(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114902610 B
(45)授权公告日 2024.09.27

(21)申请号 202080091192.5
(22)申请日 2020.12.17
(65)同一申请的已公布的文献号
申请公布号 CN 114902610 A
(43)申请公布日 2022.08.12
(30)优先权数据
201941052449 2019.12.17 IN
(85)PCT国际申请进入国家阶段日
2022.06.30
(86)PCT国际申请的申请数据
PCT/EP2020/086841 2020.12.17
(87)PCT国际申请的公布数据
WO2021/123031 EN 2021.06.24
(73)专利权人 亚萨合莱有限公司
地址 瑞典斯德哥尔摩

(72)发明人 克里希纳·库马尔·钱德兰
拉梅什巴布·R·松古克里希纳萨米

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
专利代理师 高岩 乔图
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
G07C 9/00(2020.01)
H04W 12/08(2021.01)

(56)对比文件
CN 104412536 A,2015.03.11
CN 106233704 A,2016.12.14

审查员 于兰

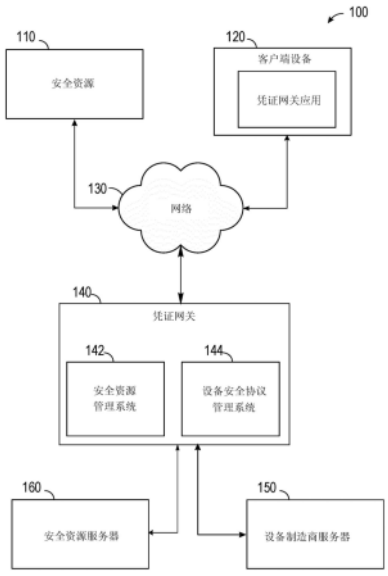
权利要求书3页 说明书17页 附图7页

(54)发明名称

凭证网关

(57)摘要

提供了用于执行操作的方法和系统,所述操作包括:通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;将该请求传送至与安全资源相关联的服务器;通过凭证网关从与安全资源相关联的服务器接收包括数字凭证的数据对象;通过凭证网关基于数据对象从多个安全协议中选择安全协议;以及通过凭证网关根据所选择的安全协议向客户端设备提供数字凭证。



CN 114902610 B

1.一种用于凭证网关的方法,包括:

通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,所述凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;

通过所述凭证网关将所述请求传送至与所述安全资源相关联的服务器;

通过所述凭证网关从与所述安全资源相关联的所述服务器接收包括所述数字凭证的数据对象;

通过所述凭证网关基于所述数据对象,从多个安全协议中选择安全协议;以及

通过所述凭证网关根据所选择的安全协议向所述客户端设备提供所述数字凭证。

2.根据权利要求1所述的方法,其中,使用物理访问数字凭证、逻辑访问数字凭证、政府数字凭证或票务事件数字凭证来访问所述安全资源。

3.根据权利要求1或2所述的方法,其中,所述不同安全资源类型包括由不同制造商提供的物理访问设备,并且其中,所述客户端设备包括智能电话、移动设备、智能手表或智能用户设备中的至少一个。

4.根据权利要求1或2所述的方法,其中,所述数字凭证包括用户的数字标识符或用于操作物理访问设备的密钥信息。

5.根据权利要求1或2所述的方法,其中,所述数据对象包括凭证配置文件,所述凭证配置文件包括用于提供所述数字凭证的标准化信息,所述标准化信息包括:配置文件标识符、接口标识符和凭证模板。

6.根据权利要求1或2所述的方法,其中,所述多个安全协议包括嵌入式安全元件(eSE)协议、可信执行环境(TEE)协议和软存储协议。

7.根据权利要求1或2所述的方法,其中,所述安全协议包括嵌入式安全元件(eSE)协议,所述方法还包括:

通过所述凭证网关确定与所述客户端设备相关联的制造商;

在所述凭证网关与所述制造商之间交换用于访问所述客户端设备的安全元件的密码密钥;以及

使用所述客户端设备的所述安全元件的密码密钥将与所述凭证网关相关联的系统密钥存储在所述安全元件的部分上。

8.根据权利要求7所述的方法,其中,通过所述凭证网关向所述客户端设备提供所述数字凭证包括:

使用所述系统密钥来对包括所述数字凭证的所述数据对象进行加密;

将经加密的数据对象发送至所述客户端设备;以及

使所述客户端设备将经加密的数据对象存储在所述安全元件的所述部分上。

9.根据权利要求8所述的方法,其中,所述安全元件的所述部分包括所述安全元件的补充安全域。

10.根据权利要求8所述的方法,还包括:

由所述客户端设备接收用于访问所述数字凭证的请求;以及

通过使用所述系统密钥将经加密的数据对象解密来检索所述数字凭证。

11.根据权利要求1或2所述的方法,还包括:

通过所述凭证网关将所述客户端设备配置成将与所述不同安全资源类型相关联的所

述数字凭证存储在所述客户端设备的安全元件上,所述配置包括:

通过所述凭证网关确定与所述客户端设备相关联的制造商;

在所述凭证网关与所述制造商之间交换用于访问所述客户端设备的所述安全元件的密码密钥;以及

使用所述客户端设备的所述安全元件的密码密钥,将与所述凭证网关相关联的系统密钥存储在所述安全元件的部分上,其中,基于所述系统密钥将所述数字凭证存储在所述客户端设备上。

12.根据权利要求1或2所述的方法,还包括:

通过所述凭证网关,将所述客户端设备配置成在所述客户端设备的可信执行环境(TEE)上存储和处理与所述不同安全资源类型相关联的所述数字凭证,所述配置包括:

通过所述凭证网关确定与所述客户端设备相关联的制造商;

在所述凭证网关与所述制造商之间交换用于操作所述客户端设备的TEE的密码密钥;以及

使用所述密码密钥,将与所述凭证网关相关联的系统密钥存储在所述客户端设备的TEE上,其中,所述客户端设备的TEE处理包含所述数字凭证的数据对象,以将所述数字凭证提供给请求应用。

13.根据权利要求1或2所述的方法,还包括:

通过所述凭证网关将所述客户端设备配置成根据软存储协议存储和处理与所述不同安全资源类型相关联的所述数字凭证,所述配置包括:

从所述安全资源类型的一个或更多个制造商接收凭证配置文件模板;

从所述凭证网关向所述客户端设备发送密码密钥信息,其中,所述凭证网关维护所述密码密钥信息的多样化版本;

使用所述密码密钥信息对所述凭证配置文件模板进行加密;

将经加密的凭证配置文件模板存储在所述客户端设备上,其中,所述客户端设备通过基于所述密码密钥信息将所述凭证配置文件模板解密,从相应的凭证配置文件模板检索所述数字凭证。

14.根据权利要求1或2所述的方法,其中,通过所述凭证网关从所述客户端设备接收用于获得所述数字凭证的请求包括:

通过在所述客户端设备上实现的凭证网关应用接收来自用户的用于添加新的数字凭证的输入,其中,所述凭证网关应用被配置成存储针对与不同制造商相关联的不同类型的安全资源的多个数字凭证,所述凭证网关应用被配置成将第一数字凭证存储在安全元件的部分上,并且所述凭证网关应用被配置成将第二数字凭证存储在所述客户端设备的可信执行环境上。

15.一种凭证网关系统,包括:

一个或更多个处理器,所述一个或更多个处理器被配置成执行包括以下的操作:

通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,所述凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;

通过所述凭证网关将所述请求传送至与所述安全资源相关联的服务器;

通过所述凭证网关从与所述安全资源相关联的所述服务器接收包括所述数字凭证的

数据对象;

通过所述凭证网关基于所述数据对象,从多个安全协议中选择安全协议;以及

通过所述凭证网关根据所选择的安全协议向所述客户端设备提供所述数字凭证。

16.根据权利要求15所述的系统,其中,使用物理访问数字凭证、逻辑访问数字凭证、政府数字凭证或票务事件数字凭证来访问所述安全资源。

17.根据权利要求15或16所述的系统,其中,所述不同安全资源类型包括由不同制造商提供的物理访问设备,并且其中,所述客户端设备包括智能电话、移动设备、智能手表或智能用户设备中的至少一个。

18.根据权利要求15或16所述的系统,其中,所述数字凭证包括用户的数字标识符或用于操作物理访问设备的密钥信息。

19.根据权利要求15或16所述的系统,其中,所述数据对象包括凭证配置文件,所述凭证配置文件包括用于提供所述数字凭证的标准化信息,所述标准化信息包括:配置文件标识符、接口标识符和凭证模板。

20.根据权利要求15或16所述的系统,其中,所述多个安全协议包括嵌入式安全元件(eSE)协议、可信执行环境(TEE)协议和软存储协议。

21.一种非暂态计算机可读介质,包括非暂态计算机可读指令,所述非暂态计算机可读指令在由一个或更多个处理器执行时,将所述一个或更多个处理器配置成执行包括以下的操作:

通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,所述凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;

通过所述凭证网关将所述请求传送至与所述安全资源相关联的服务器;

通过所述凭证网关从与所述安全资源相关联的所述服务器接收包括所述数字凭证的数据对象;

通过所述凭证网关基于所述数据对象,从多个安全协议中选择安全协议;以及

通过所述凭证网关根据所选择的安全协议向所述客户端设备提供所述数字凭证。

22.根据权利要求21所述的非暂态计算机可读介质,其中,所述操作还被配置成执行根据权利要求2至14中任一项所述的方法。

凭证网关

[0001] 相关申请的交叉引用

[0002] 本申请要求于2019年12月17日向印度(IN)专利局提交的印度申请第201941052449号的优先权权益,该印度申请的全部内容通过引用并入本文中。

背景技术

[0003] 电子凭证越来越多地被托管在智能设备(例如,智能电话、智能手表和各种其他因特网连接设备)中并且已经变得常见。这样的电子凭证用于解锁电子智能门锁(在酒店、企业中使用),呈现用户的数字标识符(例如,数字驾驶执照),以及呈现用于进入票务事件(例如,音乐会、体育赛事等)的电子票。

发明内容

[0004] 在一些方面,提供了一种方法,该方法包括:通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;将请求传送至与安全资源相关联的服务器;通过凭证网关从与安全资源相关联的服务器接收包括数字凭证的数据对象;通过凭证网关基于数据对象,从多个安全协议中选择安全协议;以及通过凭证网关根据所选择的安全协议向客户端设备提供数字凭证。

[0005] 在一些方面,使用物理访问数字凭证、逻辑访问数字凭证、政府数字凭证或票务事件数字凭证来访问安全资源。

[0006] 在一些方面,该方法包括智能电话、移动设备、智能手表或智能用户设备中的至少一个。

[0007] 在一些方面,该方法包括用户的数字标识符或用于操作物理访问设备的密钥信息。

[0008] 在一些方面,该方法包括:配置文件标识符、接口标识符和凭证模板。

[0009] 在一些方面,该方法包括智能设备易失性存储器上的嵌入式安全元件(eSE)协议、可信执行环境(TEE)协议和软存储协议。

[0010] 在一些方面,该方法包括:通过凭证网关确定与客户端设备相关联的制造商;在凭证网关与制造商之间交换用于访问客户端设备的安全元件的密码密钥;以及使用客户端设备的安全元件的密码密钥将与凭证网关相关联的系统密钥存储在安全元件的部分上。

[0011] 在一些方面,该方法包括:通过凭证网关,通过以下操作向客户端设备提供数字凭证:使用系统密钥来对包括数字凭证的数据对象进行加密;将经加密的数据对象发送至客户端设备;以及使客户端设备将经加密的数据对象存储在安全元件的该部分上。

