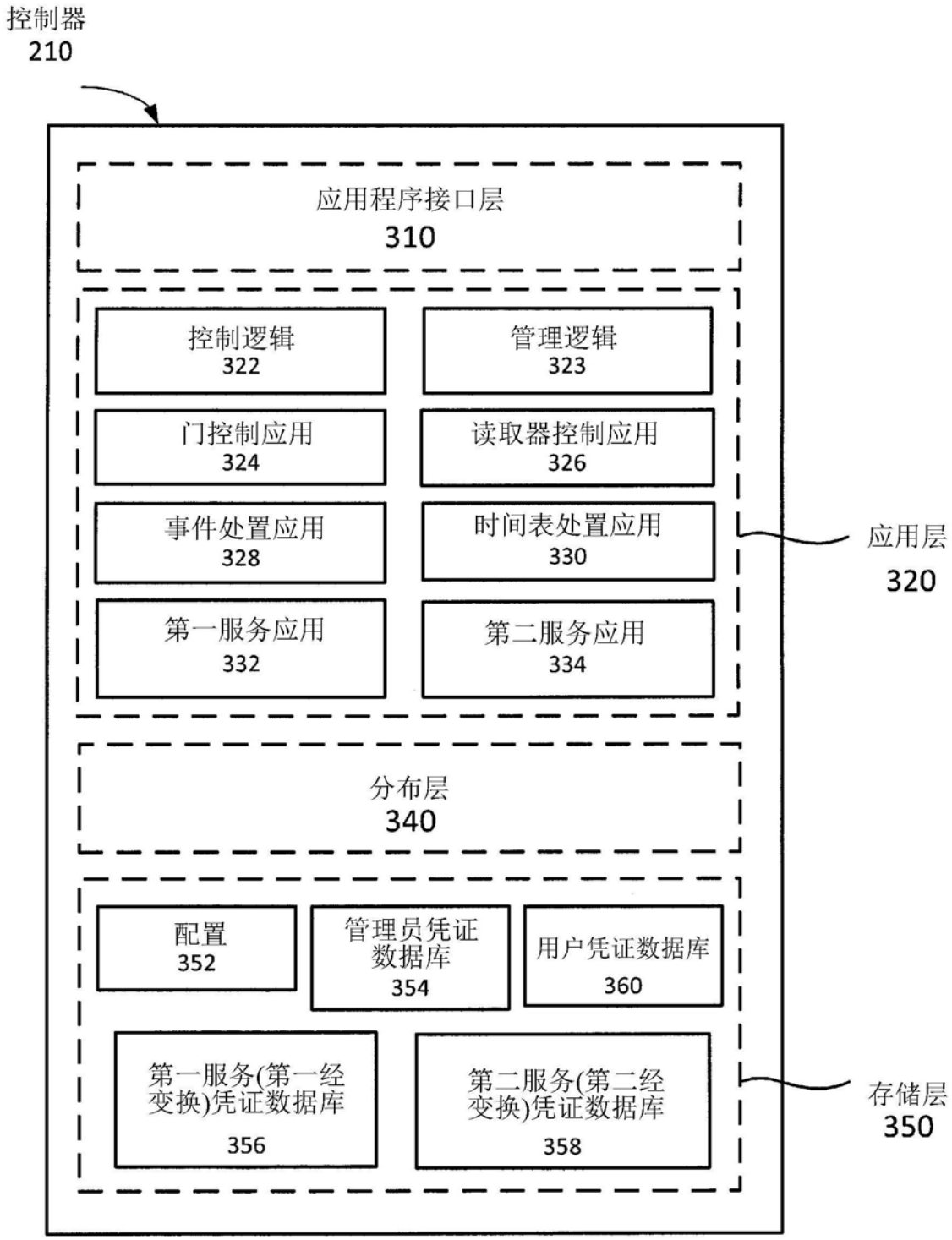

控制器
210
应用程序接口层
310
控制逻辑
322
管理逻辑
323
门控制应用
324
读取器控制应用
326
事件处置应用
328
时间表处置应用
330
第一服务应用
332
第二服务应用
334
应用层
320
分布层
340
配置
352
管理员凭证数据库
354
用户凭证数据库
360
第一服务(第一经变换)凭证数据库
356
第二服务(第二经变换)凭证数据库
358
存储层
350

