(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115037496 A
(43)申请公布日 2022.09.09

(21)申请号 202210203542.3

(22)申请日 2022.03.03

(30)优先权数据
63/156,228 2021.03.03 US
17/485,201 2021.09.24 US

(71)申请人 美光科技公司
地址 美国爱达荷州

(72)发明人 J•C•夏纳 L•W•多弗
O•杜瓦尔

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

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/08(2006.01)
G06F 21/72(2013.01)
G06F 21/79(2013.01)
G06F 21/62(2013.01)

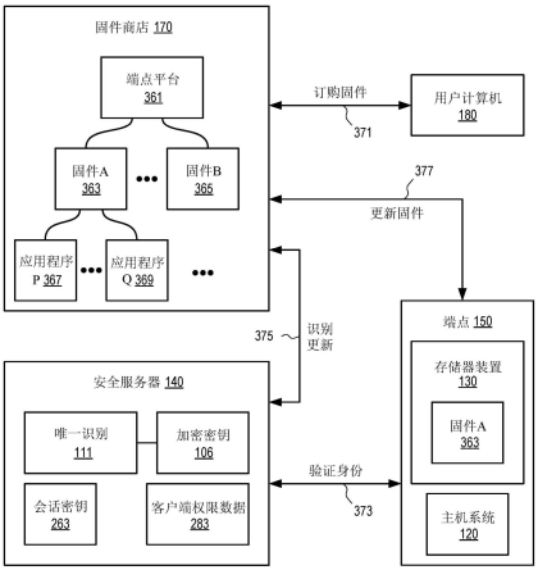
权利要求书3页 说明书60页 附图26页

(54)发明名称

经由在线固件商店的端点定制

(57)摘要

本申请涉及经由在线固件商店的端点定制。服务器系统用于经由在线固件商店定制端点的固件并验证所述端点的真实性。例如,在使用所述端点之前,可以为所述端点订购固件的定制版本。在接收具有由在所述端点中配置的存储器装置生成的身份数据的请求之后,所述服务器系统可基于所述存储器装置的秘密而确定具有当前固件的所述端点的真实性。识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的固件的更新。所述服务器系统生成可在所述存储器装置中执行以执行所述更新的命令的验证码。在接收到所述命令和所述验证码之后,所述存储器装置验证所述验证码以确定是否执行所述命令以用于固件更新。



CN 115037496 A

1.一种方法,其包括:

在服务器系统中从端点接收具有由在所述端点中配置的存储器装置生成的身份数据的请求;

响应于所述请求并基于所述存储器装置的秘密和所述身份数据,通过所述服务器系统确定所述端点的真实性;

基于在线固件商店,识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的第一固件的更新;

响应于确定所述端点是真实的,通过所述服务器系统生成能够在所述存储器装置中执行以执行所述更新的命令的验证码;以及

通过所述服务器系统向所述存储器装置提供所述验证码,其中所述存储器装置配置成接收具有所述验证码的所述命令,并且所述存储器装置具有配置成在确定是否阻止所述存储器装置中所述命令的执行时验证所述验证码的访问控制器。

2.根据权利要求1所述的方法,其进一步包括响应于确定所述端点是真实的:

与所述在线固件商店通信以将数据下载到所述存储器装置中;

其中当所述命令在所述存储器装置中执行时,所述存储器装置使用所述数据执行所述更新。

3.根据权利要求2所述的方法,其中所述数据包含第二固件,在执行所述命令之后,所述第二固件替代经执行以生成所述请求的所述第一固件。

4.根据权利要求2所述的方法,其中所述数据包含固件应用程序,在执行所述命令之后,所述固件应用程序利用经执行以生成所述请求的所述第一固件运行。

5.根据权利要求4所述的方法,其中在执行所述命令之后,所述固件应用程序和所述第一固件的组合提供所述端点的第二固件。

6.根据权利要求2所述的方法,其中在执行所述命令之后,所述端点经由第二固件配置成在所述更新之前提供在运行所述第一固件的所述端点中没有的功能。

7.根据权利要求6所述的方法,其进一步包括:

在所述请求之前,在所述固件商店中接收所述端点的固件订单;

其中所述更新基于所述订单而识别。

8.根据权利要求7所述的方法,其中所述订单在所述固件商店中接收而不通过所述端点。

9.根据权利要求7所述的方法,其中所述订单使用所述端点的公共识别针对所述端点识别;并且所述身份数据包含所述公共识别。

10.根据权利要求9所述的方法,其中在执行所述命令之后,所述存储器装置配置成使用加密密钥生成所述端点的身份数据,所述加密密钥至少部分地基于所述秘密和存储于所述存储器装置中的所述第二固件而生成。

11.根据权利要求10所述的方法,其中在安全设施中完成所述存储器装置的制造之后,所述存储器装置不将所述秘密传送到所述存储器装置之外。

12.根据权利要求11所述的方法,其进一步包括:

基于确定所述端点的所述真实性,建立会话密钥。

13.根据权利要求12所述的方法,其中所述存储器装置配置成基于以所述会话密钥为

基础配置的访问控制密钥来验证所述验证码。

14.根据权利要求12所述的方法,其进一步包括:

在所述安全设施中制造所述存储器装置期间寄存所述秘密;以及

至少部分地基于所述秘密,生成验证所述身份数据的加密密钥。

15.根据权利要求14所述的方法,其中用于验证所述身份数据的所述加密密钥进一步基于在所述主机系统的启动时间从所述存储器装置的主机系统接收的数据而生成。

16.一种计算系统,其包括:

存储器,其存储存储器装置的加密密钥;以及

至少一个处理器,其经由一组指令配置成:

从端点接收具有由在所述端点中配置的存储器装置生成的身份数据的请求;且

响应于所述请求:

基于所述存储器装置的秘密和所述身份数据,确定所述端点是真实的;

经由在线固件商店识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的第一固件的更新;且

生成能够在所述存储器装置中执行以执行所述更新的命令的验证码,其中所述在线固件商店配置成将所述命令和所述验证码传输到所述端点,其中所述存储器装置配置成接收所述命令和所述验证码,并且其中所述存储器装置配置成在确定是否阻止所述存储器装置中所述命令的执行时验证所述验证码。

17.根据权利要求16所述的计算系统,其中所述端点的所述真实性至少部分地基于所述存储器装置的安全特征而确定;并且其中所述安全特征包含:

至少部分地基于所述存储器装置的所述秘密和当前在所述存储器装置中配置以供所述端点执行的固件,生成表示所述端点的身份的加密密钥;以及

基于由加密密钥表示的权限,控制在所述存储器装置中执行的命令。

18.根据权利要求17所述的计算系统,其中所述更新基于在所述请求之前在所述固件商店中接收的固件订单而识别;其中所述固件订单使用也包含在所述身份数据中的公共识别针对所述端点识别;并且其中所述安全特征进一步包含经由所述存储器装置中的逻辑电路实施的加密引擎。

19.一种存储指令的非暂时性计算机存储媒体,所述指令在由服务器执行时使所述服务器执行方法,所述方法包括:

从端点接收具有由在所述端点中配置的存储器装置生成的身份数据的请求;以及

响应于所述请求:

基于所述存储器装置的秘密和所述身份数据,确定所述端点是真实的;

经由在线固件商店识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的第一固件的更新;以及

生成能够在所述存储器装置中执行以产生所述更新的命令的验证码,其中在所述存储器装置接收所述命令和所述验证码之后,所述存储器装置在确定是否在所述存储器装置中执行所述命令时验证所述验证码。

20.根据权利要求19所述的非暂时性计算机存储媒体,其中所述方法进一步包括:

对于与所述端点分开的计算机,在所述请求之前在所述在线固件商店中接收订单,其

中所述更新基于所述订单针对所述端点识别。

经由在线固件商店的端点定制

[0001] 相关申请

[0002] 本申请要求2020年于10月26日提交且标题为“虚拟订户识别模块和虚拟智能卡(Virtual Subscriber Identification Module and Virtual Smart Card)”的第63/105,820号临时美国专利申请的提交日的权益,其中本申请还要求于2021年3月3日提交且标题为“经由在线固件商店的端点定制(Endpoint Customization via Online Firmware Store)”的第63/156,228号临时美国专利申请的提交日的权益,所述申请的全部公开内容由此以引用的方式并入本文中。

[0003] 本申请涉及于2020年8月28日提交且标题为“用于主机装置验证的安全存储器系统编程(Secure Memory System Programming for Host Device Verification)”的第17/005,565号美国专利申请,所述申请要求以下申请的提交日的权益:2020年7月31日提交的第63/059,617号临时美国专利申请;于2020年10月26日提交且标题为“基于多个组件的启动时间绑定的端点认证(Endpoint Authentication based on Boot-Time Binding of Multiple Components)”的第17/080,684号美国专利申请;于2019年4月4日提交、标题为“用于生成装置身份以利用远程服务器认证的安全装置上的登入软件(Onboarding Software on Secure Devices to Generate Device Identities for Authentication with Remote Servers)”且于2020年10月8日公布为第2020/0322134号美国专利申请公开案的第16/374,905号美国专利申请;以及于2020年9月8日提交且标题为“半导体装置中的功能的客户特定激活(Customer-Specific Activation of Functionality in a Semiconductor Device)”的第17/014,203号美国专利申请,所述申请的全部公开内容由此以引用的方式并入本文中。

技术领域

[0004] 本文中所公开的至少一些实施例一般来说涉及认证,且更具体地但不限于网络中具有安全存储器装置的通信端点的认证。

背景技术

[0005] 存储器子系统可包含一或多个存储数据的存储器装置。存储器装置可以是例如非易失性存储器装置和易失性存储器装置。一般来说,主机系统可利用存储器子系统,将数据存储在存储器装置处并从存储器装置检索数据。

[0006] 用于装置身份合成引擎(DICE)和稳健物联网(RIoT)标准已经制定,用于基于加密计算的计算装置身份识别和认证的数据计算。

发明内容

[0007] 根据本申请的一个方面,提供一种方法。所述方法包括:在服务器系统中从端点接收具有由在所述端点中配置的存储器装置生成的身份数据的请求;响应于所述请求并基于所述存储器装置的秘密和所述身份数据,通过所述服务器系统确定所述端点的真实性;基

于在线固件商店，识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的第一固件的更新；响应于确定所述端点是真实的，通过所述服务器系统生成可在所述存储器装置中执行以执行所述更新的命令的验证码；以及通过所述服务器系统向所述存储器装置提供所述验证码，其中所述存储器装置配置成接收具有所述验证码的所述命令，并且所述存储器装置具有配置成在确定是否阻止所述存储器装置中所述命令的执行时验证所述验证码的访问控制器。

[0008] 根据本申请的另一方面，提供一种计算系统。所述计算系统包括：存储器，其存储存储器装置的加密密钥；以及至少一个处理器，其经由一组指令配置成：从端点接收具有由在所述端点中配置的存储器装置生成的身份数据的请求；且响应于所述请求：基于所述存储器装置的秘密和所述身份数据，确定所述端点是真实的；经由在线固件商店识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的第一固件的更新；且生成可在所述存储器装置中执行以执行所述更新的命令的验证码，其中所述在线固件商店配置成将所述命令和所述验证码传输到所述端点，其中所述存储器装置配置成接收所述命令和所述验证码，并且其中所述存储器装置配置成在确定是否阻止所述存储器装置中所述命令的执行时验证所述验证码。

[0009] 根据本申请的又一方面，提供一种非暂时性计算机存储媒体。所述非暂时性计算机存储媒体存储指令，所述指令在由服务器执行时使所述服务器执行方法，所述方法包括：从端点接收具有由在所述端点中配置的存储器装置生成的身份数据的请求；以及响应于所述请求：基于所述存储器装置的秘密和所述身份数据，确定所述端点是真实的；经由在线固件商店识别存储于所述存储器装置中且在所述端点中执行以生成所述请求的第一固件的更新；以及生成可在所述存储器装置中执行以产生所述更新的命令的验证码，其中在所述存储器装置接收所述命令和所述验证码之后，所述存储器装置在确定是否在所述存储器装置中执行所述命令时验证所述验证码。

附图说明

[0010] 在附图的各图中作为实例而非限制示出了实施例，在附图中，相似的参考标号指示类似的元件。

[0011] 图1示出根据本公开的一些实施例的实例计算系统。

[0012] 图2示出根据一个实施例的集成电路存储器装置中的身份数据的生成。

[0013] 图3示出根据一个实施例的用于控制存储器装置中的命令执行的技术。

[0014] 图4示出根据一个实施例的用于验证存储于存储器装置中的数据完整性的技术。

[0015] 图5示出根据一个实施例的基于在存储器装置中实施的安全特征提供给客户端服务器的安全服务器的安全服务。

[0016] 图6示出根据一个实施例的用于配置和认证基于卡的服务的端点的系统和方法。

[0017] 图7示出根据一个实施例的虚拟智能卡的卡简档。

[0018] 图8示出根据一个实施例的虚拟订户识别模块(SIM)的卡简档。

[0019] 图9示出根据一个实施例的用于认证存储器装置的技术。

[0020] 图10示出根据一个实施例的用于生成控制存储器装置的安全操作的命令的技术。

[0021] 图11示出根据一个实施例的虚拟智能卡的方法。

[0022] 图12示出根据一个实施例的基于存储器装置的安全特征提供的安全服务的方法。

[0023] 图13示出根据一个实施例的登入账户订阅的服务的端点的方法。

[0024] 图14示出根据一个实施例的使用在线固件商店的端点定制的技术。

[0025] 图15示出根据一个实施例的经由在线服务商店将服务定向到端点的技术。

[0026] 图16示出根据一个实施例的使用固件商店和安全服务器的固件更新方法。

[0027] 图17示出根据一个实施例的使用服务商店和安全服务器的端点定制方法。

[0028] 图18示出根据一个实施例的生成身份数据以促进完整性和/或端点活动的监测的图示。

[0029] 图19示出根据一个实施例的用于维持存储在端点中的包完整性的技术。

[0030] 图20示出根据一个实施例的基于跟踪端点活动而实施安全操作的系统。

[0031] 图21示出根据一个实施例的用于更新或修复存储在端点中的包的方法。

[0032] 图22示出根据一个实施例的用于基于端点的一或多个活动执行安全操作的方法。

[0033] 图23和24示出根据一个实施例的配置成在一组端点当中实施订阅共享的系统。

[0034] 图25示出根据一个实施例的用于促进一组端点中的订阅共享的方法。

[0035] 图26示出根据一个实施例的用于管理端点识别的技术。

[0036] 图27示出根据一个实施例的用于管理端点识别的方法。

[0037] 图28是其中可以操作本公开的实施例的实例计算机系统的框图。

具体实施方式

[0038] 本公开的至少一些方面涉及安全服务器和具有安全特征的存储器装置。安全服务器配置成基于存储器装置的安全特征提供计算机网络(例如,互联网)中的在线安全服务。存储器装置的主机系统可使用存储器装置的存储器和/或存储功能存储指令和/或用于处理的数据并存储处理结果。

[0039] 一般来说,存储器子系统可包含存储装置和/或存储器模块。主机系统可使用包含一或多个组件的存储器子系统,所述组件例如存储数据的存储器装置。主机系统可提供数据以存储于存储器子系统中,并且可请求数据以从存储器子系统检索。

[0040] 例如,存储于存储器装置中的数据的一部分可以是指令,例如经编程用于软件、固件、启动加载程序、操作系统、例程、装置驱动程序、应用程序包等的指令。指令可以存储用于计算装置,所述计算装置使用与存储器装置连接的主机系统实施。

[0041] 存储于存储器装置中的数据的另一部分可以在指令执行于主机系统的一或多个处理装置中时向指令提供运算元或输入。

[0042] 存储于存储器装置中的数据的又一部分可包含从使用存储于存储器装置中的输入和/或其它输入执行指令生成的结果。

[0043] 此类计算装置的实例包含个人计算机、移动计算机、平板计算机、个人媒体播放器、智能电话、智能TV、智能扬声器、智能电器、物联网(IoT)装置等。

[0044] 在存储器装置中实施的安全特征可用于存储器装置和安全服务器之间经由计算机网络的安全通信。存储器装置和安全服务器之间的通信路径可能不安全。通过安全服务器和存储器装置之间的通信可以验证存储器装置的身份和/或控制对存储器装置的访问,以便防止和检测仿冒、篡改、窃用和/或不安全操作。

[0045] 存储器装置的安全特征和安全服务器的安全服务的组合允许存储器装置和/或具有存储器装置的计算装置的使用所涉及的各方信任计算装置和/或存储器装置的真实性并信任存储于存储器装置中的数据完整性,例如将在计算装置中执行的指令和指令的输入。

[0046] 例如,安全服务器和存储器装置可以组合实施订户身份模块(SIM)的替换。

[0047] SIM卡通常用于表示电信网络中的蜂窝服务的订户身份。当SIM卡插入到蜂窝电话中时,蜂窝电话可以访问提供给订户账户的蜂窝服务;并且当SIM卡插入到替代蜂窝电话中时,订户可以使用替代蜂窝电话访问与账户相关联的蜂窝服务。

[0048] 当安装于蜂窝电话中的存储器装置的身份可以安全地配置成表示订户身份时,可以消除对物理SIM卡的需要。存储器装置的身份可经由存储器装置的安全特征和安全服务器的安全服务配置和保护。

[0049] 一般来说,安全服务器可以配置于互联网上以基于构建到存储器装置中的安全特征向第三方计算机和服务器提供安全相关服务。安全特征构建并封装到存储器装置中。安全特征和安全服务可以在不信任安装了存储器装置的计算装置的安全实施方案的情况下使用。因此,安全实施方案可以集中在存储器装置的安全特征和安全服务器的设计中。通过简单地使用具有安全特征的存储器装置,使用存储器装置的计算装置的安全性可以得到提高,而无需计算装置的设计者和/或制造商付出太多的努力。

[0050] 安全服务器可以提供服务,以验证装置的身份和/或真实性,检测仿冒装置和/或篡改装置,跟踪和管理装置所有权,促进装置所有权/控制权的转移,促进计算装置访问第三方服务器和/或服务网络的服务的配置,等等。

[0051] 存储器装置的安全特征可以在存储器装置的制造期间实施于存储器装置的集成电路(IC)封装内。存储器装置可具有在一或多个集成电路裸片上形成的逻辑电路(或控制器)和存储器单元。存储器装置中的至少一些存储器单元可以是非易失性的,使得数据可以保存在非易失性存储器单元中,即使存储器装置断电很长一段时间(例如,数日、数月,甚至数年)。存储器装置的非易失性存储器可用于存储指令和数据以用于存储器单元的主机系统的操作。

[0052] 存储器装置可具有唯一装置秘密(UDS)。唯一装置秘密可在存储器装置内受保护,使得在完成存储器装置的制造之后,唯一装置秘密不传送到存储器装置之外,并且不可被主机系统经由存储器装置的任何接口读取。

[0053] 存储器装置中的唯一装置秘密的存在可由安全服务器通过加密计算验证,例如加密密钥的生成、使用加密函数的消息散列值的生成及使用加密密钥通过消息加密的消息密文的生成。

[0054] 使用加密密钥加密消息的加密计算涉及用于表示消息的密文的计算。消息可以通过执行预定义解密计算使用对应加密密钥从密文有效恢复。在不具有用于解密的对应加密密钥的情况下,从密文恢复消息一般是不可行的。在不了解用于解密的对应加密密钥的情况下恢复消息的难度等级表示加密计算的安全等级。安全等级大体上取决于用于加密的加密密钥长度和用于加密的算法。

[0055] 当使用对称加密时,用于解密的加密密钥和用于加密的加密密钥是相同的。当使用不对称加密时,解密密钥和加密密钥不同,并且成对生成。所述对中的一个可用作私钥,且因此用作秘密;对中的另一个可用作公钥。从公钥计算私钥一般是不可行的。从公钥恢复

私钥的难度等级表示不对称加密的安全等级。

[0056] 对消息进行散列的加密计算将消息映射到表示消息的散列值。但是，在散列计算中会丢失一定量的信息，使得消息无法从散列值恢复。许多消息可以映射到相同散列值。生成可以散列到相同散列值的消息的经修改版本一般是不可行的，特别是在经修改版本类似于原始消息时。

[0057] 密钥生成的加密计算涉及基于一组数据计算针对对称加密的加密密钥或针对不对称加密的一对加密密钥。在不具有相同一组数据的情况下生成相同密钥或相同密钥对的概率较低。概率等级表示用于密钥生成的加密计算的强度。

[0058] 一般来说，用于加密、散列和密钥生成的任何加密计算技术可以与存储器装置和安全服务器一起使用。因此，本公开不限于特定的加密、散列和/或密钥生成技术。

[0059] 除了唯一装置秘密之外，存储器装置还可存储额外数据以表示存储器装置和/或安装了存储器装置的计算装置的数据和/或硬件配置。所述额外数据的一部分可以也可以不保持为存储器装置的秘密。所述唯一装置秘密和所述额外数据可用于生成表示存储器装置和/或计算装置的身份的秘密加密密钥。

[0060] 存储器装置的逻辑电路(或本地控制器)可实施加密引擎、身份引擎和访问控制器。存储器装置的加密引擎配置成在存储器装置内执行加密计算(例如，散列、加密/解密、密钥生成)以支持身份引擎和访问控制器的操作。存储器装置中的加密引擎的实施方案免去了依赖外部处理器来进行存储器装置的安全计算的需要，并因此通过防止秘密传输到存储器装置之外和防止加密计算的篡改和窃用而提高了安全性。任选地，存储器装置的安全特征所涉及的加密计算的至少部分可以经由在存储器装置中存储指令以供存储器装置的主机系统执行来实施，同时在存储器装置的逻辑电路(或本地控制器)的安全等级和复杂度之间存在一定水平的权衡。

[0061] 存储器装置的加密引擎可用于向消息应用加密散列函数以生成散列值，从一组数据生成对称加密密钥或一对不对称加密密钥，使用加密密钥生成消息的密文，和/或使用加密密钥从密文恢复消息。

[0062] 存储器装置的访问控制器配置成使用加密密钥控制在存储器装置中接收的命令的执行。例如，可能需要权限来请求存储器装置对存储器装置的非易失性存储器的各个部分执行读取、写入、删除、修改等的命令。权限可由相应加密密钥表示。在存储器装置中接收到权限命令以供执行之后，访问控制器可在确定命令是否来自具有表示权限的加密密钥的发送方时使用加密引擎以执行计算。在计算指示发送方具有加密密钥且因此具有权限之后，访问控制器允许命令装存储器装置内执行。否则，访问控制器可拒绝、忽略或舍弃命令。此类访问控制可防止对存储于存储器装置中的数据的未经授权的访问，防止对存储器装置的未经授权的改变，并防止篡改和/或窃用形成存储器装置的仿冒品和/或不安全装置。

[0063] 一般来说，验证消息发送方是否具有加密密钥涉及验证消息的验证码。验证码可呈散列摘要、数字签名、基于散列的消息认证码(HMAC)、加密消息认证码(CMAC)等形式。验证码使用加密密钥和作为散列、加密和/或其它计算等加密操作的输入的消息生成，使得在不具有加密密钥的情况下生成验证码及从消息的经修改版本生成验证码一般是不可行的。因此，当接收方确认接收到的验证码对接收到的消息和加密密钥有效时，接收方可得出结论：发送方具有对应的加密密钥，并且接收到的消息与用于生成接收到的加密密钥的消息

相同。

[0064] 在一些实施方案中，接收方使用与发送方生成验证码所使用的相同的加密密钥执行消息验证码的验证。例如，接收方使用相同加密密钥生成接收到的消息的验证码，并比较生成的验证码与接收到的验证码。如果存在匹配，那么接收到的验证码对接收到的消息有效；并且发送方可以被视为具有加密密钥。否则，接收到的验证码对接收到的消息无效；接收到的消息自验证码生成以来已经改变，或接收到的验证码是使用不同的加密密钥生成的，或这两者。

[0065] 在一些实施方案中，接收方使用密钥对中的公共加密密钥执行消息验证码的验证；并且发送方使用密钥对中的私用加密密钥生成验证码。例如，验证码可通过向消息应用散列函数以生成消息的散列值来生成。通过使用加密密钥执行的散列值加密获得的散列值的密文可用作验证码。消息和验证码的接收方使用对应的解密密钥执行验证，解密密钥在使用对称加密时与加密密钥相同，在使用不对称加密时是密钥对中的另一密钥。在使用解密密钥从密文恢复散列值之后，恢复后的散列值可与接收到的消息的散列值比较；如果存在匹配，那么接收到的验证码对接收到的消息有效；否则，接收到的验证码对接收到的消息无效。替代地，接收方可使用加密密钥执行验证而不执行解密。接收方可使用加密密钥生成消息的验证码以与接收到的验证码比较。

[0066] 在一些实施方案中，消息和加密密钥组合生成散列值作为验证码，如在基于散列的消息认证码(HMAC)的技术中。例如，加密密钥可用于生成两个密钥。在组合所述两个密钥中的一个与消息以生成通过密钥修改的消息之后，加密散列函数可应用于密钥已修改消息，以生成散列值，所述散列值进一步与另一密钥组合以生成另一消息。在向所述另一消息应用加密散列函数(或另一加密散列函数)之后，基于散列的消息认证码生成。消息接收方可使用相同的加密密钥生成接收到的消息的基于散列的消息认证码以与接收到的基于散列的消息认证码比较。如果存在匹配，那么验证成功；否则，验证失败。

[0067] 一般来说，用于生成和验证来自发送方的消息的验证码和供发送方用于生成验证码的加密密钥的任何技术可用于确定发送方是否具有加密密钥。接收方将使用适当的加密密钥执行验证，此加密密钥可与用于生成验证码的加密密钥相同，或在相同的不对称加密密钥对中。因此，本公开不限于散列摘要、数字签名和/或基于散列的消息认证码的特定技术。

[0068] 为方便起见，使用加密密钥真的消息生成的用于表示消息和加密密钥的验证码可以统称为使用加密密钥签名的消息的数字签名，但是应理解，验证码可使用各种技术生成，例如基于散列的消息认证码。

[0069] 存储器装置可配置成存储用于验证使用配置成表示请求存储器装置执行命令的权限的加密密钥签名的验证码的相关加密密钥。

[0070] 例如，访问控制器可向存储器装置的所有者提供一组权限，使得所有者可以激活或撤销激活存储器装置的一或多个安全特征，改变存储器装置的一或多个安全设置、参数、配置或偏好，和/或从存储器装置中不可被存储器装置的其他用户读取的区段读取数据。

[0071] 例如，访问控制器可向存储器装置的经授权用户提供读取、写入、擦除或修改存储器装置的特定区段的特定权限。

[0072] 当存储器装置接收需要访问权限来执行的命令时，访问控制器可检索对应的加密

密钥以验证包含所述命令的消息的验证码或数字签名。如果针对接收到的命令接收的验证码的验证成功，那么接收到的命令被视为来自具有表示在存储器装置中执行命令的权限的加密密钥的发送方。作为响应，访问控制器允许在存储器装置中执行命令。否则，访问控制器阻止命令的执行。

[0073] 存储器装置可以制造为最初由安全服务器拥有。随后，安全服务器可以在从组装到计算装置的存储器装置到具有由终端用户使用的存储器装置的计算装置的处理中，向一或多个所有者和用户提供和/或转移部分或全部权限。访问控制器可以防止篡改、窃用和未经授权的访问，同时提供灵活性，以支持不同所有者和用户的不同权限转移模式，例如安装了存储器装置的组件计算装置的制造商，安装了组件计算装置的计算装置制造商、零售商、企业用户、终端用户和替代终端用户等。

[0074] 存储器装置的身份引擎配置成生成指示存储器装置的身份和/或安装了存储器装置的计算装置的身份的数据。为生成身份数据，身份引擎使用加密引擎从唯一装置秘密和存储于存储器装置中和/或由存储器装置收集(例如，在计算装置的启动过程期间)的其它数据生成秘密加密密钥。存储器装置中的秘密加密密钥的存在可被视为存储器装置拥有唯一装置秘密和用于生成秘密加密密钥的其它数据的证据。存储器装置中的秘密加密密钥的存在可以通过安全服务器经由使用秘密加密密钥签名的验证码或数字签名来验证。

[0075] 在存储器装置的制造期间，唯一装置秘密的副本寄存在安全服务器中和/或进行安全共享而不会暴露。随后，安全服务器配置成独立于存储器装置导出相同秘密加密密钥(和/或使用不对称加密时的对应公钥)，而无需存储器装置将其唯一装置秘密传送到存储器装置之外。因此，安全服务器可通过验证存储器装置具有秘密加密密钥而验证存储器装置具有唯一装置秘密；并且作为存储器装置身份的秘密加密密钥可在存储器装置集成到组件、装置、系统中并在制造商、零售商、经销商、公司和/或终端用户当中转移的处理中改变。在不改变唯一装置秘密的情况下，由秘密加密密钥表示的存储器装置实体可以更新以表示存储器装置组装到组件、装置、系统中、定制和/或个性化和/或由不同实体或用户拥有和/或操作。

[0076] 可以执行加密操作和通信以允许安全服务器验证存储器装置具有秘密加密密钥。

[0077] 例如，存储器装置呈现的用于验证的身份数据可包含示出存储器装置的公共识别的消息。公共识别可用于分辨存储器装置与其它存储器装置。身份数据可包含使用秘密加密密钥签名的身份数据中的消息的验证码或数字签名。身份数据包含消息副本和验证码或数字签名。一旦验证码和消息数据被安全服务器验证，安全服务器就可得出结论：在身份数据中提供的公共识别是真实的，并且身份数据来自具有秘密加密密钥的存储器装置。

[0078] 存储器装置的秘密加密密钥可以不仅使用存储器装置的唯一装置秘密而且还使用表示存储器装置和/或安装了存储器装置的计算装置的一些方面的额外数据来生成。所述额外数据可以表示软件、固件、启动加载程序、应用程序、存储于存储器装置中的跟踪数据、在计算装置的最近启动时间在计算装置中的计算装置组件的标识符。如果所述额外数据已经更改，那么身份引擎生成更改后的秘密加密密钥。因此，使用更改后的秘密加密密钥生成的验证码无法通过在安全服务器处执行的验证。因此，由身份引擎生成的验证码的验证还验证存储器装置和安装了存储器装置的计算装置的硬件/软件/数据合成的完整性和真实性。

[0079] 存储器装置和/或其主机系统的身份的验证可检测仿冒、篡改及被盗/丢失装置。基于来自所有者的请求，安全服务器可将被盗/丢失装置配置成以数个降级模式中的一个操作，例如不可启动、不可读、加密/擦除非易失性存储器中的数据、存储器装置的存储器/存储功能的自我毁坏等等。

[0080] 安全服务器配置有信息数据库，用于验证由存储器装置的身份引擎生成的身份数据。数据库允许安全服务器生成存储器装置的对应秘密加密密钥(和/或使用不对称加密时的对应公钥)。加密密钥可由安全服务器生成，而无需存储器装置在存储器装置的制造之后将其唯一装置秘密传送到存储器装置之外。加密密钥可至少部分地基于在存储器装置制造之后可用的额外数据生成。

[0081] 安全服务器可存储表示存储器装置的所有者权限的加密密钥。使用加密密钥，安全服务器可生成转移存储器装置所有权并配置和/或转移选定权限使得选定命令在存储器装置中执行的命令。在报告计算装置丢失/被盗之后，安全服务器可检测其存储器装置在存储器装置验证期间的使用，以及第三方服务器对服务的请求。

[0082] 例如，当第三方服务器从具有存储器装置的计算装置接收对服务的请求时，第三方服务器将由存储器装置生成的身份数据从计算装置转发到安全服务器以用于验证。如果身份数据被安全服务器验证，那么第三方服务器可向计算装置提供服务；否则，服务请求可被拒绝、舍弃或忽略。

[0083] 当经授权方请求时，安全服务器可对命令进行签名或生成命令的验证码以准许或取消对存储器装置的非易失性存储器的访问。经授权方可签名的命令转发到存储器装置以用于执行。签名的命令包含具有命令的消息和使用表示在存储器装置中执行命令的权限的加密密钥签名/生成的消息的验证码。

[0084] 存储器装置可以安装于计算装置中作为计算装置的身份的部分，并为计算装置提供主存储器/存储容量。例如，将在计算装置中执行的指令和相关联数据可以存储于存储器装置中，并经由存储器装置的安全特征受保护而不被损坏、篡改和/或窃用。因为由存储器装置的身份引擎生成的身份数据至少部分地基于存储于存储器装置中的指令/数据，所以将供计算装置使用的指令和数据的完整性和/或真实性至少在验证存储器装置和/或计算装置的身份的过程期间验证。

[0085] 安全服务器所提供的安全服务解除了第三方服务器对操作和计算装置的安全保护。使用存储器装置和安全服务器的服务可以防止未经授权的访问，而无需计算装置制造商和第三方服务器的运营商付出很大努力。因此，第三方服务器可以在不损害安全性的情况下利用其提供各自服务的核心能力进行操作。

[0086] 第三方服务器可以使用安全服务器提供的服务向其订户提供服务，而无需订户执行手动操作来配置订户使用的计算装置。例如，订户可以使用计算装置访问订户账户中的已订阅蜂窝服务，而无需将物理SIM卡插入计算装置和/或执行其它操作来定制计算装置以使用订户账户访问。

[0087] 订户可以由账户识别表示。当订户购买计算装置时，计算装置的所有权可通过安全服务器转移给订户。在计算装置中配置的存储器装置的安全特征可用于生成装置身份。当计算装置连接到第三方服务器以获得服务时，第三方服务器请求安全服务器验证装置身份。基于计算装置的所有权和账户的所有权，计算装置可以动态地链接到账户，使得计算装

置能够使用账户访问第三方提供的服务，而无需手动操作来配置计算装置。

[0088] 例如，在验证计算装置的身份期间，通过安全服务器的所有权管理服务识别计算装置的所有者/订户。一旦识别了所有者/订户，订户识别就可以构建到计算装置的装置身份中，或与安全服务器的数据库中的装置身份相关联。随后，当验证装置身份时，订户账户中的服务可由第三方提供到计算装置，而不需要订户明确地将服务定向/请求到计算装置。

[0089] 任选地，计算装置可以与第三方服务器建立单独的证书，使得在计算装置每次连接到第三方服务器以获得服务时，第三方服务器无需联系安全服务器。

[0090] 图1示出根据本公开的一些实施例的实例计算系统。

[0091] 在图1中，集成电路存储器装置130具有如上文所论述的安全特征。

[0092] 安全存储器装置130可存储唯一装置秘密101用于其认证。在一个实例中，唯一装置秘密101注入到安全设施中的存储器装置130中并存储在存储器装置130的寄存器中。在另一实例中，唯一装置秘密101可以从存储器装置130的物理不可克隆函数(PUF)获得。唯一装置秘密101可以经由安全设施获得并寄存在安全服务器140中。例如，安全设施可以是存储器装置(例如，130)的制造设施的部分。在存储器装置130制成和/或离开安全设施之后，存储器装置130中的唯一装置秘密101不可经由存储器装置130的任何接口(例如，主机接口147)访问。因此，在存储器装置130的制造之后，如存储器装置130中的唯一装置秘密101密封在存储器装置130的集成电路封装中。唯一装置秘密101的副本在安全服务器140内利用有力的安全措施(例如，使用硬件安全模块(HSM))来保护以防窃用和未经授权的访问。

[0093] 存储器装置130包含实施加密引擎107的逻辑电路或本地控制器。加密引擎107可执行加密计算，例如散列、密钥导出、加密和/或解密，而不依赖于存储器装置130之外的处理能力，例如主机系统120的处理装置118。

[0094] 例如，根据装置身份合成引擎(DICE)和稳健物联网(RIoT)标准指定的方法或另一方法，加密密钥105可在启动时间基于唯一装置秘密101和在存储器装置130的存储器单元103中存储和/或获得的装置信息121的组合而生成。装置信息121可包含非秘密数据，它可以通过安全服务器140和存储器装置130之外的实体获得。为了提高安全性，装置信息121可包含时间相关信息。