[0012] 在一些方面,安全元件的该部分包括安全元件的补充安全域。

[0013] 在一些方面,该方法包括:由客户端设备接收访问数字凭证的请求;以及通过使用系统密钥将经加密的数据对象解密来检索数字凭证。

[0014] 在一些方面,该方法包括:通过在所述客户端设备上实现的凭证网关应用接收来

自用户的用于添加新的数字凭证的输入,其中,所述凭证网关应用被配置成存储针对与不同制造商相关联的不同类型的安全资源的多个数字凭证,所述凭证网关应用被配置成将第一数字凭证存储在所述安全元件的一部分上,并且被配置成将第二数字凭证存储在所述客户端设备的可信执行环境上。

[0015] 在一些方面,提供了一种系统,该系统包括:一个或更多个处理器,所述一个或更多个处理器被配置成执行包括以下的操作:通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;将请求传送至与安全资源相关联的服务器;通过凭证网关从与安全资源相关联的服务器接收包括数字凭证的数据对象;通过凭证网关基于数据对象,从多个安全协议中选择安全协议;以及通过凭证网关根据所选择的安全协议向客户端设备提供数字凭证。

[0016] 在一些方面,使用物理访问数字凭证、逻辑访问数字凭证、政府数字凭证或票务事件数字凭证来访问安全资源。

[0017] 在一些方面,该系统包括智能电话、移动设备、智能手表或智能用户设备中的至少一个。

[0018] 在一些方面,该系统包括用户的数字标识符或用于操作物理访问设备的密钥信息。

[0019] 在一些方面,该系统包括:配置文件标识符、接口标识符和凭证模板。

[0020] 在一些方面,该系统包括嵌入式安全元件(eSE)协议、可信执行环境(TEE)协议和软存储协议。

[0021] 在一些方面,提供了一种非暂态计算机可读介质,其包括非暂态计算机可读指令,该非暂态计算机可读指令包括:通过凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求,凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证;将请求传送至与安全资源相关联的服务器;通过凭证网关从与安全资源相关联的服务器接收包括数字凭证的数据对象;通过凭证网关基于数据对象,从多个安全协议中选择安全协议;以及通过凭证网关根据所选择的安全协议向客户端设备提供数字凭证。

附图说明

[0022] 图1是根据一些实施方式的示例凭证网关系统的框图。

[0023] 图2示出了根据示例性实施方式的示例智能设备。

[0024] 图3是根据一些实施方式的可以部署在图1的凭证网关系统内的示例凭证配置文件的框图。

[0025] 图4是根据一些实施方式的可以部署在图1的系统内的示例数据库。

[0026] 图5是示出根据示例实施方式的凭证网关系统的示例操作的流程图。

[0027] 图6是示出示例软件架构的框图,该示例软件架构可以与本文中描述的各种硬件架构结合使用。

[0028] 图7是示出根据一些示例实施方式的机器的部件的框图。

具体实施方式

[0029] 描述了用于凭证网关系统的示例方法和系统。在下面的描述中,出于说明的目的,阐述了许多具体细节以提供对示例实施方式的透彻理解。然而,对于本领域的普通技术人员来说明显的是,可以在没有这些具体细节的情况下实践本公开内容的实施方式。

[0030] 在典型的物理访问控制系统中,用户携带包含一组凭证(例如,授权信息)的物理卡或设备。当物理卡或设备被带到距物理访问设备大约20厘米范围内(极接近物理访问设备)时,与物理访问设备(例如,电子门锁)交换这样的凭证。此时,物理访问设备确定凭证是否授权用户访问物理访问设备,并且如果是,则物理访问设备准许访问(例如,打开门锁)。虽然这样的系统通常运行良好,但它们需要用户非常靠近物理访问设备来操作物理访问设备。这可能会在操作设备时引入各种延迟,并且可能会使用户感到沮丧。

[0031] 随着移动设备变得更常见,可以对这样的移动设备进行编程以承载与通常使用的物理卡相同的一组凭证。这些移动设备可以例如使用蓝牙低功耗(BLE)通信协议在较长距离上与物理访问设备通信。例如,移动设备可以在多达100米的范围内发送凭证并与物理访问设备交换凭证。在这种情况下,当与使用物理卡或设备相比用户距物理访问设备更远距离时,可以操作物理访问设备。这增加了访问诸如物理访问控制设备等各种安全资源的灵活性。

[0032] 移动设备已取代智能卡或个人身份证并且在任何适用的地方用作身份。当这些移动设备使用它们在设备上的数字身份执行这些交易时,它们需要信任。在连接至因特网的数百万的智能设备和可穿戴装置的数字世界中,对数字身份的需求变得必要,并且这些身份需要以具有无缝的用户体验的统一方式进行安全审查、递送并呈现给其他智能设备。当今市场上存在许多不同的凭证技术。多样化的专有技术和凭证技术上缺乏统一标准是数字凭证生态系统复杂性的主要原因。

[0033] 旨在向最终用户提供数字身份的客户系统通常需要与几个凭证提供商(例如,在访问控制系统的情况下的锁制造商或系统集成商)集成以支持不同的专有凭证技术。凭证提供商通常不支持多种专有凭证技术,因为每种技术在协议规范、编码模式、密码和安全方案上都有所不同。数字凭证到最终用户设备的递送机制给客户系统和凭证提供商增加了另一层复杂性。这是由于到最终用户设备的递送基于设备类型、设备存储(嵌入式安全元件(eSE)或安全元件、设备存储器等)以及数据结构和数据编码而有所不同。如果凭证要递送至安全元件存储装置或在客户端设备的可信执行环境中执行,则凭证提供商还需要与几个主要原始设备制造商建立合作关系。向最终用户提供数字凭证缺乏任何标准化限制了可以以电子方式访问的安全资源的范围,并限制了可以存储各种数字凭证的设备类型。

[0034] 所公开的实施方式提供了一种智能解决方案,该智能解决方案统一了数字凭证到客户端设备的递送并且根据给定安全资源的规范来管理这样的数字凭证的存储。具体地,所公开的实施方式提供了一种凭证网关,该凭证网关管理从与安全资源相关联的服务器接收给定的数字凭证并且将给定的数字凭证递送至最终用户的客户端设备。凭证网关与设备制造商协调安全协议,以将数字凭证安全地存储在客户端设备的可信执行环境(TEE)或安全元件上。以这种方式,凭证供应商不需要接触或学习如何利用数字凭证对不同的客户端设备进行编程。这拓宽了可以向最终用户提供数字凭证的安全资源的范围,并使得更多数量的安全资源可用于最终用户以数字和电子方式访问。凭证网关还可以通过对递送至客户

端设备的数字凭证进行加密并确保没有凭证网关的授权的任何实体不可访问这样的数字凭证来管理数字凭证的安全递送。

[0035] 在一些实施方式中,所公开的实施方式提供了系统和方法,其提供了将来自各种安全资源提供商和制造商的各种凭证加载到诸如智能设备(智能电话、智能手表或任何其他因特网连接设备)的客户端设备上的统一方法。根据所公开的实施方式,凭证网关从客户端设备接收用来获得用于访问安全资源的数字凭证的请求。凭证网关可以被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证。凭证网关将请求传送至与安全资源相关联的服务器,并从与安全资源相关联的服务器接收包括数字凭证的数据对象。凭证网关基于数据对象从多个安全协议中选择安全协议,并根据所选择的安全协议将数字凭证提供给客户端设备。

[0036] 以这种方式,凭证网关系统可以接受来自包括移动或可穿戴手机制造商的系统的任何其他外部系统的请求,并且发出包含关键个人信息、系统信息和/或访问信息的数字身份。凭证网关可以聚合不同类型的数字ID,并且可以以可互操作的方式将数字ID递送至任何种类的设备(智能电话或可穿戴装置)。凭证网关接受提供数字身份的请求,它将这样的请求安全地提供或发送至智能设备(移动电话、智能电话、可穿戴装置、智能手表或健身手表),并且还使得智能设备中的机制能够被安全地存储和呈现给各种安全资源(例如,物联网(IoT)设备、物理访问控制设备、逻辑访问控制设备、政府实体和住宅智能锁以及许多其他基于蓝牙或NFC或UWB的智能设备)。

[0037] 图1是示出根据各种示例实施方式的示例凭证网关系统100的框图。凭证网关系统100可以包括:客户端设备120;一个或更多个安全资源110,其例如通过可锁定的门来控制对受保护资产或资源的访问;凭证网关140;一个或更多个安全资源服务器160;以及一个或更多个设备制造商150,它们通过网络130(例如,因特网、BLE、超宽带(UWB)通信协议、电话网络)通信地耦接。

[0038] UWB是一种在宽频谱上使用短、低功率的脉冲的射频(RF)技术。脉冲在数量级上是每秒数百万个单独脉冲。频谱的宽度通常大于500兆赫兹或大于算术中心频率的百分之二十。UWB可以用于例如通过经由时间调制对数据进行编码(例如,脉冲位置编码)来进行通信。此处,符号由可用时间单位的集合中的时间单位子集上的脉冲来指定。UWB编码的其他示例可以包括幅度调制和/或极性调制。与基于载波的传输技术相比,宽带传输对于多路径衰落往往更稳健。此外,在任何给定频率处的脉冲的较低功率往往会减少与基于载波的通信技术的干扰。UWB可以用于雷达操作,提供数十厘米规模的定位准确度。由于脉冲中不同频率的可能可变的吸收和反射,因此可以检测到对象的表面特征和遮挡(例如,覆盖)特征两者。在一些情况下,定位除了距离之外还提供了入射角。

[0039] 客户端设备120和安全资源110可以经由电子消息(例如,通过因特网、BLE、UWB、WiFi直连或任何其他协议交换的分组)通信地耦接。尽管图1示出了单个安全资源110和单个客户端设备120,但是应当理解,在其他实施方式中,在凭证网关系统100中可以包括多个安全资源110和多个客户端设备120。如本文所使用的,术语“客户端设备”可以是指与通信网络(例如,网络130)对接以与安全资源110、凭证网关140、另一个客户端设备120或任何其他部件交换凭证从而获得对受安全资源110保护的资产或资源的访问的任何机器。

[0040] 安全资源110可以包括IoT设备、物理访问控制设备、逻辑访问控制设备、政府实体

设备、票务事件设备和住宅智能锁和/或其他基于蓝牙或NFC或UWB的智能设备中的任何一个或其组合。安全资源110可以保护安全区域并且可以被配置成从客户端设备120接收数字凭证或多个数字凭证。安全资源110可以验证所接收到的数字凭证被授权访问安全区域,并且作为响应,安全资源110可以准许对安全区域的访问。在一些实施方式中,客户端设备120将安全资源110的身份和数字凭证传送至凭证网关140和/或安全资源服务器160。凭证网关140和/或安全资源服务器160可以验证数字凭证是否被授权访问所识别的安全资源。如果验证数字凭证被授权访问所识别的安全资源,凭证网关140和/或安全资源服务器160指示安全资源110(例如,通过解锁电子门锁)准许客户端设备120的访问。在这种情况下,数字凭证从客户端设备120被传递至凭证网关140和/或安全资源服务器160而不是安全资源110。

[0041] 在一些情况下,凭证网关140的部件和功能中的一些或全部可以包括在客户端设备120和/或安全资源服务器160中。客户端设备120可以是但不限于移动电话、桌上型计算机、膝上型计算机、便携式数字助理(PDA)、智能电话、可穿戴设备(例如,智能手表)、平板电脑、超极本、上网本、笔记本电脑、多处理器系统、基于微处理器的或可编程消费电子产品或用户可以用于访问网络130的任何其他通信设备。

[0042] 图2示出了根据示例性实施方式的示例客户端设备200(例如,智能设备)。客户端设备200可以是客户端设备120(图1)的一种实现。客户端设备200可以包括多个通信接口,例如,BLE部件210、NFC部件212和UWB部件214。BLE部件210包括适用于通过BLE网络发送和接收信息的一个或更多个通信设备。NFC部件212包括适用于通过NFC网络发送和接收信息的一个或更多个通信设备。UWB部件214包括适用于通过UWB网络发送和接收信息的一个或更多个通信设备。