图3B

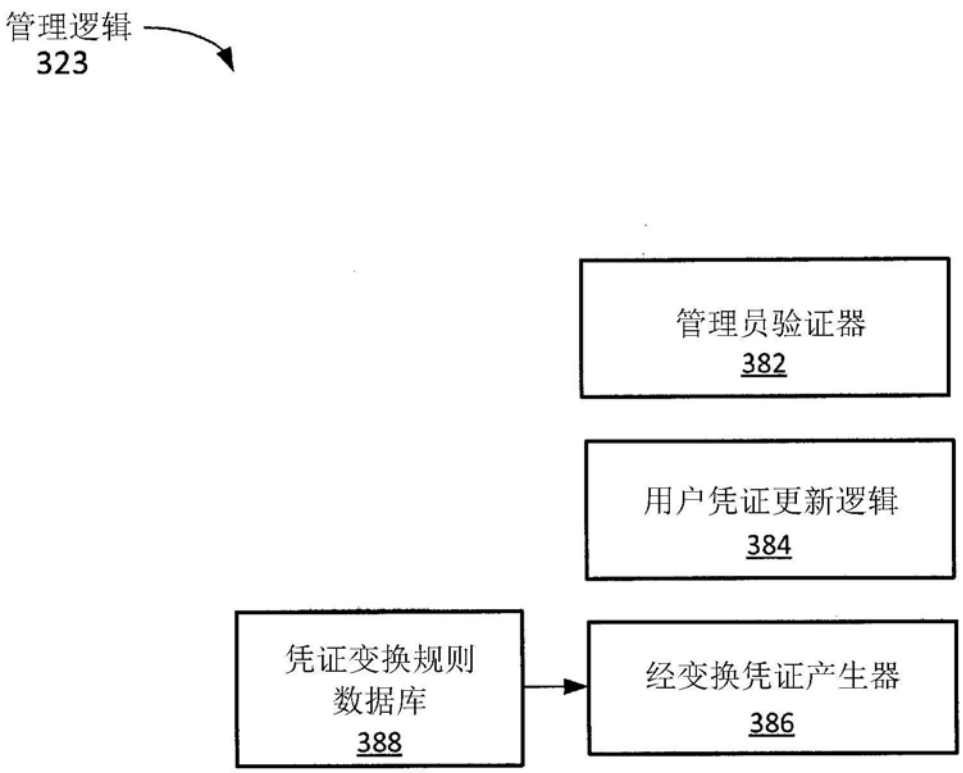

管理逻辑
323
管理员验证器
382
用户凭证更新逻辑
384
凭证变换规则
数据库
388
经变换凭证产生器
386

图3C