[0095] 例如，加密密钥105可包含两对不对称加密密钥。第一对不对称密钥被称为装置识别密钥；并且第二对不对称密钥被称为别名密钥。私有装置识别密钥用于认证别名密钥的真实性，且因此减少其使用并降低其风险。别名密钥可用于更多事务/通信；并且别名密钥的替换可比装置识别密钥更频繁，以便提高安全性，因为别名密钥的使用频率更高，因此存在风险。例如，私有装置识别密钥可以在启动时间生成并用于对证书进行签名，例如别名公钥的证书；然后，立即从存储器装置130删除私有装置识别密钥以保护其机密性。

[0096] 一般来说，使用唯一装置秘密101和装置信息121生成的加密密钥105中的一个可用作将由安全服务器140验证的存储器装置130的秘密和身份。

[0097] 例如，存储器装置130的认证可以通过验证存储器装置130具有秘密加密密钥105来执行。存储器装置130中具有秘密加密密钥105可以被视为存储器装置130具有唯一装置秘密101并存储非秘密数据的未篡改版本的证据。

[0098] 使用加密引擎107，存储器装置130可证明存储器装置130具有秘密加密密钥105，而无需将秘密加密密钥105和/或唯一装置秘密101传送到存储器装置130之外。例如，存储

器装置130可使用秘密加密密钥105对证书或消息进行数字签名，以提供消息的验证码和秘密加密密钥105。当安全服务器140验证验证码成功时，安全服务器140可得出结论：存储器装置130具有秘密加密密钥105且因此具有由唯一装置秘密101表示的身份。

[0099] 存储器装置130包含可用于从主机系统120接收命令的主机接口147。主机系统的控制器116可向存储器装置130发送命令以请求从存储器单元103读取数据、将数据写入到存储器单元103中、从存储器单元103的一部分擦除数据、修改存储器单元103的一部分中的数据、激活存储器装置130的安全特征、配置与存储器装置130中的安全特征相关的参数等等。命令中的至少一些需要由存储在安全服务器140中的加密密钥106表示的权限。具有可用于对命令进行签名的加密密钥106被认为指示具有请求存储器装置130执行命令的权限。

[0100] 存储器装置130包含访问控制器109，其配置成使用加密引擎107验证使用表示与命令相关联的权限的加密密钥106生成的验证码。如果命令接收有有效验证码，那么访问控制器109允许存储器装置130执行命令；否则，命令可被拒绝、忽略或舍弃。

[0101] 当制造存储器装置130时，一或多个相关加密密钥105存储于存储器装置130中以向安全服务器140提供所有者权限。使用所有者权限，安全服务器140可对用于在存储器装置130中执行的命令进行签名以激活或撤销激活安全特征、触发作为存储器装置130的身份的秘密加密密钥的替换、替换供访问控制器109用于验证针对存储器单元103的一或多个区域在存储器装置130中执行一或多个命令的权限的加密密钥，等等。

[0102] 任选地，在认证经授权请求者的身份之后，安全服务器140可使用加密密钥对命令进行签名，以生成命令的验证码或数字签名，使得请求者可以向存储器装置130的主机接口147发送带验证码的命令，使得命令得以在存储器装置130内执行。

[0103] 任选地，安全服务器140可通过替换存储器装置130中的加密密钥105向实体提供特定权限，或向实体提供表示权限的对应加密密钥106。

[0104] 通常，存储器装置130连接到主机系统120以形成例如互联网的通信网络110中的端点150。一般来说，端点150是计算装置。端点150的实例包含个人计算机、移动计算机、个人媒体播放器、平板计算机、智能电话、智能TV、智能扬声器、智能电器、物联网(IoT)装置等。

[0105] 存储器装置130的存储器单元103可提供存储/存储器容量供主机系统120存储用于实施端点150的功能的指令和数据。例如，主机系统120的处理装置118配置成执行从存储器装置130加载的指令以启动和执行操作。

[0106] 主机系统120可包含网络接口114或另一通信装置，以与客户端服务器141、…、143中的一或多个通信，从而从客户端服务器141、…、143接收服务。

[0107] 从端点150发送到客户端服务器141的服务请求可包含由存储器装置130的加密引擎107生成的身份数据。客户端服务器141可请求安全服务器140验证身份数据中包含的验证码。

[0108] 除了认证存储器装置130的身份的服务之外，安全服务器140还可提供安全服务以管理操作存储器装置130、配置或改变存储器装置130的安全特征或设置、检测丢失/被盗装置、撤销激活丢失/被盗装置等等的权限。

[0109] 存储器装置130和/或端点150可具有非秘密的唯一识别111。唯一识别111可用于在一群存储器装置和/或端点中唯一地识别存储器装置130和/或端点150。

[0110] 例如,存储器装置130的唯一识别111可包含存储器装置130的制造商零件号(MPN)和/或存储器装置130的序列号。例如,存储器装置130的唯一识别111可包含至少部分地基于唯一装置秘密生成的一对不对称加密密钥中的公钥。

[0111] 为了认证存储器装置130和/或端点150具有由唯一识别111表示的身份,安全服务器140经由使用存储器装置的秘密加密密钥105签名的消息的验证码验证含有唯一识别111(和其它数据127)的消息。存储器装置130中的秘密加密密钥105使用存储器装置中的唯一装置秘密101生成;并且用于验证使用存储器装置130的秘密加密密钥105签名的验证码的对应加密密钥106在安全服务器140中从对应的唯一装置秘密101生成。

[0112] 用于证明存储器装置130的身份的存储器装置130的秘密加密密钥105可不仅基于唯一装置秘密101而且还基于存储器装置130可访问的装置信息121来生成。

[0113] 例如,装置信息121可包含存储于存储器单元103中的指令和/或数据的散列值。此外,装置信息121可包含存储到存储器单元103中的跟踪数据,用于在组装组件以构建端点150期间个性化/个人化存储器装置130和/或端点150。此外,装置信息121可包含端点150中的其它组件的识别信息,例如控制器116的识别、处理装置118的识别、网络接口114的识别、不存储于存储器装置130中的端点150的额外软件或数据包的识别,和/或配置成控制/操作存储器装置130的固件的识别和/或散列值。在启动时间期间,识别数据可以收集作为用于生成存储器装置130的秘密加密密钥105的装置信息121。

[0114] 在注册过程中,当存储器装置130配置成具有装置信息121时,装置信息121的副本上载到安全服务器140用于与存储器装置130和/或端点150的唯一识别111相关联。装置信息121的注册允许存储器装置130的身份链接到由唯一装置秘密101与装置信息121的组合表示的数据、软件和/或硬件配置。

[0115] 图2示出根据一个实施例的集成电路存储器装置中的身份数据的生成。例如,图2的技术可以在图1的计算系统中实施。

[0116] 在图2中,存储器装置130(例如,如图1中)的加密引擎107用于使用其唯一装置秘密101和装置信息121至少生成秘密密钥137。

[0117] 例如,当使用不对称加密时,秘密密钥137是加密密钥对135的私钥。相关联的公钥139与私钥一起使用加密引擎107生成。

[0118] 替代地,当使用对称加密时,秘密密钥137可在不具有公钥139且不具有密钥对135的情况下生成和使用。

[0119] 在一些实施方案中,生成和使用多个密钥对135。例如,当使用装置身份合成引擎(DICE)和稳健物联网(RIoT)方法时,第一对不对称密钥被称为装置识别密钥;并且第二对不对称密钥被称为别名密钥。私有装置识别密钥可用于认证别名密钥的真实性,然后立即从存储器装置130和/或端点150删除和清除以保护其机密性,特别是在私有装置识别密钥的生成或使用至少部分地发生在主机系统120中时。别名密钥可用于认证其它事务和/或通信。例如,私有装置识别密钥可在启动时间生成并用于对证书进行签名,例如别名公钥的证书,然后删除。在使用将私有装置识别密钥用作秘密密钥137签名的证书验证或确认存储器装置130的身份和公共别名密钥的真实性之后,私有别名密钥就可在后续操作中用作存储器装置130的秘密密钥137,直到端点150重启为止。

[0120] 例如,装置信息121的存储于存储器单元103中的数据123可包含将由连接到存储

器装置130的主机接口147的主机系统120的处理装置118执行的一组指令(例如,软件、固件、操作系统、应用程序)。

[0121] 例如,数据123可包含所述一组指令的加密散列值。例如,所述一组指令的已知散列值可存储于存储器单元103中;并且所述一组指令的当前散列值可经计算以与已知散列值比较。如果这两个散列值彼此一致,那么所述一组指令的完整性得以验证;并且所述一组指令的完整性的散列值可用作计算秘密密钥137的装置信息121的部分。

[0122] 替代地,存储于存储器单元103中的所述一组指令的当前散列值可在秘密密钥137的计算中直接使用。如果指令已改变(例如,由于数据损坏和/或篡改或窃用),那么安全服务器140对秘密密钥137的验证将失败。

[0123] 任选地,数据123可包含所述一组指令的识别,例如指令的源代码的散列值、由指令表示的软件/固件包的名称、包的版本号和/或发放日期等等。

[0124] 任选地,数据123可包含在构建和/或定制包含存储器装置130的端点150的过程期间存储到存储器单元103中的跟踪数据。例如,当存储器装置130组装到组件装置(例如,存储器子系统)中时,表示组件装置的制造商、组件装置的型号和/或组件装置的序列号的一条跟踪数据存储到存储器单元103中作为装置信息121的部分。随后,当组件装置组装到端点150中时,将一条跟踪数据添加到存储器单元中作为装置信息121的部分。可以将其它跟踪数据添加到存储器单元103中作为装置信息121的部分,以反映用于个性化存储器装置130的身份的存储器装置130的历史。

[0125] 任选地,装置信息121可进一步包含从连接到存储器装置130的主机接口147的主机系统120接收的数据125。

[0126] 例如,端点150可具有主机系统120和存储器装置130。主机系统120中的一些组件可以移除或替换。在启动端点150时,存储在存储器单元103中的指令的一部分经执行以收集关于在启动时间存在于主机系统120中的组件的数据125。因此,装置信息121可表示存储器装置130和/或端点150的软件/数据和硬件组合的特定配置。基于装置信息121和唯一装置秘密101生成的秘密密钥137表示具有所述特定配置的存储器装置130的身份。

[0127] 为了证明存储器装置130和/或端点150的身份,加密引擎107从消息131和秘密密钥137生成验证码133。

[0128] 如上文所论述,秘密密钥137和消息131的验证码133可以使用各种技术构造和/或验证,例如散列摘要、数字签名或基于散列的消息认证码、对称加密和/或不对称加密。因此,验证码133不限于特定实施方案。

[0129] 任选地,消息131可包含用户识别,例如名称、电子邮件地址、注册用户名称或其中生成身份数据113的端点150的所有者或授权用户的另一标识符。

[0130] 任选地,消息131的部分可以加密形式提供信息。例如,信息可以使用安全服务器140的公钥加密,使得信息不可被第三方访问。

[0131] 消息131可以是呈现存储器装置130和/或端点150的唯一识别111的证书。消息131可进一步呈现其它数据127,例如维持在存储器装置130中的计数器值、密码随机数和/或有关身份数据113的验证的其它信息。存储器装置130可单调地增加计数器值,以使具有较低计数器值的身份数据无效,以防重放攻击。

[0132] 在一些实施方案中,数据127可包含用于生成秘密密钥137的装置信息121的部分。

[0133] 在一些实施方案中，秘密密钥137是一对不对称密钥中的私有别名密钥。数据127包含呈现所述一对不对称密钥中的对应公共别名密钥的证书。呈现公共别名密钥的证书使用存储器装置130的装置识别密钥签名。公共别名密钥可用于验证消息131的验证码133和用作秘密密钥137的私有别名密钥。一旦安全服务器140验证呈现公共别名密钥的证书，所述证书使用存储器装置130的装置识别密钥签名并提供为数据127的部分，安全服务器140就可使用公共别名密钥验证使用私有别名密钥作为秘密密钥137签名的验证码133。在此实施方案中，安全服务器140可使用消息131中提供的公共别名密钥验证验证码133，而不必重新生成所述一对别名密钥；并且存储器装置130可使用安全服务器140尚未知晓的数据生成别名密钥对135。

[0134] 呈现公共别名密钥的证书可以图2中的方式生成和验证，其中秘密密钥137是使用装置信息121和唯一装置秘密101生成的装置识别密钥。任选地，存储器装置130初始地向安全服务器140提供具有公共别名密钥的证书。随后，存储器装置130可使用私有别名密钥作为秘密密钥137，且消息131中不包含公共别名密钥，或消息131中不包含公共别名密钥的证书。

[0135] 经签名以生成验证码133的消息131中的数据127可包含质询。例如，为了质询存储器装置130证明它拥有秘密密钥137，可以呈现随机数据项作为要使用秘密密钥137签名的数据127的部分。在一些实施方案中，单调增加的计数器值可用作质询。

[0136] 此外，验证存储器装置130的身份可包含使用多个秘密密钥和用秘密密钥签名的验证码。例如，装置识别秘密密钥可用于初始地建立别名秘密密钥的真实性和存储器装置130的身份；并且随后，别名秘密密钥可用于验证存储器装置130的身份的真实性。一般来说，装置识别秘密密钥和别名秘密密钥可以基于不对称加密或对称加密，因为安全服务器140可生成由存储器装置130生成的对应加密密钥。

[0137] 为了提高安全性，存储器装置130不使用存储器装置130之外的处理能力来生成秘密密钥137的副本，且不将秘密密钥137传送到存储器装置130之外。秘密密钥137的生成和使用是使用密封在存储器装置130内的加密引擎107的逻辑电路执行的。

[0138] 替代地，生成和使用秘密密钥137的操作的部分可以经由存储于存储器单元103中且加载到主机系统120的处理装置118中以供执行的一组指令实施。为了提高安全性，秘密密钥137不以明文跨主机接口147传送；并且指令可配置成在生成之后和/或在使用之后从主机系统120清除秘密密钥137。

[0139] 身份数据113可响应于存储器装置130通电、响应于在主机接口147中接收的请求和/或响应于端点150启动(例如，通过执行存储于存储器单元103中的启动加载程序)而生成。数据127可包含维持在存储器装置130中的计数值。当执行生成身份数据113的操作时，计数值增加。因此，具有某一计数值的某一版本的身份数据113使具有低于所述计数值的计数值的先前版本的身份数据113无效。

[0140] 图3示出根据一个实施例的用于控制存储器装置中的命令执行的技术。例如，图3的技术可以在图1的计算系统中实施并与图2的技术一起使用。

[0141] 在图3中，当主机系统120的控制器116向存储器装置130的主机接口147发送命令155时，访问控制器109确定命令155的发送方是否具有请求存储器装置130执行命令155的权限。

[0142] 加密密钥145配置成表示权限。命令155的发送方可从加密密钥145和含有命令155的消息151生成验证码153。

[0143] 如上文所论述，加密密钥145和消息151的验证码153可以使用各种技术构造和/或验证，例如散列摘要、数字签名或基于散列的消息认证码、对称加密和/或不对称加密。因此，验证码153不限于特定实施方案。

[0144] 访问控制器109使用对应的访问控制密钥149验证命令155的提交给主机接口147的验证码153。访问控制器109使用加密引擎107生成接收到的消息151和接收到的验证码153的验证结果159。基于验证结果159，访问控制器109可选择性地允许命令155在存储器装置130内执行或阻止命令155的执行。

[0145] 例如，访问控制密钥149可以是存储于存储器装置130中的加密密钥105中的一个。不同的访问控制密钥可用于控制用于执行不同命令和/或用于执行作用于存储器单元103的不同区段的命令的不同权限。

[0146] 例如，加密密钥145可以存储在安全服务器140中以向安全服务器140提供相关联的权限。

[0147] 在一个实施例中，安全服务器140配置成响应于实体请求验证码153以在存储器装置130中执行命令155而生成代表实体的验证码153。

[0148] 任选地，加密密钥145在验证使用秘密密钥137产生的身份数据113的过程中生成；并且在存储器装置130和安全服务器140之间已知的秘密(例如，秘密密钥137)允许会话密钥生成为加密密钥145，用来表示在具有时间限值的通信会话期间在存储器装置130中执行选定命令的权限。任选地，装置通电的时段可用作会话定界符，使得新计数值在下一功率循环期间生成，从而能够生成新的会话密钥。

[0149] 加密密钥145可配置成在验证身份数据113并建立会话密钥之后在短时间内有效。在安全服务器140验证实体有权在存储器装置130中运行命令155之后，安全服务器140可生成验证码153，并将验证码153提供到实体。然后，实体可将消息151和验证码153发送到主机接口147。一旦存储器装置130的访问控制器109使用加密引擎107和访问控制密钥149确定验证码153有效，验证结果159就准许存储器装置130执行接收到的命令155；否则，访问控制器109可拒绝或忽略所接收到的命令155。

[0150] 在另一实施例中，在安全服务器140在存储器装置130中配置访问控制密钥149之后，安全服务器140可向实体提供表示在存储器装置130中执行命令155的权限的加密密钥145。

[0151] 消息151可包含表示对执行命令155的请求的限制的数据157。

[0152] 例如，数据157可包含维持在存储器装置130内的执行计数值，使得针对较低计数生成的验证码无效。

[0153] 例如，数据157可包含针对执行命令155的请求的特定实例建立的密码随机数，使得验证码153无法重复用于另一实例。

[0154] 例如，数据157可包含其中验证码153有效的时间窗。

[0155] 例如，数据157可包含其中允许执行命令155的存储器区域的识别。

[0156] 例如，数据157可包含允许在存储器装置130中执行命令155的操作类型。

[0157] 图4示出根据一个实施例的用于验证存储于存储器装置中的数据完整性的技术。

例如,图4的技术可用于图1的存储器装置130,并且与图2和/或图3的技术结合使用。

[0158] 在图4中,存储器装置130在存储器单元103中不仅存储内容161,而且还存储内容161的散列值163。为确定内容161的完整性状态165,加密引擎107向内容161应用加密散列函数以生成内容161的当前散列值;并且加密引擎107比较当前散列值和所存储的散列值163以确定它们是否相同。如果相同,那么确认所存储的散列值163所需要的内容161的完整性。

[0159] 散列值163可以存储为用于生成秘密密钥137以验证存储器装置130的身份的装置信息121的部分。

[0160] 内容161和散列值163存储在存储器装置130的不同区段中。访问控制器109提供和/或施行不同水平的权限以访问内容161和散列值163。

[0161] 例如,端点150的制造商可将内容161存储到存储器单元103中,使得端点150中主机系统120的处理装置118可以在内容161中运行程序或例程以提供端点150的所设计功能。此外,制造商和/或安全服务器140可将散列值163存储到单独区段中以用于完整性检查。端点150的终端用户可访问和使用存储器单元中的内容161,但是无法访问散列值163。如果内容161被损坏或篡改,那么加密引擎107可以检测改变并生成完整性状态165,使访问控制器109阻止内容161的使用。当制造商具有更新版本的内容161(或替换)时,制造商可在存储器单元103中执行更新,并发出带验证码153的命令155以更新散列值163。任选地,安全服务器140可响应于来自制造商的请求而生成验证码153。

[0162] 存储器装置130中的装置信息121和加密密钥105可以存储在存储器装置130中的安全区段中,并经由访问控制器109通过表示为存储在安全服务器140中的加密密钥106的所有者权限受保护。

[0163] 不同秘密(例如,唯一装置秘密101、秘密密钥137)和内容(例如,装置信息121、内容161)可以不同安全等级和/或使用用来平衡安全性和实用性的不同安全策略受保护。

[0164] 唯一装置秘密101可在存储器装置130中以最高安全等级受保护。例如,一旦存储器装置130离开存储器装置的制造安全设施和/或在完成存储器装置130的制造操作之后,唯一装置秘密101不可经由去往主机接口147(和/或存储器装置130的任何接口)的命令改变。优选地,唯一装置秘密101在用于表示存储器装置130和/或端点150的身份的秘密密钥(例如,137)的生成期间仅可由加密引擎107访问。例如,唯一装置秘密101可配置成在端点150启动时仅在有限时间内可用。

[0165] 例如,装置识别密钥可经由最小化其使用而受保护。别名识别密钥的安全性比装置识别密钥更高,替换频率也更高。不同的操作和/或权限可用于替换装置识别密钥和别名识别密钥。

[0166] 图5示出根据一个实施例的基于在存储器装置中实施的安全特征提供给客户端服务器的安全服务器的安全服务。

[0167] 例如,图5中所示的安全服务可以基于图2、3和/或4中所示的安全特征在图1的计算系统中实施。

[0168] 在图5中,客户端服务器141配置成将服务提供到计算装置,例如图1中的具有连接到主机系统120的存储器装置130的端点150。

[0169] 为了向客户端服务器141请求服务,主机系统120(例如,运行从存储器装置130检

索的指令)请求存储器装置130的身份数据113。例如,身份数据113可以图2中示出的方式生成。

[0170] 主机系统120将身份数据113嵌入在传输到客户端服务器141的请求171中。

[0171] 为了确定端点150是否有权受到服务,客户端服务器141从请求171提取身份数据113并生成针对安全服务器140基于身份数据113提供安全服务的请求173。

[0172] 安全服务器140可执行身份数据113的验证,确定存储器装置130和/或端点150的真实性,并在响应174中向客户端服务器141提供结果。基于结果,客户端服务器141可向主机系统120提供响应172。

[0173] 例如,响应174可指示身份数据113是来自仿冒装置,还是来自其中与端点150和/或存储器装置130的身份相关的数据123或内容161已经更改、损坏、改变或篡改的装置,还是来自丢失或被盗装置。

[0174] 在一些实施方案中,请求173可识别要在存储器装置130中执行的命令155。在验证身份数据113并验证客户端服务器141和/或端点150请求命令155在存储器装置130内执行的权限之后,安全服务器140可使用加密密钥145生成命令155的验证码153,并在响应174中将验证码153提供到客户端服务器141。使用安全服务,客户端服务器141可以从与权限和表示权限的加密密钥145的管理相关联的安全负担中解脱出来。

[0175] 任选地,响应174可包含表示在存储器装置130中执行命令155的权限的加密密钥145。为了减小客户端服务器141的安全负担,加密密钥145可配置成在短时间内到期。

[0176] 任选地,当确定身份数据113与丢失或被盗装置相关联时,响应174可包含命令155和/或其验证码153,使得当命令155在存储器装置130中执行时,访问控制器109可以停用主机系统120可经由主机接口147访问的至少一些特征。

[0177] 例如,在存储器装置130中执行命令155之后,访问控制器109可配置成停用存储于存储器装置130的存储器单元103中的启动加载程序。

[0178] 例如,命令155可使访问控制器109阻止对存储器单元103的一或多个区段的访问。

[0179] 例如,命令155可使访问控制器109需要权限来访问存储器单元103的一或多个区段,所述权限由存储在安全服务器140中的新加密密钥106表示。

[0180] 例如,命令155可使访问控制器109通过清除用于解密存储在存储器单元的一或多个区段中的数据的解密密钥来破坏所述一或多个区段中的数据。

[0181] 例如,命令155可使存储器装置130执行自我毁坏,并不可逆地受损。

[0182] 从存储器单元103检索以在主机系统120中执行的指令可包含可接受命令155作为对存储器装置130提供身份数据113的响应的例程。在一些实施方案中,客户端服务器141可提供允许安全服务器140向存储器装置130发送命令155以供执行的连接。

[0183] 上文所论述的技术可用于实施认证服务订户的新方式。

[0184] 例如,存储器装置130可配置成以改进的安全性生成端点150的多因子装置平台身份。身份可通过组合以下来生成:存储器装置130的唯一装置秘密101、识别在端点150上运行以建立到服务或网络(例如,客户端服务器141或143)的安全连接的一或多个应用程序的平台源代码,和网络接口114或通信装置的唯一标识符。例如,唯一标识符可以是安装于端点150上以通过通信网络110通信的调制解调器的标识符。例如,多因子装置平台身份可至少部分地基于配置成访问蜂窝服务的端点150的国际移动设备身份(IMEI)编号。例如,当端

点150涉及车辆时，多因子装置平台身份可至少部分地基于车辆识别号(VIN)。此类有力的身份可在登入、云服务(例如蜂窝订阅服务)的网络访问和注册中与基于云的订户身份模块(SIM)函数结合使用。

[0185] 安全服务器140和存储器装置(例如，130)的安全特征可提供安全存储器装置技术平台。平台可配置成通过测量存储在安全存储器装置(例如，130)的存储器单元103中的数据来支持端点150的认证。端点的额外网络安全保护可以通过控制对存储在存储器装置(例如，130)中的内容161的访问来实现。访问控制可以通过安全硬件制造操作和基于密码的许可控制来实施，如上文结合图1到5所论述。配备有此类存储器装置(例如，130)的平台可到达足够的网络安全保护等级，以支持基于云的虚拟SIM解决方案并且不再需要端点150上的物理SIM卡访问蜂窝连接。

[0186] 安全存储器装置技术平台可包含安全存储器装置(例如，130)和满足DICE RIoT要求的软件的组合，用于生成使用安全存储器装置启动的端点(例如，150)的身份数据113。端点150的此类身份数据113基于用于启动端点150的安全存储器装置130的身份和其它因素生成。此类身份数据113可以在登入(例如，注册服务)期间传递到客户端服务器141上。客户端服务器141可与安全服务器140通信以确认端点150的身份。当身份数据113被验证时，客户端服务器141可信任端点150为真实的，且因此向端点150注册服务。

[0187] 例如，此类服务可以是通常注册到物理SIM卡的蜂窝连接。由安全存储器装置技术平台验证并通过安全登入保护的身份数据113可以以与使用物理SIM卡识别端点一样安全或更安全的方式提供端点(例如，150)的识别。基于云的虚拟SIM可以绑定到安全存储器装置技术平台在服务订阅生命周期内验证的身份数据113。

[0188] 通常，服务网络(例如，支付卡网络、蜂窝通信网络)可经由智能卡识别订户。传统智能卡被配置为嵌入在塑料卡中的集成电路芯片。智能卡中的集成电路芯片存储识别客户账户的数据，并且可以任选地存储与服务网络向账户提供的服务有关的数据。集成电路芯片可以通过配置在塑料卡和/或无线收发器的表面区域上的金属触点读取。

[0189] 例如，订户识别模块(SIM)(也被称为SIM卡)是一种智能卡。SIM卡通常用于移动电话中，以识别用于访问蜂窝通信网络服务的账户。当SIM卡附接到移动电话时，蜂窝通信网络根据SIM卡所识别的账户向移动电话提供服务。当SIM卡附接到替换移动电话时，替换移动电话可以访问为账户配置的服务。

[0190] 例如，SIM卡可存储移动订户身份，例如国际移动订户身份(IMSI)编号。移动/蜂窝网络运营商可以为IMSI编号和SIM卡分配认证密钥。SIM卡存储认证密钥。可以基于使用认证密钥签名的数字签名对SIM卡进行认证。在对SIM卡进行认证之后，具有SIM卡的移动电话可以在与移动订户身份相关联的账户中接收移动/蜂窝服务。

[0191] Europay MasterCard Visa(EMV)卡是智能卡的另一实例。EMV卡可用于在支付卡处理网络中接收金融服务，以访问银行账户，如借记账户和信用账户。

[0192] 集成电路存储器装置130可配置成防止对其存储器单元103的未经授权的访问，并确保存储器装置130本身和/或安装了存储器装置130的端点150的唯一身份。如图6所示，具有安全特征的安全存储器装置130可用于使用远程供应给安全存储器装置的数据和/或使用存储在安全服务器中的数据来实施诸如SIM卡和EMV卡等智能卡的功能。

[0193] 图6示出根据一个实施例的用于配置和认证基于卡的服务的端点的系统和方法。

[0194] 例如,图6的系统和方法可以使用图2到5的技术在图1的计算系统中实施。

[0195] 在图6中,存储器装置130可以使用具有图1到5的安全特征的集成电路存储器装置130实施。存储器装置130的访问控制器109可使用一或多个访问控制密钥213来控制访问存储器装置130中的至少一些存储器区域的读取和写入操作。

[0196] 例如,存储器装置130初始地制造有访问控制密钥213,允许安全服务器140能够完整访问存储器装置130中的存储器区域。存储器装置130进一步制造成包含在一群存储器装置中唯一地识别存储器装置130的装置身份数据211的至少一部分。

[0197] 例如,装置身份数据211可使用图2中示出的技术生成。

[0198] 例如,在存储器装置130的制造期间,在存储器注册231的操作中将存储器装置130的根秘密(例如,唯一装置秘密101)加载到安全服务器140中。根秘密可以是由存储器装置130的物理不可克隆函数(PUF)生成的数字,或者是在存储器装置130的制造期间选择并存储到存储器装置130中的随机数。安全服务器140可包含配置成管理安全存储器装置(例如,130)的加密密钥的密钥管理服务器。根密钥可被视为和/或用作秘密加密密钥。当制造存储器装置130时,可以从存储器装置130获得根秘密,或者将根秘密注入存储器装置130以用于存储器注册231。优选地,存储器装置130的制造使得在其制造之后,存储器装置130不在存储器装置130之外提供根秘密。

[0199] 装置身份数据211可以是不在存储器装置130之外公开、改变和提供的根秘密。

[0200] 在存储器装置130离开制造设施之后,装置身份数据211中的根秘密和其它秘密不可经由存储器装置130的通信接口(例如,主机接口147)获取。因为存储器装置130施行一组数据访问策略来防止秘密泄漏和存储在存储器装置130的访问受保护区域中的数据篡改,存储器装置130可被视为安全存储器装置。安全服务器140存储可模仿由存储器装置130执行以独立于存储器装置130生成派生秘密的计算的信息。因此,安全服务器140可重新生成存储器装置130的派生秘密,而无需存储器装置130经由其通信接口(例如,主机接口147)传送派生秘密。

[0201] 例如,存储器装置130的根秘密可以经由物理不可克隆函数(PUF)实施。存储器装置130的根秘密可以从存储器装置130检索并存储到安全服务器140中以用于存储器装置130制造期间的存储器注册231。根秘密可用于从装置身份数据211生成派生秘密。例如,PUF可用于导出迪菲-赫尔曼(Diffie Hellman)密钥对;并且迪菲-赫尔曼密钥对可用于创建可在装置和安全服务器之间安全共享的唯一装置秘密(UDS)101。

[0202] 例如,装置身份数据211可使用图2的技术生成。

[0203] 派生秘密以某一方式(例如,基于加密散列函数、随机数和/或单调计数值)生成,使得根秘密无法从派生秘密和/或用于生成派生秘密的其它信息计算出。例如,派生秘密可包含一对不对称加密密钥的私钥。例如,派生秘密可包含对称加密密钥。

[0204] 装置身份数据211可包含存储器装置130的非秘密公共识别号,例如存储器装置130的序列号、存储器装置130的唯一识别号和/或一对不对称加密密钥的公钥等等。公开识别号可用于在一群存储器装置中唯一地识别存储器装置130,而不泄露存储器装置130的秘密;并且存储器装置130的秘密可用于认证/确认存储器装置130是由公共识别号识别的。

[0205] 在存储器装置130离开制造设施之后,可以生成和/或替换装置身份数据211中的派生秘密。访问控制密钥213可用于控制生成和/或替换派生秘密以防篡改的操作的执行。

例如,派生秘密可包含根据装置身份合成引擎(DICE)标准生成的加密密钥和/或证书。

[0206] 在存储器注册231期间,至少存储器装置130的根秘密与存储器装置130的公共识别号相关联地存储到安全服务器140中。在存储器装置130的制造过程中,存储器装置130的根秘密在安全环境中在存储器注册231期间在存储器装置130和安全服务器140之间是已知的。随后,用于生成派生秘密的额外信息可以公开,而不损害派生秘密的保密性。派生秘密可用于存储器装置130的认证,并且可任选地替换。

[0207] 访问控制密钥213配置成防止对装置身份数据211中的秘密的未授权访问和/或操作。例如,一旦访问控制密钥213配置于存储器装置130中,秘密就限于供加密引擎107使用(例如,重新生成派生秘密和/或生成数字签名)。例如,在存储器装置130的主机接口147中接收的命令/请求需要以能够使用访问控制密钥213验证的方式进行数字签名,如图3中所示。如果应用在命令/请求上的数字签名根据访问控制密钥213无效,那么命令/请求可被拒绝和/或忽略。

[0208] 例如,访问控制密钥213可用于认证应用在命令上的数字签名以执行与装置身份数据211有关的特定操作,例如替换加密密钥或不对称加密密钥对。

[0209] 此外,一或多个额外访问控制密钥213可用于认证存储器装置130的所有者和/或经授权用户的数字签名。不同的经授权用户可限于访问存储器装置的不同区域进行特定操作(例如,写入、擦除、读取)。所有者和其他经授权用户可具有不同的范围和/或权限来操作存储器装置130。

[0210] 安全服务器140可配置为存储器装置130的初始所有者。例如,安全服务器140的公钥可初始地存储于存储器装置130中作为所有者访问控制密钥213,以提供针对使用安全服务器140的私钥签名的命令的所有者权限。在存储器装置130递送到客户之后,客户的公钥可以存储为所有者访问控制密钥213的替代,以将所有者权限转移到客户。

[0211] 任选地,存储器装置130的特定安全功能可为客户激活。与安全功能的激活有关的存储器装置130的一些方面可见于2020年9月8日提交且标题为“半导体装置中的功能的客户特定激活”的第17/014,203号美国专利申请,所述申请的全部公开内容由此以引用的方式并入本文中。

[0212] 端点150可构造成包含存储器装置130和其它组件187。在端点150的构造233期间,存储器装置130安装/组装到端点150中;并且软模块217和跟踪数据215可以存储到存储器装置130中。

[0213] 例如,软模块217可包含端点150的启动加载程序、存储器装置130和/或含有存储器装置130的存储器子系统的固件或端点150的操作系统或软件应用程序。软模块217可包含配置成实施功能的指令和数据。指令可由存储器装置130的逻辑电路、安装了存储器装置130的存储器子系统的控制器和/或存储器装置130和/或存储器子系统的主机系统120的处理装置118执行。

[0214] 在端点构造233期间,端点注册235可经执行以将跟踪数据215存储到安全服务器140和/或存储器装置130中。跟踪数据215可以作为端点150的配置和/或身份的部分。

[0215] 例如,跟踪数据215可包含使用加密散列函数计算的软模块217的散列值。例如,跟踪数据215可包含分配给端点150的秘密。

[0216] 端点150的仿冒品不具有跟踪数据215,它无法通过依赖于跟踪数据215的端点认

证239。因此，系统的安全性有所提高。与跟踪数据215有关的技术的其它细节和实例可见于2020年8月28日提交且标题为“用于主机装置验证的安全存储器系统编程”的第17/005,565号美国专利申请，所述申请的全部公开内容由此以引用的方式并入本文中。

[0217] 端点身份数据188可使用图2的技术生成，以表示端点150在其启动时间的配置。例如，端点身份数据188可包含基于装置身份数据211的一部分、跟踪数据215和在启动端点150时存在的其它组件(例如，网络接口114、处理装置118、控制器116)的识别数据的组合生成的证书(例如，消息131)。

[0218] 装置身份数据211和/或端点身份数据188可包含根据由可信计算小组(TCG)开发的标准使用装置身份合成引擎(DICE)生成的一或多个证书，所述标准组合硬件秘密和源代码形成了可信身份。用于生成装置身份的技术的其它细节和实例可见于2019年4月4日提交的标题为“用于生成装置身份以利用远程服务器认证的安全装置上的登入软件”且于2020年10月8日公布为第2020/0322134号美国专利申请公开案的第16/374,905号美国专利申请，所述申请的全部公开内容由此以引用的方式并入本文中。