[0043] 客户端设备200包括可由运行在客户端设备200上的任何应用公开访问的标准存储装置(未示出)。客户端设备200还包括例如TEE 220、eSE 230和补充安全域(SSD)240的安全存储位置。在一些情况下,第一组数字凭证和/或凭证配置文件300(图3)可以存储在标准存储装置中。第二组数字凭证和/或凭证配置文件300(图3)可以存储在eSE中以及/或者存储补充安全域240上。第三组数字凭证和/或凭证配置文件300(图3)可以是存储在TEE 220中。在一些情况下,凭证网关应用的一些或所有部分可以由TEE 220和/或补充安全域240存储和/或执行。

[0044] 返回参照图1,安全资源110可以包括物理访问控制设备,该物理访问控制设备可以包括连接至物理资源(例如,门锁定机构或后端服务器)并控制物理资源(例如,门锁定机构)的访问读取器设备。与物理访问控制设备相关联的物理资源可以包括门锁、车辆的点火系统、或准许或拒绝对物理部件的访问并且可以被操作成准许或拒绝对物理部件的访问的任何其他设备。例如,在门锁的情况下,物理访问控制设备可以拒绝访问,在这种情况下,门锁保持锁定并且门无法打开,或者物理访问控制设备可以准许访问,在这种情况下,门锁变得解锁以允许门被打开。作为另一示例,在点火系统的情况下,物理访问控制设备可以拒绝访问,在这种情况下车辆点火系统保持禁用并且车辆不能启动,或者物理访问控制设备可以准许访问,在这种情况下车辆点火变为启用以允许车辆启动。

[0045] 物理访问控制涵盖用于管理例如人员对安全区域或安全资产的访问的一系列系统和方法。物理访问控制包括授权用户或设备(例如车辆、无人机等)的识别以及用于保护区域安全的大门、门或其他设施的启动或者例如物理或电子/软件控制机构的控制机构的

启动,允许访问安全资产。物理访问控制设备形成物理访问控制系统(PACS)的一部分,该物理访问控制系统可以包括读取器(例如,在线读取器或离线读取器),该读取器保存授权数据并且可以能够确定凭证(例如,来自在卡、扣或诸如移动电话的个人电子设备中的诸如射频识别(RFID)芯片的凭证或密钥设备)是否被授权用于执行器或控制机构(例如,门锁、开门器、软件控制机制、关闭警报等),或者PACS可以包括主机服务器,在集中管理的配置中,读取器和执行器(例如,经由控制器)连接至主机服务器。在集中管理的配置中,读取器可以从凭证或密钥装置获取凭证,并将这些凭证传递至PACS主机服务器。主机服务器然后确定是否凭证授权访问安全区域或安全资产并相应地命令执行器或其他控制机构。

[0046] 通常,安全资源110可以包括存储器、处理器、一个或更多个天线、通信模块、网络接口设备、用户接口和电源或供电部中的一个或更多个。

[0047] 安全资源110的存储器可以与由安全资源110的处理器对应用程序或指令的执行结合使用,并且用于暂时或长期存储程序指令或指令集和/或凭证或授权数据,例如凭证数据、凭证授权数据或访问控制数据或指令。例如,存储器可以包含由处理器用来运行安全资源110的其他部件和/或基于凭证或授权数据进行访问确定的可执行指令。安全资源110的存储器可以包括计算机可读介质,该计算机可读介质可以是可以包含、存储、传送或传输数据、程序代码或指令以供安全资源110使用或与安全资源110结合使用的任何介质。计算机可读介质可以是例如但不限于电子的、磁的、光学的、电磁的、红外或半导体系统、装置或设备。合适的计算机可读介质的更具体示例包括但不限于具有一个或更多个线的电连接或有形存储介质,例如便携式计算机软盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM或闪速存储器)、动态RAM(DRAM)、通常为致密盘只读存储器(CD-ROM)的任何固态存储设备或其他光或磁存储设备。计算机可读介质包括但不应与计算机可读存储介质混淆,计算机可读存储介质旨在涵盖计算机可读介质的所有物理、非暂态或类似实施方式。

[0048] 安全资源110的处理器可以对应于一个或更多个计算机处理设备或资源。例如,处理器可以被提供为硅芯片、被提供为现场可编程门阵列(FPGA)芯片、专用集成电路(ASIC)芯片、任何其他类型的集成电路(IC)芯片、IC芯片的集合等。作为更具体的示例,处理器可以被提供为微处理器、中央处理单元(CPU)或被配置成执行存储在物理访问控制设备110的存储器和/或内部存储器中的指令集的多个微处理器或CPU。

[0049] 安全资源110的天线可以对应于一个或多个天线并且可以被配置成提供安全资源110与凭证或密钥设备(例如,客户端设备120)之间的无线通信。天线可以被布置成使用一个或更多个无线通信协议和操作频率进行操作,所述一个或更多个无线通信协议和操作频率包括但不限于IEEE 802.15.1、蓝牙、蓝牙低功耗(BLE)、近场通信(NFC)、ZigBee、GSM、CDMA、Wi-Fi、RF、UWB等。通过示例的方式,天线可以是RF天线,并且因此,可以通过自由空间发送/接收RF信号以由具有RF收发器的凭证或密钥设备接收/传输。在一些情况下,至少一个天线是设计或配置成用于发送和/或接收UWB信号的天线(在本文中为简单起见称为“UWB天线”),使得读取器可以使用UWB技术与客户端设备120进行通信。

[0050] 安全资源110的通信模块可以被配置成根据任何合适的通信协议对安全资源110远程或本地的一个或更多个不同系统或设备(例如,一个或更多个客户端设备120和/或凭证网关140)进行通信。

[0051] 安全资源110的网络接口设备包括硬件,其用于促进利用许多传输协议(例如,帧中继、互联网协议(IP)、传输控制协议(TCP)、用户数据报协议(UDP)、超文本传输协议(HTTP)等)中的任何一个,通过通信网络(例如,网络130)与诸如一个或更多个客户端设备120和/或凭证网关140的其他设备进行通信。示例通信网络可以包括局域网(LAN)、广域网(WAN)、分组数据网络(例如,因特网)、移动电话网络(例如,蜂窝网络)、普通老式电话(POTS)网络、无线数据网络(例如,被称为Wi-Fi的IEEE 802.11标准系列、被称为WiMax的IEEE802.16标准系列)、IEEE 802.15.4标准系列和对等(P2P)网络等。在一些示例中,网络接口设备可以包括以太网端口或其他物理插孔、Wi-Fi卡、网络接口卡(NIC)、蜂窝接口(例如,天线、过滤器和相关电路)等。在一些示例中,网络接口设备可以包括多个天线以使用单输入多输出(SIMO)、多输入多输出(MIMO)或多输入单输出(MISO)技术中的至少一种进行无线通信。

[0052] 安全资源110的用户接口可以包括一个或更多个输入设备和/或显示设备。可以包括在用户接口中的合适的用户输入设备的示例包括但不限于一个或更多个按钮、键盘、鼠标、触敏表面、触控笔、摄像装置、麦克风等。可以包括在用户接口中的合适用户输出设备的示例包括但不限于一个或更多个LED、LCD面板、显示屏、触摸屏、一个或更多个灯、扬声器等。应当理解,用户接口还可以包括例如触敏显示器等组合的用户输入设备和用户输出设备。

[0053] 网络130可以包括自组织网络、内联网、外联网、虚拟专用网络(VPN)、LAN、无线网络、无线LAN(WLAN)、广局域网(WAN)、无线WAN(WWAN)、城域网(MAN)、BLE、UWB、因特网、因特网的一部分、公共交换电话网络(PSTN)的一部分、普通的老式电话服务(POTS)网络、蜂窝电话网络、无线网络、Wi-Fi®网络、另一种类型的网络或两个或更多个这样的网络的组合。例如,网络或网络的一部分可以包括无线网络或蜂窝网络,并且耦接可以是码分多址(CDMA)连接、全局移动通信系统(GSM)连接或其他类型的蜂窝或无线耦接。在该示例中,耦接可以实现各种类型的数据传输技术中的任何数据传输技术,例如单载波无线电传输技术(1xRTT)、演进数据优化(EVDO)技术、通用分组无线电服务(GPRS)技术、增强数据速率的GSM演进(EDGE)技术、包括3G的第三代合作伙伴计划(3GPP)、第四代无线(4G)网络、第五代无线(5G)网络、通用移动电信系统(UMTS)、高速分组接入(HSPA)、全球微波接入互操作性(WiMAX)、长期演进(LTE)标准、由各种标准设置组织限定的其他数据传输技术、其他长距离协议或其他数据传输技术。

[0054] 在一个示例中,客户端设备120将凭证直接提供给安全资源110。在这种情况下,安全资源110将凭证传送至凭证网关140。图1中的凭证网关140包括安全资源管理系统142和设备安全协议管理系统144。凭证网关140还可以包括关于图6和图7描述的元件,例如其上存储有指令的存储器和处理器,所述指令在由处理器执行时,使处理器控制凭证网关140的功能。

[0055] 凭证网关140搜索存储在安全资源管理系统142中的凭证列表以确定所接收到的凭证是否与来自用于访问由安全资源110保护的安全资产或资源(例如,门或安全区域)的授权凭证列表匹配。响应于确定所接收到的凭证被授权访问安全资源110,凭证网关140指示安全资源110执行准许客户端设备120的访问的操作(例如,指示安全资源110解锁门的锁定)。

[0056] 在另一示例中,客户端设备120将凭证提供给凭证网关140。凭证网关140搜索存储在安全资源管理系统142中的凭证列表以确定所接收到的凭证是否与来自用于访问由安全资源110保护的安全资产或资源(例如,门或安全区域)的授权凭证列表匹配。响应于确定所接收到的凭证被授权访问安全资源110,凭证网关140指示安全资源110(与所接收到的凭证相关联并且在客户端设备120的地理距离内)以执行准许客户端设备120的访问的操作(例如,指示物理访问控制设备110解锁门的锁定)。

[0057] 在一些实施方式中,客户端设备120实现凭证网关应用。凭证网关应用可以在客户端设备120上运行并且可以由客户端设备120的用户访问。凭证网关应用可以管理存储在客户端设备120上的多个数字凭证。例如,凭证网关应用可以包括数字凭证钱包。凭证网关应用可以向用户呈现列出由凭证网关应用存储和维护的所有数字凭证的用户接口。响应于从用户接收到从用户接口选择给定数字凭证的输入,凭证网关应用执行操作以检索相关联的数字凭证。在一些情况下,数字凭证被存储在安全元件的客户端设备120的安全元件部分中(例如,在补充安全域中)。在一些情况下,数字凭证存储在客户端设备120的TEE中。在一些情况下,数字凭证以加密形式存储在客户端设备120的不安全存储器中。

[0058] 凭证网关应用确定数字凭证如何存储在客户端设备120上并且检索和/或解密数字凭证。在检索和/或解密数字凭证时,凭证网关应用可以在客户端设备的屏幕上呈现数字凭证(例如,凭证网关应用可以显示与电子票对应的条形码、与诸如数字ID的数字凭证相关联的用户的图片等)。在一些情况下,检索到的数字凭证用于访问安全资源110。在这种情况下,凭证网关应用将获得的凭证发送至安全资源110和/或凭证网关140和/或安全资源服务器160以获得对受安全资源110保护的资源的访问。

[0059] 凭证网关应用被配置成允许用户添加新的数字凭证。例如,凭证网关应用呈现用于添加新的数字凭证的屏幕上选项。响应于接收到对用于添加新数字凭证的选项的选择,凭证网关应用获得与新数字凭证相关联的安全资源110的识别信息。凭证网关应用将添加新数字凭证的请求连同安全资源110的识别信息一起发送至凭证网关140。