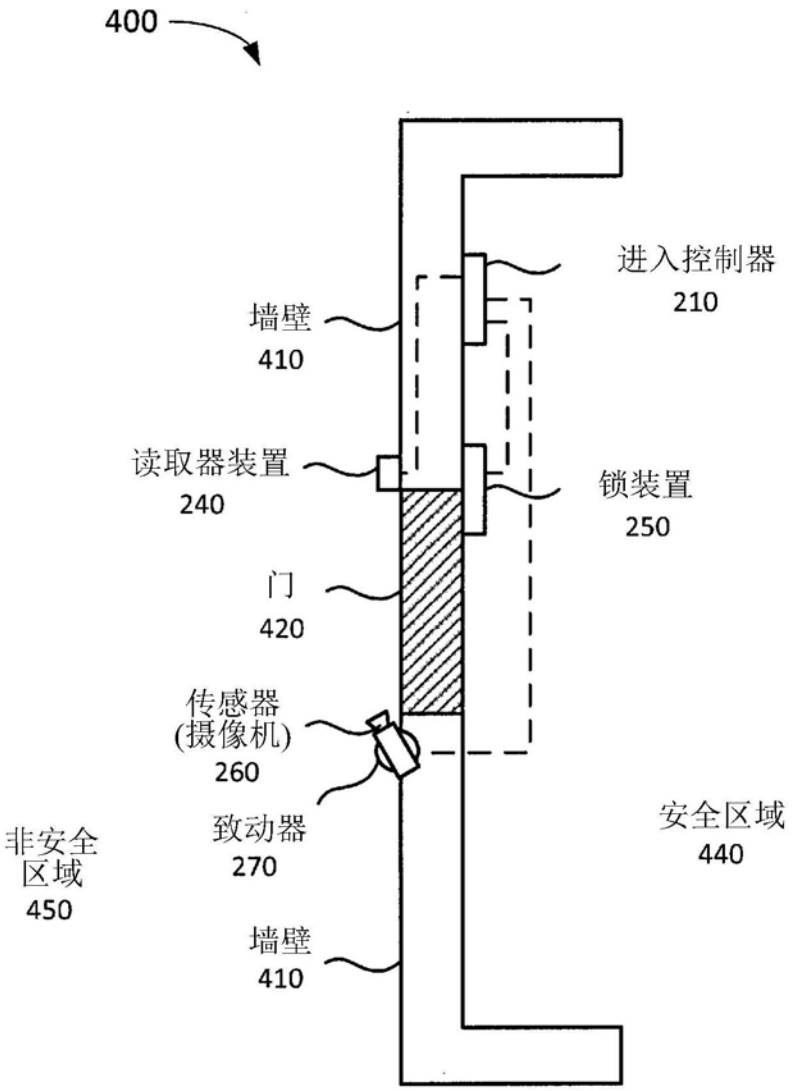

400
进入控制器
210
墙壁
410
读取器装置
240
锁装置
250
门
420
传感器
(摄像机)
260
致动器
270
非安全
区域
450
安全区域
440
墙壁
410