[0219] 虚拟卡注册237的操作可经执行以将端点150配置用于基于卡的服务网络225的服务，例如移动/蜂窝通信网络、银行卡处理网络等。

[0220] 例如，端点150可以连接到卡服务器223，以请求由装置身份数据211表示的端点150的卡简档219。为了请求卡简档219，端点150将端点身份数据188的公共部分传输到卡服务器223。卡服务器223将端点身份数据188转发给安全服务器140，用于端点150的认证239。例如，可以使用结合图2论述的认证技术。

[0221] 一旦安全服务器140验证端点身份数据188是使用在端点注册235期间在安全服务器140中提交和/或记录的存储器装置130的装置身份数据211、跟踪数据215和端点150的其它数据的正确组合形成的，卡服务器223可以将卡简档219分配和/或存储到存储器装置130，或者将卡简档219与端点身份数据188相关联。

[0222] 虚拟卡注册237可以经由在存储器装置130中受保护的软模块217和/或经由安全管理器来执行，使得存储在存储器装置130中的卡简档219不能被篡改。任选地，安全服务器140可生成用于将卡简档219写入存储器装置130的安全区段中的命令155的验证码。可以经由存储在安全服务器140中的加密密钥来控制安全区段的写入权限。例如，访问控制器109可以使用与卡服务器223或安全服务器140相对应的访问控制密钥213来控制存储器装置130中的卡简档219的存储和/或替换。

[0223] 此外，存储器装置130可以图4中示出的方式验证卡简档和/或负责使用卡简档219的软模块217的完整性。

[0224] 当卡简档219在端点150中的存储器装置130中受保护时，存储器装置130和/或端点150可以以与安装在端点150中的对应智能卡等效的方式工作。安全地附接到装置身份数据211的卡简档219可以被视为虚拟智能卡。

[0225] 在一些实施方案中，软模块217配置成使用集成电路存储器装置130的逻辑电路的加密函数和/或处理能力来实施卡简档219的使用所涉及的加密操作。例如，卡简档219可包含认证密钥；并且软模块217可配置成生成用于认证/验证卡简档219包含认证密钥的数字签名。

[0226] 例如，卡简档219可如图7和图8中所示。

[0227] 图7示出根据一个实施例的虚拟智能卡的卡简档。

[0228] 在图7中，卡简档219可包含卡数据241和软卡模块243。任选地，软卡模块243可以安装为存储于存储器装置130中的软模块217的部分。

[0229] 卡数据241可包含智能卡(例如，虚拟卡)、账户和/或订户的识别。例如，卡数据241可识别智能卡的类型、账户/卡订阅的服务和/或与服务有关的客户数据(例如，余量、交易记录、消息等)。在一些实施方案中，卡数据241可包含存储在物理智能卡(例如，嵌入在根据通用集成电路卡(UICC)标准配置的塑料卡中的集成电路芯片)中的相同一组数据。

[0230] 软卡模块243可包含通过存储器装置130的加密引擎107对卡数据241进行操作的指令。例如，用于特定类型的智能卡的集成电路芯片的计算功能可以通过经由安全存储器装置130执行软卡模块243来实施。软卡模块243允许端点150模拟物理智能卡的计算操作。

[0231] 图8示出根据一个实施例的虚拟订户识别模块(SIM)的卡简档。

[0232] 在图8中，卡简档245包含卡数据241，例如集成电路卡标识符(ICCI)251、移动设备身份编号253、国际移动订户身份编号255、分配给国际移动订户身份编号255的认证密钥257，以及与国际移动订户身份编号255的移动/蜂窝通信服务有关的服务数据247。

[0233] 在使用传统SIM卡的传统移动电话中，集成电路卡标识符(ICCI)251用于在一群SIM卡中识别SIM卡。移动设备身份编号253(例如，以国际移动设备身份(IMEI)编号或IMEI软件版本(IMEISV)的形式)用于在一群移动电话中识别移动电话。国际移动订户身份(IMSI)编号用于在群体当中识别订户/客户/账户。当卡简档245附接到端点150时，卡简档245中的此类编号可用于类似功能。例如，当端点150是没有物理SIM卡的移动电话时，卡简档245可以用作虚拟SIM卡来识别卡、订户和端点/移动电话。例如，集成电路卡标识符(ICCI)251对应于和/或表示存储器装置130的装置身份数据211；移动设备身份编号253对应于和/或表示端点150的端点身份数据188；并且，国际移动订户身份编号255表示移动/蜂窝通信网络中的订户/客户/账户。

[0234] 例如，认证密钥257是分配给国际移动订户身份编号255的秘密。当端点150使用国际移动订户身份编号255来请求移动/蜂窝通信网络中的连接时，移动/蜂窝网络运营商可以从数据库中查找认证密钥257，并质询端点150以证明其拥有认证密钥257。安全质询可包含使用认证密钥257对包含随机数(RAND)的消息进行数字签名。对安全质询的回复可包含用于由移动/蜂窝网络运营商验证的数字签名的一部分。运营商使用与数据库中的国际移动订户身份编号255相关联的对应认证密钥257对消息进行独立签名。如果回复与移动/蜂窝网络运营商计算的应答一致，那么数字签名被验证；并且因此，端点150被认为具有分配给国际移动订户身份编号255的认证密钥257，并且有资格接收与国际移动订户身份编号255相关联的服务。此外，可以从数字签名导出对称加密密钥，用于在后续通信会话中保护端点150和移动/蜂窝通信网络之间的通信。

[0235] 例如，当卡简档245安装在端点150中时，端点150可以与移动/蜂窝网络运营商通信，以使用具有物理SIM卡的移动电话所使用的相同协议来请求连接并响应安全质询。因此，移动/蜂窝网络不必区分具有作为虚拟SIM卡的卡简档245的端点150和具有物理SIM卡的其它移动电话。

[0236] 任选地，卡简档245可包含认证模块259，其配置成由安全存储器装置130的加密引擎和/或端点150的处理装置118执行，以在使用卡简档245期间执行加密计算，例如为通信

会话生成对安全质询的回复和/或对称加密密钥。

[0237] 在图6中，在虚拟卡注册237之后，端点150可以使用卡简档219从基于卡的服务网络225接收服务以识别订户/客户/账户。例如，初始地配置成向传统智能卡提供服务的基于卡的服务网络225可以无缝地进一步向具有通过将卡简档(例如，219)存储在安全存储器装置(例如，130)中实施的虚拟智能卡的端点(例如，150)提供服务。

[0238] 任选地，端点150可配置成以与具有物理智能卡(例如，SIM卡)或智能卡(例如，EMV卡)的移动装置相同的方式执行与基于卡的服务网络225的通信。

[0239] 例如，端点150可以用作读卡器的智能卡。端点150可包含用于连接到读卡器的金属触点。例如，端点150可包含与无线智能卡的读卡器相当的收发器。替代地，可以在基于卡的服务网络225中配置额外的读卡器，以使用替代通信连接从端点150读取虚拟卡。替代连接的实例可包含近场通信(NFC)连接、蓝牙连接、Wi-Fi连接、通用串行总线(USB)连接等。

[0240] 在另一实例中，端点150可以用作移动站，其具有内置读卡器以读取插入移动站中的智能卡，例如具有SIM卡的移动电话。端点150可以使用具有物理SIM卡的移动站的相同通信协议与基于卡的服务网络225通信以访问服务227。

[0241] 任选地，卡简档219可以与端点身份数据188相关联地存储在卡服务器223中。端点150可以使用端点身份数据188访问基于卡的服务网络225中的服务227。作为响应，基于卡的服务网络225可以与卡服务器223通信以基于端点身份数据188识别卡简档219。此外，基于端点身份数据188，卡服务器223可以与安全服务器140通信以执行端点认证239，以验证端点150在虚拟卡注册时具有安全存储器装置130，并且具有由跟踪数据215、软模块217和组件187的组合表示的相同配置。当端点150被篡改和/或修改时，可以在状态检查229和/或端点认证239中检测到改变；作为响应，基于卡的服务网络225可以拒绝访问服务227的请求。

[0242] 任选地，可以结合访问服务227的请求及时执行虚拟卡注册237。响应于请求，通过端点认证239验证端点身份数据188。在端点验证成功之后，卡简档219可以将卡简档219与端点身份数据188相关联和/或存储到存储器装置130中。

[0243] 在一些实施方案中，卡服务器223被实施为安全服务器140的部分。

[0244] 在一些实施方案中，卡服务器223被实施为基于卡的服务网络225的网络运营商的部分。

[0245] 例如，图6的系统可用于简化、保护和加速物联网(IoT)装置和丰富的IoT服务生态系统的大规模全球部署。例如，虚拟订户身份模块(SIM)卡可由IoT装置(例如，端点150)使用，以通过移动/蜂窝通信网络连接到互联网。

[0246] 安全服务器140可用作诸如IoT边缘装置的端点(例如，150)的基于存储器的安全即服务平台。卡服务器可用于为此类端点提供蜂窝连接解决方案。如图6所示的组合可以创建一个通用的端到端解决方案，用于将蜂窝连接的IoT装置零接触登入到云服务上。

[0247] 企业IoT实施方案的复杂性给IoT装置的大规模全球部署带来了挑战。挑战包含在蜂窝连接和网络安全方面的实施困难。与无线局域网(例如，Wi-Fi)相比，蜂窝连接在IoT部署方面具有显著优势，例如更远的距离、更好的室外性能、更强的安全性和现有的全球基础设施。物理SIM卡的要求以及与移动/蜂窝网络运营商签订的合同减缓了IoT装置对蜂窝连接的使用。如图6所示的解决方案解决了此类挑战。

[0248] 通过将卡简档219与端点身份数据188和/或装置身份数据211安全地相关联而实施的虚拟SIM卡可以消除对物理SIM卡的需要。虚拟SIM卡的部署提供了高度可扩展的IoT安全、基于云的SIM管理、安全的零接触装置注册和IoT服务登入、流畅的全球连接、即时SIM激活。

[0249] 如图6所示的解决方案对于工业、基础设施、汽车、航空、运输和物流部门尤其有利，这些部门甚至在最偏远的位置也需要为便携式装置提供无边界的远距离连接，不受边界和近距离Wi-Fi网络的限制。

[0250] 如图6所示的系统可以极大地简化灵活的全球连接，并为IoT市场的创新提供丰富的可能性。

[0251] 物理智能卡的使用要求在制造期间将卡身份和/或装置身份与网络(例如，225)提供的服务紧密配对，以防装置不安全、操作不安全、欺诈和/或仿冒。

[0252] 安全服务器140可用于实施第三方服务的零接触认证和证书的后期绑定，使得终端用户能够自由地安全访问更多样化的第三方IoT服务。

[0253] 安全服务器140和/或卡服务器223可用于安全地安装软模块以定制IoT装置。例如，可以提供在线软模块商店以允许将软模块存储到端点150中，以类似于上文所论述的不同类型的智能卡和/或SIM卡的功能供应的方式来定制其功能。这种定制允许企业访问与供应商无关的IoT服务，以新的方式利用和试验智能特征和数据洞察。

[0254] 随着从IoT鱼缸到婴儿监视器等装置上的复杂不良行为和黑客攻击，威胁环境变得越来越危险，网络安全一直是IoT采用的薄弱环节。安全服务器140可以提供由在控制访问和装置身份数据211的存储器装置(例如，130)中实施的安全特征所支持的安全即服务。通过其硅信任根，安全存储器装置130为IoT软件的最低层提供唯一级别的保护——从引导过程开始，且具有存储器装置130中自有的强加密身份和安全特征。

[0255] 例如，经由安全服务器140和安全存储器装置(例如，130)中嵌入的安全特征的组合实施的安全即服务可包含通过验证存储器装置(例如，130)是否具有在存储器装置130的制造期间执行的经由存储器注册231记录的根秘密来验证声称具有公共识别号的存储器装置(例如，130)的真实性。

[0256] 例如，安全即服务可任选地进一步包含基于与经实施以提供所有者权限的访问控制密钥213相对应的加密密钥来识别存储器装置130的所有者。

[0257] 例如，安全即服务还可任选地进一步包含在将端点150分发给终端用户/客户之前，基于存储器装置130的所有者/制造商的身份识别具有存储器装置130的端点150的服务提供商。基于服务提供商，安全服务器140可以下载与服务提供商提供的服务相关的软模块217，以定制端点150。例如，可以在端点注册235期间执行定制。任选地，终端用户或企业用户可以选择服务提供商；并且安全服务器140和/或卡服务器223可以将软模块217推送到存储器装置130。此外，响应于端点认证239，安全服务器140可以自动将软件更新推送到存储器装置中。因此，现场端点(例如，150)的安全漏洞可以自动减少和/或最小化，而无需端点(例如，150)的各个OEM额外努力。

[0258] 例如，安全即服务可任选地进一步包含对丢失/被盗装置的跟踪。响应于在安全服务器140中注册为丢失或被盗的端点150的端点认证239，安全服务器140可以请求存储器装置130的访问控制器109停用对特定存储器区域的访问和/或从特定存储器区域擦除数据。

在一些情况下，访问控制器109可以通过限制对诸如启动加载程序、操作系统、应用程序等资源的访问来停用端点150的正常操作。在一些情况下，访问控制器109可以执行不可逆地破坏存储器装置130的存储器功能的操作。

[0259] 例如，安全即服务可任选地进一步包含端点150的完整性的审核服务。例如，存储器装置130可以基于存储于存储器装置130中的软模块217的加密散列值构建端点身份数据188，使得当软模块217改变时，安全服务器140可以验证当前软模块217是不是来自软模块217的相应供应商的有效分发。当发现软模块217损坏、篡改和/或受损时，安全服务器140可以发起更新操作，以使用来自在线软件商店的有效分发来修复软模块。

[0260] 当软模块217的更新版本可用时，安全服务器140可以重新计算端点身份数据188以用于端点150的认证。因此，当端点150具有过时的软模块217时，安全服务器140可以检测到过时版本的存在，并通过空中请求/发起软模块217的更新。任选地，安全服务器140可以跟踪影响端点身份数据188的端点150的配置变化历史。例如，当被请求时，安全服务器140可以与存储器装置130通信以恢复到先前的配置。

[0261] 例如，安全即服务可任选地进一步包含装置跟踪服务，其可以向端点150的所有者提供与所有者访问控制密钥213(或与另一访问控制密钥相对应的另一授权用户)对应的活动数据。例如，活动数据可包含位置数据和端点150在来自基于卡的服务网络225的各种服务中的使用。

[0262] 端点身份数据188可包含端点150的公共身份，例如国际移动设备身份(IMEI)编号(例如，移动设备身份编号253)。端点150的公共身份对基于卡的服务网络225的服务(例如，蜂窝连接)的订阅可以在卡服务器(223)预注册而不使用端点150。例如，IMEI编号可与卡服务器223的数据库中的国际移动订户身份编号255相关联。

[0263] 当端点150尝试连接到基于卡的服务网络225时，端点150的公共身份(例如，IMEI编号)在端点认证239中使用端点身份数据188认证。作为响应，注册到国际移动订户身份编号255的订阅被识别并用于生成卡简档219以将卡简档219绑定到端点150。绑定可以呈将卡简档219存储到端点150中的安全存储器装置130中的形式。替代地，绑定可以呈在卡服务器223的数据库中卡简档219与端点身份数据188关联的形式。

[0264] 在一些情况下，一组端点(例如，由企业客户端拥有)可以共享数量减少的虚拟SIM卡以实现蜂窝连接。例如，企业客户端的IoT装置可能不需要同时进行蜂窝连接。当企业客户端的端点150需要蜂窝连接时，表示虚拟SIM卡的可用卡简档219在通信会话期间的端点认证239之后为端点150动态地“安装”以及时用于蜂窝服务。当通信会话结束时，虚拟SIM卡可由企业客户端的另一端点使用。物理SIM卡可以从一部移动电话移动到另一移动电话，以允许不同的移动电话访问注册到同一SIM卡的蜂窝服务。但是，物理地将SIM卡从一个移动电话移动到另一移动电话效率低下，并且无法进行大规模部署。虚拟SIM卡的即时安装可以克服物理SIM卡的限制，并在安装虚拟SIM卡之前经由端点认证239提供改进的安全性。

[0265] 例如，虚拟SIM卡的这种即时安装可用于促进对蜂窝连接的不经常或一次性使用。例如，蜂窝连接可用于执行空中固件/软件更新。例如，蜂窝连接可用于定期报告端点150的状态(例如，每天、每周或每月一次)。例如，端点150可以报告其与基于端点150的位置的保修服务相关的健康和/或位置。

[0266] 例如，安全即服务可任选地进一步包含允许以安全方式改变端点150的公共身份

的身份服务。例如，企业客户端的一组端点可以共享数目减少的IMEI编号。当端点150尝试使用端点身份数据188中的替代公共身份编号连接到基于卡的服务网络225时，卡服务器223和/或安全服务器140可以执行端点认证239，将未使用的IMEI编号分配给端点150，将卡简档219与分配给端点150的IMEI编号相关联，以使端点150能够作为由IMEI编号表示的装置从网络225获得服务。

[0267] 当这样的安全存储器装置130与安全服务器140提供的安全即服务一起使用时，端点(例如，150)的原始设备制造商(OEM)可以通过将安全存储器装置130组装到端点(例如，150)中来提供安全性，而无需执行其单独的安全操作，例如安全密钥注入、设计和实施安全元件、硬件组件或专用片上系统(SoC)特征。因此，安全服务器140和安全存储器装置(例如，130)可以为IoT装置(例如，端点150)的OEM提供即插即用安全性。

[0268] 安全服务器140的服务可用于在部署后在边缘处认证、激活和管理安全存储器装置(例如，130)。此能力可在整个生命周期内从制造供应链扩展到现场安装和管理实现平台强化和装置保护。

[0269] 图9示出根据一个实施例的用于认证存储器装置的技术。例如，图9的技术可用于使用图2的身份数据实施图5的安全服务。

[0270] 通过图9的认证操作，可以建立会话密钥263以保护安全服务器140和存储器装置130之间的通信，而不信任客户端服务器141处理安全性以保护存储器装置130的秘密。任选地，会话密钥263可由访问控制器109用于实施请求在存储器装置130中执行的选定命令155的权限。

[0271] 在图9中，客户端服务器141可向存储器装置130发送对存储器装置130的身份数据113的请求271。

[0272] 请求271可包含密码随机数267。例如，密码随机数267可由安全服务器140响应于来自客户端服务器141的请求而生成，或由客户端服务器141生成并与安全服务器140共享用于请求271。替代地，存储器装置130可响应于请求271生成密码随机数267并提供包含密码随机数267的对应响应273。

[0273] 响应于对存储器装置130的身份数据113的请求271，存储器装置130提供包含识别存储器装置130的唯一识别111的消息的响应273。

[0274] 使用存储器装置130的秘密密钥137为响应273中提供的消息生成验证码133。如上文所论述，验证码133可以使用诸如散列摘要、数字签名和/或基于散列的消息认证码等技术来实施。验证码133的验证可由安全服务器140使用与唯一识别111相关联地存储的对应加密密钥106来执行。

[0275] 为了保护响应273和/或验证码133免受安全攻击(例如，重新使用响应273和/或尝试恢复密钥137)，为包含唯一识别111、计数器值265和密码随机数267的消息131生成验证码133。计数器值265从存储器装置130中的计数器261获得。计数器261的值单调地增加。例如，计数器261可用于存储表示针对身份数据和/或与安全性相关的其它数据项或操作而接收的请求的计数的值。因此，含有低于先前看到的计数器值的计数器值265的响应可被视为无效。密码随机数267在响应273的生成中使用一次，并被存储器装置130舍弃。当先前已向安全服务器140提供或由安全服务器140生成密码随机数267时，响应273不必在响应273中显式地包含密码随机数267。

[0276] 客户端服务器141将响应273转发到安全服务器140以请求认证存储器装置130。使用在响应273中提供的唯一识别111，安全服务器140可定位对应加密密钥106以验证验证码133。例如，对应的加密密钥106可以是秘密密钥137，或使用不对称加密时的对应公钥。

[0277] 基于验证码133的验证，安全服务器140向客户端服务器141提供真实性指示符275。真实性指示符275指示存储器装置130是否真实。例如，安全服务器140可生成并提供由安全服务器140签名的证书，以将存储器装置130的证书链延伸回到验证器(例如，安全服务器)。任选地，安全服务器140可允许下载证书签名请求(CSR)，其允许请求者使用他们选择的证书颁发机构(CA)(而不是安全服务器140)。

[0278] 通过存储器装置130的认证，存储器装置130和安全服务器140可建立用于在后续通信会话中彼此通信的会话密钥263。会话可受在响应273或验证码133的验证之后的预定长度的时间段限制。在所述时间段之后，会话密钥263到期，且因此可被破坏或舍弃。此外，对身份数据的后续请求可结束通过对身份数据的先前请求开始的先前会话。

[0279] 会话密钥263可至少部分地基于在安全服务器140和存储器装置130之间已知但不可用于安全服务器140和存储器装置130之间的通信信道的秘密生成。

[0280] 例如，会话密钥263可以至少部分地基于秘密密钥137导出。此外，会话密钥263可以至少部分地基于计数器值265和/或密码随机数267。任选地，会话密钥263可以至少部分地基于验证码133。例如，验证码133和秘密密钥137可以组合生成会话密钥263。

[0281] 在一些实施方案中，会话密钥263独立于验证码133；并且验证码133可使用从秘密密钥137或安全服务器140和存储器装置130之间已知的另一秘密导出的会话密钥263生成。

[0282] 图10示出根据一个实施例的用于生成控制存储器装置的安全操作的命令的技术。例如，图9的技术可用于使用图3和10的技术实施图5的安全服务。

[0283] 例如，在客户端服务器141请求在存储器装置130中执行命令155的权限使用客户端权限数据283验证之后，安全服务器140可响应于来自客户端服务器141的请求281而向客户端服务器141提供命令155的验证码153。

[0284] 图9和图10中的一些通信可以组合。例如，在一些情况下，请求281可包含存储器装置130所提供的身份数据113作为对存储器装置130的请求271的响应273。

[0285] 在客户端服务器141发送识别命令155和存储器装置130的请求281之后，如果确定客户端服务器141具有使用命令155控制或操作存储器装置130的权限，那么安全服务器140可生成命令155的验证码153。请求281可包含其中将执行命令155的存储器装置130的唯一识别111。例如，唯一识别111可由客户端服务器141从对存储器装置130的身份数据的请求271的响应273和/或安全服务器140所提供的真实性指示符275提取。

[0286] 如上文所论述，验证码153可以使用诸如散列摘要、数字签名和/或基于散列的消息认证码等技术来实施。验证码153的验证可由访问控制器109使用命令155的访问控制密钥149来执行。验证码153可以使用存储在安全服务器140中的加密密钥277生成，所述加密密钥表示在存储器装置130中执行命令155的权限。例如，当不使用经由不对称加密的加密时，加密密钥277可以是访问控制密钥149；替代地，当使用不对称加密时，访问控制密钥149是密钥对中的公钥，而加密密钥277是密钥对中的私钥。

[0287] 在一个实施例中，访问控制密钥149和加密密钥277是针对命令155的权限预先配置的。在另一实施例中，访问控制密钥149和加密密钥277基于会话密钥263。例如，会话密钥

263可以用作用于命令155的访问控制的访问控制密钥149和加密密钥277。在一些实施例中，会话密钥263是一对不对称密钥中的密钥，可用于实施涉及使用不对称加密执行的加密的加密密钥277和访问控制密钥149。

[0288] 当验证码153是基于会话密钥263时，验证码153在会话密钥263到期时到期，这防止在会话密钥263有效的会话之外重复使用验证码153。

[0289] 在请求285中提供的消息151可包含命令155和密码随机数287。密码随机数287布置成用于命令155/请求285，且因此不同于用于传输存储器装置130的身份数据的密码随机数267。

[0290] 例如，响应于请求281，安全服务器140可生成密码随机数287，并将其用于生成验证码153。密码随机数287可设有验证码153以供客户端服务器141生成请求285。替代地，客户端服务器141可生成密码随机数287，并将其与请求281一起提供到安全服务器140。替代地，为生成请求281，客户端服务器141可请求来自安全服务器140的密码随机数287。

[0291] 在客户端服务器141发送具有从安全服务器140获得的验证码153的请求285之后，存储器装置130使用访问控制密钥149验证包含在请求285中的消息151的验证码153。如果验证码153有效，那么访问控制器109允许存储器装置130执行命令155；否则，访问控制器109可阻止在存储器装置130中执行命令155。

[0292] 例如，命令155可配置成激活存储器装置130的安全特征。

[0293] 例如，命令155可配置成替换存储器装置130中的访问控制密钥149或秘密密钥137。例如，新秘密密钥137可使用在计算装置的制造期间提供的额外非秘密数据生成，所述计算装置安装了存储器装置130，但存储器装置130在其制造时不可用。例如，新访问控制密钥149可配置成向客户端服务器141提供一组权限。

[0294] 在执行命令155之后，存储器装置130提供可由客户端服务器141转发到安全服务器140的响应289。安全服务器140可确定响应289是否正确。例如，存储器装置130可使用会话密钥263对响应进行签名以供安全服务器140验证。

[0295] 在一些实施方案中，用于替换存储器装置130的现有秘密密钥137的替换秘密密钥由存储器装置130和安全服务器140从通过客户端服务器141交换的秘密(例如，唯一装置秘密101)和额外数据独立地生成。任选地，所述额外数据可以通过使用会话密钥263执行的加密受保护。

[0296] 在一些实施方案中，替换秘密密钥以使用会话密钥263生成的密文的加密形式从存储器装置130传送到安全服务器140。

[0297] 图11示出根据一个实施例的虚拟智能卡的方法。例如，图11的方法可以使用图9和10的技术在图6中所示的具有上文结合图1-5所论述的安全服务器140和存储器装置130的安全特征的系统中实施。

[0298] 在框301处，至少部分地基于存储器装置130的根秘密，由围封在存储器装置130的集成电路封装中的逻辑电路或控制器生成表示存储器装置130的装置身份数据211。

[0299] 例如，存储器装置130可具有物理不可克隆函数(PUF)以生成根秘密。

[0300] 例如，逻辑电路或控制器可包含配置成执行加密计算而不使用集成电路封装之外的处理器的加密引擎。

[0301] 在框303处，存储器装置130在形成于围封在集成电路封装内的一或多个集成电路

裸片上的集成电路存储器单元的第一存储器区域中存储装置身份数据211。

[0302] 在框305处，逻辑电路基于访问控制密钥213控制对第一存储器区域的访问。

[0303] 在框307处，存储器装置130在集成电路存储器单元的第二存储器区域中存储可由具有存储器装置130作为端点150的多个组件中的一个的端点150执行的启动指令。

[0304] 例如，装置身份数据211可以基于向存储在存储器装置130的第二存储器区域中的启动指令应用加密散列函数得到的散列值来计算和/或更新。因此，装置身份数据211不仅可以锁定存储器装置130的硬件，而且还可以锁定存储于存储器装置中的启动指令(和/或其它数据，例如跟踪数据215)。

[0305] 在框309处，将卡简档219写入到存储器装置130的集成电路存储器单元，以基于卡简档219模拟智能卡的功能。

[0306] 例如，端点150可经由存储器装置130配置成生成表示端点150在其启动时间的组件配置的端点身份数据188。端点身份数据188可以使用以下来计算：装置身份数据211、在端点150的构造233期间存储到存储器装置130中的跟踪数据215，以及端点150的位于存储器装置130的集成电路封装之外的组件的识别数据。

[0307] 例如，卡简档219可以基于端点身份数据188的认证而识别、生成和/或分配给端点150。

[0308] 例如，卡简档219可包含软模块(例如，软卡模块243、认证模块259)，所述软模块具有可由逻辑电路或端点150的处理器或其任何组合执行以模拟智能卡的功能的指令。

[0309] 例如，卡简档219可以存储于存储器装置130中以模拟在访问蜂窝通信网络时通常用于认证移动电话的订户识别模块(SIM)卡。例如，卡简档219可包含国际移动订户身份编号255和与国际移动订户身份编号255相关联的认证密钥257。

[0310] 例如，当端点150请求到国际移动订户身份编号255的蜂窝连接时，移动/蜂窝网络运营商可提出安全质询以认证端点150。作为响应，卡简档219可用于通过使用认证密钥257对具有随机数的消息进行签名来生成对安全质询的响应，以证明端点拥有认证密钥257。例如，可以使用认证密钥257对具有随机数的消息进行签名。对安全质询的响应可包含用于认证的数字签名的一部分；数字签名的另一部分可用作用于加密与蜂窝连接相关联的通信会话的对称加密密钥。

[0311] 图12示出根据一个实施例的基于存储器装置的安全特征提供的安全服务的方法。例如，图12的方法可以使用图9和10的技术基于上文结合图1-5所论述的存储器装置130的安全特征在图1的计算系统中实施。

[0312] 在框321处，安全服务器140从客户端服务器141接收请求(例如，173和/或281)。请求包含具有访问控制器109的存储器装置130的身份数据113。

[0313] 在框323处，安全服务器140基于存储器装置130的秘密和身份数据113确定存储器装置130的真实性。

[0314] 例如，秘密可以是在安全设施中完成存储器装置130的制造之后不传送到存储器装置130之外的唯一装置秘密101。身份数据113基于至少部分地基于唯一装置秘密101生成的秘密密钥137。在存储器装置在安全设施中的制造期间，秘密注册到安全服务器140中，以至少部分地基于秘密生成验证身份数据113的加密密钥106。用于验证身份数据113加密密钥106可进一步基于在存储器装置130的主机系统120的启动时间期间从主机系统120接收

的数据125而生成。在安全设施中完成存储器装置130的制造之后，存储器装置130可以组装到具有连接到存储器装置130的主机接口147的主机系统120的端点150中。配置成在主机系统120的处理装置118中执行的指令的至少一部分存储于存储器装置130中。

[0315] 在框325处，安全服务器140生成命令155的验证码153。

[0316] 例如，在基于存储在安全服务器140中的客户端权限数据283确定客户端服务器141具有在存储器装置130中执行命令155的权限之后，可为客户端服务器141生成验证码153，并基于权限在响应174中提供验证码153。

[0317] 例如，在确定存储器装置130处于已报告丢失或被盗的端点150中之后，可为停用存储器装置130的命令155生成验证码153。

[0318] 在框327处，安全服务器140向客户端服务器141传送含有验证码153的响应174。

[0319] 例如，响应174可基于当身份数据113含有使用秘密生成的验证码133时确定存储器装置130具有秘密。

[0320] 在框329处，客户端服务器141向存储器装置130传输命令155和验证码153。

[0321] 在框331处，存储器装置130的访问控制器109验证验证码153以确定是否阻止在存储器装置130中执行命令155。

[0322] 例如，在存储器装置130中执行时，命令155使供访问控制器109用于验证使用加密密钥145生成的验证码(例如，153)的访问控制密钥149改变，所述加密密钥表示在存储器装置130中执行一或多个命令的权限。

[0323] 例如，在存储器装置130中执行时，命令155使存储器装置130的安全特征的设置改变。例如，改变可包含存储器装置130的安全特征的激活或安全特征的撤销激活。

[0324] 例如，在含有存储器装置130的端点150已经报告丢失或被盗之后，在存储器装置130中执行时，命令155使存储器装置130停用存储于存储器装置130中的启动加载程序。

[0325] 例如，在存储器装置130中执行时，命令155使访问控制器116阻止对存储器装置130中的存储器单元103的一或多个区段的访问。

[0326] 例如，在存储器装置130中执行时，命令155使存储器装置130清除存储于存储器装置130中的数据的解密密钥。

[0327] 例如，在存储器装置130中执行时，命令155使存储器装置130不可逆地破坏存储器装置130的至少一个方面。

[0328] 例如，基于身份数据113的验证，会话密钥263可以在安全服务器140和存储器装置130之间建立且已知，而无需经由安全服务器140和存储器装置130之间的连接传送会话密钥263。供访问控制器109用于验证命令155的验证码153的访问控制密钥149可基于会话密钥263。

[0329] 任选地，安全服务器140可基于从存储器装置130加载且在主机系统120中执行的指令使命令155和验证码153传输到存储器装置130。

[0330] 图13示出根据一个实施例的登入账户订阅的服务的端点的方法。例如，图13的方法可以使用图9和10的技术基于上文结合图1-5所论述的存储器装置130的安全特征在图1的计算系统中实施。

[0331] 在框341处，服务器系统从端点150接收与服务相关联的请求(例如，171和/或173)。服务经由服务由不同账户表示的多个订户的计算机网络(例如，网络110)提供。请求

包含由配置于端点150中的存储器装置130生成的身份数据113。

[0332] 例如，服务器系统可包含安全服务器140和/或卡服务器223。任选地，服务器系统可进一步包含与安全服务器140通信的客户端服务器141。

[0333] 例如，服务可以是蜂窝连接服务、支付卡服务、视频监控服务、基于云的存储或计算服务等等。

[0334] 在框343处，服务器系统响应于请求并基于存储器装置130的秘密和身份数据113而确定端点150的真实性。例如，框343中的操作可以类似于在框323中执行的操作的方式执行。

[0335] 在框345处，基于身份数据113，基于端点150的所有权数据在多个订户当中识别一订户。

[0336] 例如，在端点(例如，150)的制造商的设施中制造端点150期间，存储器装置130连接到主机系统120；并且在存储器装置130中安装用于端点150的操作的软件包。测试端点150。在端点注册235中，存储器装置130配置成生成密钥137，该密钥137不仅表示具有唯一装置秘密101的存储器装置130，而且还表示具有存储器装置130的端点150，存储器装置130在启动时间具有存储器单元103中的数据123和来自主机系统120的数据125。

[0337] 当端点150从制造商转移到经销商和终端用户或订户时，使端点150的公共识别与订户的身份相关联的数据存储在服务器系统中。所有权数据可以存储在服务器系统中，而无需物理地操作端点150(例如，无需打开自端点150制造以来围封端点150的封装)。例如，端点150的公共识别可包含端点150的唯一识别111和/或识别端点150的制造商已知的端点150的品牌、型号和序列号的数据127。

[0338] 当订户为提供给端点150的服务开通账户时，订户的身份可与账户相关联。

[0339] 例如，客户端权限数据283可包含端点150的所有权数据和/或展示订户账户的订户数据。

[0340] 在框347处，响应于在框341中接收的请求，确定所识别订户的账户。

[0341] 例如，可通过匹配与所有权数据中的身份数据113相关联的订户身份和与订户数据中的账户相关联的订户身份来识别账户。

[0342] 在框349处，服务器系统基于账户使服务提供给端点150。

[0343] 在一些实施方案中，存储在安全服务器140中的客户端权限数据283指示订户的身份数据113和账户之间的关联。因此，在基于接收到的身份数据113验证端点150的真实性期间，可以根据客户端权限数据283识别账户。

[0344] 在替代实施方案中，存储在安全服务器140中的客户端权限数据283指示作为所有者的订户的身份数据113和身份之间的关联。因此，在基于接收到的身份数据113验证端点150的真实性期间，可以根据客户端权限数据283识别订户。另一服务器(例如，客户端服务器141或卡服务器223)存储订户数据以基于安全服务器140所识别的订户识别账户。

[0345] 使用图13的方法，账户订阅的服务可以提供/定向到端点150，而无需为订户和/或订户的账户定制端点150本身。例如，订户可以在制造端点150期间简单地打开围封端点150的封装，并使用端点150访问订户账户订阅的服务，而无需插入卡(例如，SIM卡)识别订户或账户和/或无需与在端点150中运行的应用程序或实用程序交互以识别订户或账户。