[0060] 凭证网关140从安全资源管理系统142检索与所识别的安全资源110相关联的服务器的标识符。具体地,凭证网关140指示安全资源管理系统142与安全资源服务器160通信以获得与由在客户端设备120上运行的凭证网关应用识别的安全资源110相关联的所请求的新数字凭证。安全资源管理系统142向安全资源服务器160发送与客户端设备120的用户相关联的信息和与安全资源110相关联的信息(例如,安全资源110的唯一地址或唯一序列号)。

[0061] 在一些情况下,安全资源管理系统142选择与安全资源110的类型相关联的凭证配置文件300(图3)(或凭证配置文件模板),并将所选择的凭证配置文件300提供给安全资源服务器160。可以从存储在数据库400(图4)中的凭证网关模板410中选择凭证配置文件模板。具体地,凭证网关模板410可以包括多个凭证配置文件类型。每个凭证配置文件类型可以包括不同数量和/或类型的参数,这取决于与存储在相应配置文件中的凭证相关联的安全资源110。

[0062] 例如,安全资源管理系统142可以确定:用于识别安全资源110的信息指示安全资源是物理访问控制设备。在这种情况下,安全资源管理系统142选择第一类型的凭证配置文件300(第一类型的凭证配置文件模板),该第一类型的凭证配置文件300包括一个或更多个

字段,所述一个或更多个字段需要由安全资源服务器160填充以访问物理访问控制设备和/或与物理访问控制设备通信。作为另一示例,安全资源管理系统142可以确定:用于识别安全资源110的信息指示安全资源是扫描电子票的票务事件设备。在这种情况下,安全资源管理系统142选择第二类型的凭证配置文件300(第二类型的凭证配置文件模板),该第二类型的凭证配置文件300包括一个或更多个字段,该一个或更多个字段需要由安全资源服务器160填充以将电子票呈现至票务事件设备。作为另一示例,安全资源管理系统142可以确定:用于识别安全资源110的信息指示安全资源是扫描数字ID(例如,数字护照)的边境控制设备。在这种情况下,安全资源管理系统142选择第三类型的凭证配置文件300(第三类型的凭证配置文件模板),该第三类型的凭证配置文件300包括需要由安全资源服务器160填充以呈现电子护照的一个或更多个字段。

[0063] 安全资源服务器160生成用于访问所识别的安全资源110的数字凭证。安全资源服务器160获得从安全资源管理系统142接收的凭证配置文件300的字段。安全资源服务器160基于被生成的数字凭证和各种其他信息(例如,配置文件标识符310、小程序信息320、接口信息330、凭证模板340和安全资源信息350)来填充凭证配置文件300的字段。例如,安全资源管理系统142可以在小程序信息320中包括用于与安全资源110通信的软件类型或API信息。安全资源服务器160可以在接口信息330中包括与安全资源110通信的方式(例如,WiFI、因特网、WiFi直连、BLE等)。安全资源服务器160可以将所生成的数字凭证连同数字凭证的一个或更多个安全协议一起存储在凭证模板340中。也就是说,安全资源服务器160可以指定与数字凭证相关联的安全级别和/或类型(例如,数字凭证是否需要存储在客户端设备120的安全元件部分、客户端设备120的TEE、和/或在客户端设备120上以加密形式存储在标准存储器中)。安全资源服务器160可以在安全资源信息350中包括任何其他类型的必要信息(例如,与数字凭证相关联的时间限制,其指示数字凭证何时不再有效且需要被删除;地理限制,其指示客户端设备120需要在其中检索数字凭证的指定位置,等等)。

[0064] 在一些情况下,凭证配置文件300的信息的一些部分可以由安全资源管理系统142填充。例如,安全资源服务器160可以以非标准形式提供与访问安全资源110相关联的信息。然后,安全资源管理系统142可以通过填充相关联的凭证配置文件300来使信息标准化。

[0065] 安全资源管理系统142在从安全资源服务器160接收到包含凭证配置文件300(或与凭证配置文件300相关联的数据)的数据对象时,确定与用于访问安全资源110的数字凭证相关联的安全协议。例如,安全资源管理系统142可以处理凭证配置文件300以确定由安全资源服务器160要求的用于存储数字凭证的安全级别和/或类型。安全资源管理系统142将包括凭证配置文件300的数据对象发送至客户端设备120以用新的数字凭证配置客户端设备120。凭证网关应用处理所接收到的凭证配置文件300,并且基于凭证配置文件300中指定的参数来管理数字凭证的存储和检索。然后,凭证网关应用通知用户数字凭证已被接收并准备好使用。

[0066] 凭证网关应用存储与凭证配置文件300的配置文件标识符310相关联的数字凭证。也就是说,在接收到用于访问数字凭证的用户请求时,凭证网关应用检索所请求的数字凭证的配置文件标识符310。凭证网关应用获得对应的凭证配置文件300并且检索用于获得数字凭证和传送或访问相关联的安全资源110的参数。

[0067] 例如,凭证网关应用基于凭证配置文件300中包括的接口信息330存储与数字凭证

相关联的通信协议。以这种方式,当检索和访问数字凭证时,与安全资源110相关联的通信配置文件用于与安全资源110进行通信。具体地,如果通信协议是BLE,则凭证网关应用可以激活客户端设备120的BLE部件210并通过BLE网络将数字凭证发送至对应的安全资源110。在另一实现中,如果通信协议是NFC,则凭证网关应用可以激活客户端设备120的NFC部件212并通过NFC网络将数字凭证发送至对应的安全资源110。在另一实现中,如果通信协议是UWB,则凭证网关应用可以激活客户端设备120的UWB部件214并且通过UWB网络将数字凭证发送至对应的安全资源110。

[0068] 作为另一示例,凭证网关应用基于存储在安全资源信息350中的信息来确定是否有任何时间或地理限制与数字凭证相关联。凭证网关应用验证当前时间和/或地理位置不违反凭证配置文件中指定的任何限制。作为另一示例,凭证网关应用基于存储在凭证模板340中的信息来确定数字凭证如何存储在客户端设备120上(例如,在客户端设备120的安全元件上、在TEE上、或以加密形式存储在标准存储器上)。然后,凭证网关应用基于数字凭证被存储在何处和如何存储来从存储装置检索数字凭证。

[0069] 在一个实现中,安全资源管理系统142确定所指定的安全协议对应于将数字凭证存储在客户端设备120的补充安全域240(图2)上。在这种情况下,安全资源管理系统142指示设备安全协议管理系统144从设备制造商服务器150获得对补充安全域240的访问(如下面所讨论的)。在一些情况下,可以在初始安装和设置凭证网关应用时获得对补充安全域240的访问,这避免了每次将新的数字凭证添加到客户端设备120时都必须获得这样的访问。在这种情况下,安全资源管理系统142将包括凭证配置文件300的数据对象发送至客户端设备120。凭证网关应用处理凭证配置文件300并确定数字凭证需要存储在补充安全域240中。作为响应,凭证网关应用访问补充安全域240并将数字凭证存储在补充安全域240中。

[0070] 为了获得对补充安全域240的访问,设备安全协议管理系统144首先确定安装有凭证网关应用的客户端设备120的类型。然后,设备安全协议管理系统144识别与客户端设备120的类型相关联的设备制造商服务器150。设备安全协议管理系统144从凭证网关应用获得客户端设备120的序列号或其他唯一标识符。设备安全协议管理系统144将客户端设备120的序列号或其他唯一标识符传送至识别的设备制造商服务器150以获得用于访问客户端设备120的安全元件的一组密码密钥。设备安全协议管理系统144将所接收到的密码密钥存储在数据库400的设备密码密钥420中。在一个示例中,设备密码密钥420将每个设备标识符或序列号与从设备制造商服务器150接收到的对应一组密码密钥相关联。

[0071] 在一个示例中,设备安全协议管理系统144提供与客户端设备120相关联的一组密码密钥并从设备制造商服务器150接收密码密钥以用于访问补充安全域240。设备安全协议管理系统144将所接收到的密码密钥提供至凭证网关应用。然后,凭证网关应用使用所接收到的密钥来获得对补充安全域240的访问。设备安全协议管理系统144还向凭证网关应用提供一组凭证网关密钥。可以从存储在数据库400中的网关密码密钥430中检索凭证网关密钥。在一些情况下,设备安全协议管理系统144将凭证网关密钥维护为密码密钥信息的多样化版本。然后,凭证网关应用将该组凭证网关密钥存储在补充安全域240上。当凭证网关应用确定凭证配置文件300包括需要存储在补充安全域240中的数字凭证时,凭证网关应用从补充安全域240获得凭证网关密钥并使用凭证网关密钥对接收到的数字凭证进行加密,并

将经加密的数字凭证存储在补充安全域240上。可以以如下类似的方式执行从补充安全域240检索数字凭证:使用安全元件的密码密钥从补充安全域240访问数字凭证,然后使用存储在补充安全域240中的凭证网关密钥对数字凭证进行解密。

[0072] 在另一实现中,安全资源管理系统142确定指定的安全协议对应于将数字凭证存储在客户端设备120的TEE 220(图2)上。在这种情况下,安全资源管理系统142指示设备安全协议管理系统144从设备制造商服务器150获得对TEE 220的访问。在一些情况下,可以在初始安装和设置凭证网关应用时获得对TEE 220的访问,这避免了每次将新的数字凭证添加到客户端设备120时都必须获得这样的访问。在这种情况下,安全资源管理系统142将包括凭证配置文件300的数据对象发送至客户端设备120。凭证网关应用处理凭证配置文件300并且确定数字凭证需要存储在TEE 220中。作为响应,凭证网关应用访问TEE 220并且将数字凭证存储在TEE 220中。

[0073] 为了获得对TEE 220的访问,设备安全协议管理系统144首先确定安装有凭证网关应用的客户端设备120的类型。然后,设备安全协议管理系统144识别与客户端设备120的类型相关联的设备制造商服务器150。设备安全协议管理系统144从凭证网关应用获得客户端设备120的序列号或其他唯一标识符。设备安全协议管理系统144将客户端设备120的序列号或其他唯一标识符传送至所识别的设备制造商服务器150以获得用于访问客户端设备120的TEE 220的一组密码密钥。设备安全协议管理系统144将所接收到的密码密钥存储在数据库400的设备密码密钥420中。在一个示例中,设备密码密钥420将每个设备标识符或序列号与从设备制造商服务器150接收到的对应一组密码密钥相关联。在一个示例中,设备安全协议管理系统144提供与客户端设备120相关联的一组密码密钥,并且从设备制造商服务器150接收密码密钥以用于访问TEE 220。设备安全协议管理系统144将所接收到的密码密钥提供至凭证网关应用。然后,凭证网关应用使用所接收到的密钥来获得对TEE220的访问。然后,凭证网关应用将数字凭证存储在TEE 220上。可以以如下类似的方式执行从TEE 220中检索数字凭证:使用TEE 220的密码密钥从TEE 220访问数字凭证。

[0074] 在另一实现中,安全资源管理系统142确定所指定的安全协议对应于将数字凭证以加密形式存储在客户端设备120的标准存储器上。在这种情况下,安全资源管理系统142获得来自网关密码密钥430的一组凭证网关密钥,并且使用凭证网关密钥对凭证配置文件和/或数字凭证进行加密。安全资源管理系统142可以向凭证网关应用提供凭证网关密钥。凭证网关应用以加密形式存储所接收到的数字凭证以及/或者使用凭证网关密钥对所接收到的数字凭证进行加密。可以以如下类似的方式执行检索数字凭证:从标准存储器访问数字凭证并使用凭证网关密钥对数字凭证进行解密。

[0075] 图5是示出根据示例实施方式的凭证网关系统100的示例过程500的流程图。过程500可以以由一个或更多个处理器执行的计算机可读指令实现,使得过程500的操作可以部分地或全部地由凭证网关系统100的功能部件执行;因此,下面参照凭证网关系统100通过示例的方式描述过程500。然而,在其他实施方式中,过程500的操作中的至少一些操作可以部署在各种其他硬件配置上。过程500的操作中的一些操作或全部操作可以并行、无序或完全省略。