图4

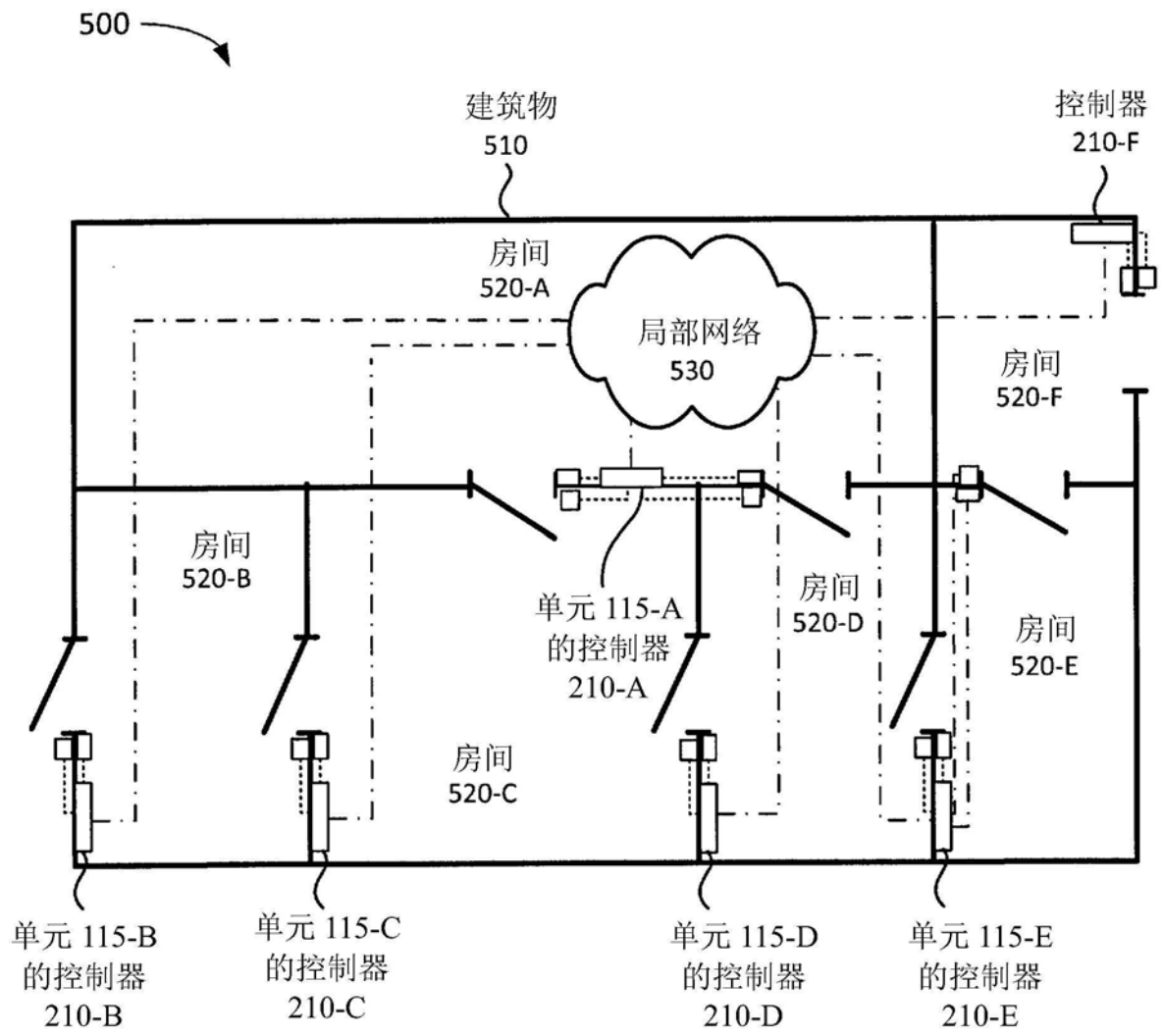

500
建筑物
510
控制器
210-F
房间
520-A
局部网络
530
房间
520-F
房间
520-B
单元 115-A
的控制器
210-A
房间
520-D
房间
520-E
房间
520-C
单元 115-B
的控制器
210-B
单元 115-C
的控制器
210-C
单元 115-D
的控制器
210-D
单元 115-E
的控制器
210-E