[0346] 例如，在制造端点150之后，在框341中接收的请求之前，端点150没有针对订户的

定制，也没有针对账户的定制。端点150制造成可由多个订户中的任何一个使用。响应于在框341中接收到的请求，端点150自动链接到获得服务的订户的特定账户。

[0347] 例如，在接收用于订户账户的服务之前和/或之后，端点150不含插入到端点150中以表示订户、账户或其任何组合的硬件组件。

[0348] 例如，至少在框341中接收的请求之前，端点150不含存储到端点150中以表示订户、账户或其任何组合的数据。

[0349] 例如，至少在框341中接收的请求之前，端点150不含订户、账户或其任何组合的指示，且不具有端点150的所有权数据；并且所有权数据存储在服务器系统中而不在端点150中。

[0350] 任选地，响应于在框341中接收的请求，服务器系统和/或端点150可存储端点150的身份数据与订户账户的关联。

[0351] 例如，安全服务器140可使用加密密钥145生成命令155的验证码153。服务器系统可使存储器装置130接收命令155和验证码153。在存储器装置130中执行命令155之前，存储器装置130的访问控制器109配置成基于访问控制密钥149验证验证码153。任选地，访问控制密钥149和加密密钥145可基于以图9中论述的方式建立的会话密钥。

[0352] 在存储器装置130中执行时，命令155使存储器装置130存储识别账户的额外数据。例如，所述额外数据可以是在生成更新后的身份数据113时用于生成秘密密钥137的装置信息121的部分。例如，所述额外数据包含在更新后的身份数据113中的消息131的数据127中，所述更新后的身份数据113由存储器装置130在命令的执行之后生成。例如，所述额外数据可包含识别订户账户的卡简档219。

[0353] 替代地，使存储器装置130和/或端点150的身份数据113相关联的数据可以存储在服务器系统中(例如，作为客户端权限数据283和/或卡简档219的部分)，而无需改变用于对身份数据113进行签名的秘密密钥137。

[0354] 由于不需要在端点150上进行操作来将订户的账户的服务定向到端点150，因此端点150可以被配置为具有蜂窝连接能力的IoT装置，而不需要用于其定制以接收蜂窝连接服务的用户接口。例如，可以在没有用于插入卡来识别订户的插槽的情况下配置端点150。例如，可以在没有用于接收来自终端用户的输入以识别订户的用户接口的情况下配置端点150。

[0355] 在一些实施方案中，端点150具有可运行不同固件以提供不同功能的通用硬件配置。此外，固件的更新版本可以安装在端点150中，以校正运行先前版本的固件的端点150中的缺陷或错误，以提高性能和/或提供新功能。任选地，固件应用程序可运行于基础版本的固件上以添加功能、特征和/或服务。

[0356] 例如，不同的客户端服务器141、…、143可使用运行不同固件的端点150的相同硬件提供不同服务。例如，所述不同的客户端服务器141、…、143可使用端点150的相同硬件提供类似服务，但是执行使用不同固件实施的不同处理。

[0357] 在通过安装不同固件组装端点150并将其运送到终端用户或订户之后，可以针对不同的客户端服务器141、…、143定制端点150。

[0358] 例如，可以在通信网络110上配置在线固件商店，以允许终端用户购买某一版本的固件。安装选定版本的固件可能包含也可能不包含安装使用基线版本的固件运行的固件应

用程序。在安装选定版本的固件之后，将端点150定制为在至少一个方面不同于运行先前固件的端点150。

[0359] 在一些情况下，更新后的固件表示由端点150的用户请求的端点150的服务。端点150的服务可以依赖于也可以不依赖于客户端服务器或服务提供商提供的服务。

[0360] 端点150的功能可以至少部分地由其固件定义。例如，当端点150运行一个版本的固件时，端点150可以向端点150的用户提供一个功能；并且当端点150运行另一版本的固件时，端点150可以向端点150的用户提供不同的功能。

[0361] 例如，不同的第三方服务提供商可以基于公共的通用硬件平台提供IoT装置的软件/固件解决方案。例如，在线商店中提供的固件可编程为使通用IoT装置能够与第三方服务器协作以提供特定类型的服务。任选地，在线商店中提供的固件应用程序可以在通用版本的固件上运行，并使用通用固件提供的基本服务来提供特定类型的服务。基线版本的固件和固件应用程序的组合可视为增强版本的固件。当不同端点硬件平台的基线版本的固件提供标准化服务时，固件应用程序可以是与装置无关的，并支持来自不同供应商的一类IoT装置。替代地，固件应用程序可能依赖于装置，并使用不同供应商的不同硬件能力。

[0362] 安全服务器140可耦合到在线固件商店以响应于验证端点的真实性而向端点(例如，150)提供固件更新。

[0363] 例如，当端点150初始地连接到客户端服务器141时，客户端服务器141与安全服务器140通信以验证端点150的身份和/或真实性。端点150的所有者可在验证过程中确定。在端点150的订阅服务被识别之后，相关固件应用程序可以从在线固件商店下载并通过空中(OTA)更新安装到端点150中。

[0364] 例如，安全服务器140可生成命令155的验证码153以将固件应用程序安装到存储器装置130中。在执行命令155之后，固件应用程序变成存储于存储器装置130的存储器单元103中的数据123的部分，并在生成用于存储器装置130和端点150的更新后的身份数据113的更新后的秘密密钥137时用作装置信息121的部分。

[0365] 随后，当在线固件商店中存在固件应用程序的更新时，在身份数据113的验证期间可以检测到端点150中的过时固件应用程序；并且安全服务器140可以为端点150发起空中(OTA)更新以降低安全风险。

[0366] 例如，在线服务商店可提供经由端点(例如，150)提供的基于云的服务，例如物联网(IoT)装置。同一端点150可经由与可操作不同客户端服务器141、…、143的不同服务提供商一起使用的固件更新来定制。

[0367] 例如，端点150的用户可以访问在线商店以订阅服务提供商的服务、更改订阅的服务和/或将订阅从一个服务提供商移动到另一个服务提供商。用户为端点150订购的订阅可以作为与端点150的身份相关联的客户端权限数据283的部分进行跟踪。当安全服务器140验证端点150的身份数据113时，安全服务器140可以检查端点150是否需要用于订阅服务和/或替换过时版本的固件的固件更新。如果是，那么安全服务器140可以在端点150从服务提供商接收订阅的服务之前，经由在线商店使固件更新定制和/或更新端点150。任选地，安全服务器140与端点150通信以将端点150定向到服务提供商的当前客户端服务器141。替代地，更新后的固件使端点150连接到服务提供商的当前客户端服务器141。

[0368] 一般来说，安全服务器140可以连接到或包含在线服务商店和/或在线固件商店。

服务器系统可具有安全服务器140、在线服务商店和/或在线固件商店。服务器系统可跟踪用于订阅不同服务提供商的服务的账户，并跟踪端点(例如，150)的用户所选择/购买的固件定制。

[0369] 端点150的用户的账户与为端点150订阅的服务提供商可以使用用户的身份进行跟踪，并与作为用于自动固件更新的端点150的所有者的用户的身份相关联。通过相关，用户在在线服务商店和/或在线固件商店中进行的固件和/或服务选择可以映射到用户的端点150。替代地，端点150的用户可以使用作为端点150的身份数据113的部分的端点150的公共识别来明确地为端点150选择固件和/或服务。

[0370] 在一些实施方案中，端点150初始连接到用于服务的安全服务器140。安全服务器140可以基于客户端权限数据283识别在线服务商店中注册的订阅服务的当前提供商。在验证端点150的真实性并确定服务提供商之后，安全服务器140为服务提供商配置端点150的固件(例如，使用在线固件商店)，并将端点150定向到服务提供商的客户端服务器(例如，141、…、或143)。因此，端点150可以最小的用户努力无缝地提供从在线服务商店订购的服务。

[0371] 图14示出根据一个实施例的使用在线固件商店的端点定制技术。例如，图14的技术可以在具有参考图1到5论述的安全服务和特征的图1和/或图6的计算系统中实施。图14的技术可与图9到13的技术组合使用。

[0372] 在图14中，在线固件商店170配置成促进用于端点(例如，150)定制和/或更新的固件和/或固件应用程序的选择，以及安全服务器140对端点(例如，150)的身份的验证。

[0373] 端点150具有一组硬件，包含主机系统120和具有安全特征的存储器装置130。端点150的功能可由存储于存储器装置130中且执行于端点150的主机系统120中的固件363定义、定制和更新。

[0374] 端点150的制造商可以安装基线版本的固件363，此固件363编程成允许端点150生成并提交身份数据113以供安全服务器140验证。基线版本的固件363进一步配置成促进经由固件商店170对固件的更新以及安全服务器140对身份数据113的验证。

[0375] 一般来说，端点150的固件更新可以是替换在主机系统120中执行的整个固件363，或添加和/或替换一或多个固件应用程序(例如，应用程序367、…、369)。

[0376] 端点平台361可用于表示一类端点硬件。所述类别中的每个端点(例如，150)可运行不同版本的固件(例如，363、…、365)以提供不同功能和/或服务。

[0377] 在一些实施方案中，固件363可以经由一或多个固件应用程序(例如，应用程序367、…、369)定制。例如，运行固件363的端点150可进一步运行任选的应用程序(例如，应用程序367、…、或369)以提供固件363中不存在的新功能，停用固件363中的现有功能，改变或定制固件363中的现有功能，等等。

[0378] 例如，当固件应用程序(例如，应用程序367)在端点150中的固件363上运行时，端点150定制用于与服务提供商的客户端服务器141通信以实施服务或功能和/或从服务提供商接收服务。当另一固件应用程序(例如，应用程序369)在端点150中的固件363上运行时，端点150以不同方式定制以与不同服务提供商的另一客户端服务器143通信，以实施替代性或类似服务或功能和/或从所述不同服务提供商接收替代性或类似服务。

[0379] 例如，固件应用程序(例如，应用程序367)可编程成实施特定于客户端服务器141

的通信协议。

[0380] 例如,固件应用程序(例如,应用程序367)可编程成执行生成新类型的结果的新计算功能。

[0381] 例如,固件应用程序(例如,应用程序367)可编程成与客户端服务器141通信以获得经由客户端服务器141提供的服务。客户端服务器141的服务的实例包含客户端服务器141处理端点150的数据的计算资源、用于由端点150生成的数据的客户端服务器141的数据存储设施、用于针对与端点150相关联的一或多个其它装置的通知和/或警告的消息传递设施、经由客户端服务器141和与端点150相关联的一或多个其它装置的连接、端点150经由Wi-Fi访问点、通信卫星和/或由客户端服务器141控制的通信连接或设备的互联网访问,等等。

[0382] 一般来说,不同服务提供商可以提供不同版本的固件和/或不同固件应用程序来定制相同端点平台361中的端点(例如,150)。平台361中的端点可由同一制造商或不同制造商制造和/或组装。

[0383] 任选地,基线版本的固件(例如,363)可提供一组标准化功能,固件应用程序(例如,应用程序367、…、369)可基于这些功能运行。因此,可以安装同一固件应用程序(例如,应用程序367)以定制具有不同硬件配置和/或不同基线版本的固件(例如,363、…、365)的端点(例如,150)。替代地,不同固件应用程序可针对在具有不同硬件实施方案的端点上运行的不同基线版本的固件(例如,363、…、365)编程,以提供相应端点的同一定制功能和/或客户端服务器141的相同服务。

[0384] 固件应用程序(例如,应用程序367、…、369)的使用可减少在执行固件更新时要从固件商店170下载到端点150的数据大小。替代地,不同组的固件功能可以使用不同固件(例如,363、…、365)实施,而无需额外的固件应用程序。一般来说,端点150中的固件更新可涉及替换整个现有固件363或安装固件应用程序(例如,应用程序367)。

[0385] 任选地,固件商店170配置成允许端点150的用户使用计算机180选择和/或订购371用于定制端点150的固件。在一些情况下,选定版本的固件(例如,363)和/或固件应用程序(例如,367)的购买表示对来自服务提供商和/或客户端服务器(例如,141)的某一服务的请求。作为响应,固件商店170和/或安全服务器140可存储指示端点150的所需固件配置和/或所请求服务的数据。例如,客户端权限数据283可以更新成反映使用用户计算机180进行的固件和/或服务选择。

[0386] 一般来说,用户计算机180可与端点150不同且分开。因此,不需要可被端点150的用户访问以定制端点150使其与账户和/或服务提供商一起使用的硬件和/或软件接口。任选地,一些实施方案和/或类别的端点150可包含允许其用作用户计算机180来为端点150订购371固件的用户接口。

[0387] 例如,端点150的所有者或用户可使用用户计算机180访问在线固件商店170,以便通过选择固件应用程序(例如,应用程序367)、替换版本的固件或替换版本的固件和固件应用程序的组合来为端点150订购371固件。用户的订单可被识别为服务订户和/或端点150被识别为待定制装置。

[0388] 例如,端点150可经由端点150的公共识别识别,例如端点150的型号和序列号、移动设备身份编号253、国际移动订户身份编号255、唯一识别111和/或包含在身份数据113的

数据127中的另一标识符。

[0389] 例如，用户或订户的身份可以经由账户标识符和/或一条可识别个人的信息识别，例如电子邮件地址、电话号码、名称和地址等等。

[0390] 安全服务器140可验证373从端点150和/或其存储器装置130提交的身份数据113，如上文结合图2、5和9所论述。

[0391] 一般来说，身份数据113可以经由客户端服务器(例如，141或143)、经由固件商店170、经由另一服务器或网关或在不经过客户端服务器141、…、143和固件商店170中的任一个的情况下提交到安全服务器140。

[0392] 例如，端点150可经由现有固件363配置以自动访问固件商店170和/或安全服务器140，以进行身份验证、固件更新和/或服务定制。因此，身份数据113在一些情况下可以经由固件商店170提交到安全服务器140，在其它情况下直接提交到安全服务器140。

[0393] 例如，当服务器(例如，客户端服务器141或143、固件商店170或另一服务器)从端点150接收请求171的身份数据113时，服务器(例如，141)在请求173中向安全服务器140提供身份数据113以供验证。响应于此类请求173，安全服务器140可与固件商店170通信，以识别375端点150是否存在固件更新。如果是，安全服务器140可使固件商店170更新377端点150的固件。例如，在执行固件下载以在存储器装置130中存储新版本的固件和/或固件应用程序(例如，应用程序367)之后，在存储器装置130中执行使用加密密钥145签名的命令155，以使得新版本的固件和/或固件应用程序(例如，应用程序367)在存储器装置130中执行并成为存储器装置130和/或端点150的身份的部分。

[0394] 例如，固件363可以初始地安装于端点150中(例如，通过端点150的制造商)以经由客户端服务器141提供服务。在固件商店170中提供新版本的固件363以用于访问客户端服务器141的相同服务之后，安全服务器140可以响应于身份数据113的成功验证而发起新版本的安装。任选地，更新377可以经由安装在现有固件363上运行的固件应用程序(例如，应用程序367)来实施，或者经由安装新固件(例如，365)来实施。

[0395] 例如，在固件363的用户访问固件商店170订购371替代版本的固件365以定制端点150之后，当端点150的身份数据113在安全服务器140中成功验证时，固件商店170可根据订单371更新377端点150的固件。

[0396] 在一些情况下，端点150首先访问安全服务器140。在安全服务器140验证373端点150的身份之后，安全服务器140可与在线固件商店170通信以识别375端点150的固件更新。

[0397] 一般来说，固件更新可包含安装固件应用程序(例如，应用程序367)、用另一固件应用程序替换现有固件应用程序和/或安装新固件365。

[0398] 在识别出合乎需要的固件更新之后，固件商店170与端点150通信以更新377端点150。

[0399] 存储器装置130的访问控制器配置成需要验证请求存储器装置130执行命令155以改变存储于存储器装置130中的固件的权限。

[0400] 例如，在固件更新所需的数据存储到存储器装置130的区段中之后，命令155可以发送到主机接口147以在存储器装置130中执行固件更新的操作。在存储器装置130中执行命令155的权限可以由加密密钥145表示。加密密钥145可在先前配置，或响应于验证来自端点150的存储器装置130的身份数据113而生成。例如，加密密钥145可以是基于验证端点150

的真实性以类似于图9的方式生成的会话密钥263;并且安全服务器140可使用加密密钥145生成命令的验证码153以供固件商店170更新端点150。替代地,安全服务器140可向固件商店170提供会话密钥263和/或加密密钥145来更新377端点150的固件。

[0401] 在成功进行固件更新之后,用于生成秘密密钥137的装置信息121更新以反映安装的固件和/或固件应用程序。例如,所安装固件和/或固件应用程序的散列值163可以存储为装置信息121的部分,以用于验证它们的完整性,如图4中所示。随后,由端点150的存储器装置130生成的身份数据113是基于更新后的装置信息121,并反映具有更新后的固件功能或配置的端点150的配置。

[0402] 在一些实施例中,固件商店170是实施安全服务器140的服务器系统的部分。在另一实施例中,固件商店170托管在单独的服务器计算机上。

[0403] 在一些实施方案中,固件的更新377可以基于为端点150订阅的服务而自动执行,如下文结合图15进一步论述。

[0404] 图15示出根据一个实施例的经由在线服务商店将服务定向到端点的技术。例如,图15的技术可与图14的技术组合使用。

[0405] 在图15中,在线服务商店190配置成促进为端点150从一或多个服务提供商(例如,381)所提供的多个服务中选择一个服务。服务提供商(例如,381)的服务可以经由一或多个端点平台(例如,361、…、362)实施。

[0406] 例如,端点150的用户可使用计算机180访问在线服务商店190,以便使用计算机180向服务提供商381订购391服务。服务提供商381提供的服务可以与多个端点平台(例如,361、…、362)的端点一起使用。端点平台(例如,361、…、362)中的端点(例如,150)运行不同固件以获得服务提供商381的服务。服务商店190具有识别订户所订购的服务和/或端点(例如,150)的订阅数据387。

[0407] 例如,服务提供商381所提供的服务可以经由客户端服务器141实施;并且订阅数据387可识别连接到端点以相应地接收为端点订阅的服务的服务器。

[0408] 例如,可以参考端点150的公共识别、端点150的型号和序列号、移动设备身份编号253、国际移动订户身份编号255、唯一识别111和/或包含在身份数据113的数据127中的另一标识符,为端点150明确订购服务。

[0409] 替代地或组合地,可以参考用户或订户的身份来订购服务,用户或订户的身份可以通过账户标识符和/或一条可识别个人的信息来识别,例如电子邮件地址、电话号码、姓名和地址等等。

[0410] 如在图14中,用户计算机180通常与端点150不同且分开。在一些情况下,端点150可包含允许其用作计算机180以便为端点150订购391服务的用户接口。

[0411] 当为端点150隐式地订购服务时,订户的身份可用于基于用于订购服务的订户的身份与端点150的所有者的身份的匹配来确定订户的端点的服务。

[0412] 例如,为了从服务提供商381订购391服务,端点150的用户(或用户的代表)可以访问服务商店190以建立用于订阅服务提供商381的服务的账户。

[0413] 响应于服务被订购或改变,或响应于端点150的身份数据113被验证,安全服务器140和服务商店190可彼此通信以识别393为端点150订阅的服务。

[0414] 响应于来自端点150的服务请求171,安全服务器140验证373在服务请求171中提

供的端点150的身份数据113。

[0415] 一般来说，服务请求171可初始地在客户端服务器(例如，141或143)中或在服务商店190或固件商店170中或直接在安全服务器140中接收。

[0416] 在安全服务器140验证373端点150的身份和真实性之后，基于存储在安全服务器140中的客户端权限数据283和/或基于服务商店190中的订阅数据387，安全服务器140可识别393为端点150订阅的服务。

[0417] 基于所识别的服务，安全服务器140可与固件商店170通信以识别375端点150的固件更新。例如，端点150可以经由替换固件或安装固件应用程序(例如，应用程序367)以针对所订阅服务定制端点150来进行更新。固件更新可以上文结合图14所论述的方式来执行和保护。

[0418] 例如，端点150可以使用通用版本的固件363制造，此固件363不能从服务提供商381接收服务，对于服务提供商381提供的服务不了解客户端服务器141，和/或未实施用于与客户端服务器141通信的通信协议。固件应用程序(例如，应用程序367)可安装在通用固件363上运行，以针对为端点150订购的服务定制端点150。一旦经由固件应用程序(例如，应用程序367)定制，端点150就可以从客户端服务器141接收服务提供商381的服务。例如，在安装固件应用程序(例如，应用程序367)以更新377固件之后，端点150具有关于客户端服务器141的知识、根据客户端服务器141使用的通信协议与客户端服务器141通信的通信能力，以及用于使用客户端服务器141提供的服务的处理例程。

[0419] 例如，为端点150的操作订阅的服务可包含由客户端服务器141执行以处理端点150的数据的计算、在客户端服务器141中存储由端点150生成的数据，向与端点150相关联的一或多个其它装置发送通知和/或警告，经由客户端服务器141和与端点150相关联的一或多个其它装置连接，使用蜂窝基站、Wi-Fi访问点、通信卫星和/或由客户端服务器141控制的通信连接或设备将端点150连接到计算机网络或互联网，等等。

[0420] 任选地，在固件更新377之后，端点150经由其固件363和/或固件应用程序(例如，应用程序367)配置成自动访问客户端服务器141以获得订阅的服务。替代地，安全服务器140可在验证具有更新后的固件的端点150的身份数据113之后将端点150重定向到客户端服务器141以访问379订阅的服务。

[0421] 一般来说，服务商店190可供用户(或用户的代表)用于为端点150订阅服务提供商381的服务，更改订阅的服务，将订阅从一个服务提供商381移动到另一服务提供商。端点150的固件363自动更新以支持当前订阅的服务，而无需端点150的用户对端点150进行操作来针对订阅的服务定制端点150。

[0422] 图16示出根据一个实施例的使用固件商店和安全服务器的固件更新方法。例如，图16的方法可以使用图14的技术实施。

[0423] 在框401处，服务器系统从端点150接收具有由配置于端点150中的存储器装置130生成的身份数据113的请求。

[0424] 例如，服务器系统可包含安全服务器140。任选地，服务器系统可进一步包含在线固件商店170和/或一或多个客户端服务器(例如，141、…、143)。

[0425] 例如，端点150可处于从端点(例如，150)制造商装运的状态，而无需针对特定服务器和/或服务提供商进行定制。

[0426] 在框403处，服务器系统响应于在框401中接收的请求并基于存储器装置130的秘密和身份数据113确定端点150的真实性。例如，框403中的操作可以类似于在框323和/或框343中执行的操作的方式执行。

[0427] 例如，身份数据113包含在身份数据113中呈现的消息131的验证码133。安全服务器140可以验证验证码133是使用存储器装置130的秘密密钥137和消息131生成的，而无需端点呈现秘密密钥137。秘密密钥137使用存储器装置130的唯一装置秘密101和表示端点150的软件和硬件配置的装置信息121生成。

[0428] 在框405处，基于在线固件商店170，确定第一固件363的更新。第一固件存储于存储器装置130中并在端点150中执行以生成在框401中接收的请求。

[0429] 例如，在框401中接收请求之前，固件商店170可接收端点150的固件的订单391。可以做出订单391以使用用户计算机180定制端点150的功能，无需经过端点150。在固件商店170中接收的订单391可用于识别375更新377。

[0430] 例如，可以使用端点150的公共识别来识别端点150的订单391。身份数据113可包含使用秘密密钥137签名的消息131中的公共识别，以生成身份数据113中提供的验证码133。在验证消息131尚未更改之后，安全服务器140可以指示在线固件商店170和/或端点150更新377端点150的固件363。

[0431] 在框407处，响应于确定端点150是真实的，服务器系统生成可在存储器装置130中执行的命令155的验证码153以执行更新。

[0432] 在框409处，服务器系统提供验证码153以在存储器装置130中执行命令155，以便进行固件更新。

[0433] 例如，响应于确定端点是真实的，安全服务器140可与在线固件商店170通信以将数据下载到存储器装置130中。当命令155在存储器装置130中执行时，存储器装置130使用数据执行固件更新。

[0434] 例如，下载到存储器装置130的数据可包含第二固件，在执行命令155以进行固件更新之后，第二固件替换经执行以生成在框401中接收的请求的第一固件。

[0435] 例如，下载到存储器装置130的数据可包含固件应用程序(例如，应用程序367)，在执行命令155以进行固件更新之后，所述固件应用程序利用经执行以生成请求的第一固件运行。固件应用程序(例如，应用程序367)和第一固件的组合提供端点150的第二固件。

[0436] 例如，在执行命令155以进行固件更新之后，端点150经由第二固件配置成提供在更新之前在运行第一固件的端点中没有的功能。

[0437] 在执行命令155以进行固件更新之后，第二固件可变为存储器装置130和端点150的身份的部分。例如，基于装置信息121，存储器装置130配置成生成表示存储器装置130和端点150的身份的秘密密钥137。在执行命令155以更新377固件之后，装置信息121更新成包含在存储器单元103中存储为内容161的第二固件的散列值163。随后，存储器装置130配置成使用加密密钥生成端点150的身份数据113，所述加密密钥至少部分地基于存储器装置的秘密(例如，唯一装置秘密101)和存储于存储器装置130中的第二固件而生成。

[0438] 图17示出根据一个实施例的使用服务商店和安全服务器的端点定制方法。例如，图17的方法可以使用图14和图15的技术实施。

[0439] 在框421处，服务器系统从端点150接收具有由配置于端点150中的存储器装置130

生成的身份数据113的请求，类似于框401。

[0440] 例如，服务器系统可包含安全服务器140和/或服务商店190。

[0441] 在框423处，安全服务器140响应于在框421中接收的请求并基于存储在安全服务器140中的关于端点150的信息来验证身份数据113。此类信息包含存储器装置130的秘密，例如唯一装置秘密101。此类信息可进一步包含表示端点150的软件/硬件配置的装置信息121。验证可以上文结合图2所论述的方式执行。

[0442] 响应于确定在框421中接收的请求中的身份数据113有效，在框425处，服务器系统识别在在线服务商店190中为端点150订购的服务。

[0443] 在框427处，识别配置成提供服务的客户端服务器141。

[0444] 例如，在框421中接收请求之前，在线服务商店190可接收端点150的服务的订单391。客户端服务器141可以基于订单391来识别。

[0445] 例如，订单391可在在线服务商店190中通过用户计算机180且因此不经过端点150来接收。端点150的订单391可以使用端点150的公共识别来识别/放置。身份数据113可包含公共识别。替代地，订单391可与在安全服务器的客户端权限数据283中作为端点150的所有者的用户的身份相关联。

[0446] 在框429处，服务器系统将端点150定向到客户端服务器141。

[0447] 例如，响应于确定在框421中接收的请求中的身份数据113有效，服务器系统可针对在在线服务商店190中订购的服务配置端点150。

[0448] 例如，为了针对服务配置端点150，服务器系统可更新端点150的固件。例如，固件更新可以上文结合图14到16所论述的方式执行。

[0449] 例如，在固件更新377之前，端点150不能从客户端服务器141接收服务，并且不具有关于客户端服务器141的了解。例如，初始地由端点(例如，150)的制造商配置的端点150编程成访问服务商店190、固件商店170、安全服务器140或另一网守，使得端点150可经正确地配置和/或更新以供使用，而无需终端用户对端点150操作来进行定制。

[0450] 例如，在固件更新377之后，第二固件存储于存储器装置130中，以替换用于生成在框421中接收的请求的第一固件。当端点150运行第二固件时，端点具有在固件更新377之前在运行第一固件的端点中没有的功能。例如，第二固件可包含客户端服务器141的识别，用于引导端点访问客户端服务器141以获得在在线服务商店190中订购的服务。在某一实施方案中，第二固件是第一固件和添加的固件应用程序的组合。在固件更新377之后，存储器装置130配置成使用秘密密钥137生成端点150的更新后的身份数据113，所述秘密密钥至少部分地基于秘密(例如，唯一装置秘密101)和存储于存储器装置130中的第二固件而生成。

[0451] 任选地，为了针对在服务商店190中订购的服务配置端点150，服务器系统识别用于为端点150订阅服务的账户。存储器装置130配置成存储账户的标识符，并且在更新后的身份数据113中包含标识符作为消息131的部分。

[0452] 例如，为了执行固件更新377，服务器系统可使用表示在存储器装置130中执行命令155的权限的加密密钥145生成命令155的验证码153。在存储器装置130中执行时，命令155使第一固件替换为第二固件。在存储器装置130接收命令155和验证码153之后，存储器装置130在执行命令155之前针对所述权限验证验证码153。

[0453] 安全服务器140不仅可以用于基于在端点150中配置的存储器装置130的安全特征

验证端点150的身份，而且还可以用于监测存储于存储器装置130和/或端点150中的包的完整性。例如，存储在端点150中的包可以是启动加载程序、固件、软件、模块、操作系统或应用程序的至少一部分、指定资源的一组文件、配置参数和/或程序或例程的其它数据，等等。当发现包被损坏、修改、篡改或过时时，安全服务器140可发起空中(OTA)更新以维持端点150的完整性。

[0454] 存储器装置130可在存储器单元103中存储内容161，并单独地存储散列值163作为装置信息121的部分，如图4所示。当根据存储于存储器单元103中的内容161计算的当前散列值不匹配作为装置信息121的部分存储的预期散列值163时，存储器装置130可检测到内容161的修改或损坏，并发起内容修复。

[0455] 例如，内容161可包含端点150的核心包。在验证373端点150的身份时，核心包的完整性可影响端点150在与安全服务器140通信时的操作。核心包的实例可包含端点150的启动加载程序、固件和/或操作系统的至少一部分。当核心包被修改、损坏或篡改时，为进行身份验证而执行的端点150的操作的安全性可能不被信任。当由加密引擎107生成的完整性状态165指示核心包改变时，访问控制器109可阻止主机系统120访问内容161，直到核心包被修复为止。

[0456] 例如，存储器装置130可在单独区段中存储核心包的可靠备份副本；并且当存储于存储器单元103中的内容161中的核心包的散列值不同于存储的装置信息121的对应散列值163时，存储器装置130可使用存储在单独区段中的副本来替换存储于存储器单元103中的核心包。任选地，端点150中的替换副本的执行可配置成开始恢复过程以从可靠源(例如，固件商店170)获得最新版本的包。替代地，安全服务器140可在验证经由替换副本提交的存储器装置130和/或端点150的身份数据113之后发起更新(例如，使用固件商店170)。

[0457] 存储于存储器单元103中的一些包对验证373端点150的身份数据113的初始操作以及更新端点150的后续操作的安全性没有影响。因此，不必在存储器装置130中存储此类包的恢复副本。可经由安全服务器140执行此类包的修复和/或更新。例如，当完整性状态165指示非核心包已经改变时，访问控制器109可以阻止主机系统120访问损坏或改变的包，直到端点150与安全服务器140通信以修复或恢复损坏的包。

[0458] 任选地，在身份数据113中提供的数据127可包含存储于存储器单元103中的内容161中的包的当前散列值。在验证373端点150的身份数据113的操作期间，安全服务器140可检查在身份数据113中提供的包的当前散列值。如果包的当前散列值指示包已经改变、损坏或过时，那么安全服务器140可发起包的修复或恢复。

[0459] 此外，端点150的一些包可以存储在不具有存储器装置130的安全特征的另一装置中。在主机系统120中执行核心包可以生成包的当前散列值作为包的健康指示符。健康指示符可以作为嵌入在端点150的身份数据113中的数据127的部分提供，以允许安全服务器140监测包的完整性。

[0460] 一般来说，身份数据113可包含指示端点150中的包的健康状况的数据。作为验证373端点150的身份数据113的操作的部分，安全服务器140可确定是否要修复和/或更新任何包。修复或更新可以在安全服务器140确认端点150的真实性之前执行。

[0461] 此外，响应于验证373端点150的身份数据113以访问客户端服务器(例如，141、…、143)的服务，安全服务器140可配置成在访问服务时跟踪和/或监测端点150的活动以实施

进一步的安全操作。

[0462] 例如，端点150的所有者或用户可请求安全服务器140跟踪端点150的活动。端点150的活动的方面可由端点150和/或客户端服务器(例如，141、…、143)在身份数据113和/或请求173中呈现以验证身份数据113。

[0463] 例如，关于所跟踪活动的信息可包含端点150的位置信息和/或端点150经由提交身份数据113所请求的服务类型。

[0464] 例如，为了从客户端服务器141的服务生成身份数据113，端点150可以在身份数据113的消息131中不仅包含端点150的唯一识别111，而且还包含服务的上下文和/或方面，例如客户端服务器141的识别、端点150的位置，请求的日期和时间、服务的类别/类型、服务的参数等。

[0465] 例如，当端点150向客户端服务器141发送针对服务的请求171时，客户端服务器141可在请求中向安全服务器140不仅提供端点150的身份数据113，而且还提供关于对客户端服务器141的服务的请求171的信息。

[0466] 例如，响应于来自端点150的请求171，客户端服务器141可基于到连接到客户端服务器141的一或多个访问点的无线通信连接来估计端点150的位置，并将所述位置以及请求173提供到安全服务器140以认证身份数据113。

[0467] 任选地，端点150的所有者或用户可访问安全服务器140的门户来查看所跟踪活动。例如，基于所跟踪活动，所有者或用户可以根据端点150的一或多个最近位置来确定端点150是否被盗或丢失。

[0468] 任选地，家长可以使用安全服务器140的门户来设置家长控制偏好以限制端点150的活动；并且安全服务器140可以结合认证端点150的身份来实施限制偏好。

[0469] 图18示出根据一个实施例的生成身份数据以促进完整性和/或端点活动的监测的图示。

[0470] 例如，图18的技术可用于具有关于图1到5论述的安全服务和特征的图1和/或图6的计算系统。图18的技术可与图9到17的技术组合使用。

[0471] 在图18中，端点150存储具有散列值169的包167。包167可存储于具有上文所论述的安全特征的存储器装置130中，或存储于可具有也可不具有存储器装置130的安全特征的端点150的另一存储器装置。当包167存储于存储器装置130中时，存储器装置130的加密引擎107可计算包167的散列值169，而不依赖于端点150中的主机系统120的处理装置118。当包167存储在存储器装置130之外时，散列值169可通过主机系统120的处理装置118执行存储于存储器装置130中且已经验证其尚未改变(例如，如图4中)的例程来获得。

[0472] 一般来说，包167可包含指令和/或数据，例如对于一组端点(例如，150)可为相同的资源、对于不同端点(例如，150)可为不同的配置参数。

[0473] 包167的散列值169指示包167的健康状况。

[0474] 在图18中，用于生成身份数据113的验证码133的秘密密钥137独立于包167的散列值169。为了促进安全服务器140对包167的完整性的监测，在身份数据113中将散列值169提供为消息131的部分。

[0475] 在安全服务器140确定身份数据113有效之后，安全服务器140可提取身份数据113中提供的散列值169，以确定端点150中的包167是否已改变和/或包167是否过时。

[0476] 例如，包167的健康且最新副本可以存储在服务器(例如，安全服务器140、固件商店170或另一服务器)中以促进端点150中的包167的修复或恢复。如果从身份数据113中提取的散列值169不同于健康且最新的副本的散列值，那么安全服务器140可以类似于结合图14到17所论述的端点150的固件363的更新377的方式发起更新。

[0477] 包167可针对端点150进行个体化。例如，当包167包含特定于平台361中的端点150但不可应用于平台361中的其它端点的配置参数时，包167的健康副本可以在端点150中的包167成功配置后立即上载到服务器(例如，安全服务器140、固件商店170或另一服务器)。

[0478] 在一些实施方案中，存储器装置130和/或端点150可配置成存储包167的健康个体化副本的散列值。例如，健康散列值可以存储为用于创建秘密密钥137的装置信息121的部分。身份数据113中的消息131可包含当前包167是否健康的指示，但不具有包167的当前散列值169。

[0479] 为了改进安全性和/或隐私保护，个体化包167的健康副本可以使用存储器装置130的加密密钥以加密形式上载并存储在服务器中。为了使用健康副本重新安装包167，存储器装置130使用存储器装置130的对应秘密加密密钥对加密版本进行解密。