[0076] 在操作501处,凭证网关140接收用来获得用于访问安全资源的数字凭证的请求,凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证。例

如,凭证网关140可以从客户端设备120上的凭证网关应用接收用于将新的数字凭证添加到凭证网关应用以用于访问安全资源110的请求。

[0077] 在操作502处,凭证网关140将请求传送至与安全资源相关联的服务器。例如,凭证网关140识别与由凭证网关应用识别的安全资源相关联的安全资源服务器160,并且请求安全资源服务器160生成或提供用于访问安全资源110的数字凭证。

[0078] 在操作503处,凭证网关140从与安全资源相关联的服务器接收包括数字凭证的数据对象。例如,凭证网关140接收由安全资源服务器160使用包括用于访问所识别的安全资源110的数字凭证的各种信息填充的凭证配置文件300(图3)。

[0079] 在操作504处,凭证网关140基于数据对象从多个安全协议中选择安全协议。例如,凭证网关140处理凭证配置文件300以确定数字凭证需要存储在客户端设备120的补充安全域240中。

[0080] 在操作505处,凭证网关140根据所选择的安全协议向客户端设备提供数字凭证。例如,凭证网关140向凭证网关应用提供数字凭证和/或凭证配置文件300。凭证网关应用处理所接收到的数字凭证和/或凭证配置文件300以根据在凭证配置文件中指定的安全协议存储数字凭证(例如,以加密形式存储在标准存储器中、存储在客户端设备120的TEE 220中、和/或存储在客户端设备120的eSE或补充安全域240中)。

[0081] 图6是示出示例软件架构606的框图,其可以与本文中描述的各种硬件架构结合使用。图6是软件架构的非限制性示例,并且将认识到,可以实现许多其他架构以促进本文中描述的功能。软件架构606可以在诸如图7的机器700的硬件上执行,机器700包括处理器704、存储器714和输入/输出(I/O)部件718等。示出了代表性硬件层652并且该代表性硬件层652可以表示例如图7的机器700。代表性硬件层652包括具有相关联的可执行指令604的处理单元654。可执行指令604表示软件架构606的可执行指令,包括本文中描述的方法、部件等的实现。硬件层652还包括也具有可执行指令604的存储器和/或存储设备存储器/存储装置656。硬件层652还可以包括其他硬件658。软件架构606可以部署在图1中所示的部件中的任何一个或更多个部件中。

[0082] 在图6的示例架构中,软件架构606可以被概念化为层的堆栈,在该层的堆栈中,每个层提供特定功能。例如,软件架构606可以包括诸如操作系统602、库620、框架/中间件618、应用616和表示层614的层。在操作上,层内的应用616和/或其他部件可以通过软件堆栈激活应用编程接口(API)调用608并且接收响应于API调用608的消息612。所示出的层本质上是代表性的,并且并非所有软件架构都具有所有层。例如,一些移动操作系统或专用操作系统可能不提供框架/中间件618,而其他操作系统可能提供这样的层。其他软件架构可以包括另外的或不同的层。

[0083] 操作系统602可以管理硬件资源并提供公共服务。操作系统602可以包括例如内核622、服务624和驱动器626。内核622可以充当硬件与其他软件层之间的抽象层。例如,内核622可以负责存储器管理、处理器管理(例如调度)、部件管理、联网、安全设置等。服务624可以为其他软件层提供其他公共服务。驱动器626负责控制底层硬件或与底层硬件对接。例如,取决于硬件配置,驱动器626包括显示驱动器、摄像装置驱动器、BLE驱动器、UWB驱动器、Bluetooth®驱动器、闪速存储器驱动器、串行通信驱动器(例如,通用串行总线(USB)驱

动器)、Wi-Fi®驱动器、音频驱动器、电源管理驱动器等。

[0084] 库620提供由应用616和/或其他部件和/或层使用的公共基础设施。库620提供如下功能,该功能允许其他软件组件以比与底层操作系统602的功能(例如,内核622、服务624、和/或驱动器626)直接对接的方式更容易的方式来执行任务。库620可以包括系统库644(例如,C标准库),该系统库1444可以提供诸如存储器分配功能、字符串操纵功能、数学函数等的功能。此外,库620可以包括API库646,例如媒体库(例如,支持诸如MPREG4、H.264、MP3、AAC、AMR、JPG、PNG的各种媒体格式的呈现和操纵的库)、图形库(例如,可以用于在显示器上以图形内容呈现二维和三维的OpenGL框架)、数据库库(例如,可以提供各种关系数据库功能的SQLite)、web库(例如,可以提供web浏览功能的WebKit)等。库620还可以包括各种各样的其他库648,以向应用616和其他软件组件/设备提供许多其他API。

[0085] 框架/中间件618(有时也称为中间件)提供可以由应用616和/或其他软件组件/设备使用的较高级别的公共基础设施。例如,框架/中间件618可以提供各种图形用户接口功能、高级资源管理、高级位置服务等。框架/中间件618可以提供可以由应用616和/或其他软件组件/设备使用的广泛范围的其他API,其中一些API可以专用于特定的操作系统602或平台。

[0086] 应用616包括内置应用638和/或第三方应用640。代表性内置应用638的示例可以包括但不限于联系人应用、浏览器应用、图书阅读器应用、位置应用、媒体应用、消息应用和/或游戏应用。第三方应用640可以包括由除特定平台的供应商之外的实体使用ANDROID™或IOS™软件开发工具包(SDK)开发的应用,并且可以是在诸如IOS™、ANDROID™、WINDOWS®Phone的移动操作系统或其他移动操作系统上运行的移动软件。第三方应用640可以激活由移动操作系统(例如,操作系统602)提供的API调用608以促进本文中描述的功能。

[0087] 应用616可以使用内置操作系统功能(例如,内核622、服务624和/或驱动器626)、库620以及框架/中间件618来创建UI以与系统的用户交互。替选地或附加地,在一些系统中,可以通过例如表示层614的表示层发生与用户的交互。在这些系统中,应用/部件"逻辑"可以与应用/部件的与用户交互的方面分开。

[0088] 图7是示出了根据一些示例实施方式的机器700的部件的框图,机器700能够从机器可读介质(例如,机器可读存储介质)读取指令并执行本文中讨论的方法中的任一种或更多种方法。具体地,图7以计算机系统的示例形式示出了机器700的图形表示,在该机器700中可以执行用于使机器700执行本文中讨论的方法中的任何一种或更多种的指令710(例如,软件、程序、应用、小程序、app或其他可执行代码)。

[0089] 同样地,指令710可以被用来实现本文中描述的设备或部件。指令710将通用的、未编程的机器700转换成被编程为以所描述的方式执行所描述和示出的功能的特定机器700。在替选实施方式中,机器700作为独立设备操作或者可以耦接(例如,联网)至其他机器。在联网部署中,机器700可以在服务器客户端网络环境中以服务器机器或客户端机器的身份操作,或者在对等(或分布式)网络环境中作为对等机器操作。机器700可以包括但不限于服务器计算机、客户端计算机、个人计算机(PC)、平板计算机、膝上型计算机、上网本、STB、PDA、娱乐媒体系统、蜂窝电话、智能电话、移动设备、可穿戴设备(例如,智能手表)、智能家

居设备(例如,智能家用电器)、其他智能设备、web设备、网络路由器、网络交换机、网络桥接器、或能够顺序地或以其他方式执行指令710的任何机器,该指令710指定机器700要采取的动作。此外,虽然仅示出了单个机器700,但是术语“机器”还应被认为包括单独地或联合地执行指令710以执行本文中讨论的方法中的任何一种或更多种方法的机器的集合。

[0090] 机器700可以包括处理器704、存储器/存储装置706和I/O部件718,所述处理器704、存储器/存储装置706和I/O部件718可以被配置成例如经由总线702彼此通信。在示例实施方式中,处理器704(例如,CPU、精简指令集计算(RISC)处理器、复杂指令集计算(CISC)处理器、图形处理单元(GPU)、数字信号处理器(DSP)、专用集成电路(ASIC)、射频集成电路(RFIC)、另一处理器或其任何合适的组合)可以包括例如可以执行指令710的处理器708和处理器712。术语“处理器”旨在包括多核处理器704,该多核处理器704可以包括可以同时执行指令的两个或更多个独立的处理器(有时被称为“核”)。虽然图7示出了多处理器704,但是机器700可以包括具有单个核的单个处理器、具有多个核的单个处理器(例如,多核处理器)、具有单个核的多个处理器、具有多个核的多个处理器或者其任何组合。

[0091] 存储器/存储装置706可以包括诸如主存储器或其他存储器存储装置的存储器714以及存储单元716,处理器704能够例如经由总线702访问存储器714和存储单元716两者。存储单元716和存储器714存储体现本文中描述的方法或功能中的任何一个或更多个的指令710。指令710还可以在其被机器700执行期间完全地或部分地驻留在存储器714内、存储单元716内、处理器704中的至少一个内(例如,处理器的高速缓冲存储器内)或其任何合适的组合内。因此,存储器714、存储单元716以及处理器704的存储器是机器可读介质的示例。

[0092] I/O部件718可以包括用于接收输入、提供输出、产生输出、传送信息、交换信息、捕获测量等的各种部件。包括在特定机器700中的特定I/O部件718将取决于机器的类型。例如,诸如移动电话的便携式机器可能会包括触摸输入设备或其他这样的输入机构,而无头服务器机器可能不会包括这样的触摸输入设备。应当认识到,I/O部件718可以包括图7中未示出的许多其他部件。I/O部件718仅为了简化以下讨论而根据功能被分组,并且该分组决不是限制性的。在各种示例实施方式中,I/O部件718可以包括输出部件726和输入部件728。输出部件726可以包括视觉部件(例如,诸如等离子显示面板(PDP)、LED显示器、LCD、投影仪或阴极射线管(CRT)的显示器)、听觉部件(例如,扬声器)、触觉部件(例如,振动马达、阻力机构)、其他信号生成器等。输入部件728可以包括字母数字输入部件(例如,键盘、被配置成接收字母数字输入的触摸屏、光电键盘或其他字母数字输入部件)、基于点的输入部件(例如,鼠标、触摸板、轨迹球、操纵杆、运动传感器或其他指向仪器)、触觉输入部件(例如,物理按钮、提供触摸或触摸姿势的位置和/或力的触摸屏或其他触觉输入部件)、音频输入部件(例如,麦克风)等。

[0093] 在另外的示例实施方式中,I/O部件718可以包括生物计量部件739、运动部件734、环境部件736或定位部件738等各种其他部件。例如,生物计量部件739可以包括用于检测表达(例如,手表达、面部表情、声音表达、身体姿势或眼睛跟踪)、测量生物信号(例如,血压、心率、体温、出汗或脑波)、识别人(例如,语音识别、视网膜识别、面部识别、指纹识别或基于脑电图的识别)等的部件。运动部件734可以包括加速度传感器部件(例如加速度计)、重力传感器部件、旋转传感器部件(例如陀螺仪)等。环境部件736可以包括例如照明传感器部件(例如,光度计)、温度传感器部件(例如,检测周围温度的一个或更多个温度计)、湿度传感

器部件、压力传感器部件(例如,气压计)、听觉传感器部件(例如,检测背景噪声的一个或更多个麦克风)、接近传感器部件(例如,检测附近对象的红外传感器)、气体传感器(例如,为了安全而检测危险气体的浓度或者测量大气中的污染物的气体检测传感器)或者可以提供与周围物理环境对应的指示、测量或信号的其他部件。定位部件738可以包括位置传感器部件(例如,GPS接收器部件)、海拔传感器部件(例如,检测可以得到海拔的气压的高度计或气压计)、取向传感器部件(例如,磁力计)等。