图5

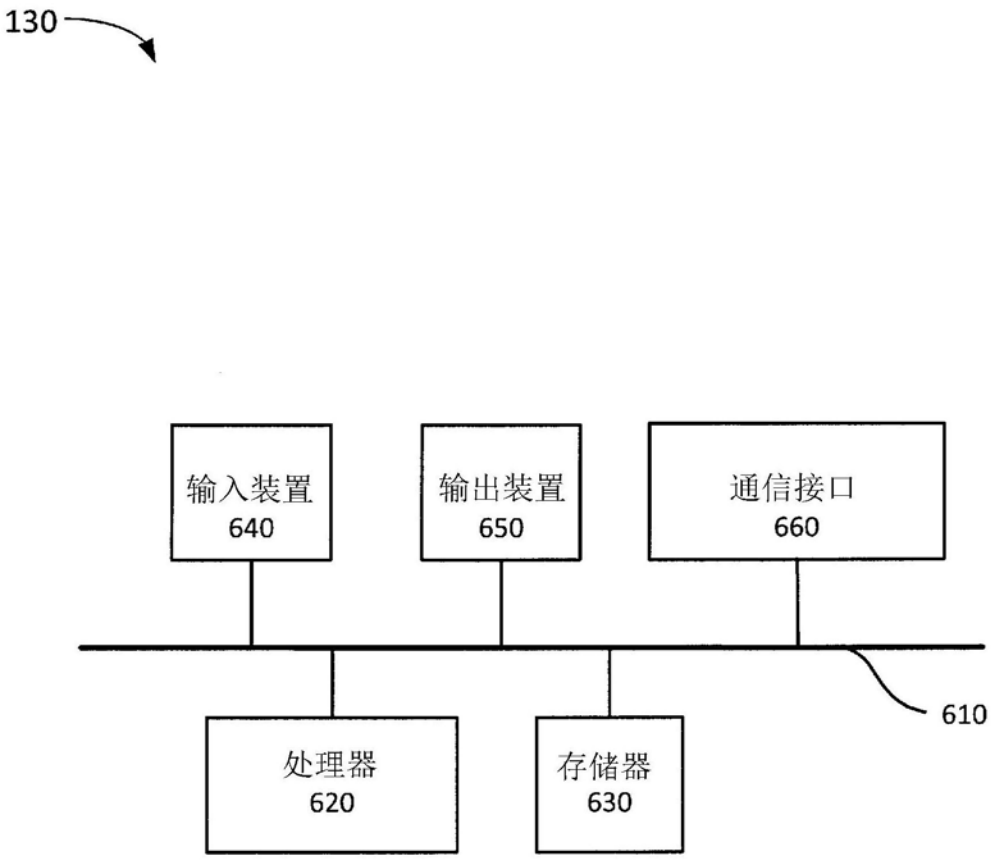


图6

管理员凭证
数据库
354

管理员用户名 702	经加密口令 704	经加密主密钥 706
ADMIN1	C(PW1, 主密钥)	C(主密钥 , PW1)
ADMIN2	C(PW2, 主密钥)	C(主密钥 , PW2)

图7A

用户凭证数据库
360

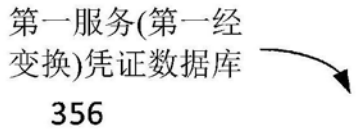
用户名 742	服务 744	装置 746	凭证 748
马格努斯	安全壳层， 虚拟专用网络	全部	MONKEY
萨拜娜	安全壳层， 虚拟专用网络	全部， 无摄像机 260	LETMEIN

图7B

(经更新)
用户凭证数据库
360'

用户名 742	服务 744	装置 746	凭证 748
马格努斯	安全壳层， 虚拟专用网络	全部	MONKEY
萨拜娜	安全壳层， 虚拟专用网络	全部， 无控制器 210-F	GOTLAND
贡纳尔	**虚拟专用 网络**	**控制器 210-A、210-B、 210-C，无摄像 机 260**	MUNKKALLAREN

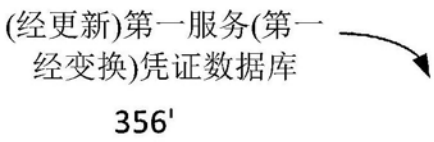
图7C



安全壳层凭证表

用户名 722	经变换凭证 724
马格努斯	SDFGH
萨拜娜	UYDAG

图7D



经更新安全壳层凭证表

用户名 722	经变换凭证 724
马格努斯	SDFGH
萨拜娜	DSISO

图7E

第二服务(第二经变换)凭证数据库
358

虚拟专用网络凭证数据库

用户名 732	经变换凭证 734
马格努斯	SDFGH
萨拜娜	UHYRV

图7F

(经更新)第二服务(第二经变换)凭证数据库
358'