[0480] 例如，在成功配置端点150中的个体化包167后，端点150和/或存储器装置130可计算个体化包167的健康副本的散列值，并使用公钥139对个体化包167进行加密。端点150可提交散列值和加密包167以存储在服务器中，从而促进监测和/或恢复。在恢复期间，密钥对135中的秘密密钥137将用于对加密包进行解密。任选地，加密引擎107可生成单独的密钥对来保护个体化包167。

[0481] 替代地，秘密密钥可以与对称加密一起使用来保护个体化包167。例如，在成功配置端点150中的个体化包167时在验证端点150的身份数据113期间生成的会话密钥263可用于对个体化包167进行加密以用于传输到和/或存储在服务器(例如，安全服务器140、固件商店170或另一服务器)。

[0482] 在图18中，身份数据113不仅包含包167的当前散列值169，而且还包含识别其中使用身份数据113的上下文的一些方面的活动信息177。例如，活动信息177可通过主机系统120执行或运行包(例如，167或另一包，如固件、应用程序、例程)来生成。

[0483] 例如，活动信息177可包含其中生成身份数据113的端点150的当前位置。

[0484] 例如，活动信息177可包含身份数据113的生成日期和时间。

[0485] 例如，活动信息177可包含向其提交身份数据113以请求171服务的客户端服务器141的识别。

[0486] 例如，活动信息177可包含所请求服务的一或多个属性，例如服务的类别、服务所涉及的另一方的识别、服务所涉及的数量或量，等等。

[0487] 例如，当提交身份数据113以进行通信连接时，属性可包含连接类型的识别、连接的标示等。

[0488] 例如，当提交身份数据113以进行支付时，属性可包含购买类别的识别、收款人、支付金额等。

[0489] 活动信息177可供安全服务器140用于检测欺诈性活动、端点的未经授权使用，并施行活动限制(例如，如家长控制偏好中所指定)，等等。

[0490] 为了改进安全性和/或隐私保护，活动信息177可以加密形式包含在消息131中。例

如,与身份数据113的验证相关联的会话密钥263可用于生成活动信息177的密文;并且在成功验证身份数据113的验证码133之后,安全服务器140可使用会话密钥263从密文恢复活动信息177。

[0491] 图19示出根据一个实施例的用于维持存储在端点中的包完整性的技术。

[0492] 在图19中,端点150存储多个包441、443、…、445。一些包存储于具有安全特征的存储器装置130中。一些包可以存储在存储器装置130之外。

[0493] 存储于存储器装置130中的核心包441可以在连接到端点150中的存储器装置130的主机系统120的处理装置118中执行。包441控制端点150在向安全服务器140提交端点150的身份数据113时及用于与包存储库191通信以修复和/或更新包441、443、…、445的操作。例如,包存储库191可包含图14和15的固件商店170。

[0494] 存储器装置130的安全特征确保端点150运行有效版本的包441以免在验证373端点150的身份和修复385包的操作中发生篡改和/或损坏。

[0495] 例如,存储器装置130可在存储器装置130的安全区段中存储备份版本的核心包441。如果发现包441已改变,那么存储器装置130可用备份版本替换已改变版本的包441,以至少保护验证373端点150的身份和修复385和/或更新377包的操作。

[0496] 在端点150生成身份数据113之后,执行包441的端点150将身份数据113传送到安全服务器140以用于验证373。例如,身份数据113可使用图18的技术生成。

[0497] 身份数据113可包含包健康信息447,例如包441、443、…、445的当前散列值,和/或基于比较相应包的健康版本的当前散列值和所存储散列值做出的包443、…、445中的任一个是否损坏的指示。

[0498] 任选地,消息131的部分可以使用会话密钥263生成的密文提供。例如,消息的经加密部分可包含包健康信息447和/或活动信息177。会话密钥263可以关于图9所论述的方式生成以在存储器装置130和安全服务器之间共享,并用于验证373端点150的身份。

[0499] 一般来说,身份数据113可以直接经由通信连接或间接地经由中间服务器(例如,图5、9或10中的客户端服务器141、图14或15中的固件商店170、图15中的服务商店190或图19的包存储库191)从端点150传输到安全服务器140。

[0500] 在验证373身份数据113之后,安全服务器140可与包存储库191通信,以基于在身份数据113中提供的包健康信息447来检查383包441、443、…、445的完整性。

[0501] 例如,包441在端点150中可以是有效的。但是,因为新版本的包441在包存储库191中已发布,包441可为过时的。因此,更新包441可以提高端点150的操作的安全性和系统的完整性。

[0502] 例如,包443或445在端点150中可能已改变,且因此被损坏。存储库191中的对应包193的健康数据195可与在身份数据113中提供的包健康信息447比较以检测所述改变。

[0503] 如果发现包(例如,441、443、…、445)过时或损坏,那么安全服务器140可指示端点150和/或包存储库191修复385或更新377包。

[0504] 修复385或更新377包的操作可包含安全服务器140生成命令155的验证码153以将数据写入到存储器装置130中。当包包含敏感信息(例如,为端点150定制的配置参数)时,替换包可以使用会话密钥263或另一秘密密钥生成的密文提供给存储器装置130。

[0505] 在修复385或更新377之后,端点150可提交更新身份数据113。当安全服务器140确

定身份数据113有效且身份数据113中的包健康信息447指示端点150中的包441、443、…、445健康且最新时，安全服务器140可认证端点150的真实性。

[0506] 图20示出根据一个实施例的基于跟踪端点活动而实施安全操作的系统。

[0507] 例如，图20的安全操作可以使用结合图1到5论述的存储器装置的安全特征结合图9、10、14、15和/或19的技术并结合图1和/或6的系统实施。

[0508] 在图20中，用户计算机180可用于访问活动跟踪器451，以设置偏好455和/或检查具有唯一识别111的端点150的所跟踪活动记录453。

[0509] 如在图14和15中，用户计算机180通常与端点150不同且分开。在一些情况下，端点150可包含允许其用作计算机180以设置偏好455和/或检查活动记录453的用户接口。

[0510] 活动跟踪器451与安全服务器140耦合以存储关于端点150的活动的活动记录453，其中端点150的身份数据113由安全服务器140验证。

[0511] 偏好455可包含端点150的活动的安全设置。例如，安全设置可用于实施家长控制，检测端点150的欺诈性使用，跟踪端点150的位置，等等。

[0512] 例如，参考455可识别端点150的地理区域。当端点150从地理区域之外的位置发送身份数据113时，活动跟踪器451可向端点150的已注册所有者或用户生成安全警告。

[0513] 例如，安全警告可传输到所有者或用户的移动装置、在偏好中识别的电子邮件地址或电话号码，和/或在用户计算机180中运行的应用程序、个人媒体播放器、移动电话、智能电话等等。

[0514] 例如，偏好455可包含与在偏好455中指定的预定条件相关联的用户选定的选择方案。当与身份数据113的提交相关联的活动符合条件时，选定的选择方案使安全服务器140和/或客户端服务器141生成对对应访问请求171的访问响应172的拒绝。替代地或组合地，选择方案可触发对在偏好455中登记的联系人的安全警告。

[0515] 端点150可向客户端服务器141传输访问请求171以请求服务。例如，服务可向端点150提供蜂窝通信连接、互联网连接、到用户计算机180的连接、在线存储设施、在线计算资源等等。例如，服务可包含支付、交易、消息等等的处理。

[0516] 在访问请求171中提供的身份数据113可包含活动信息177，如图18中所示。替代地或组合地，客户端服务器141可在传输到安全服务器140的验证请求173中提供类似或单独的活动信息。例如，客户端服务器141可在验证请求173中指定访问属性449。访问属性449识别其中端点150的身份将由安全服务器140认证的端点150的当前活动的某些方面。客户端服务器141向安全服务器140传输验证请求173，所述安全服务器验证身份数据113以确定端点150的身份的真实性。

[0517] 在验证373验证请求173中提供的身份数据113之后，安全服务器140可生成活动跟踪器451的活动记录453。活动记录453可包含从身份数据113中提取的活动信息177和/或从验证请求173中提取的端点150的当前活动的访问属性449。

[0518] 基于活动记录453，活动跟踪器451确定当前活动是否满足在偏好455中指定的任一条件。如果满足偏好455中的条件，那么活动跟踪器451可执行安全操作以实施被选定用于所述条件的选择方案。

[0519] 例如，安全操作可包含针对端点150的注册所有者或用户的通知。

[0520] 例如，安全操作可包含指示安全服务器140提供指示安全限制、安全问题、端点150

的未授权使用等等的验证响应174。

[0521] 任选地，活动跟踪器451可根据过往活动的记录453识别端点150的活动模式。

[0522] 例如，模式可包含端点150过去曾在其中运行的端点150的地理区域或区。例如，模式可包含端点150过去没有活动的一天或一周中的时间段。例如，模式可包含端点150的过往活动的访问属性449的范围。

[0523] 当当前活动偏离模式时，活动跟踪器451可生成通知，且任选地使安全服务器140和/或客户端服务器141拒绝访问请求171。

[0524] 任选地，安全服务器140可检查在身份数据113中提供的活动信息177以检测安全风险。

[0525] 例如，在活动信息177中指定的日期和时间和/或位置可以与访问属性449中的对应信息比较以检测不匹配。不匹配可以是对被盗身份数据113被使用或端点150被篡改或不安全操作的指示。

[0526] 图21示出根据一个实施例的用于更新或修复存储在端点中的包的方法。例如，图21的方法可以使用图18和19的技术实施。

[0527] 在框461处，服务器系统从端点150接收由配置在端点150中的存储器装置130生成的身份数据113。

[0528] 例如，服务器系统可包含存储存储器装置(例如，130)和/或其它服务器的秘密的安全服务器140，所述其它服务器例如包存储库191、固件商店170和/或另一服务器。

[0529] 在框463处，安全服务器140基于存储在安全服务器140中的关于端点150的信息(包含存储器装置130的秘密)来验证身份数据。

[0530] 例如，框463中的操作可以类似于在框323、框343、框403和/或框423中执行的操作的方式执行。

[0531] 在框465处，安全服务器140从已经验证的身份数据113提取存储在端点150中的包(例如，167、441、443、…、445)的健康信息447。

[0532] 例如，健康信息447可包含存储在端点150中的包167的当前散列值169。安全服务器140可比较从身份数据113中提取的当前散列值169与存储在服务器系统(例如，存储库191、固件商店170)中的健康的最新版本的包167的散列值。

[0533] 例如，框461中的身份数据的接收可以是端点150执行存储在端点150中的包167的结果。包167可包含固件363或端点150的操作系统的至少一部分。健康信息447可用于确定包167是否过时。

[0534] 在另一实例中，框461中的身份数据的接收可以是端点150执行存储在端点150中的第一包441的结果。第一包441可包含固件363或端点150的操作系统的至少一部分。健康信息447可用于确定第二包(例如，443或445)是否过时、损坏或改变。

[0535] 当第二包装(例如，443或445)包含为端点150定制的数据时，服务器系统可获得成功配置端点150中的第二包(例如，443或445)时的第二包(例如，443或445)的副本。例如，第二包(例如，443或445)可包含端点150的一或多个配置参数。响应于成功配置第二包(例如，443或445)，服务器系统可从端点150接收健康版本的第二包(例如，443或445)。随后，如果在框465处提取的健康信息447指示需要修复第二包(例如，443或445)，那么可使用存储在存储库191中的健康版本。

[0536] 在一些实施方案中，从身份数据113提取健康信息447包含对在身份数据113中提供的消息131的一部分进行解密(例如，使用会话密钥263)。

[0537] 身份数据113包含第一验证码133。安全服务器140通过确定第一验证码133是否从消息131和存储器装置130的秘密生成来验证身份数据113。例如，秘密可以是存储器装置130的唯一装置秘密101和/或秘密密钥137。在存储器装置130组装到端点150中之后，存储器装置130的秘密不传输到存储器装置130之外。

[0538] 在框467处，至少部分地基于健康信息447，安全服务器140确定存储在端点150中的包需要更新或修复。

[0539] 在框469处，安全服务器140发起操作以执行存储在端点150中的包的更新或修复。

[0540] 例如，为了替换或修复存储于存储器装置130中的包，安全服务器140使用表示在存储器装置130中执行命令155的权限的加密密钥生成命令155的第二验证码153。例如，在存储器装置130中执行时，命令155使存储器装置130中的包(例如，441或443)替换。

[0541] 在一些实施方案中，为了修复存储在存储器装置130之外的包445，包445的替换初始存储到存储器装置130中。在存储器装置验证替换的完整性之后，包445可经由执行从存储器装置130加载的包441中的指令而替换。任选地，第二验证码153可经生成以将替换写入到存储器装置130中和/或允许执行包445的修复或替换。

[0542] 图22示出根据一个实施例的基于端点的一或多个活动执行安全操作的方法。例如，图22的方法可以使用图18和20的技术实施。

[0543] 在框481处，服务器系统存储表示端点150的一或多个偏好455的数据。

[0544] 例如，服务器系统可包含存储存储器装置(例如，130)和/或其它服务器的秘密的安全服务器140，所述其它服务器例如活动跟踪器451、包存储库191、固件商店170和/或另一服务器。

[0545] 在框483处，服务器系统接收含有由配置在端点150中的存储器装置130生成的身份数据113的验证请求173。

[0546] 在框485处，服务器系统至少部分地基于存储器装置的秘密而确定身份数据113有效。

[0547] 例如，框485中的操作可以类似于在框323、框343、框403、框423和/或框463中执行的操作的方式来执行。

[0548] 在框487处，服务器系统确定与身份数据113相关联的活动满足为端点150指定的条件。

[0549] 例如，所述条件可在端点150的偏好455中指定。

[0550] 在框489处，在响应于验证请求173而提供验证响应174时，服务器系统执行与条件相关联的安全操作。

[0551] 例如，安全操作可包含向在所述一或多个参考455中注册的联系人传输警告或通知。

[0552] 例如，安全操作可包含识别验证响应174中的安全风险或限制。任选地，鉴于存储器装置130的秘密密钥137和在身份数据113中提供的消息131，安全服务器140可提供即使在身份数据113具有有效验证码133时也不确认端点150的真实性的验证响应174。当与身份数据113相关联的活动满足条件时，验证响应174可配置成使客户端服务器拒绝对由身份数

据113识别的端点150的服务的请求171。

[0553] 可以基于存储器装置130嵌入在身份数据113中的活动信息177和/或由客户端服务器141在验证请求173中提供的访问属性449针对活动来评估条件。

[0554] 例如，在安全服务器140确定身份数据113中的验证码133有效之后，安全服务器140可信任嵌入在身份数据113中的活动信息177在存储器装置130生成验证码133之后尚未改变。因此，活动信息177可以从身份数据113中提取以评估条件。任选地，活动信息177可以密文形式在消息中提供，所述密文要使用以图9中所论述的方式生成的会话密钥263或存储器装置130的另一秘密加密密钥进行解密。

[0555] 替代地或组合地，安全服务器140可从验证请求173提取访问属性449。例如，在客户端服务器141接收对由客户端服务器141提供的服务的访问请求171之后，客户端服务器141可生成验证请求173到安全服务器140。验证请求173经生成以包含来自访问请求171的身份数据113。此外，在请求客户端服务器141的服务的背景下，客户端服务器141可添加访问属性449以提供关于端点150的活动的信息。

[0556] 例如，条件可包含活动信息177和访问属性449的不匹配；并且不匹配可在验证响应174中触发访问请求171的拒绝和/或身份数据113的拒绝，即使在身份数据113具有有效验证码133时。

[0557] 在一些实施方案中，服务器系统与用户计算机180通信以接收表示端点150的所述一或多个偏好455的数据。

[0558] 替代地或组合地，服务器系统可从过往活动的记录453推断偏好455。

[0559] 例如，服务器系统的活动跟踪器451可存储端点150的活动的多个记录453。基于多个记录453，活动跟踪器451可确定端点150的活动模式。模式可包含地理区域、一天或一周中的时间段或活动属性的范围，或其任何组合。触发框489的安全操作的条件可被偏离模式的活动满足。

[0560] 任选地，活动跟踪器451可基于记录453而向端点150的所有者或授权用户呈现端点150的活动。例如，基于过往活动的检查，所有者或授权用户可指定实施家长控制、访问限制等的条件。

[0561] 经安全服务器140认证的端点150的身份可动态地与由账户标识符表示的订阅账户相关联以接收客户端服务器141提供到账户的服务。当端点150不使用服务时，端点150的身份和订阅账户之间的关联可以去除以允许另一端点使用订阅账户。因此，一组端点(例如，150)可配置成共享订阅账户，并一次一个地使用订阅账户。

[0562] 例如，一组端点可配置成使用客户端服务器141的服务进行蜂窝连接。传统上，订户识别模块(SIM)卡将用于表示订户/订阅账户。这一组端点可通过每次在群组中的一个端点中物理地安装SIM卡来使用由SIM卡表示的订阅账户。为了使群组中的另一端点能够使用订阅账户，SIM卡将物理地从一个端点移动到另一端点。

[0563] 如上文结合图6所论述的系统允许使用虚拟订户识别模块(vSIM)通过虚拟卡注册237并基于使用安全服务器140执行的身份验证或端点认证239而附接到端点(例如，150)上。图6的系统可进一步配置成解除端点(例如，150)与表示订阅账户的卡简档219的关联，使得虚拟卡注册237可经执行以供另一端点使用订阅账户。

[0564] 例如，提供给订阅账户的订阅服务(例如，蜂窝连接)可以在企业(或另一实体)所

拥有的一群端点当中共享。这一群中的端点(例如,150)可能不会同时需要账户的服务。因此,将这一群中的端点配置成共享一或多个订阅账户可能是有利的。当超过一个订阅账户配置成由一群端点(例如,物联网(IoT)装置)共享时,这一群中的小部分可以同时使用订阅账户的服务。

[0565] 例如,服务器系统可配置成跟踪群体中的端点的当前使用状态。当端点与客户端服务器通信以请求服务时,端点可以动态地绑定到订阅账户。当端点不是正在使用服务时,订阅账户可以从所述端点释放。当正在使用提供给订阅账户的服务的端点的数目大于可以共享的订阅账户的数目时,作用中端点可同时使用账户的服务。当订阅账户当前绑定到群体的一部分且正在被这一部分使用时,来自另一端点的对服务的请求可被拒绝,直到订阅账户中的一个不使用且因此变得可用于共享为止。

[0566] 例如,响应于企业的物联网(IoT)装置请求蜂窝连接,虚拟订户识别模块(vSIM)可以绑定到IoT装置。当蜂窝连接在长于阈值的一段时间内一直空闲时,蜂窝连接可以断开连接;并且虚拟订户识别模块(vSIM)可以从IoT装置释放,并且可用于与企业的另一IoT装置绑定。因此,企业可订阅减少数目的vSIMs;并且当这些vSIMs全都在使用时,来自另一装置的蜂窝连接的请求可处于保持状态,直到连接中的一个断开且vSIM被释放用于分配给保持中装置为止。

[0567] 任选地,安全服务器140可配置成抑制和/或调度连接请求的转发以管理有限数目的订阅蜂窝连接的使用。

[0568] 图23和24示出根据一个实施例的配置成在一组端点当中实施订阅共享的系统。

[0569] 在图23和24中,服务商店190具有使端点群组501与订户群组503相关联的订阅数据387。

[0570] 端点群组501具有多个唯一识别111、…、112。唯一识别(例如,111)中的每一个表示安装于一组端点中的相应端点(例如,150)中的存储器装置(例如,130)。

[0571] 订户群组503具有一或多个订户身份编号(例如,505)。订户群组503中的每个订户身份编号(例如,505)表示客户端服务器141的服务的订户。例如,每个订户身份编号(例如,505)可用于识别每次供一个订户使用的唯一订阅账户。

[0572] 例如,订户身份编号505可用于表示唯一订户,方式与订户识别模块(SIM)表示蜂窝通信网络中的订户相同。

[0573] 当SIM卡插入在蜂窝电话中时,与订户的通信连接到蜂窝电话;并且蜂窝电话具有订户账户中的服务。当SIM卡插入到替代蜂窝电话中时,与订户的通信连接到当前具有SIM卡的替代蜂窝电话。

[0574] 类似地,当订户身份编号505与唯一识别111相关联时,提供到由订户身份编号505表示的订户账户的服务被提供给具有唯一识别111的端点150。当订户身份编号505与替代性唯一识别112相关联时,提供到由订户身份编号505表示的订户账户的服务被提供给具有唯一识别112的替代端点。

[0575] 在图23中,安全服务器140配置成动态地链接订户群组503中的订户身份编号505和端点群组501中的唯一识别111。

[0576] 例如,响应于具有身份数据113的来自客户端服务器141的验证请求173,安全服务器140可确定身份数据113是否具有用于具有唯一识别111的存储器装置130的有效验证码

133。如果身份数据113有效，那么安全服务器140可确定订户群组503当前是否具有空闲以供具有唯一识别111的存储器装置130和/或端点150使用的订户身份编号505。如果是，那么安全服务器140可提供确认身份数据113的真实性及其与订户身份编号505的关联的验证响应174。作为响应，客户端服务器141可将提供到由订户身份编号505识别的账户的服务提供给端点150。

[0577] 在一些实施方案中，如果当前在订户群组503中没有订户身份编号505可供端点150使用，那么验证响应174未识别出身份数据113的订户身份编号，这可使客户端服务器141拒绝来自端点150的服务请求。

[0578] 图23中的验证请求173可包含访问属性449，其指示用于使身份数据113中所识别的唯一识别111与可供具有唯一识别111的端点150使用的订户身份编号(例如，505)相关联的所请求时间段。

[0579] 在一些实施方案中，系统配置成在识别唯一识别111和/或身份数据113的订户身份编号505的验证响应174之后的预定时间段内使唯一识别111和订户身份编号505相关联。在所述预定时间段之后，服务商店190去除订户身份编号505到唯一识别111的分配，使得订户身份编号505可用于端点群组501中的具有不同的唯一识别(例如，112)的另一端点。在所述预定时间段之后，客户端服务器141不将提供到由订户身份编号505表示的账户的服务提供到端点群组501中具有唯一识别111、…、112的端点(例如，150)中的任一个，直到从安全服务器140接收到使订户身份编号505与端点群组501中的唯一识别111、…、112中的一个相关联的另一验证响应174为止。

[0580] 当具有唯一识别111、…、112的端点竞争使用订户群组503中的订户身份编号(例如，505)时，服务商店190可控制订户群组503中的订户身份编号(例如，505)的使用分配。

[0581] 例如，服务商店190可跟踪群组501中因为没有可用订户身份编号505而拒绝访问请求的端点，并基于所跟踪的优先级，对可用订户身份编号505的后续分配进行优先级排序。

[0582] 例如，当订户身份编号505可供使用时，服务商店190可打开其中可以接收来自不同端点的访问请求的时间窗；当接收到群组501的多个访问请求时，具有在所述时间窗之前被拒绝的最早请求的端点可具有获得使用订户身份编号505的机会的最高优先级。

[0583] 在一些实施方案中，端点群组501中的具有唯一识别111、…、112的端点可基于一或多个预定义规则来竞争使用订户群组503中的订户身份编号(例如，505)的机会。例如，在接收到对服务请求的拒绝之后，端点(例如，150)可等待进行后续请求的随机时间段。通过拒绝之后的等待时段的随机性，使用订户群组503获得服务访问的机会可以分配给需要服务的端点。

[0584] 在一些实施方案中，被临时分配订户身份编号505的端点150可通知客户端服务器141和/或安全服务器140将订户身份编号505从对端点150的分配中释放出来。例如，在端点150使用提供给订户身份编号505的服务完成通信之后，端点150可以将订户身份编号505返回到群组503中的订户身份编号池，此订户身份编号池可以分配给群组501中具有唯一识别112的另一个端点和/或由所述另一个端点使用。

[0585] 在一些实施方案中，系统可跟踪使用订户身份编号505的端点150的作用中活动。在非作用中时段之后，服务商店190可从唯一识别111中去除订户身份编号505的分配。

[0586] 图23示出其中由安全服务器140结合验证请求173和/或验证响应174控制将订户身份编号505分配给唯一识别111的配置。替代地和/或组合地，客户端服务器141可以连接到服务商店190以实施分配和/或使用分配来提供服务，如图24所示。

[0587] 在图24中，客户端服务器141耦合到服务商店190和活动跟踪器451。基于指示具有唯一识别111的端点150的真实性和订户身份编号505用于端点群组501的可用性的验证响应174，客户端服务器141可使服务商店190存储指示订户身份编号505到唯一识别111的临时分配的数据。

[0588] 随后，客户端服务器141可使用活动跟踪器451确定是否从唯一识别111中去除订户身份编号505的分配。

[0589] 例如，在其中端点150不使用提供到由订户身份编号505表示的账户的服务的预定长度的非作用中时间段之后，客户端服务器141可使服务商店190更新订阅数据387，并终止订户身份编号505到唯一识别111的分配。

[0590] 例如，在从端点150接收指示或通知之后，客户端服务器141可使服务商店190终止订户身份编号505到唯一识别111的分配。

[0591] 在一些实施方案中，在订户身份编号505分配到唯一识别111后某一时间段，客户端服务器141可使服务商店190终止订户身份编号505到唯一识别111的分配。所述时间段可以是预定的，或根据从端点150接收的访问请求171确定。

[0592] 图25示出根据一个实施例的用于促进一组端点中的订阅共享的方法。例如，图25的方法可以使用上文结合图23和24所论述的技术在具有结合图1到19论述的安全特征的系统中实施。

[0593] 在框521处，服务器系统存储使端点群组501与至少一个订户标识符(例如，身份编号505)相关联的数据。端点群组501可具有由唯一识别111、…、112所识别的多个端点(例如，150)。

[0594] 例如，服务器系统可包含存储存储器装置(例如，130)和/或其它服务器的秘密的安全服务器140，所述其它服务器例如服务商店190、活动跟踪器451、包存储库191、固件商店170和/或另一服务器。服务器系统可进一步包含图6中所示的客户端服务器141和/或卡服务器223。

[0595] 在框523处，服务器系统接收含有由配置在端点150中的存储器装置130生成的身份数据113的验证请求173。身份数据113使用其在端点群组501中的唯一识别111来识别端点150。

[0596] 在框525处，响应于验证请求173，服务器系统至少部分地基于存储器装置130的秘密而确定身份数据113有效。

[0597] 例如，框525中的操作可以类似于在框323、框343、框403、框423、框463和/或框485中执行的操作的方式执行。

[0598] 在框527处，服务器系统确定订户标识符(例如，身份编号505)当前未分配给端点群组501中的任何端点。

[0599] 在框529处，服务器系统基于使端点群组501与订户标识符(例如，身份编号505)相关联的数据而向端点150分配订户标识符。所述分配使提供到由订户标识符(例如，身份编号505)表示和/或与其相关联的账户的服务能够提供给端点。

[0600] 例如，订户标识符(例如，身份编号505)表示在具有多个端点(例如，150)的网络(例如，225)中提供的服务的唯一订户，所述端点包含端点群组501中的多个端点以及不在端点群组501中的其它端点。

[0601] 例如，服务网络(例如，225)可配置成向端点提供服务，例如蜂窝通信连接、互联网连接、到用户计算机的连接、在线存储设施、在线计算资源、支付、交易或消息，或其任何组合。

[0602] 例如，向端点150分配订户标识符(例如，身份编号505)包含将端点150配置成在服务网络(例如，225)中具有由订户标识符(例如，身份编号505)表示的唯一身份。

[0603] 例如，服务网络(例如，225)可能需要网络(例如，225)中的不同端点具有由不同订户标识符(例如，身份编号505)表示的不同身份。由存储器装置130生成的身份数据113不包含订户标识符。存储器装置130和/或端点150的身份数据113和/或唯一识别111可以动态地分配给订户标识符(例如，身份编号505)或与其相关联，以为服务网络(例如，225)配置端点150。

[0604] 例如，向端点150分配订户标识符(例如，身份编号505)包含存储表示在某一时间段内订户标识符到端点的分配的数据。

[0605] 例如，服务器系统可在所述时间段之后去除表示订户标识符到端点的分配的数据，以中断端点150作为订户接收网络中的服务。在数据去除之后，端点150在服务网络(例如，225)中不再具有由订户标识符(例如，身份编号505)表示的订户身份。

[0606] 例如，服务系统可监测端点150在服务网络(例如，225)中作为订户接收服务时的活动；并且响应于检测到端点150在网络(例如，225)中作为订户接收服务时的非作用中时段，服务器系统可去除数据以将端点150重新配置成在服务网络(例如，225)中不具有由订户标识符(例如，身份编号505)表示的订户身份。

[0607] 替代地，响应于来自端点150的消息或请求，可以执行将端点150从服务网络(例如，225)中配置为订户标识符(例如，身份编号505)释放出来。

[0608] 替代地，订户标识符(例如，身份编号505)从绑定到端点150的释放之后的时间段的长度可以是从将订户标识符(例如，身份编号505)分配到端点150的时间开始的预定长度。

[0609] 替代地，所述时间段的长度可以在验证请求173中指定。

[0610] 例如，验证请求173从服务网络(例如，225)中的客户端服务器141接收。为了将端点150配置成具有由订户标识符(例如，身份编号505)表示的订户身份，安全服务器140可响应于验证请求173向客户端服务器141传输验证响应174。验证响应174配置成指示身份数据113的有效性及身份数据113与订户标识符(例如，身份编号505)的关联。

[0611] 一般来说，端点150可以使用不同服务的不同识别、在不同网络中和/或在不同上下文中来识别。端点150的每个识别可用于将端点150表示为特定于某一类型的服务、连接、通信等的群组中的许多的成员、订户、账户、经授权装置和/或实体。

[0612] 例如，端点150可配置成与分别用于其服务的不同客户端服务器141、…、143通信。端点150可以使用不同订户识别利用不同客户端服务器141、…、143识别。端点150的每一个订户识别表示由相应客户端服务器(例如，141、…、143)针对其对订户群体的服务辨识出的唯一订户和/或账户。

[0613] 例如，端点150可配置成与客户端服务器141通信以获得不同类型的服务。端点150的不同识别可用于将端点150表示为不同服务类型的订户。

[0614] 例如，端点150可被分配集成电路卡标识符251以用作智能卡、移动设备身份编号253以用作蜂窝通信装置、移动订户身份编号255以用作蜂窝连接服务的订户，等等。

[0615] 安全服务器140可配置成使用配置在端点150中的存储器装置130的安全特征来管理端点150的身份。

[0616] 例如，第三方可以请求安全服务器140将账户中的订阅服务绑定到端点150的公共识别。由于识别可为公众所知，因此存在欺诈性使用公共识别的潜在风险。端点150的身份数据113可配置成包含公共识别。基于在端点150中配置的存储器装置130的唯一装置秘密(UDS)101，安全服务器140可以验证从端点150接收的身份数据113是真实的；因此，端点150具有由包含在身份数据113中的公共识别表示的身份。通过安全服务器140执行的验证，可以检测到将公共识别作为身份的欺诈性使用。

[0617] 安全服务器140可配置成管理公共识别与端点150的安全、动态绑定。例如，响应于来自应用域中的被授权方的请求，安全服务器140可以将唯一公共识别绑定到应用域的端点150。例如，可以基于跟踪在端点(例如，150)中配置的存储器装置的所有权权限来验证被授权方。每个应用域可以具有表示应用域中的单独身份的多个公共识别。安全服务器140每次将唯一的公共识别绑定到一个端点。

[0618] 例如，响应于将公共识别绑定到端点150的请求，安全服务器140可以验证公共识别当前未绑定到另一个端点，并且可以使用表示所有者权限的加密密钥生成命令来操作存储器装置130，将公共识别存储在存储器装置130中作为用于生成存储器装置130和/或端点150的身份数据113的装置信息121的一部分。

[0619] 替代地，安全服务器140可以在应用域中存储将端点150与端点150的公共识别相关联的数据。响应于应用域中的验证请求173，安全服务器140验证端点150中提供的身份数据113，并在应用域中查找端点150的公共识别。可在验证响应174中提供公共识别。

[0620] 公共识别与端点150的安全、动态绑定可用于促进安全操作。例如，当端点150丢失/被盗时，端点150的所有者可以请求安全服务器140将丢失/被盗端点150的公共识别绑定到替换端点。一旦安全服务器140将丢失/被盗端点150的公共识别绑定到替换端点，订阅给丢失/被盗端点150的服务就转移到替换端点。任选地，丢失/被盗端点150的所有者可以请求将数据从丢失/被盗端点150转移到替换装置；并且在转移之后，所有者可以请求停用丢失/被盗端点150以最小化端点150的丢失/影响。

[0621] 图26示出根据一个实施例的用于管理端点识别的技术。

[0622] 例如，图26的技术可使用结合图1到5和9到10论述的存储器装置的安全特征在图1和/或6的系统中使用。例如，图26的技术可以与图14和15的固件商店、图15、23和24的服务商店190和/或图20的活动跟踪器451的服务一起使用。

[0623] 在图26中，安全服务器140存储存储器装置130的唯一识别111和其唯一装置秘密101。此外，安全服务器140存储表征安装了存储器装置130的端点150的硬件、软件和/或数据配置的装置信息121。如在图2中，秘密密钥137是基于唯一装置秘密101和装置信息121。秘密密钥137供存储器装置130用于生成身份数据113的验证码133；并且安全服务器140验证验证码133是使用秘密密钥137生成的，其指示身份数据113是由具有唯一装置秘密101的

存储器装置130生成的。

[0624] 在图26中，安全服务器140可将唯一识别111绑定到端点150的公共识别541。例如，在公共识别541分配给应用域中的端点150之后，安全服务器140可将公共识别541存储为与存储器装置130和/或端点150的唯一识别相关联的装置信息121的部分。

[0625] 例如，应用域可配置成用于蜂窝连接、智能卡处理、客户端服务器141的服务等。识别541可用于表示应用域中的一群端点中的端点150。识别541可用于将端点150表示为装置、成员、服务订户、账户、联系人等。

[0626] 例如，在应用域中操作的客户端服务器141可以请求安全服务器140将公共识别541绑定到具有唯一识别111的端点150。在请求549中，客户端服务器141可以提供从端点150接收的身份数据113和要绑定到端点150的公共识别541。响应于请求549，安全服务器140通过确定身份数据113中的验证码133是否是使用具有唯一识别111的存储器装置130的秘密密钥137生成的来验证身份数据113。

[0627] 在身份数据113的验证之后，安全服务器140可以将公共识别541添加到装置信息121，并使端点150中的存储器装置130更新543装置信息121。在更新543之后，存储器装置130具有用于其生成包含公共识别541的新身份数据113的新秘密密钥。例如，除了唯一识别111之外，新身份数据113中的消息131还可包含公共识别541。配置成防止对唯一识别111的欺诈性使用的存储器装置130的安全特征还可以防止对公共识别541的欺诈性使用。例如，当客户端服务器141接收到含有公共识别541的新身份数据113时，客户端服务器141可以请求安全服务器140验证新身份数据113。如果新身份数据113具有有效的验证码133，那么其由被分配公共识别541的端点150生成。

[0628] 安全服务器140可以以类似于端点150的固件的更新377和/或端点150中安装的包的修复385的方式更新543装置信息121。例如，安全服务器140可以生成命令155的验证码153，以将公共识别541存储在存储器装置130的存储器单元103中。使用表示操作存储器装置130的所有者权限的加密密钥145生成验证码153，所述所有者权限包含由存储器装置130的访问控制器109控制的用于在存储器装置130中执行命令155的权限。

[0629] 任选地，公共识别541与端点150的关联不需要生成新的秘密密钥来表示存储器装置130和/或端点150。公共识别541可以包含在用于生成使用秘密密钥137签名的验证码133的消息131中。验证码133的验证指示消息131中提供的公共识别541尚未改变；并且验证码133由安装在端点150中的存储器装置130签名。