[0094] 可以使用各种技术来实现通信。I/O部件718可以包括通信部件740,该通信部件740可操作以分别经由耦接724和耦接722将机器700耦接至网络737或设备729。例如,通信部件740可以包括网络接口部件或其他合适的装置以与网络737接口。在又一示例中,通信部件740可以包括有线通信部件、无线通信部件、蜂窝通信部件、近场通信(NFC)部件、Bluetooth®部件(例如,Bluetooth®低功耗)、Wi-Fi®部件和经由其他模态提供通信的其他通信部件。设备729可以是其他机器或各种外围设备中的任何一个外围设备(例如,经由USB耦接的外围设备)。

[0095] 此外,通信部件740可以检测标识符或者可以包括能够操作以检测标识符的部件。例如,通信部件740可以包括RFID标签阅读器部件、NFC智能标签检测部件、光学阅读器部件(例如,用于检测诸如通用产品代码(UPC)条形码的一维条形码、诸如快速反应(QR)码的多维条形码、Aztec码、数据矩阵、数据符号(Dataglyph)、最大码(MaxiCode)、PDF417、超码(Ultra Code)、UCC RSS-2D条形码和其他光学码的光学传感器)或声学检测部件(例如,用于识别标记的音频信号的麦克风)。此外,可以经由通信部件740得到各种信息,例如经由因特网协议(IP)地理位置得到位置、经由Wi-Fi®信号三角测量得到位置、经由检测可以指示特定位置的NFC信标信号得到位置等。

[0096] 术语表:

[0097] 该上下文中的“载波信号”是指能够存储、编码或携载由机器执行的暂态或非暂态指令的任何无形介质并且包括数字或模拟通信信号或其他无形介质以便于这些指令的通信。可以使用暂态或非暂态传输介质经由网络接口设备并且使用多个公知的传输协议中的任何一个来通过网络发送或接收指令。

[0098] 该上下文中的“客户端设备”是指与通信网络对接以从一个或更多个服务器系统或其他客户端设备获得资源的任何机器。客户端设备可以是但不限于移动电话、桌上型计算机、膝上型计算机、PDA、智能电话、平板计算机、超极本、上网本、膝上型计算机、多处理器系统、基于微处理器或可编程消费电子产品、游戏控制台、机顶盒或用户可以用于访问网络的任何其他通信设备。

[0099] 上下文中的“通信网络”是指网络的一个或更多个部分,该网络可以是自组织网络、内联网、外联网、VPN、LAN、BLE网络、UWB网络、WLAN、WAN、WWAN、城域网(MAN)、因特网、因特网的一部分、PSTN的一部分、普通老式电话服务(POTS)网络、蜂窝电话网络、无线网络、Wi-Fi®网络、另一类型的网络或两个或更多个这样的网络的组合。例如,网络或网络的一部分可以包括无线网络或蜂窝网络,并且耦接可以是码分多址(CDMA)连接、全局移动通信系统(GSM)连接或其他类型的蜂窝或无线耦接。在该示例中,耦接可以实现各种类型的数据传输技术中的任何一种,例如单载波无线电传输技术(1xRTT)、演进数据优化(EVDO)技

术、通用分组无线电业务(GPRS)技术、增强数据速率的GSM演进(EDGE)技术、包括3G的第三代合作伙伴计划(3GPP)、第四代无线(4G)网络、通用移动电信系统(UMTS)、高速分组接入(HSPA)、全球微波接入互操作性(WiMAX)、长期演进(LTE)标准、由各种标准设置组织定义的其他标准、其他远程协议或其他数据传输技术。

[0100] 该上下文中的“机器可读介质”是指能够临时或永久地存储指令和数据的部件、设备或其他有形介质,并且可以包括但不限于RAM、ROM、缓冲存储器、闪速存储器、光学介质、磁介质、高速缓冲存储器、其他类型的存储装置(例如,可擦除可编程只读存储器(EEPROM))和/或它们的任何合适的组合。术语“机器可读介质”应当被视为包括能够存储指令的单个介质或多个介质(例如,集中式或分布式数据库或相关联的高速缓存和服务器)。术语“机器可读介质”还将被视为包括能够存储由机器执行的指令(例如,代码)的任何介质或多个介质的组合,使得指令在由机器的一个或更多个处理器执行时使机器执行本文中描述的任何一种或更多种方法。因此,“机器可读介质”指的是单个存储装置或设备,以及包括多个存储装置或设备的“基于云”的存储系统或存储网络。术语“机器可读介质”不包括信号本身。

[0101] 该上下文中的“部件”是指具有由功能或子例程调用、分支点、API或者对特定处理或控制功能提供分区或模块化的其他技术定义的边界的设备、物理实体或逻辑。部件可以经由其接口与其他部件组合以执行机器处理。部件可以是被设计用于与其他部件一起使用的封装功能硬件单元并且可以是通常执行相关功能中的特定功能的程序的一部分。部件可以构成软件组件(例如,体现在机器可读介质上的代码)或硬件部件。“硬件部件”是能够执行某些操作的有形单元,并且可以以某种物理方式来配置或布置。在各种示例实施方式中,一个或更多个计算机系统(例如,独立计算机系统、客户端计算机系统或服务器计算机系统)或计算机系统的一个或更多个硬件部件(例如,处理器或处理器组)可以通过软件(例如,应用或应用部分)被配置为用于执行如本文中描述的某些操作的硬件部件。

[0102] 也可以机械地、电子地或以其任何合适的组合来实现硬件部件。例如,硬件部件可以包括被永久地配置成执行某些操作的专用电路系统或逻辑。硬件部件可以是例如FPGA或ASIC的专用处理器。硬件部件还可以包括通过软件被短暂配置成执行某些操作的可编程逻辑或电路。例如,硬件部件可以包括由通用处理器或其他可编程处理器执行的软件。一旦通过这样的软件而配置,硬件部件就成为被独特地定制成执行所配置功能的特定机器(或机器的特定部件),而不再是通用处理器。将认识到,可以通过成本和时间考虑来驱动在专用且永久配置的电路系统中或在临时配置的电路系统(例如,由软件进行配置)中机械地实现硬件部件的决策。相应地,短语“硬件部件”(或者“硬件实现的部件”)应当被理解成包含有形实体,即为被物理构造、永久配置(例如,硬连线)或暂时配置(例如,编程)成以某种方式操作或者执行本文中描述的某些操作的实体。考虑硬件部件被临时配置(例如,被编程)的实施方式,无需在任一时刻对每一个硬件部件进行配置或实例化。例如,在硬件部件包括通过软件配置成专用处理器的通用处理器的情况下,该通用处理器可以在不同时间处分别被配置为不同的专用处理器(例如,包括不同的硬件部件)。软件相应地配置一个特定处理器或多个特定处理器以例如在一个时刻处构成特定硬件部件并且在不同的时刻处构成不同的硬件部件。

[0103] 硬件部件可以向其他硬件部件提供信息以及从其他硬件部件接收信息。相应地,所描述的硬件部件可以被认为是通信上耦接的。在同时存在多个硬件部件的情况下,可以

通过在两个或更多个硬件部件之间(例如,通过适当的电路和总线)的信号传输来实现通信。在其中多个硬件部件在不同时间处被配置或实例化的实施方式中,可以例如通过将信息存储在多个硬件部件能够访问的存储器结构中并且在该存储器结构中检索信息来实现这样的硬件部件之间的通信。例如,一个硬件部件可以执行操作并且将该操作的输出存储在其通信地耦接至的存储器设备中。然后,其他硬件部件可以在随后的时间处访问存储器设备以检索所存储的输出并对其进行处理。

[0104] 硬件部件还可以启动与输入设备或输出设备的通信,并且可以对资源(例如,信息的集合)进行操作。本文中描述的示例的方法的各种操作可以至少部分地由临时配置(例如,由软件)或永久配置成执行相关操作的一个或更多个处理器来执行。无论是短暂配置还是永久配置,这样的处理器可以构成进行操作以执行本文描述的一个或更多个操作或功能的处理器实现的部件。如本文所使用的,“处理器实现的部件”是指使用一个或更多个处理器实现的硬件部件。类似地,本文描述的方法可以至少部分地由处理器实现,其中特定的一个或多个处理器是硬件的示例。例如,方法的操作中的至少一些操作可以由一个或更多个处理器或者处理器实现的部件来执行。此外,一个或更多个处理器还可以进行操作以支持“云计算”环境中的相关操作的执行或作为“软件即服务”(SaaS)操作。例如,操作中的至少一些操作可以由计算机组(作为包括处理器的机器的示例)执行,其中,这些操作能够经由网络(例如,因特网)并且经由一个或更多个适当的接口(例如,API)进行访问。某些操作的执行可以分布在处理器之间,不是仅驻留在单个机器内,而是跨多个机器部署。在一些示例实施方式中,处理器或处理器实现的部件可以位于单个地理位置中(例如,在家庭环境、办公室环境或服务器群内)。在其他示例实施方式中,处理器或处理器实现的部件可以跨若干地理位置分布。

[0105] 该上下文中的“处理器”是指根据控制信号(例如,“命令”、“操作码”、“机器码”等)操纵数据值并且产生相对应的输出信号的任何电路或虚拟电路(通过在实际处理器上执行的逻辑模拟的物理电路),该输出信号被用于操作机器。例如,处理器可以是CPU、RISC处理器、CISC处理器、GPU、DSP、ASIC、RFIC或其任何组合。处理器还可以是具有两个或更多个可以同时执行指令的独立处理器(有时称为“核”)的多核处理器。

[0106] 该上下文中的“时间戳”指的是识别某个事件何时发生,例如,给出日期和一天中的时间,有时精确到几分之一秒的编码信息或字符的序列。

[0107] 在不脱离本公开内容的范围的情况下,可以对所公开的实施方式进行改变和修改。这些和其他改变或修改旨在被包括在如在所附权利要求中被表达的本公开内容的范围内。此外,在前述具体实施方式中,可以看到的是,出于使本公开内容精简的目的,各种特征在单个实施方式中被组合在一起。本公开内容的方法不被解释为反映如下意图:所要求保护的实施方式需要比在每个权利要求中明确列举的特征更多的特征。相反,如所附权利要求所反映的,发明主题可以以少于单个公开的实施方式中的所有特征而呈现。因此,所附权利要求由此被并入具体实施方式中,其中每个权利要求自身独立地作为单独的实施方式。