经更新虚拟专用网络凭证数据库

用户名 732	经变换凭证 734
马格努斯	SDFGH
萨拜娜	UYTRW
贡纳尔	JKOUT

图7G

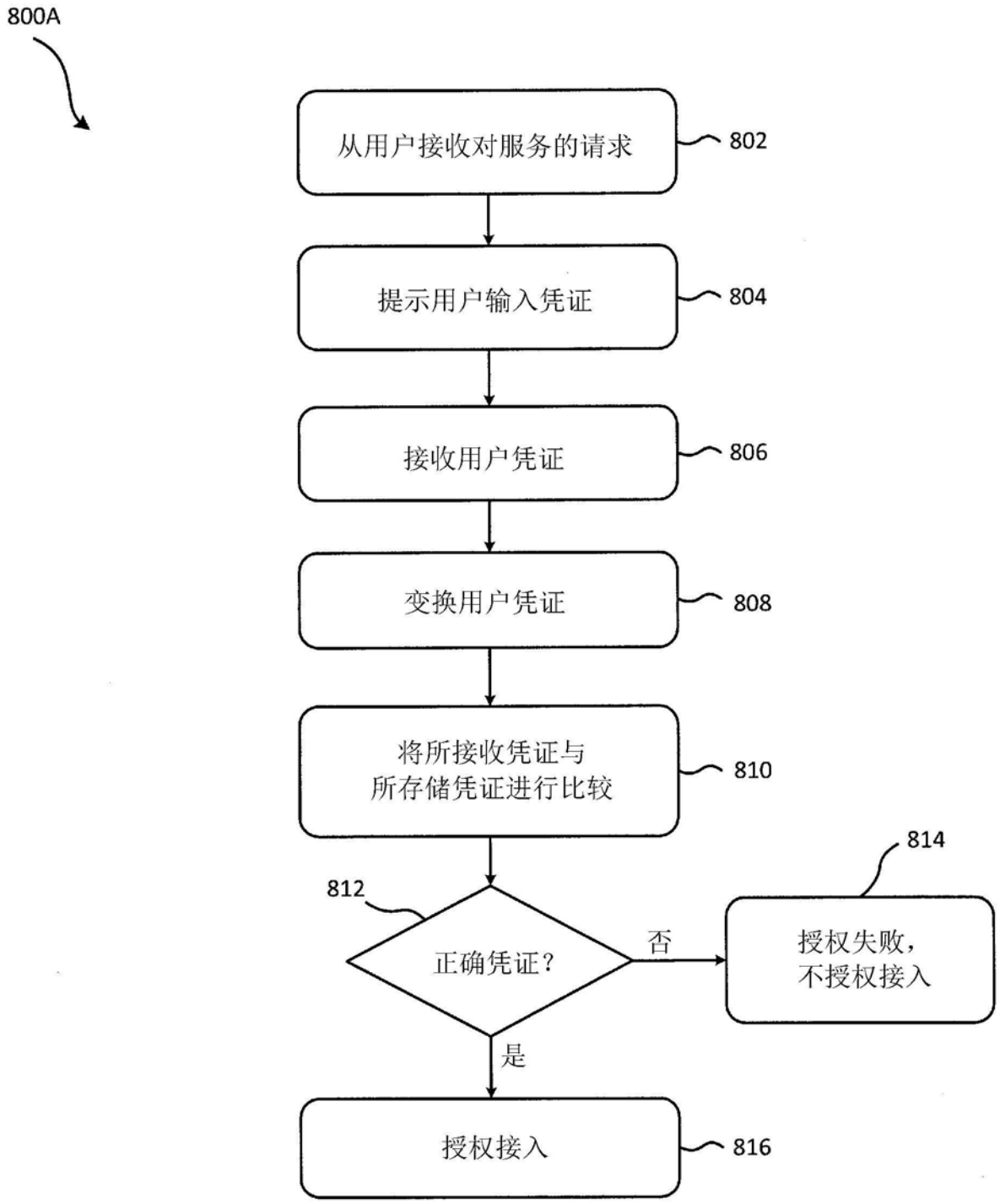

800A
从用户接收对服务的请求
802
提示用户输入凭证
804
接收用户凭证
806
变换用户凭证
808
将所接收凭证与
所存储凭证进行比较
810
812
正确凭证？
否
814
授权失败，
不授权接入
是
授权接入
816