[0630] 任选地，跳过更新543；并且存储器装置130和/或端点150不存储公共识别541。安全服务器140存储将唯一识别111与公共识别541相关联的数据。在安全服务器140验证在验证请求中提供的身份数据113之后，安全服务器140可以查找与应用域相关的公共识别541，以查找在身份数据113的消息131中识别的唯一识别111，并在验证响应中提供公共识别541，方式类似于在图23所示的验证响应174中呈现订户身份编号505的方式。

[0631] 任选地，安全服务器140具有门户545，其允许计算机180提交请求547以将公共识别541与具有唯一识别111的端点150相关联。在门户545验证计算机180由端点150的授权所有者或用户操作之后，门户545可以与安全服务器140通信以更新唯一识别111的装置信息121。

[0632] 在一个实施例中，端点150具有存储于存储器装置130中的包。当包从存储器装置

130加载并在主机系统120中执行时，端点150可与服务器140通信以获得更新543。端点150和服务器140之间的通信可通过客户端服务器(例如，141)、固件商店170、服务商店190、活动跟踪器451或另一服务器(例如，门户545)，也可不通过任何中间服务器。

[0633] 例如，端点(例如，150)的制造商可使用计算机180配置端点(例如，150)并请求由制造商分配的识别(例如，541)绑定到端点(例如，150)。例如，此类公共识别可以是表示通信网络中的各个装置的移动设备身份编号(例如，253)。

[0634] 例如，服务提供商可以将订户身份编号(例如，255)分配给提供商提供的服务的订户。当端点150的所有者或用户注册提供商的服务时，服务提供商可以使用计算机180请求将订户身份编号255与端点150绑定。

[0635] 图27示出根据一个实施例的用于管理端点的识别的方法。例如，图27的方法可以使用上文结合图26所论述的技术在具有结合图1到19论述的安全特征的系统中实施。

[0636] 在框561处，服务器系统存储使在端点150中配置的存储器装置130的秘密(例如，101)、端点150的第一识别111和装置信息121相关联的数据。

[0637] 例如，服务器系统可包含安全服务器140。任选地，服务器系统可进一步包含门户545、固件商店170、服务商店190、活动跟踪器451、包存储库191和/或另一服务器。在一些实施方案中，服务器系统可进一步包含图6中所示的客户端服务器141和/或卡服务器223。

[0638] 在框563处，服务器系统接收将第二识别541绑定到由第一识别111识别的端点150的请求(例如，547或549)。

[0639] 例如，将第二识别541绑定到端点150的请求(例如，547或549)可以在服务器系统中从与端点150分开的计算机(例如，180或服务器141)接收和/或在所述计算机中发起。服务器系统配置成确定计算机是否具有将此类第二识别541附接到端点150的权限。如果是，那么服务器系统140可存储将第一识别111和第二识别541相关联的数据。

[0640] 在一个实施例中，将此类第二识别541附接到端点150的权限与操作计算机且具有存储器装置130的所有权(例如，作为制造商、零售商、服务提供商、端点150的终端用户)相关联的实体。

[0641] 例如，实体可使用计算机与端点150和/或存储器装置130通信以检索由存储器装置130生成的当前身份数据113。当前身份数据113包含第一识别111，并且可由服务器系统就来自存储器装置130的当前身份数据113是否真实进行验证。

[0642] 例如，响应于请求，服务器系统可存储使第一识别111与第二识别541相关联的数据。

[0643] 例如，服务器系统可更新第一识别111的装置信息121以包含第二识别541。

[0644] 例如，服务器系统可与端点150通信以更新存储于存储器装置130中的数据和/或在存储器装置130中存储第二识别541。

[0645] 任选地，第二识别541可用作在存储器装置130中用于生成秘密密钥137的装置信息121的部分，其中秘密密钥137用于生成存储器装置130和/或端点150的身份数据113的验证码133。

[0646] 任选地，第二识别541不改变秘密密钥137的生成。但是，第二识别541存储到存储器装置130的访问受控区中，并且包含在呈现于身份数据113中的消息131中(例如，作为数据C 127的部分)。

[0647] 例如,响应于将第二识别541绑定到端点150的请求,服务器系统可以生成命令155的验证码153,并且使存储器装置130根据验证码153执行命令155。在接收到命令155和命令155的验证码153之后,存储器装置130的访问控制器109配置成使用表示在存储器装置130中执行命令155的权限的加密密钥(例如,访问控制密钥149)来验证命令155的验证码153。存储器装置130配置成响应于确定命令155的验证码153有效而执行命令155;在存储器装置130中执行命令155可将第二识别541存储在存储器装置130中以用于身份数据113的后续生成。例如,第二识别541可以存储为装置信息121的部分和/或用于在身份数据113的消息131中呈现。

[0648] 例如,存储器装置在端点150中存储可执行的一组指令。所述一组指令可以是内容161的一部分,或者是端点的固件或操作系统的包441。存储器装置130配置成在允许端点150加载所述一组指令以供执行之前验证所述一组指令的完整性。由于所述一组指令经由存储器装置130受保护,因此服务器系统可以与执行所述一组指令的端点150可靠地通信,以使存储器装置130执行命令155。端点150和服务器系统之间的通信路径可以任选地通过客户端服务器141和/或任选地经由会话密钥263和对称加密受保护。

[0649] 在框565处,服务器系统接收含有由存储器装置130生成的身份数据113的验证请求173。身份数据113包含从在身份数据113中呈现的消息131生成的验证码133和至少部分地从秘密(例如,101)导出的加密密钥(例如,秘密密钥137)。

[0650] 例如,在一些实施方案中,在身份数据中呈现的消息131含有第二识别541。任选地,当第二识别541被配置为装置信息121的部分时,用于对呈验证码133形式的消息131进行签名的加密密钥(例如,秘密密钥137)可以进一步基于第二识别541导出;替代地,加密密钥与第二识别541无关。

[0651] 在一些实施方案中,在身份数据113中呈现的消息131不包含第二识别541。

[0652] 在框567处,服务器系统至少部分地基于存储器装置130的秘密(例如,101)而验证身份数据113的有效性。

[0653] 例如,框567中的操作可以类似于在框323、框343、框403、框423、框463、框485和/或框525中执行的操作的方式执行。

[0654] 在框569处,服务器系统响应于确定身份数据113有效而提供对验证请求173的验证响应174。验证响应174配置成指示身份数据113是由具有第二识别541的端点150生成的。

[0655] 例如,服务器系统可通过在存储于安全服务器140中的数据中查找与第一识别相关联的第二识别541或从身份数据113提取第二识别541来识别验证响应174中的第二识别541。替代地,服务器系统可指示身份数据113有效,包含在包含于身份数据113中的消息131中呈现的第二识别541。

[0656] 图28示出计算机系统600的实例机器,其内可以执行用于使机器执行本文所论述的任何一或多个方法的一组指令。在一些实施例中,计算机系统600可对应于包含、耦合到或使用存储器子系统的主机系统,或者可用于执行安全管理器160的操作(例如,执行指令以执行对应于参考图1-27描述的安全服务器140和/或存储器装置130的安全特征的操作)。在替代实施例中,所述机器可以在LAN、内联网、外联网和/或互联网中连接(例如,联网)到其它机器。所述机器可以客户端-服务器网络环境中的服务器或客户端机器的资格操作,作为对等(或分布式)网络环境中的对等机器操作,或作为云计算基础设施或环境中的服务器

或客户端机器操作。

[0657] 所述机器可以是个人计算机(PC)、平板PC、机顶盒(STB)、个人数字助理(PDA)、蜂窝电话、网络器具、服务器、网络路由器、交换机或桥接器,或能够执行(依序或以其它方式)指定将由所述机器采取的动作的一组指令的任何机器。另外,尽管示出单个机器,但术语“机器”还应被认为包含机器的任何集合,所述机器的集合单独地或共同地执行一组(或多组)指令以执行本文论述的方法中的任何一或多个。

[0658] 实例计算机系统600包含处理装置602、主存储器604(例如,只读存储器(ROM)、快闪存储器、动态随机存取存储器(DRAM),例如同步DRAM(SDRAM)或Rambus DRAM(RDRAM)、静态随机存取存储器(SRAM)等),以及数据存储系统618,它们经由总线630(其可包含多个总线)彼此通信。

[0659] 处理装置602表示一或多个通用处理装置,例如微处理器、中央处理单元等。更具体地说,处理装置可以是复杂指令集计算(CISC)微处理器、精简指令集计算(RISC)微处理器、超长指令字(VLIW)微处理器,或实施其它指令集的处理器,或实施指令集的组合的处理器。处理装置602还可以是一或多个专用处理装置,例如专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)、网络处理器等。处理装置602配置成执行用于执行本文中所论述的操作和步骤的指令626。计算机系统600可进一步包含经由网络620通信的网络接口装置608。

[0660] 数据存储系统618可包含机器可读媒体624(也被称为计算机可读媒体),在其上存储一组或多组指令626或体现本文中所描述的方法或功能中的任何一或多个的软件。指令626在由同样构成机器可读存储媒体的计算机系统600、主存储器604和处理装置602执行期间还可完全地或至少部分地驻存在主存储器604内和/或处理装置602内。机器可读媒体624、数据存储系统618和/或主存储器604可对应于存储器子系统。

[0661] 在一个实施例中,指令626包含实施对应于安全管理器160(例如,参考图1-27描述的安全服务器140和/或存储器装置130的安全特征的操作)的功能性的指令。尽管在实例实施例中机器可读存储媒体624示出为单个媒体,但是术语“机器可读存储媒体”应被认为包含存储一组或多组指令的单个媒体或多个媒体。术语“机器可读存储媒体”还应被认为包含能够存储或编码供机器执行的一组指令且使机器执行本公开的方法中的任何一或多个的任何媒体。术语“机器可读存储媒体”因此应被认为包含但不限于固态存储器、光学媒体和磁性媒体。

[0662] 一般来说,端点150、服务器(例如,安全服务器140、客户端服务器141或143或卡服务器223)可以是具有主机系统120和存储器子系统的计算系统。存储器子系统可包含媒体,例如一或多个易失性存储器装置、一或多个非易失性存储器装置(例如,存储器装置130)或这些都组合。

[0663] 存储器子系统可以是存储装置、存储器模块或存储装置和存储器模块的混合物。存储装置的实例包含固态驱动器(SSD)、快闪驱动器、通用串行总线(USB)快闪驱动器、嵌入式多媒体控制器(eMMC)驱动器、通用快闪存储(UFS)驱动器、安全数字(SD)卡和硬盘驱动器(HDD)。存储器模块的实例包含双列直插式存储器模块(DIMM)、小外廓DIMM(SO-DIMM)和各种类型的非易失性双列直插式存储器模块(NVDIMM)。

[0664] 例如,计算系统可为计算装置,例如台式计算机、膝上型计算机、网络服务器、移动

装置、交通工具(例如,飞机、无人机、火车、汽车或其它运输工具)、具有物联网(IoT)功能的装置、嵌入式计算机(例如,交通工具、工业设备或联网商业装置中包含的嵌入式计算机),或包含存储器和处理装置的此类计算装置。

[0665] 计算系统的主机系统120耦合到一或多个存储器子系统。如本文中所使用,“耦合到”或“与……耦合”大体上是指组件之间的连接,此连接可以是间接通信连接或直接通信连接(例如,不具有中间组件),不管是有线还是无线,包含电气、光学、磁性等连接。

[0666] 主机系统120可包含处理器芯片组(例如,处理装置118)和由处理器芯片组执行的软件堆栈。处理器芯片组可包含一或多个核心、一或多个高速缓存、存储器控制器(例如,控制器116)(例如,NVDIMM控制器)和存储协议控制器(例如,PCIe控制器、SATA控制器)。主机系统120使用存储器子系统,例如以便将数据写入到存储器子系统和从存储器子系统读取数据。

[0667] 主机系统120可以经由物理主机接口耦合到存储器子系统。物理主机接口的实例包含但不限于串行高级技术附件(SATA)接口、外围组件互连高速(PCIe)接口、通用串行总线(USB)接口、光纤通道、串行连接的SCSI(SAS)接口、双倍数据速率(DDR)存储器总线接口、小型计算机系统接口(SCSI)、双列直插式存储器模块(DIMM)接口(例如,支持双倍数据速率(DDR)的DIMM套接接口)、开放NAND快闪接口(ONFI)、双倍数据速率(DDR)接口、低功率双倍数据速率(LPDDR)接口,或任何其它接口。物理主机接口可用于在主机系统120和存储器子系统之间传输数据。主机系统120可进一步利用NVM快速(NVMe)接口,在存储器子系统通过PCIe接口与主机系统120耦合时访问组件(例如,存储器装置130)。物理主机接口可提供用于在存储器子系统和主机系统120之间传递控制、地址、数据和其它信号的接口。一般来说,主机系统120可经由同一个通信连接、多个单独的通信连接和/或通信连接的组合访问一或多个存储器子系统。

[0668] 主机系统120的处理装置118可以是例如微处理器、中央处理单元(CPU)、处理器的处理核心、执行单元等。在一些情况下,控制器116可称为存储器控制器、存储器管理单元和/或起始器。在一个实例中,控制器116控制通过耦合在主机系统120与存储器子系统之间的总线进行的通信。一般来说,控制器116可向存储器子系统发送期望访问存储器装置130的命令或请求。控制器116可进一步包含用于与存储器子系统通信的接口电路系统。接口电路系统可将从存储器子系统接收到的响应转换成用于主机系统120的信息。

[0669] 主机系统120的控制器116可与存储器子系统的控制器进行通信以执行操作,例如在存储器装置130处读取数据、写入数据或擦除数据以及其它此类操作。在一些情况下,控制器116集成在处理装置118的同一封装内。在其它情况下,控制器116与处理装置118的封装分开。控制器116和/或处理装置118可包含硬件,例如一或多个集成电路(IC)和/或离散组件、缓冲存储器、高速缓存存储器或其组合。控制器116和/或处理装置118可以是微控制器、专用逻辑电路系统(例如现场可编程门阵列(FPGA)、专用集成电路(ASIC)等)或另一合适的处理器。

[0670] 存储器装置130可包含不同类型的非易失性存储器组件和/或易失性存储器组件的任何组合。易失性存储器装置可以是但不限于随机存取存储器(RAM),例如动态随机存取存储器(DRAM)和同步动态随机存取存储器(SDRAM)。

[0671] 非易失性存储器组件的一些实例包含“与非”(或NOT AND)(NAND)型快闪存储器和

就地写入存储器，例如三维交叉点(“3D交叉点”)存储器。非易失性存储器交叉点阵列可结合可堆叠交叉网格化数据存取阵列基于体电阻的变化而执行位存储。另外，与许多基于快闪的存储器相比，交叉点非易失性存储器可执行原位写入操作，其中非易失性存储器单元可以在其先前已进行擦除的情况下进行编程。NAND型快闪存储器包含例如二维NAND(2D NAND)和三维NAND(3D NAND)。

[0672] 存储器装置130中的每一个可包含一或多个存储器单元阵列。一种类型的存储器单元，例如单层级单元(SLC)，可每单元存储一个位。其它类型的存储器单元，例如多层级单元(MLC)、三层级单元(TLC)、四层级单元(QLC)和五层级单元(PLC)，可每单元存储多个位。在一些实施例中，存储器装置130中的每一个可包含例如SLC、MLC、TLC、QLC、PLC或它们的任何组合的一或多个阵列。在一些实施例中，特定存储器装置可包含存储器单元的SLC部分、MLC部分、TLC部分、QLC部分和/或PLC部分。存储器装置130的存储器单元可以分组为页，页可以指用于存储数据的存储器装置的逻辑单元。在一些类型的存储器(例如，NAND)中，可以将页分组以形成块。

[0673] 尽管描述了非易失性存储器装置，例如3D交叉点型和NAND型存储器(例如，2D NAND、3D NAND)，但是存储器装置130可以基于任何其它类型的非易失性存储器，例如只读存储器(ROM)、相变存储器(PCM)、自选存储器、其它基于硫属化物的存储器、铁电晶体管随机存取存储器(FeTRAM)、铁电随机存取存储器(FeRAM)、磁随机存取存储器(MRAM)、自旋转移力矩(STT)-MRAM、导电桥接RAM(CBRAM)、电阻性随机存取存储器(RRAM)、基于氧化物的RRAM(OxRAM)、或非(NOR)快闪存储器，以及电可擦除可编程只读存储器(EEPROM)。

[0674] 存储器子系统控制器可与存储器装置130通信以执行操作，例如在存储器装置130处读取数据、写入数据或擦除数据和其它此类操作(例如，响应于在命令总线上由控制器116调度的命令)。存储器子系统控制器可包含例如一或多个集成电路(IC)和/或离散组件、缓冲存储器或其组合的硬件。硬件可包含具有专用(例如，硬译码)逻辑的数字电路系统以执行本文中所描述的操作。存储器子系统控制器可以是微控制器、专用逻辑电路系统(例如，现场可编程门阵列(FPGA)、专用集成电路(ASIC)等)，或另一合适的处理器。

[0675] 存储器子系统控制器可包含处理装置(例如，处理器)，其配置成执行存储在本地存储器中的指令。在所示的实例中，存储器子系统控制器的本地存储器包含嵌入式存储器，其配置成存储用于执行控制存储器子系统的操作的各种过程、操作、逻辑流和例程的指令，包含处置存储器子系统与主机系统120之间的通信。

[0676] 在一些实施例中，本地存储器可包含存储存储器指针、所提取数据等的存储器寄存器。本地存储器还可包含用于存储微码的只读存储器(ROM)。尽管一些存储器子系统具有存储器子系统控制器，但是其它存储器子系统不包含存储器子系统控制器，而是可以依赖于外部控制(例如，由外部主机或者由与存储器子系统分离的处理器或控制器提供)。

[0677] 一般来说，存储器子系统控制器可从主机系统120接收命令或操作，并且可将命令或操作转换成指令或适当的命令以实现期望的对存储器装置130的访问。存储器子系统控制器可负责其它操作，例如耗损均衡操作、垃圾数据收集操作、错误检测和错误校正码(ECC)操作、加密操作、高速缓存操作及与存储器装置130相关联的逻辑地址(例如，逻辑块地址(LBA)、命名空间)和物理地址(例如，物理块地址)之间的地址转换。存储器子系统控制器可进一步包含主机接口电路系统，用于经由物理主机接口与主机系统120通信。主机接口

电路系统可将从主机系统接收到的命令转换成访问存储器装置130的命令指令，并将与存储器装置130相关联的响应转换成用于主机系统120的信息。

[0678] 存储器子系统还可包含未示出的额外电路系统或组件。在一些实施例中，存储器子系统可包含可以从存储器子系统控制器接收地址并将地址解码以访问存储器装置130的高速缓存或缓冲器(例如，DRAM)和地址电路系统(例如，行解码器和列解码器)。

[0679] 在一些实施例中，存储器装置130包含结合存储器子系统的存储器子系统控制器用于对存储器装置130的一或多个存储器单元103执行操作的本地媒体控制器。本地媒体控制器可用于实施加密引擎107和/或访问控制器109。外部控制器(例如，存储器子系统控制器或主机系统120的控制器116)可在外部管理存储器装置130(例如，对存储器装置130执行媒体管理操作)。在一些实施例中，存储器装置130是受管理存储器装置，它是与本地媒体控制器组合以用于相同存储器装置封装内的媒体管理的原始存储器装置。受管理存储器装置的实例是受管理NAND(MNAND)装置。

[0680] 存储器子系统控制器和/或存储器装置130可包含配置成提供上文所论述的安全特征的安全管理器160。在一些实施例中，存储器子系统控制器和/或存储器子系统中的本地媒体控制器可包含安全管理器160的至少一部分。在其它实施例中，或组合地，主机系统120中的控制器116可包含安全管理器160的至少一部分。例如，存储器子系统控制器、控制器116和/或安全服务器140可包含逻辑电路系统和/或在实施安全管理器160时执行指令。例如，存储器子系统控制器或主机系统120的处理装置118(例如，处理器)可配置成执行存储于存储器装置130中用于执行本文中所描述的安全管理器160的操作的指令。在一些实施例中，安全管理器160实施于安置在存储器子系统中的集成电路芯片中。在其它实施例中，安全管理器160可以是存储器子系统的固件、主机系统120的操作系统、装置驱动程序或应用程序的部分，或其任何组合。

[0681] 先前详细描述的一些部分已经关于计算机存储器内的数据位的操作的算法和符号表示呈现。这些算法描述和表示是数据处理领域中的技术人员用来将他们的工作内容传达给本领域的其他技术人员的最有效方式。此处且一般来说，算法被设想为产生所需结果的操作的自一致序列。所述操作是需要物理量的物理操控的那些操作。通常但是不一定，这些量采取能够存储、组合、比较和以其它方式操控的电气或磁性信号的形式。已经证实，将这些信号称为位、值、元件、符号、字符、项、数字等等有时是方便的，主要是出于常用的原因。

[0682] 然而，应牢记，所有这些和类似术语与适当物理量相关联，且仅为应用于这些量的方便的标签。本公开可以指操控和变换计算机系统的寄存器和存储器内的表示为物理(电子)量的数据为计算机系统存储器或寄存器或其它这类信息存储系统内的类似地表示为物理量的其它数据的计算机系统或类似电子计算装置的动作和过程。

[0683] 本公开还涉及用于执行本文中的操作的设备。此设备可以出于所需目的而专门构造，或其可以包含通过存储在计算机中的计算机程序选择性地激活或重新配置的通用计算机。此类计算机程序可存储在计算机可读存储媒体中，例如但不限于任何类型的盘，包含软盘、光盘、CD-ROM和磁光盘、只读存储器(ROM)、随机存取存储器(RAM)、EPROM、EEPROM、磁卡或光卡，或适合于存储电子指令的任何类型的媒体，它们分别耦合到计算机系统总线。

[0684] 本文中呈现的算法和显示器在本质上并不与任何特定计算机或其它设备相关。各

种通用系统可以与根据本文中的教示的程序一起使用，或可以证明构造用以执行所述方法更加专用的设备是方便的。将从下文描述中呈现用于各种这些系统的结构。此外，并不参考任何特定编程语言来描述本公开。应了解，可以使用多种编程语言来实施如本文所描述的本公开的教示内容。

[0685] 本公开可提供为计算机程序产品或软件，其可包含在其上存储有可用于编程计算机系统(或其它电子装置)以执行根据本公开的过程的指令的机器可读媒体。机器可读媒体包含用于以机器(例如，计算机)可读的形式存储信息的任何机构。在一些实施例中，机器可读(例如，计算机可读)媒体包含机器(例如，计算机)可读存储媒体，例如只读存储器(“ROM”)、随机存取存储器(“RAM”)、磁盘存储媒体、光学存储媒体、快闪存储器组件等。

[0686] 在本说明书中，为了简化描述，将各种功能和操作描述为由计算机指令执行或由计算机指令引起。然而，所属领域的技术人员将认识到，此类表达的意图是所述功能源自由一或多个控制器或处理器(例如，微处理器)执行计算机指令。替代地或组合地，所述功能和操作可使用具有或不具有软件指令的专用电路系统实施，例如使用专用集成电路(ASIC)或现场可编程门阵列(FPGA)来实施。可使用无软件指令的硬接线电路系统或结合软件指令实施实施例。因此，技术既不限于硬件电路系统和软件的任何特定组合，也不限于由数据处理系统执行的指令的任何特定来源。

[0687] 在前述说明书中，本公开的实施例已经参考其特定实例实施例进行描述。将显而易见的是，可在不脱离所附权利要求书中阐述的本公开的实施例的更广精神和范围的情况下对其进行各种修改。因此，应在说明性意义上而非限制性意义上看待说明书和图式。

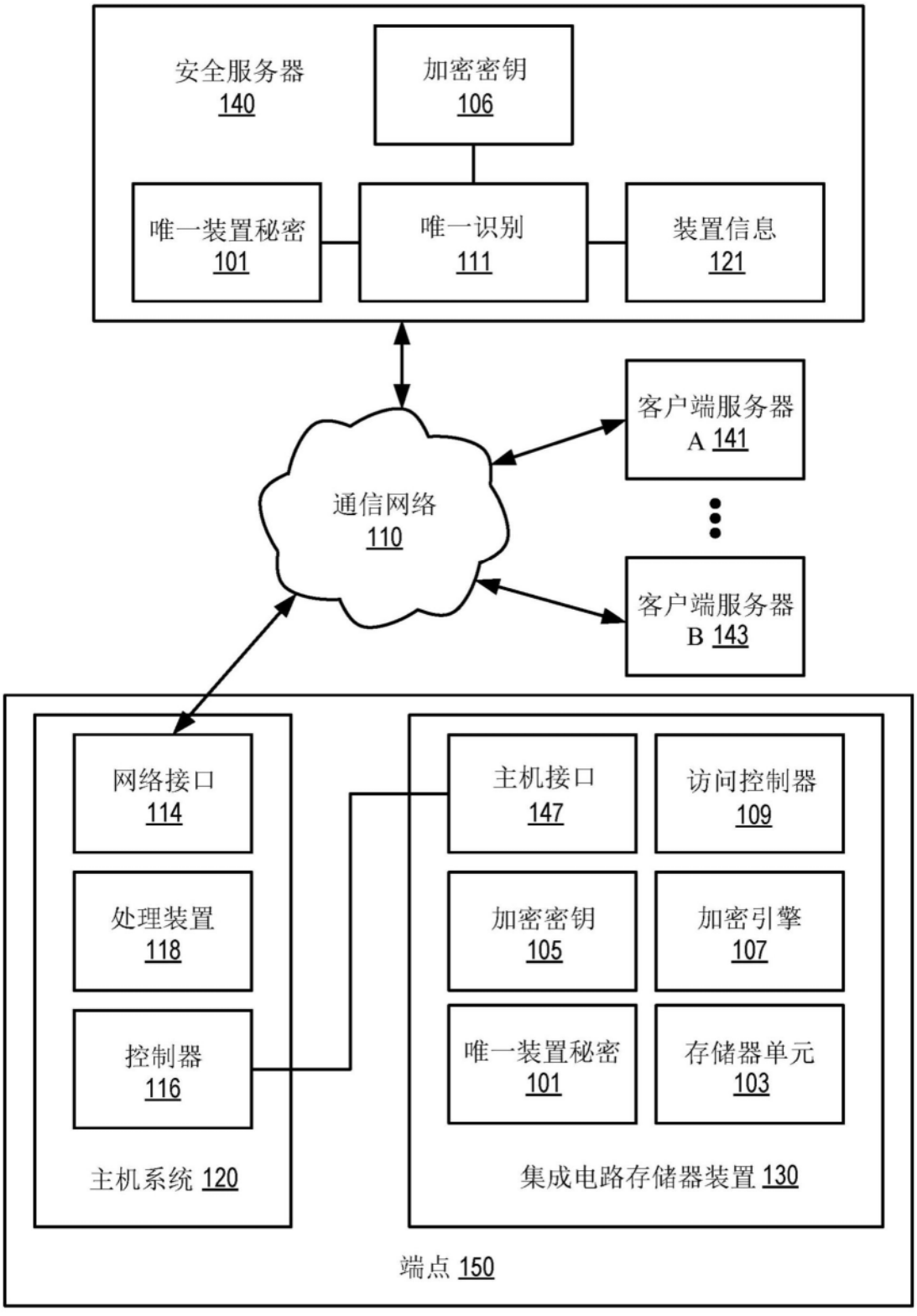

安全服务器
140
加密密钥
106
唯一装置秘密
101
唯一识别
111
装置信息
121
通信网络
110
客户端服务器
A 141
客户端服务器
B 143
网络接口
114
处理装置
118
控制器
116
主机系统 120
主机接口
147
访问控制器
109
加密密钥
105
加密引擎
107
唯一装置秘密
101
存储器单元
103
集成电路存储器装置 130
端点 150

图1

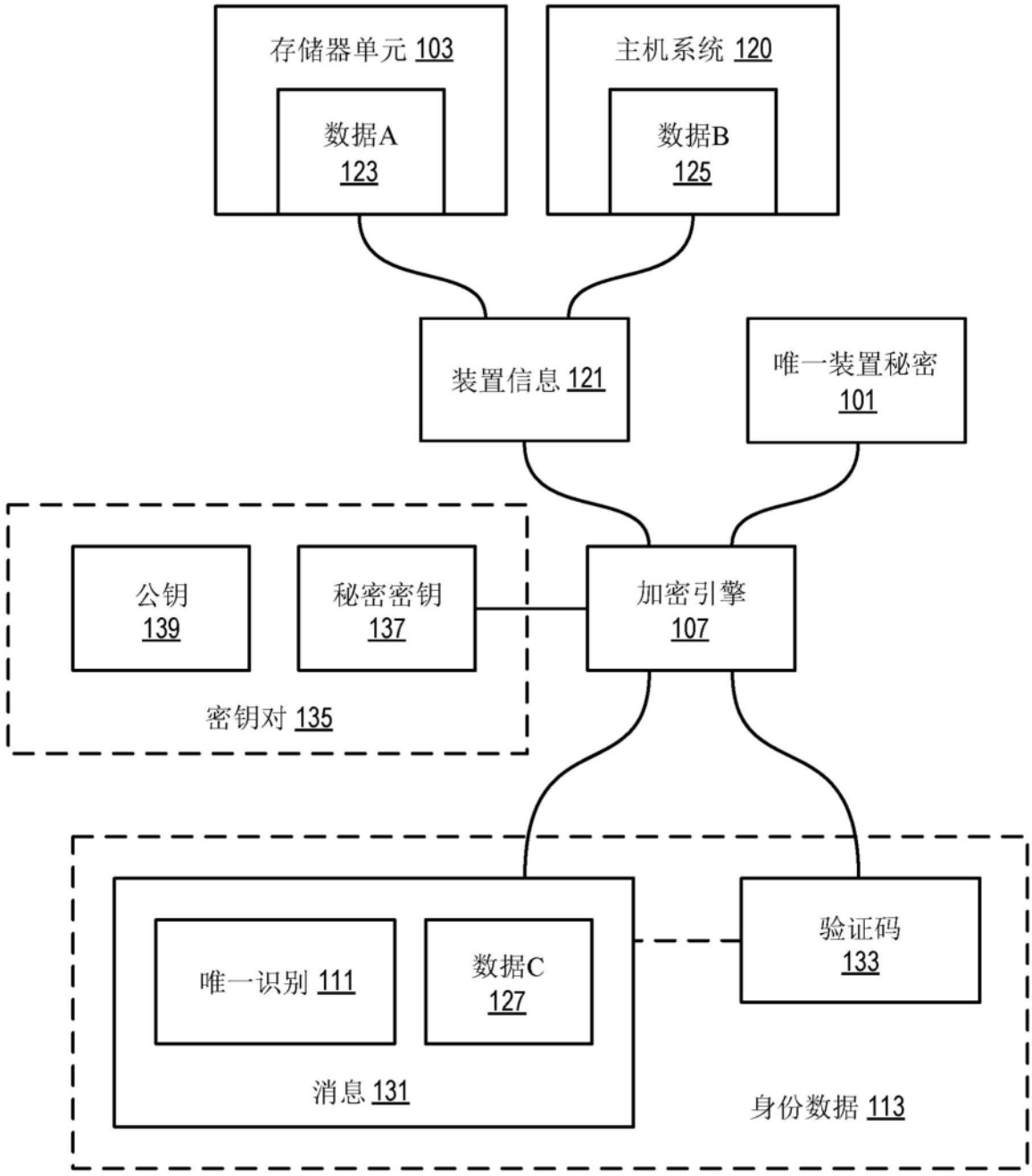

存储器单元 103
数据A
123
主机系统 120
数据B
125
装置信息 121
唯一装置秘密
101
公钥
139
秘密密钥
137
加密引擎
107
密钥对 135
唯一识别 111
数据C
127
验证码
133
消息 131
身份数据 113

图2

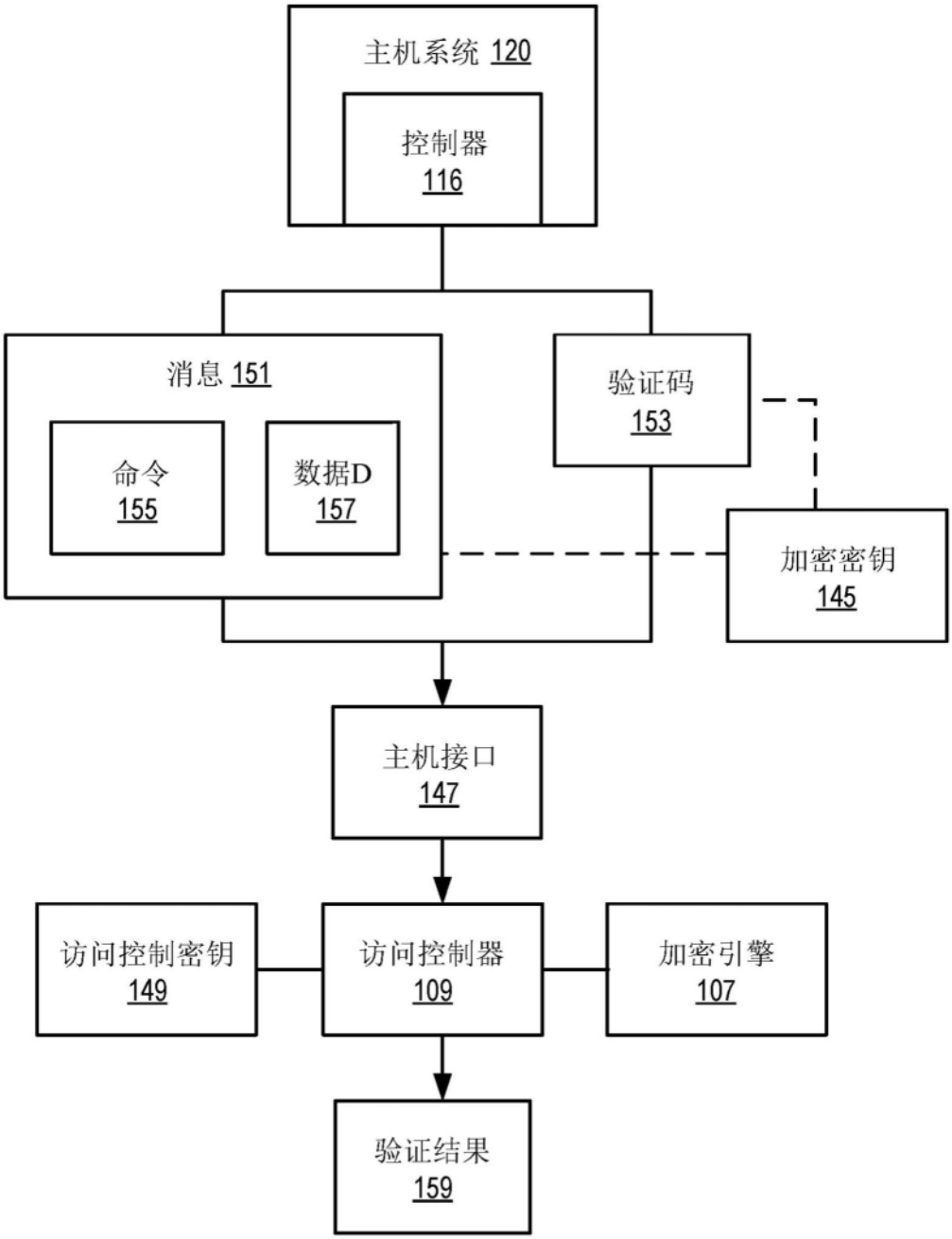

主机系统 120
控制器
116
消息 151
命令
155
数据D
157
验证码
153
加密密钥
145
主机接口
147
访问控制密钥
149
访问控制器
109
加密引擎
107
验证结果
159