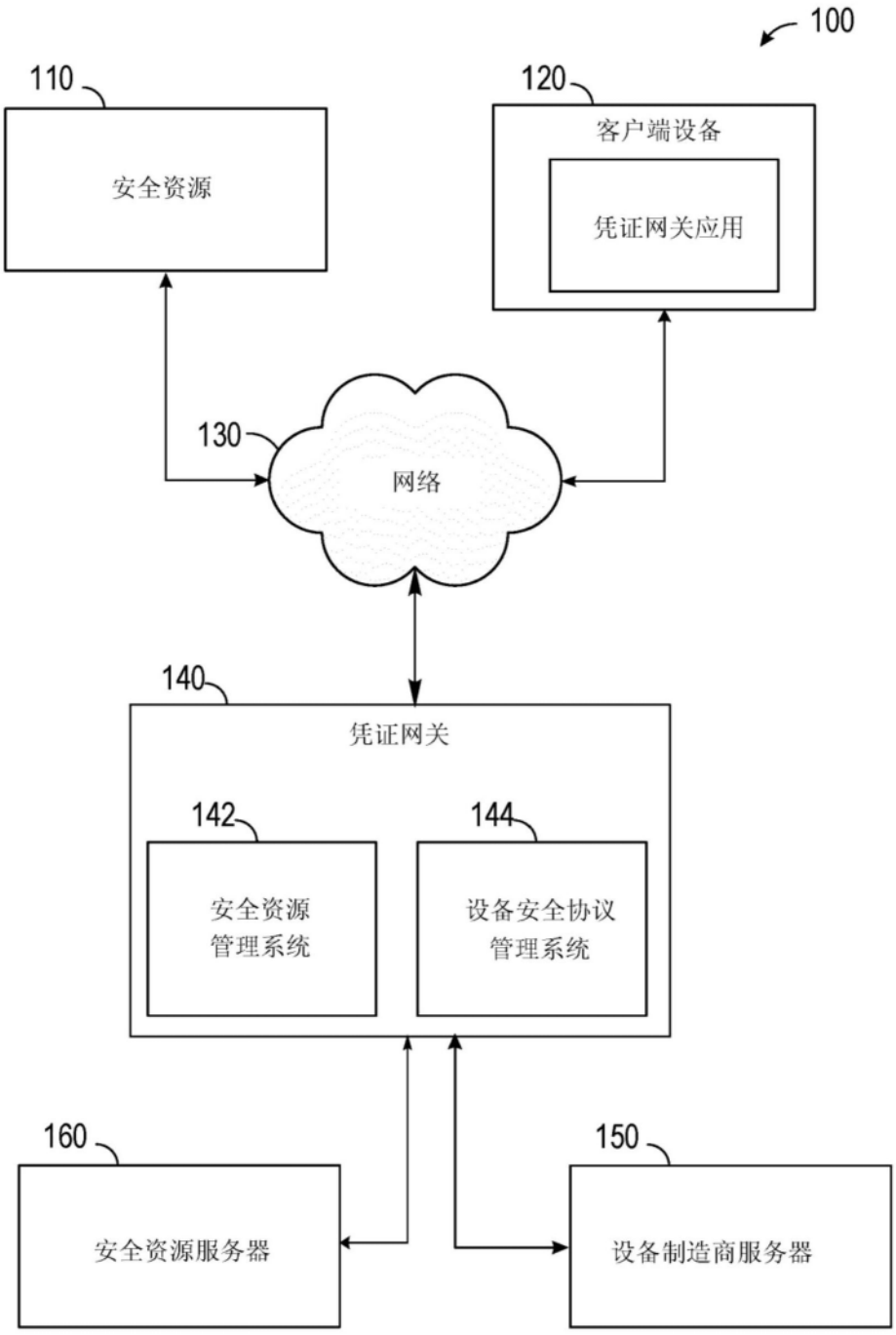

100
110
安全资源
120
客户端设备
凭证网关应用
130
网络
140
凭证网关
142
安全资源
管理系统
144
设备安全协议
管理系统
160
安全资源服务器
150
设备制造商服务器