图8A

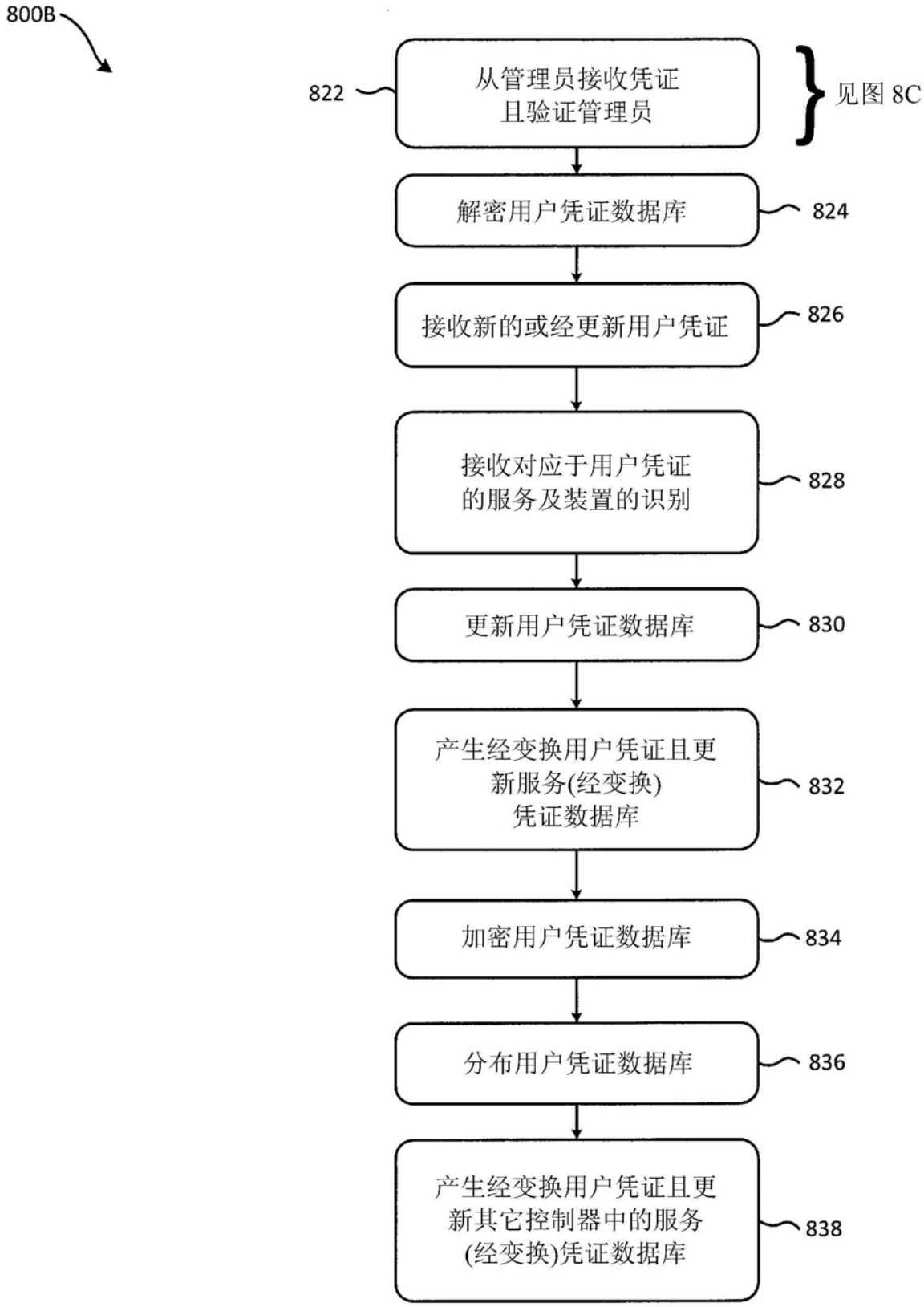

800B
822
从管理员接收凭证
且验证管理员
见图 8C
解密用户凭证数据库
824
接收新的或经更新用户凭证
826
接收对应于用户凭证
的服务及装置的识别
828
更新用户凭证数据库
830
产生经变换用户凭证且更
新服务(经变换)
凭证数据库
832
加密用户凭证数据库
834
分布用户凭证数据库
836
产生经变换用户凭证且更
新其它控制器中的服务
(经变换)凭证数据库
838