图3

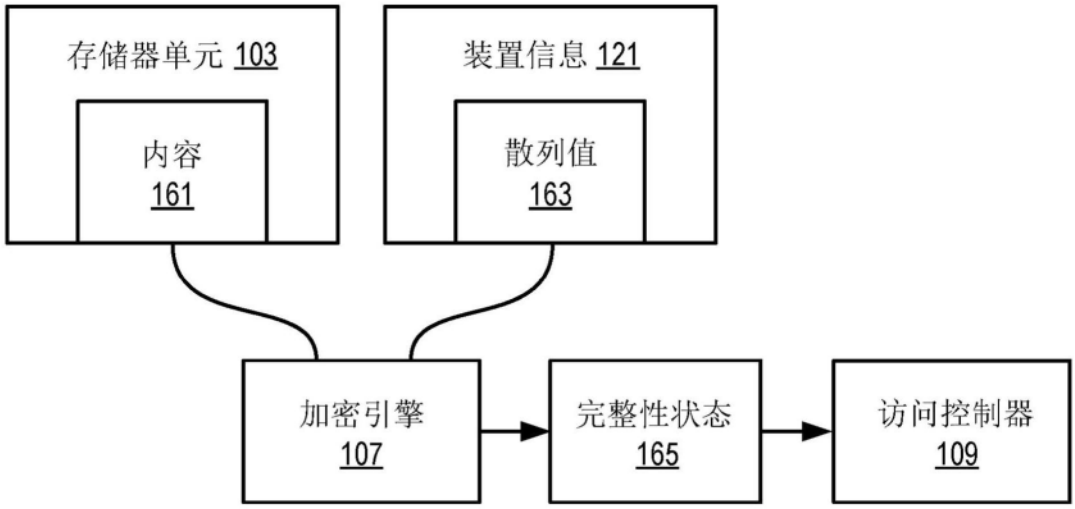

存储器单元 103
内容
161
装置信息 121
散列值
163
加密引擎
107
完整性状态
165
访问控制器
109

图4

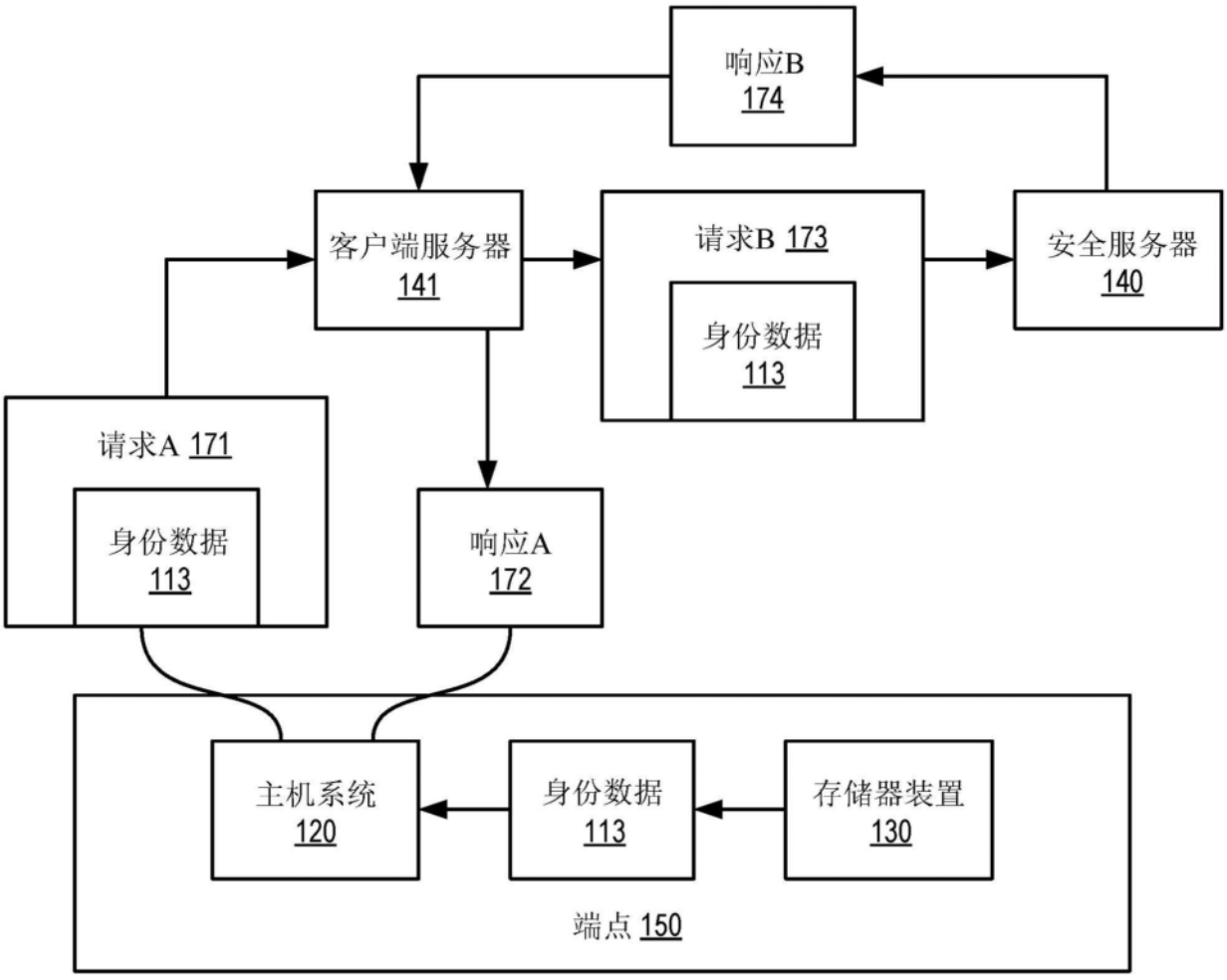

响应B
174
客户端服务器
141
请求B 173
身份数据
113
安全服务器
140
请求A 171
身份数据
113
响应A
172
主机系统
120
身份数据
113
存储器装置
130
端点 150

图5

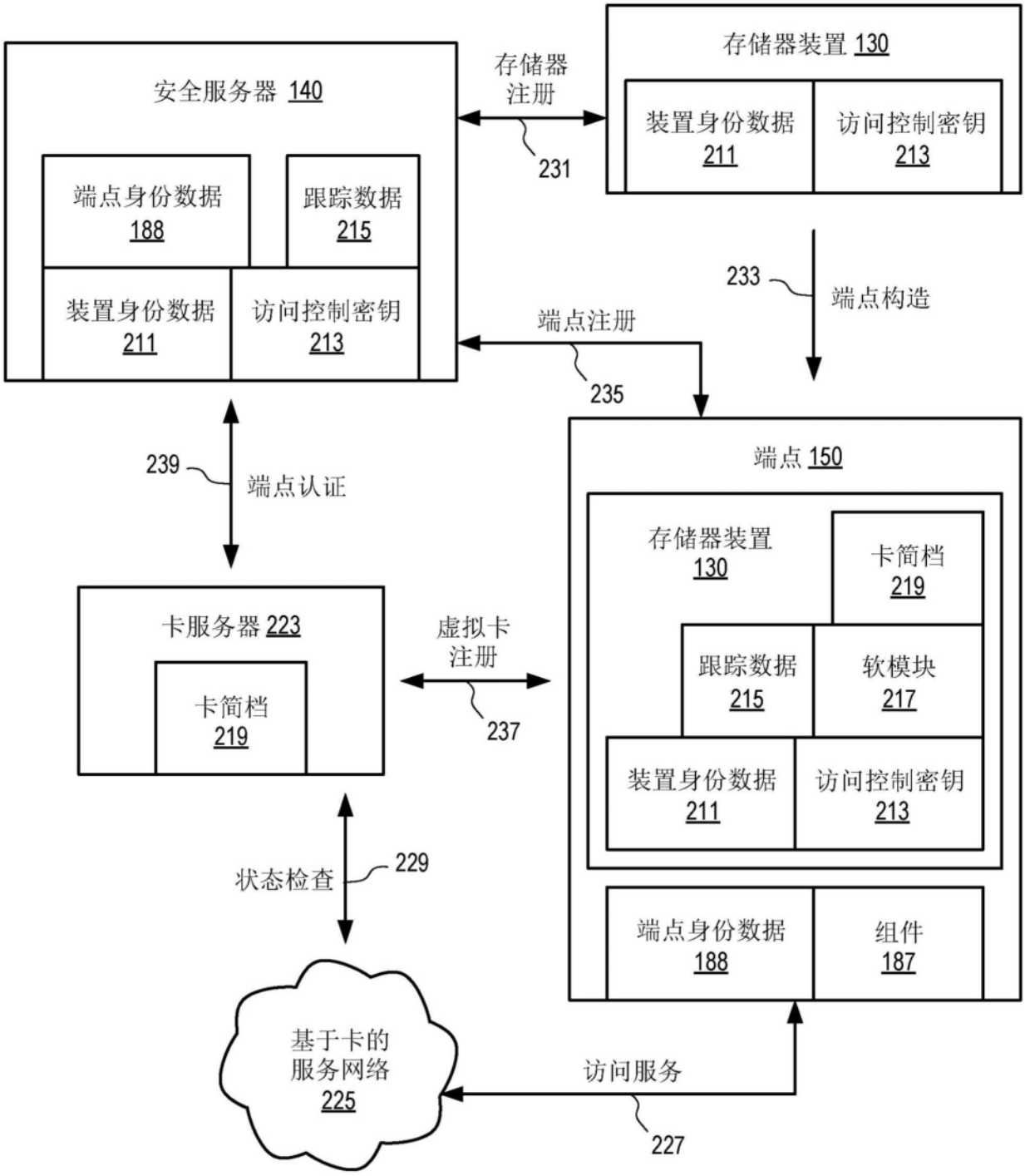

安全服务器 140
端点身份数据 188
跟踪数据 215
装置身份数据 211
访问控制密钥 213
存储器注册
231
存储器装置 130
装置身份数据 211
访问控制密钥 213
233
端点构造
端点注册
235
239
端点认证
端点 150
存储器装置 130
卡简档 219
跟踪数据 215
软模块 217
装置身份数据 211
访问控制密钥 213
端点身份数据 188
组件 187
卡服务器 223
卡简档 219
虚拟卡注册
237
状态检查
229
基于卡的服务网络 225
访问服务
227

图6

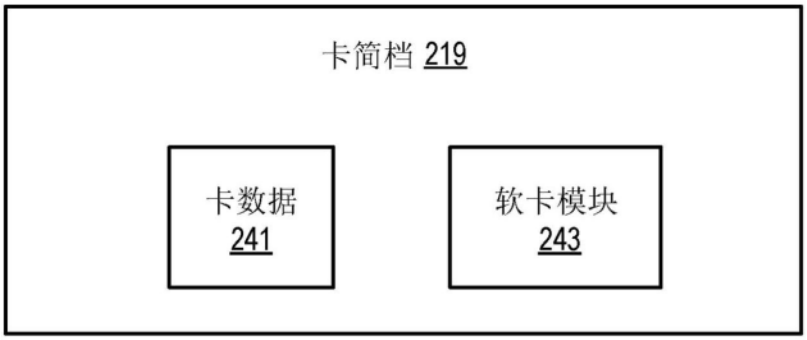

卡简档 219
卡数据
241
软卡模块
243

图7

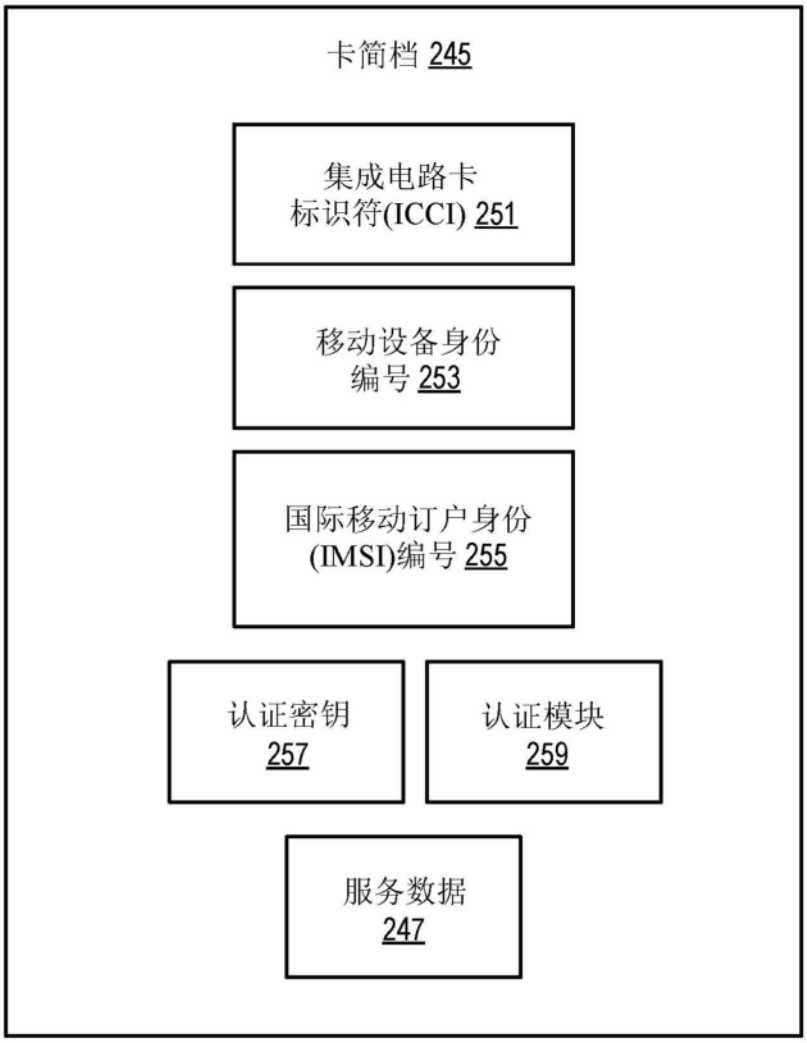

卡简档 245
集成电路卡
标识符(ICCI) 251
移动设备身份
编号 253
国际移动订户身份
(IMSI)编号 255
认证密钥
257
认证模块
259
服务数据
247

图8

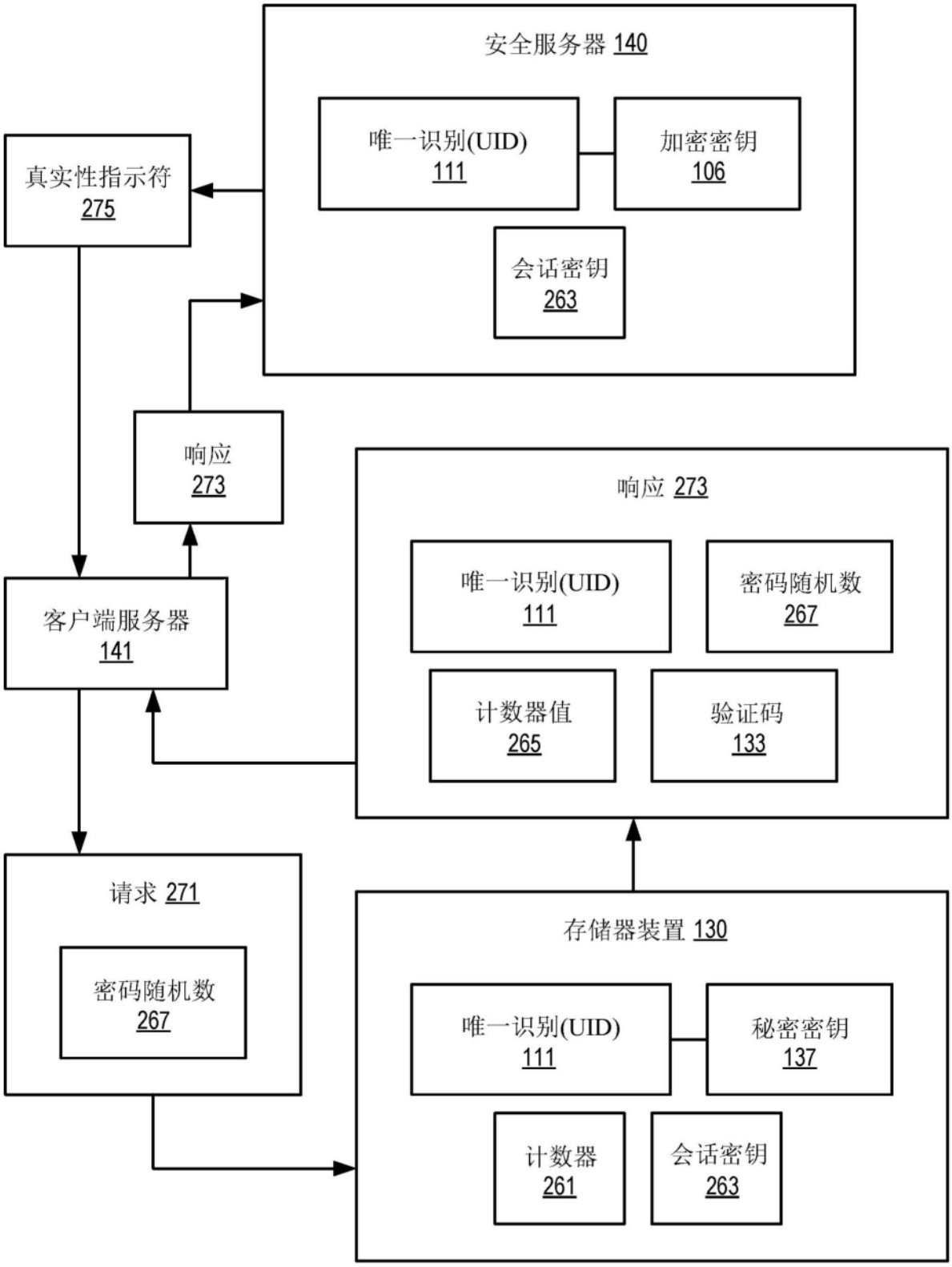

安全服务器 140
唯一识别(UID)
111
加密密钥
106
会话密钥
263
真实性指示符
275
响应
273
响应 273
唯一识别(UID)
111
密码随机数
267
计数器值
265
验证码
133
客户端服务器
141
请求 271
密码随机数
267
存储器装置 130
唯一识别(UID)
111
秘密密钥
137
计数器
261
会话密钥
263

图9

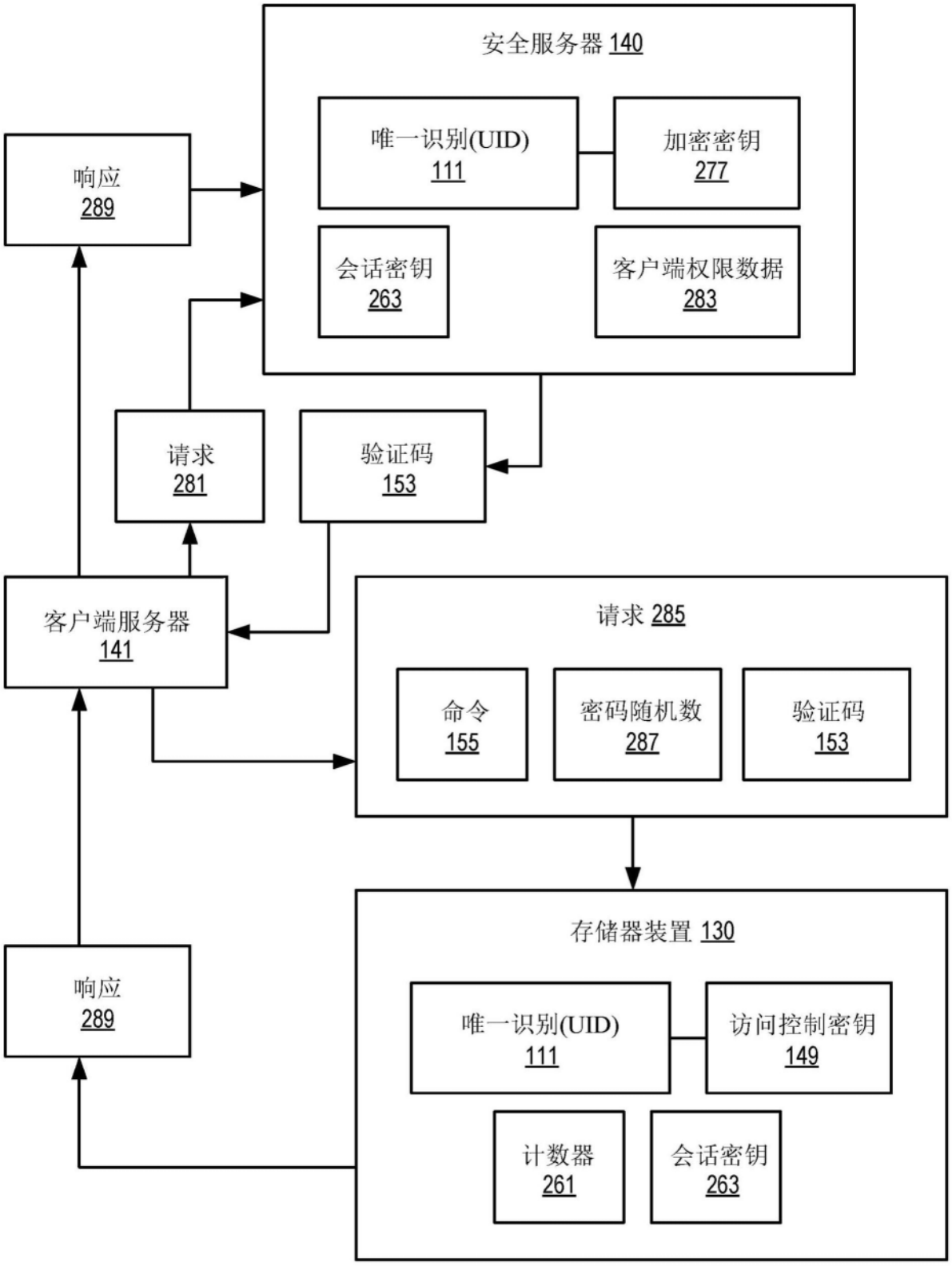

安全服务器 140
唯一识别(UID)
111
加密密钥
277
会话密钥
263
客户端权限数据
283
响应
289
请求
281
验证码
153
客户端服务器
141
请求 285
命令
155
密码随机数
287
验证码
153
存储器装置 130
唯一识别(UID)
111
访问控制密钥
149
计数器
261
会话密钥
263
响应
289

图10

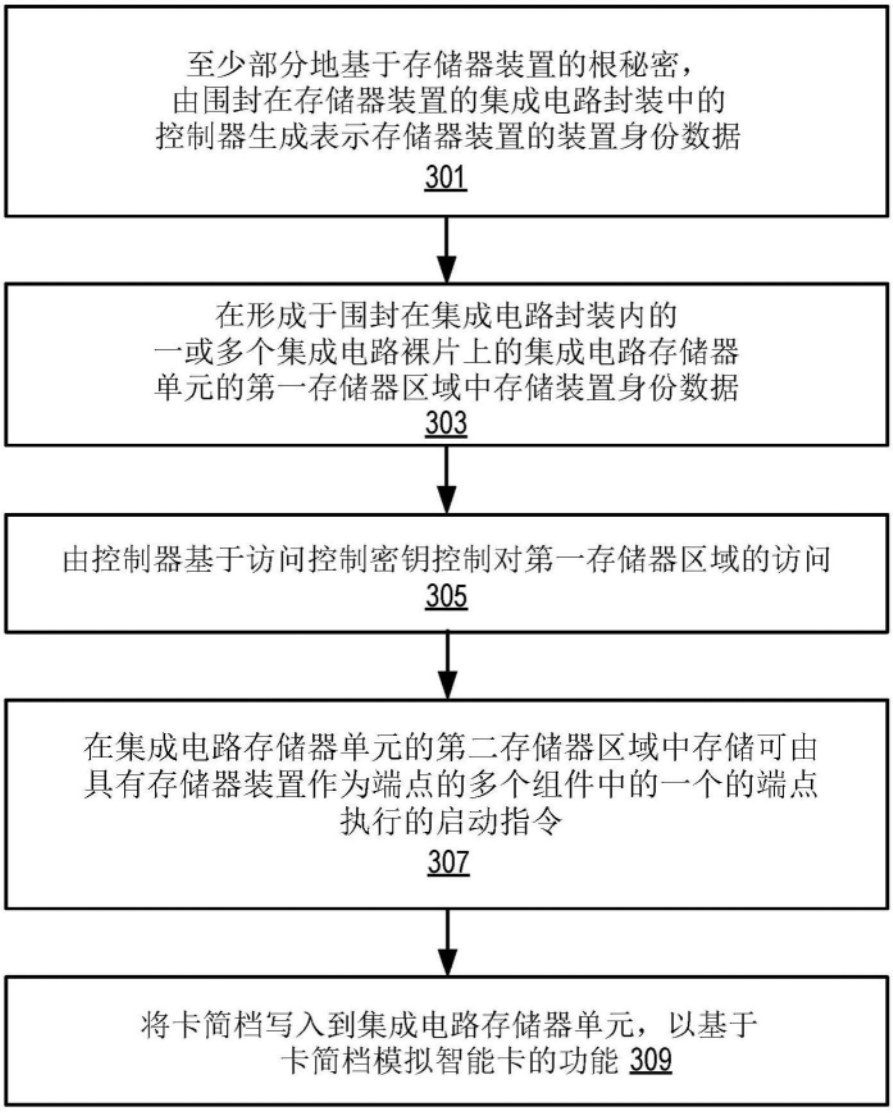

至少部分地基于存储器装置的根秘密，
由围封在存储器装置的集成电路封装中的
控制器生成表示存储器装置的装置身份数据
301
在形成于围封在集成电路封装内的
一或多个集成电路裸片上的集成电路存储器
单元的第一存储器区域中存储装置身份数据
303
由控制器基于访问控制密钥控制对第一存储器区域的访问
305
在集成电路存储器单元的第二存储器区域中存储可由
具有存储器装置作为端点的多个组件中的一个的端点
执行的启动指令
307
将卡简档写入到集成电路存储器单元，以基于
卡简档模拟智能卡的功能 309

图11

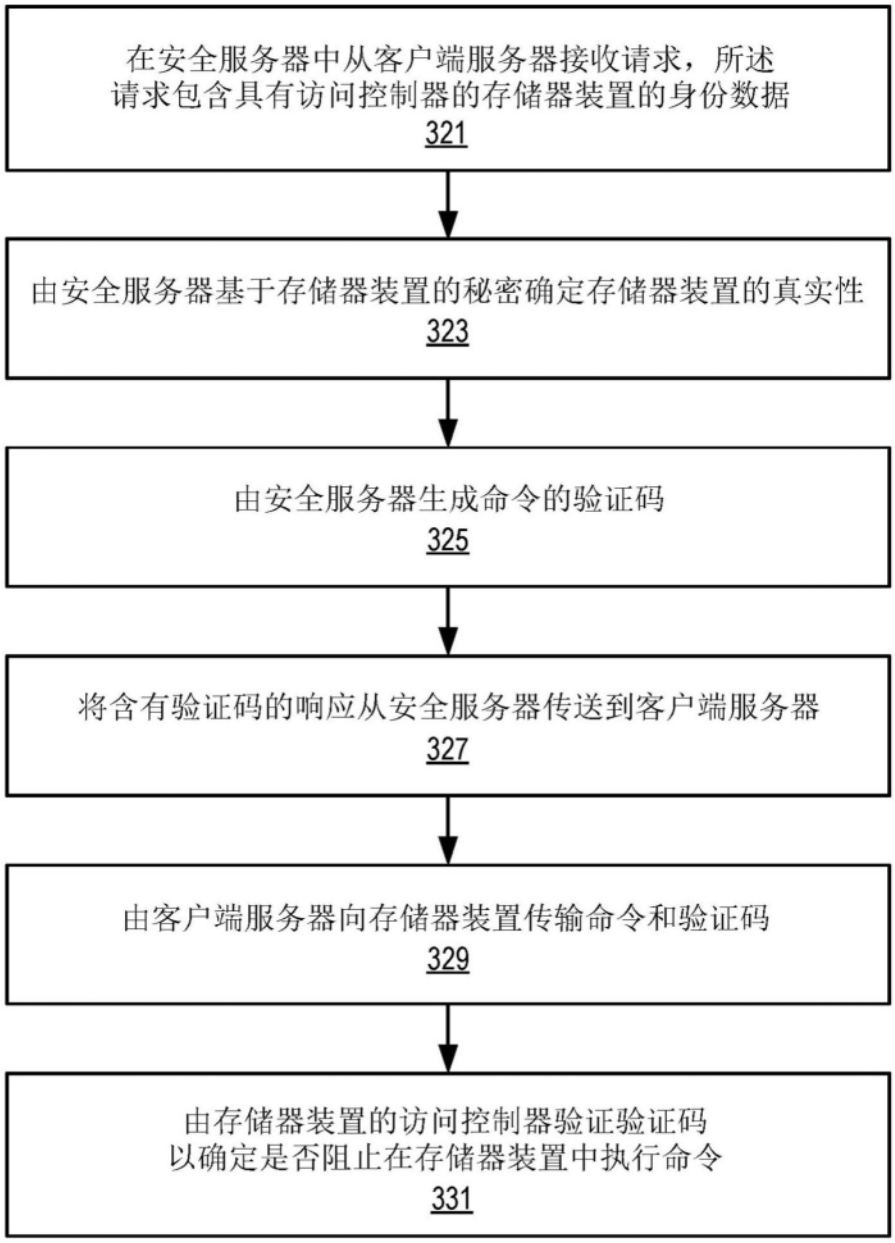

在安全服务器中从客户端服务器接收请求，所述请求包含具有访问控制器的存储器装置的身份数据
321
由安全服务器基于存储器装置的秘密确定存储器装置的真实性
323
由安全服务器生成命令的验证码
325
将含有验证码的响应从安全服务器传送到客户端服务器
327
由客户端服务器向存储器装置传输命令和验证码
329
由存储器装置的访问控制器验证验证码以确定是否阻止在存储器装置中执行命令
331

图12

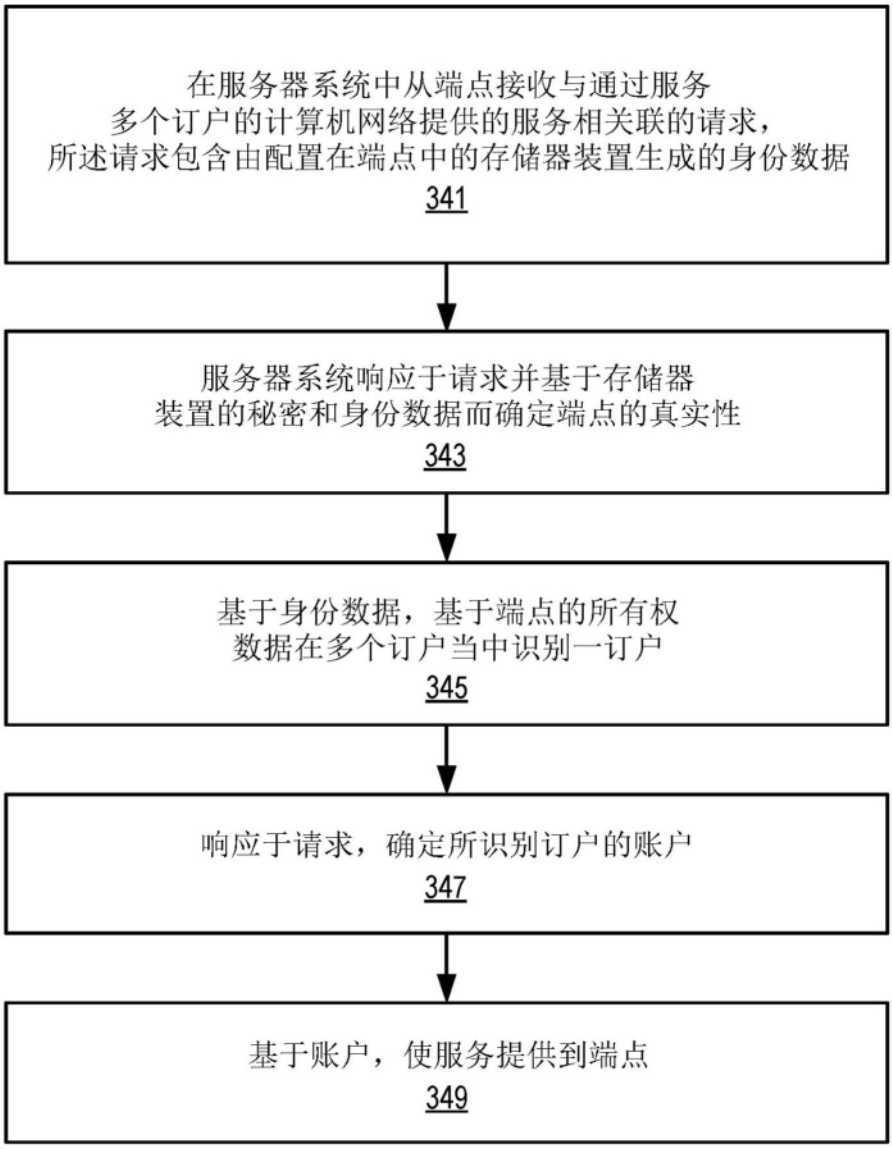

在服务器系统中从端点接收与通过服务
多个订户的计算机网络提供的服务相关联的请求，
所述请求包含由配置在端点中的存储器装置生成的身份数据
341
服务器系统响应于请求并基于存储器
装置的秘密和身份数据而确定端点的真实性
343
基于身份数据，基于端点的所有权
数据在多个订户当中识别一订户
345
响应于请求，确定所识别订户的账户
347
基于账户，使服务提供到端点
349

图13

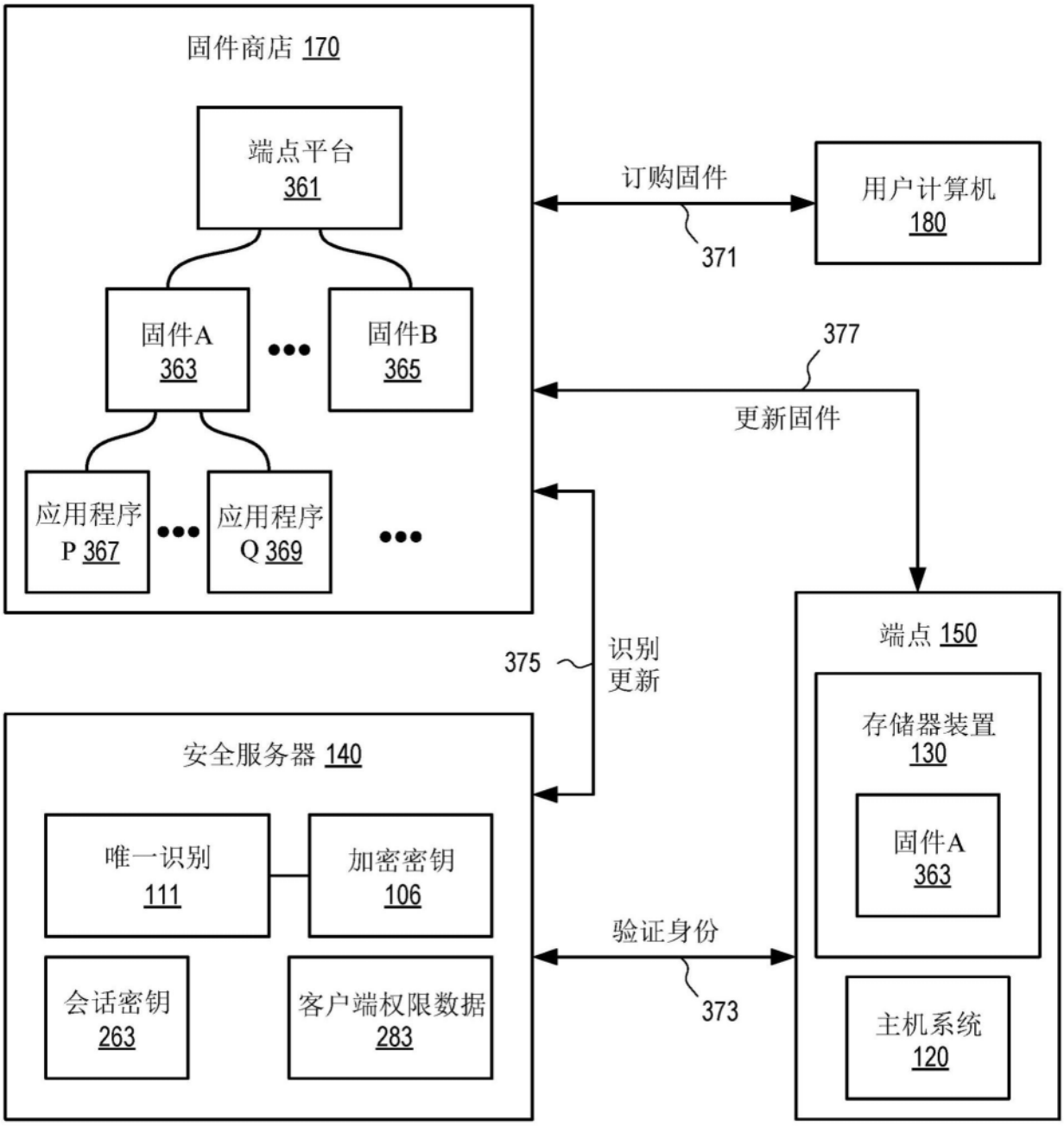

固件商店 170
端点平台
361
固件A
363
固件B
365
应用程序
P 367
应用程序
Q 369
订购固件
371
用户计算机
180
377
更新固件
375
识别
更新
端点 150
存储器装置
130
固件A
363
主机系统
120
安全服务器 140
唯一识别
111
加密密钥
106
会话密钥
263
客户端权限数据
283
验证身份
373