图1

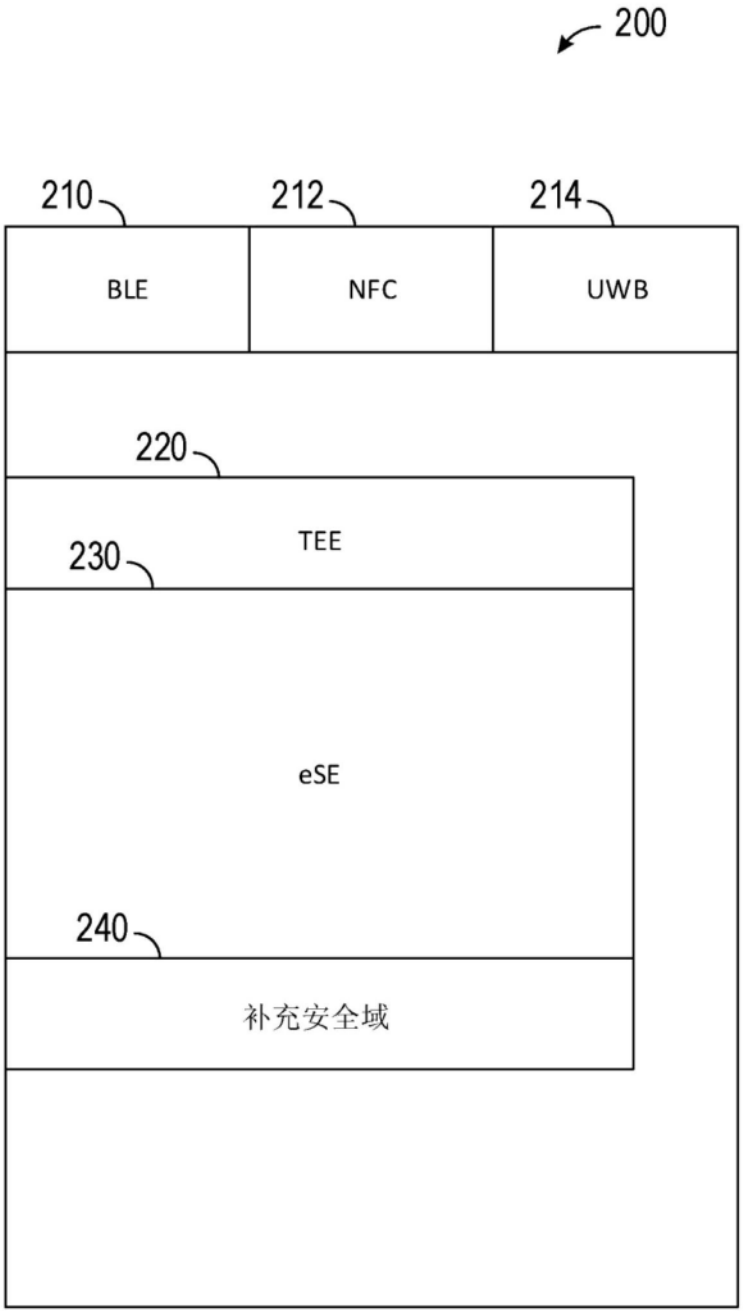


图2

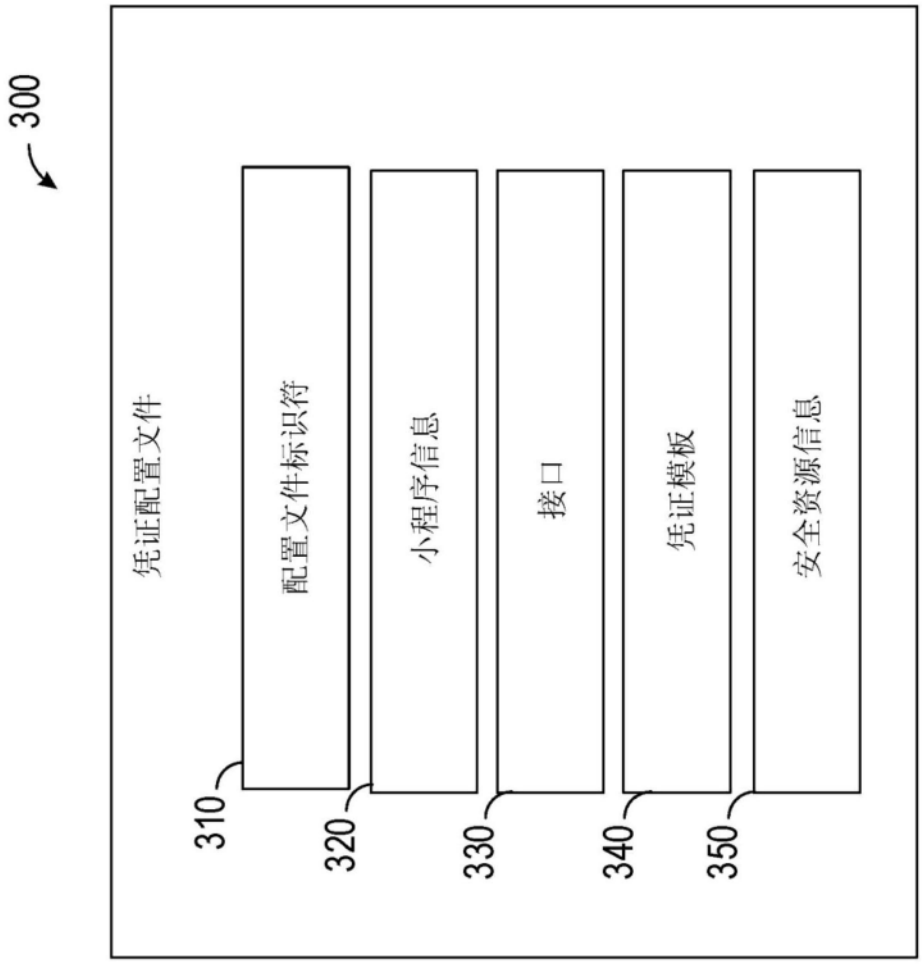


图3

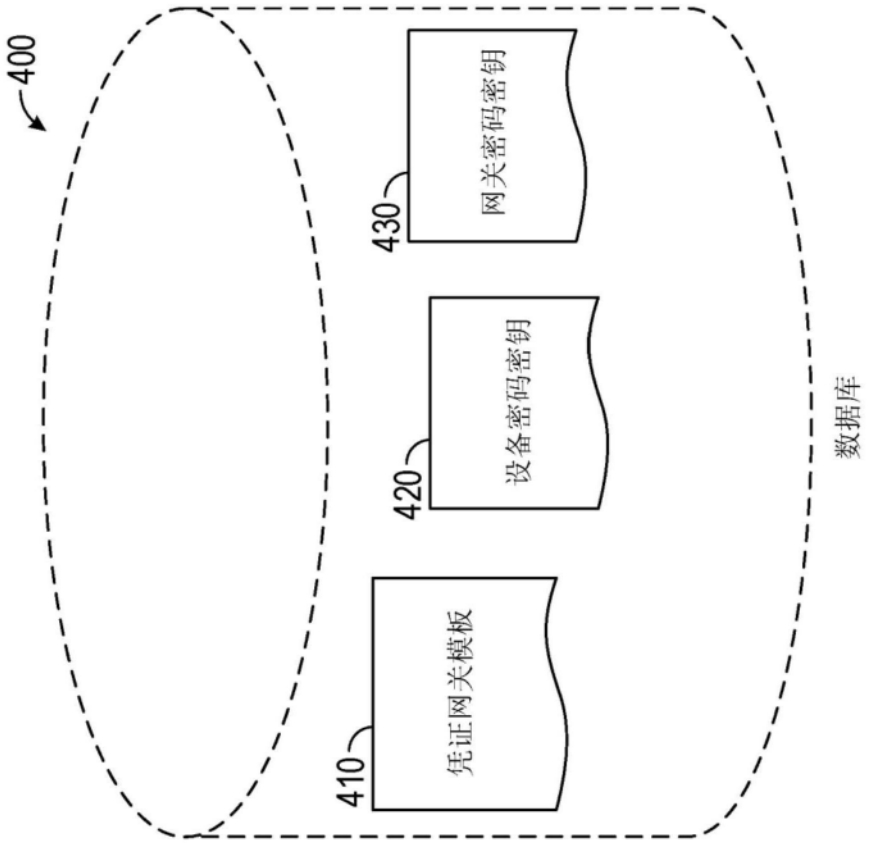


图4

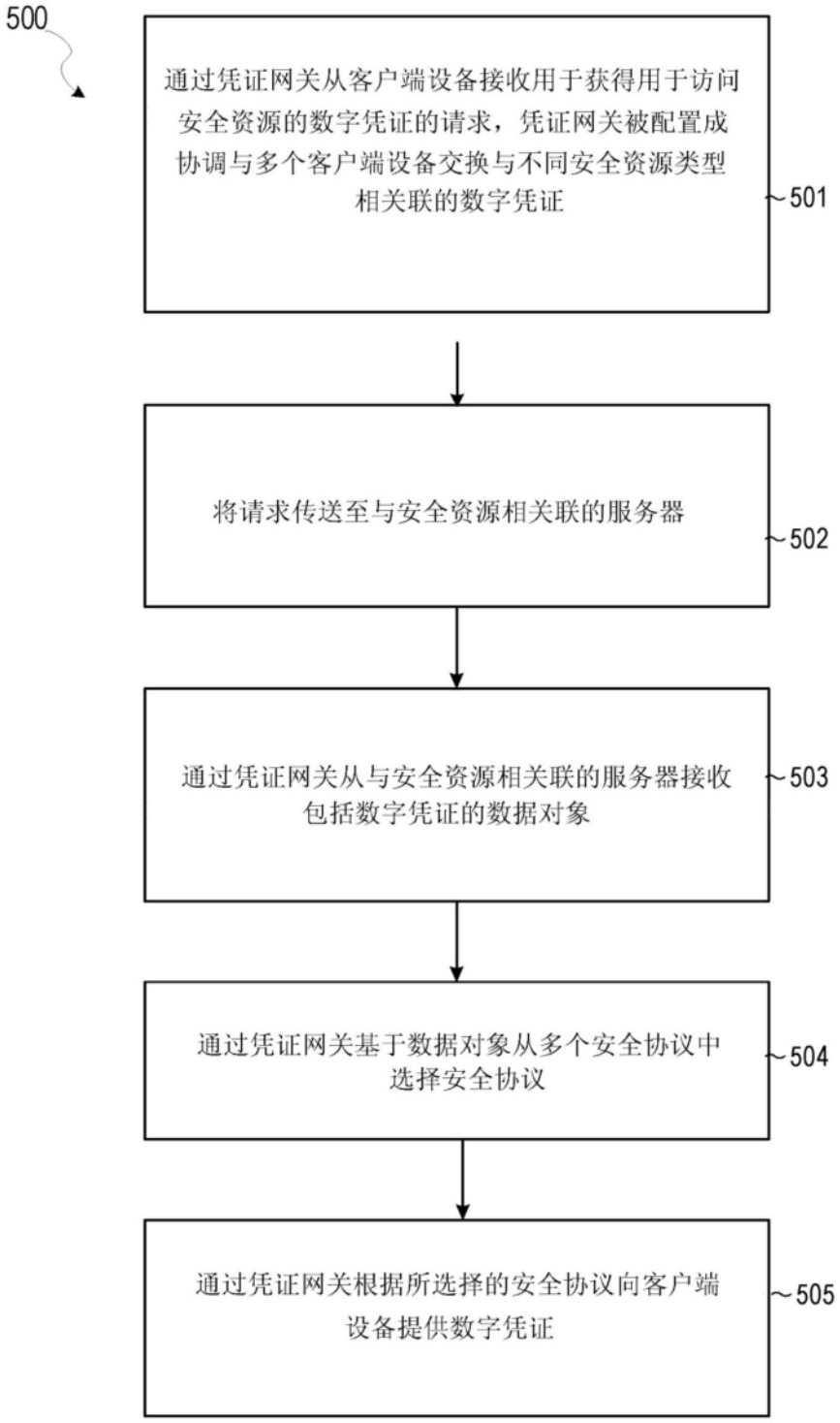

500
通过凭证网关从客户端设备接收用于获得用于访问安全资源的数字凭证的请求，凭证网关被配置成协调与多个客户端设备交换与不同安全资源类型相关联的数字凭证
501
将请求传送至与安全资源相关联的服务器
502
通过凭证网关从与安全资源相关联的服务器接收包括数字凭证的数据对象
503
通过凭证网关基于数据对象从多个安全协议中选择安全协议
504
通过凭证网关根据所选择的安全协议向客户端设备提供数字凭证
505

图5

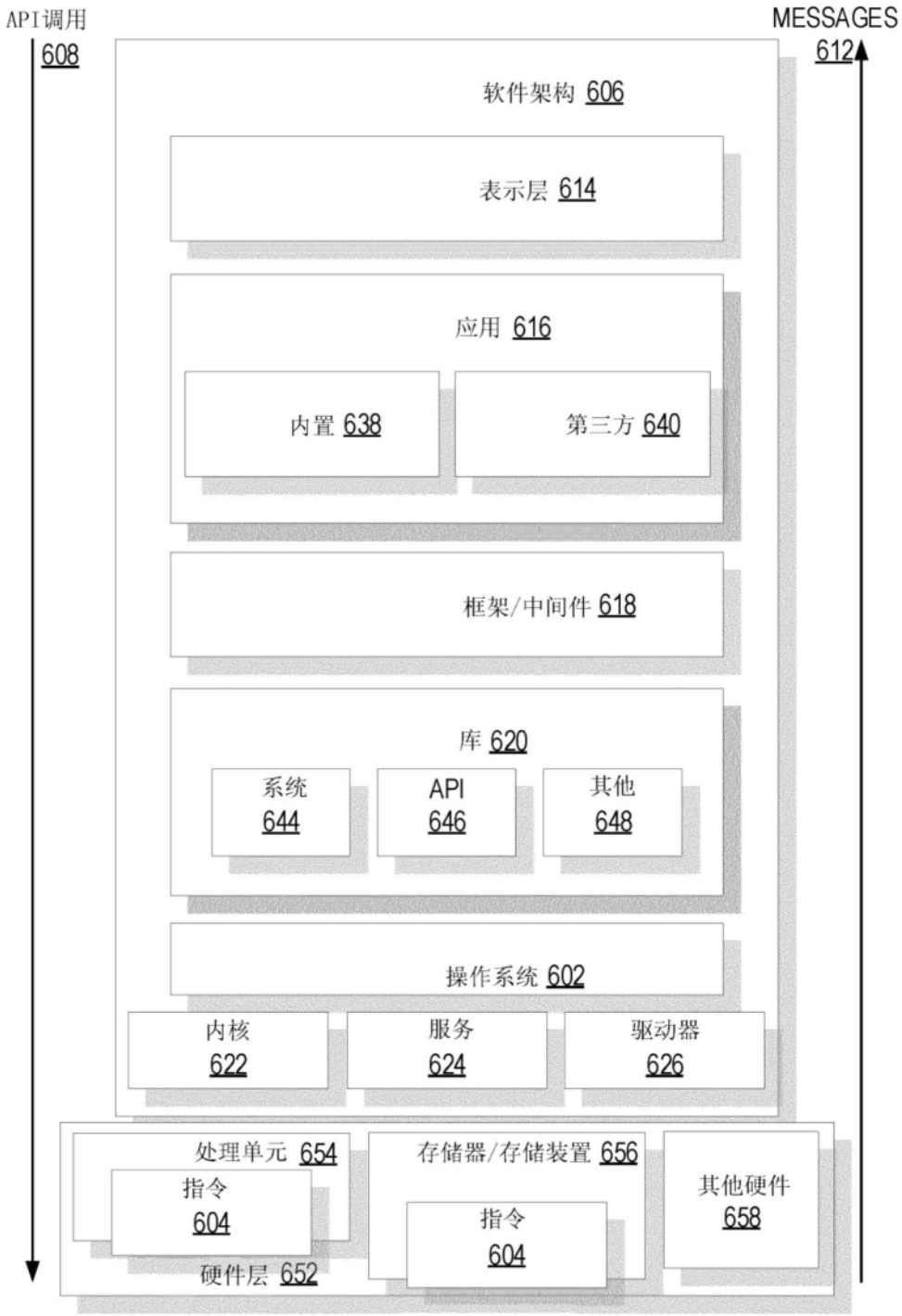

API调用
608
MESSAGES
612
软件架构 606
表示层 614
应用 616
内置 638
第三方 640
框架/中间件 618
库 620
系统
644
API
646
其他
648
操作系统 602
内核
622
服务
624
驱动器
626
处理单元 654
指令
604
硬件层 652
存储器/存储装置 656
指令
604
其他硬件
658

图6

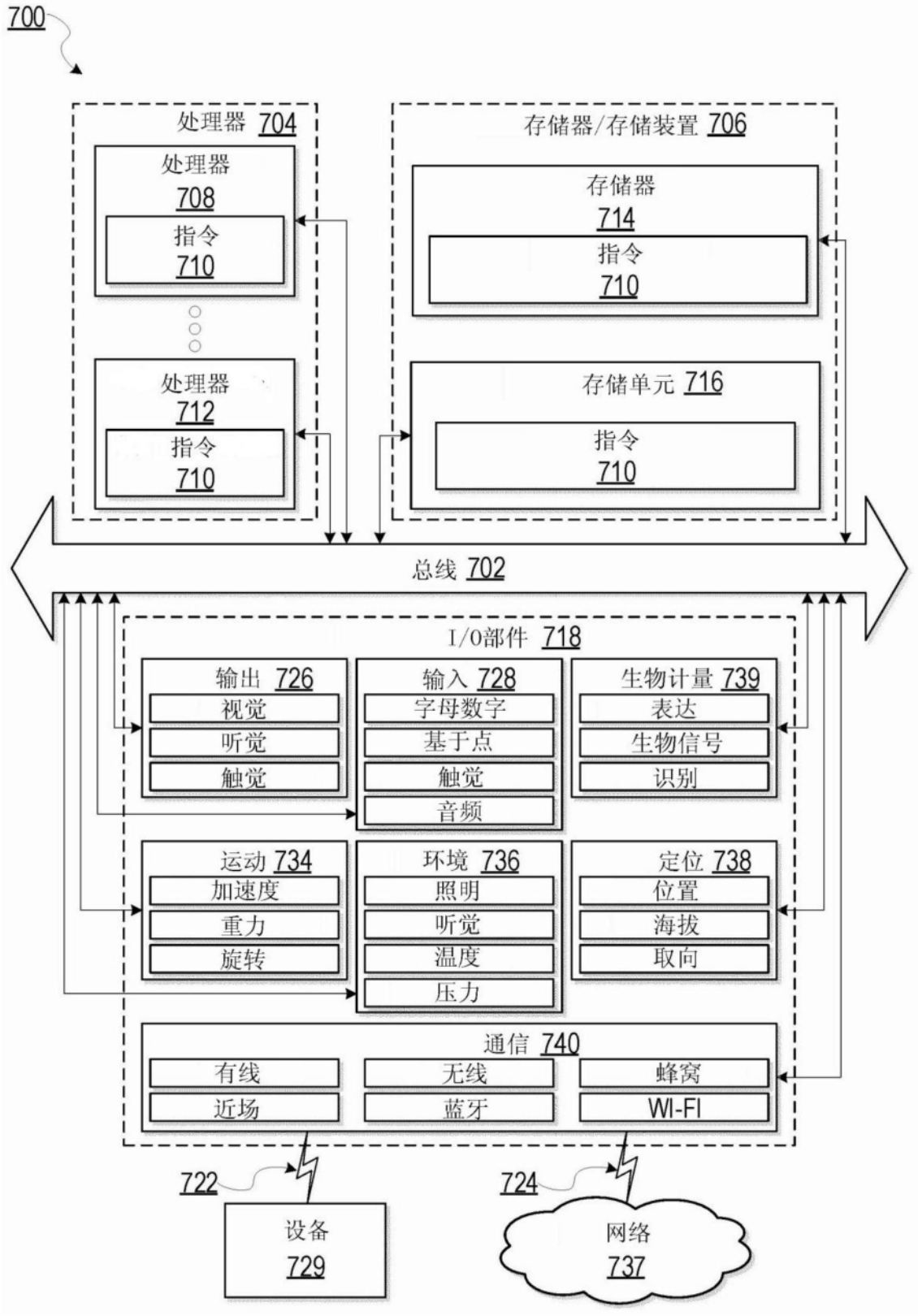

700
处理器 704
处理器
708
指令
710
处理器
712
指令
710
存储器/存储装置 706
存储器
714
指令
710
存储单元 716
指令
710
总线 702
I/O部件 718
输出 726
视觉
听觉
触觉
输入 728
字母数字
基于点
触觉
音频
生物计量 739
表达
生物信号
识别
运动 734
加速度
重力
旋转
环境 736
照明
听觉
温度
压力
定位 738
位置
海拔
取向
通信 740
有线
无线
蜂窝
近场
蓝牙
WI-FI
722
设备
729
724
网络
737

图7