图8B

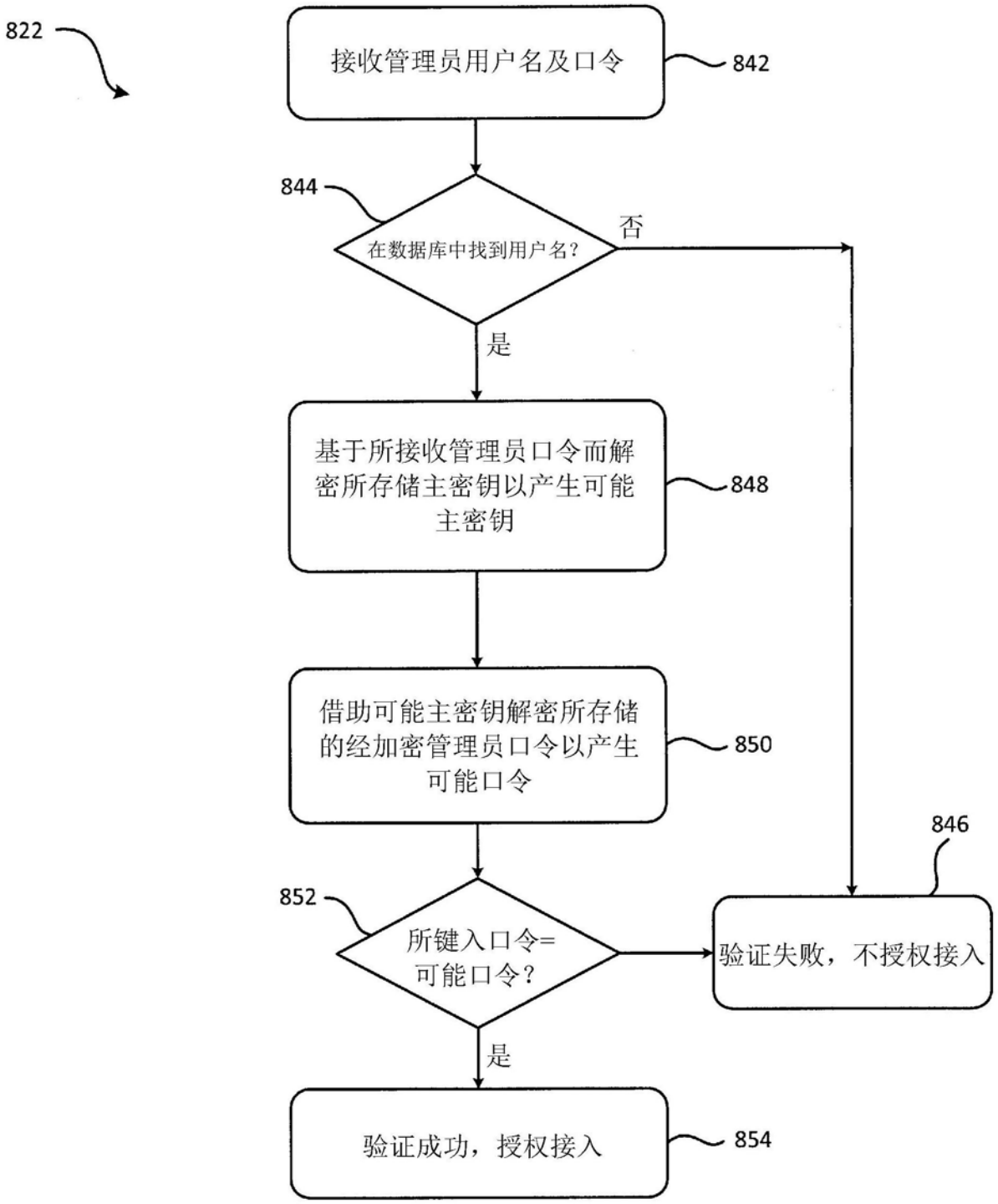

822
接收管理员用户名及口令
842
844
在数据库中找到用户名?
否
是
基于所接收管理员口令而解密所存储主密钥以产生可能主密钥
848
借助可能主密钥解密所存储的经加密管理员口令以产生可能口令
850
846
852
所键入口令=可能口令?
验证失败，不授权接入
是
验证成功，授权接入
854

图8C