图14

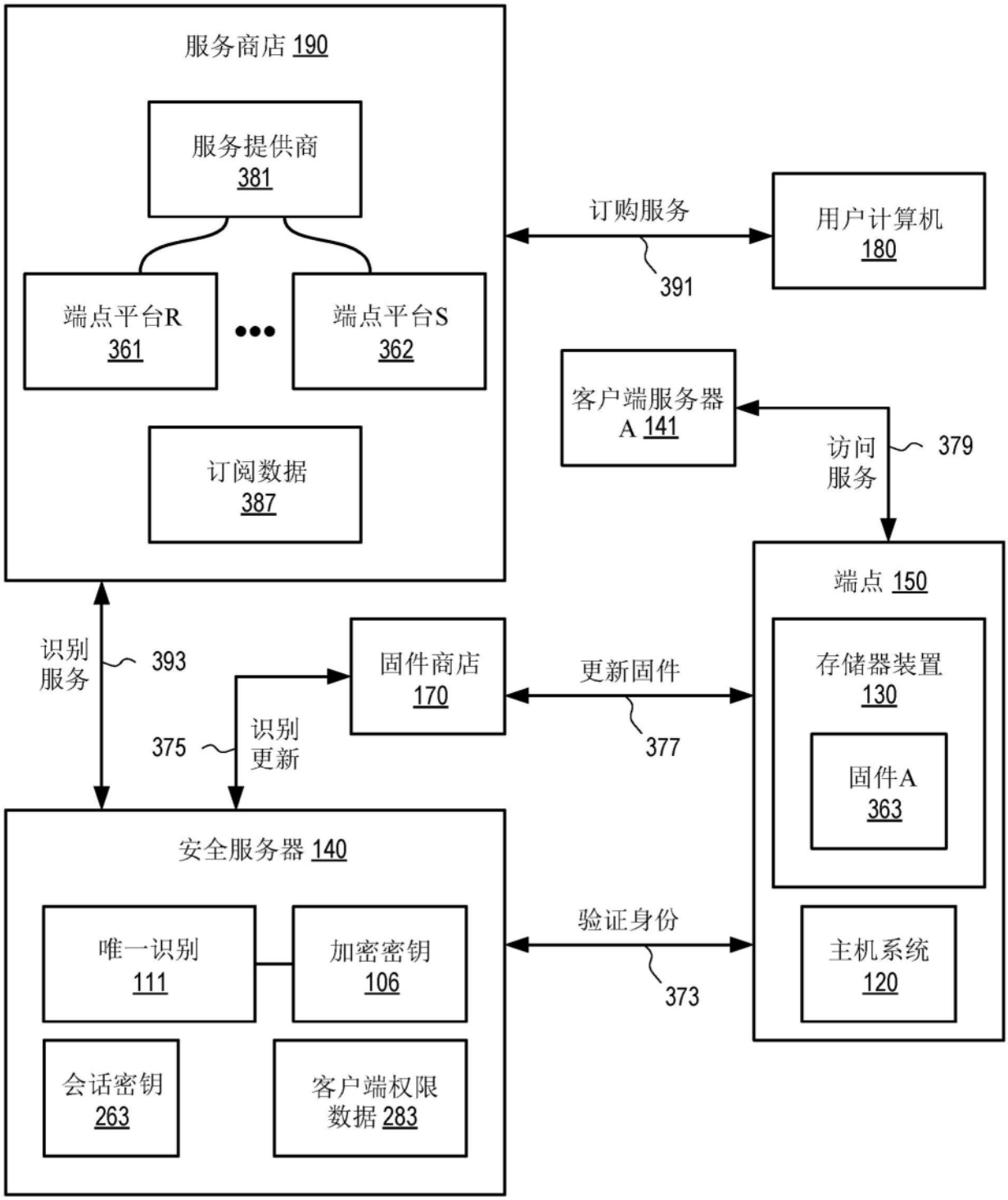

服务商店 190
服务提供商 381
端点平台R 361
端点平台S 362
订阅数据 387
订购服务
391
用户计算机 180
客户端服务器 A 141
访问服务
379
端点 150
存储器装置 130
固件A 363
主机系统 120
识别服务
393
固件商店 170
更新固件
377
375
识别更新
安全服务器 140
唯一识别 111
加密密钥 106
会话密钥 263
客户端权限数据 283
验证身份
373

图15

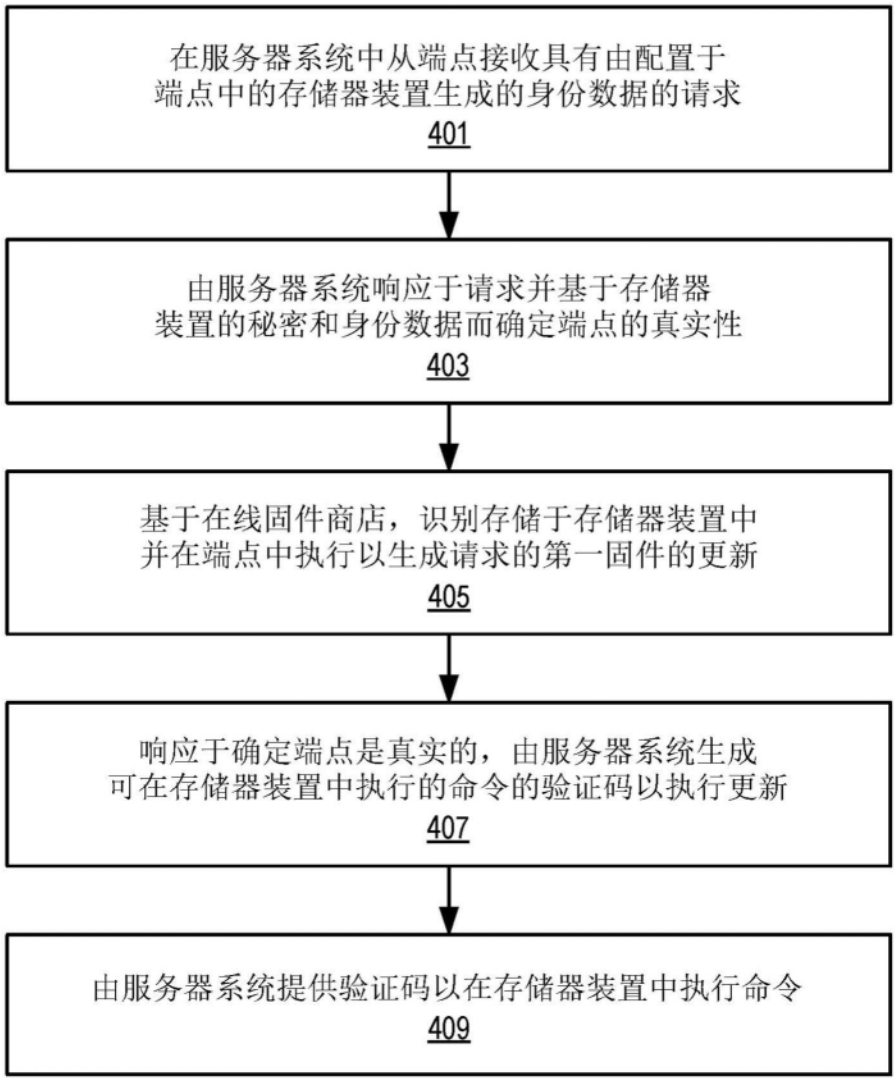

在服务器系统中从端点接收具有由配置于
端点中的存储器装置生成的身份数据的请求
401
由服务器系统响应于请求并基于存储器
装置的秘密和身份数据而确定端点的真实性
403
基于在线固件商店，识别存储于存储器装置中
并在端点中执行以生成请求的第一固件的更新
405
响应于确定端点是真实的，由服务器系统生成
可在存储器装置中执行的命令的验证码以执行更新
407
由服务器系统提供验证码以在存储器装置中执行命令
409

图16

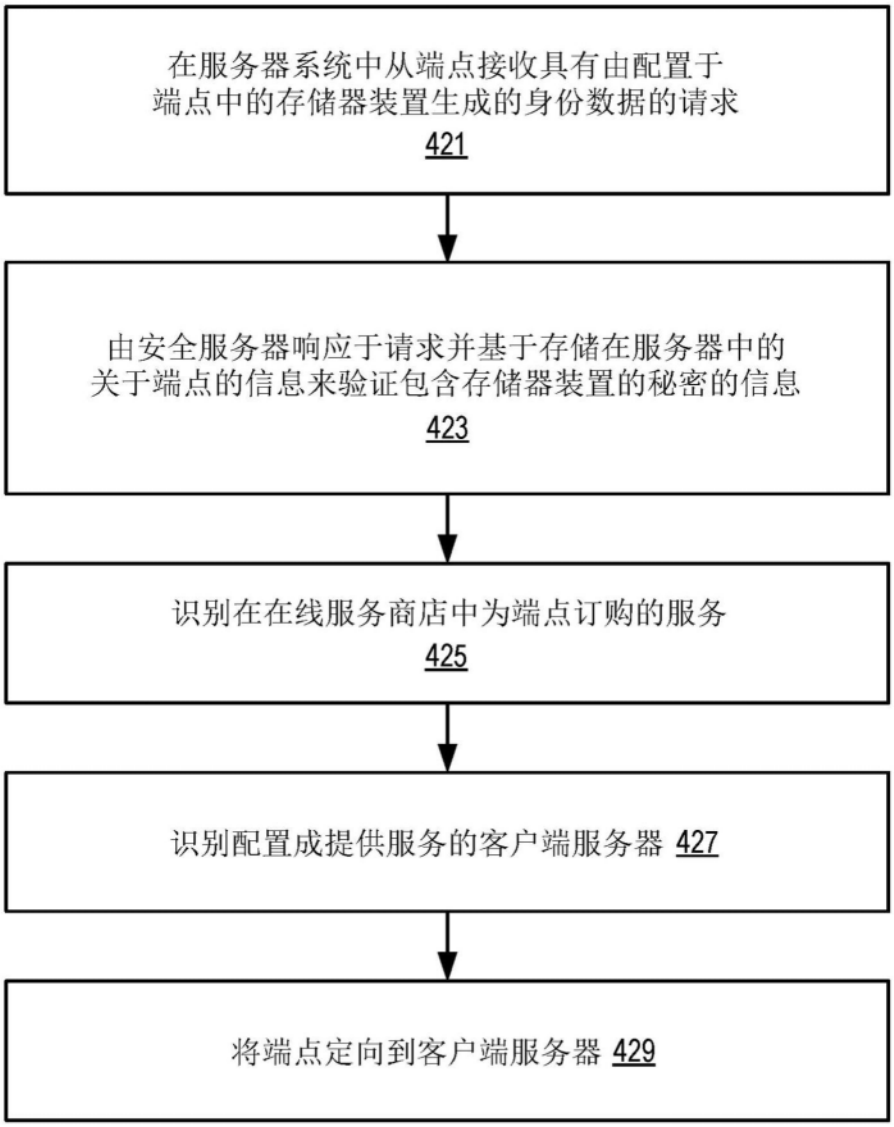

在服务器系统中从端点接收具有由配置于端点中的存储器装置生成的身份数据的请求
421
由安全服务器响应于请求并基于存储在服务器中的关于端点的信息来验证包含存储器装置的秘密的信息
423
识别在在线服务商店中为端点订购的服务
425
识别配置成提供服务的客户端服务器 427
将端点定向到客户端服务器 429

图17

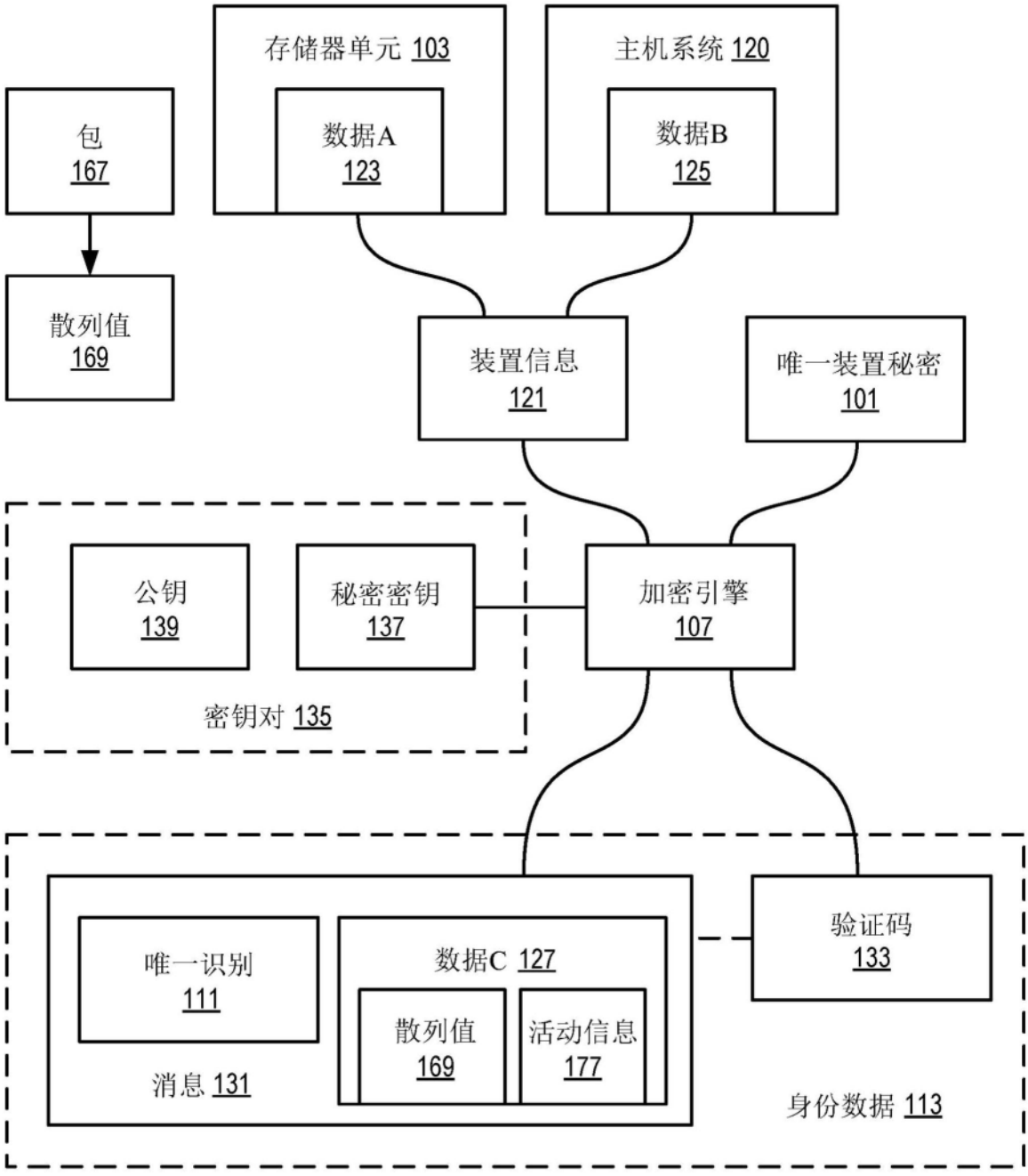

存储器单元 103
数据A
123
主机系统 120
数据B
125
包
167
散列值
169
装置信息
121
唯一装置秘密
101
公钥
139
秘密密钥
137
加密引擎
107
密钥对 135
唯一识别
111
数据C 127
散列值
169
活动信息
177
验证码
133
消息 131
身份数据 113

图18

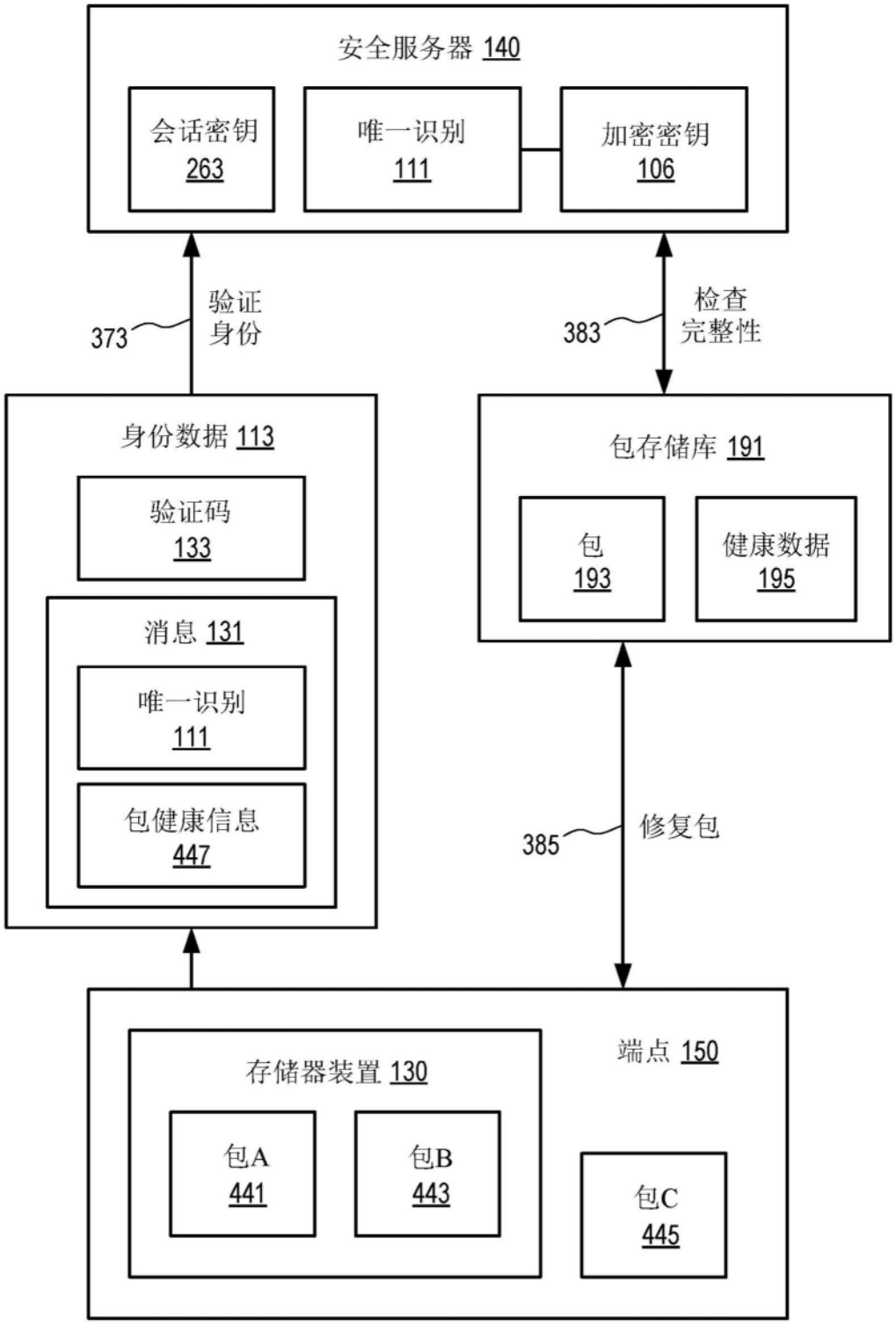

安全服务器 140
会话密钥 263
唯一识别 111
加密密钥 106
373
验证身份
383
检查完整性
身份数据 113
验证码 133
消息 131
唯一识别 111
包健康信息 447
包存储库 191
包 193
健康数据 195
385
修复包
存储器装置 130
包A 441
包B 443
端点 150
包C 445

图19

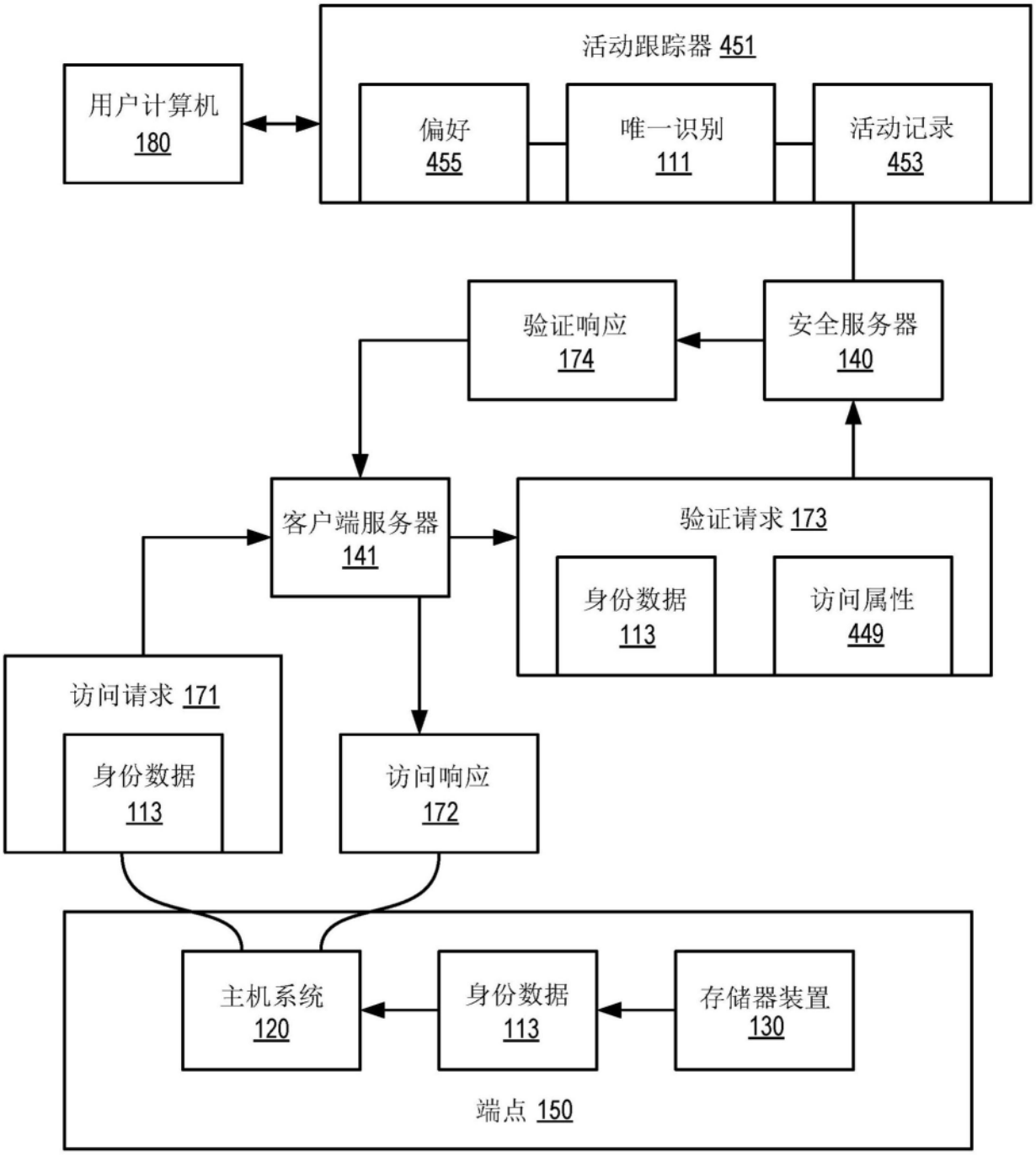

活动跟踪器 451
用户计算机
180
偏好
455
唯一识别
111
活动记录
453
验证响应
174
安全服务器
140
客户端服务器
141
验证请求 173
身份数据
113
访问属性
449
访问请求 171
身份数据
113
访问响应
172
主机系统
120
身份数据
113
存储器装置
130
端点 150

图20

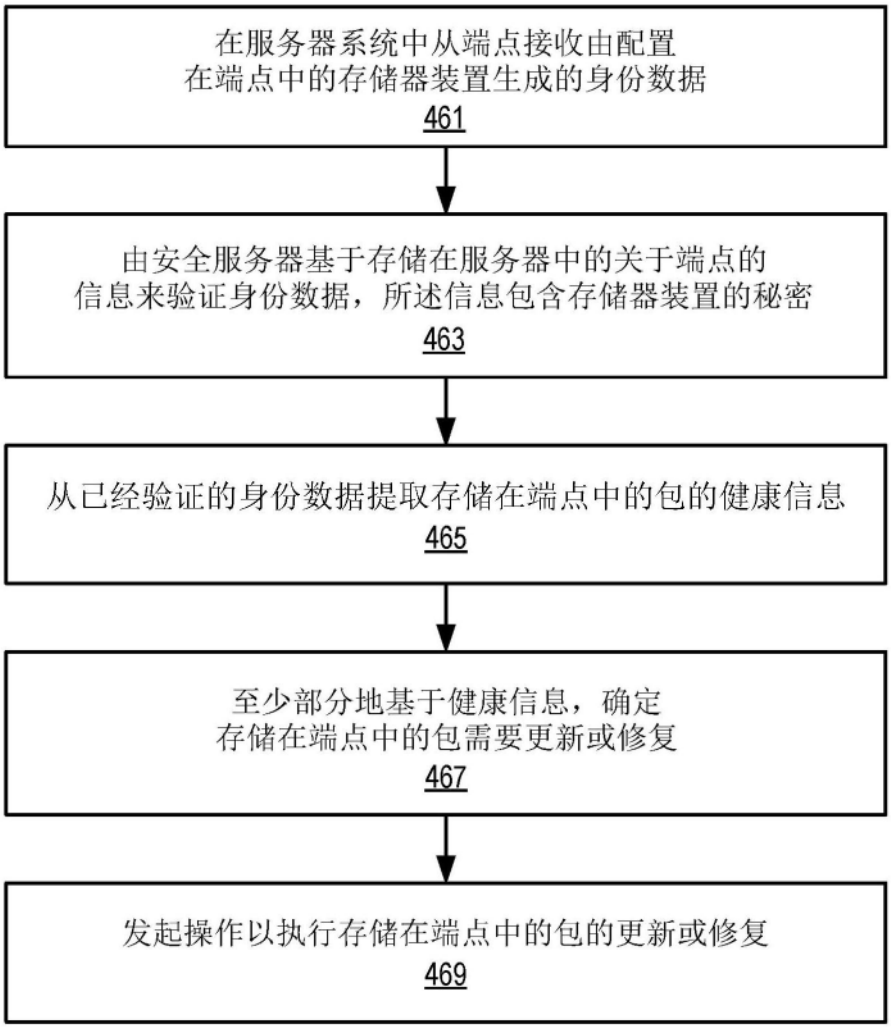

在服务器系统中从端点接收由配置
在端点中的存储器装置生成的身份数据
461
由安全服务器基于存储在服务器中的关于端点的
信息来验证身份数据，所述信息包含存储器装置的秘密
463
从已经验证的身份数据提取存储在端点中的包的健康信息
465
至少部分地基于健康信息，确定
存储在端点中的包需要更新或修复
467
发起操作以执行存储在端点中的包的更新或修复
469

图21

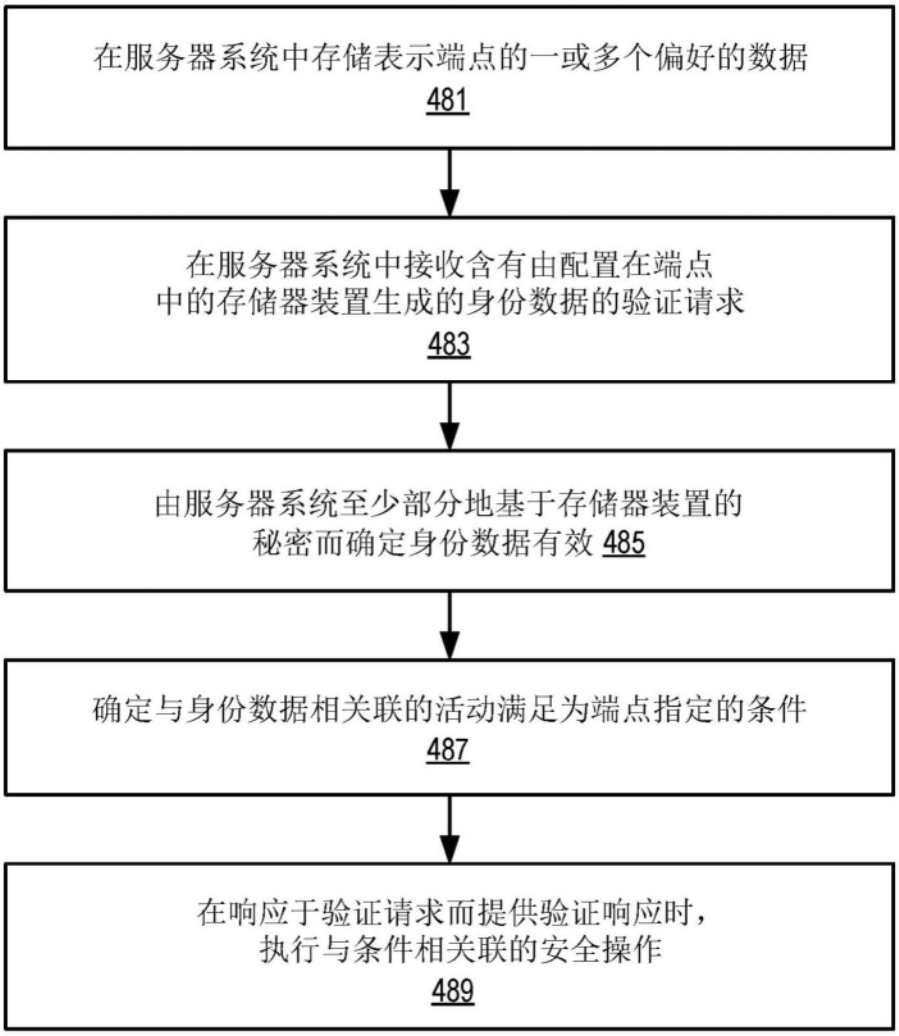

在服务器系统中存储表示端点的一或多个偏好的数据
481
在服务器系统中接收含有由配置在端点
中的存储器装置生成的身份数据的验证请求
483
由服务器系统至少部分地基于存储器装置的
秘密而确定身份数据有效 485
确定与身份数据相关联的活动满足为端点指定的条件
487
在响应于验证请求而提供验证响应时，
执行与条件相关联的安全操作
489

图22

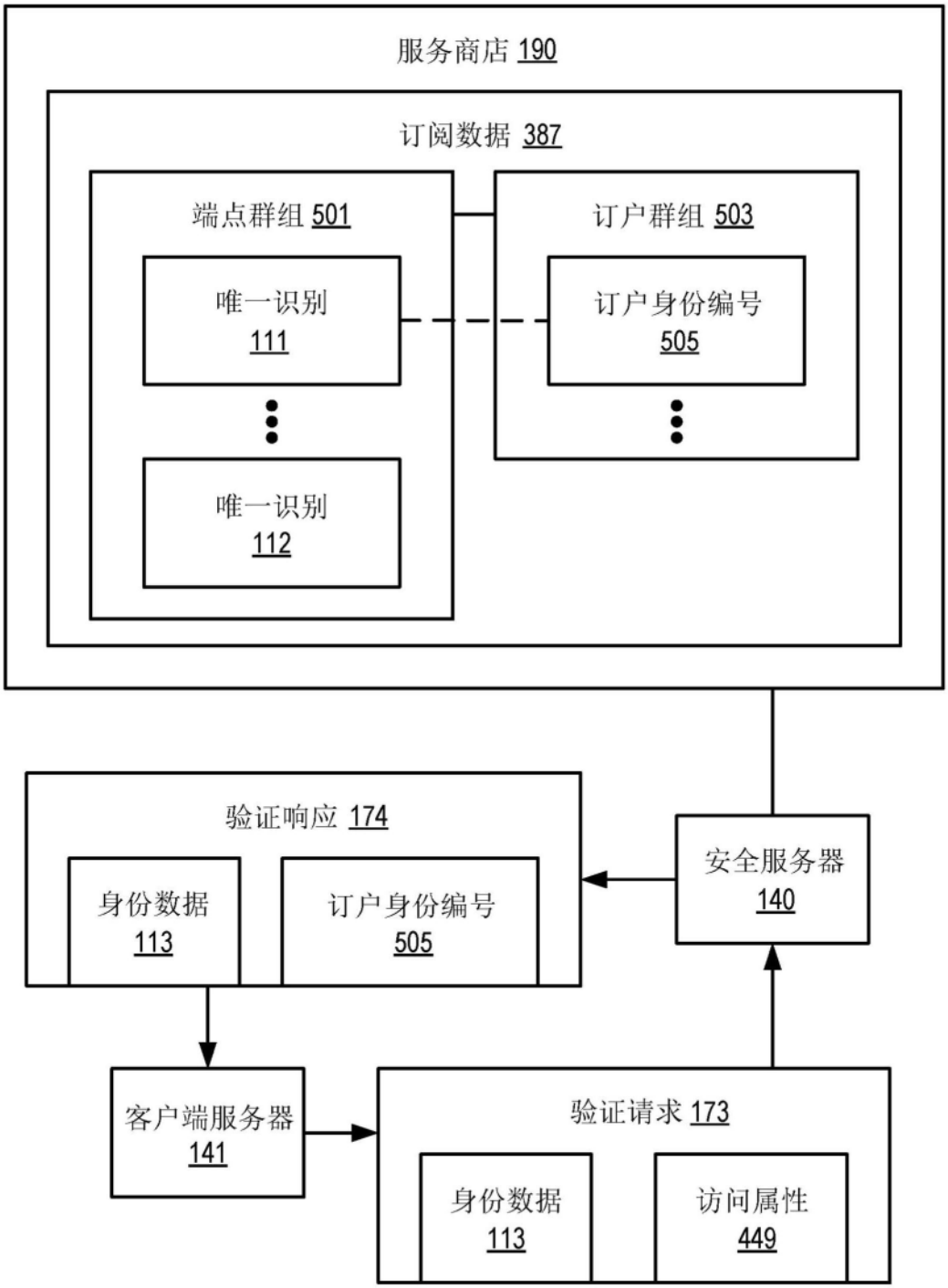

服务商店 190
订阅数据 387
端点群组 501
唯一识别 111
唯一识别 112
订户群组 503
订户身份编号 505
验证响应 174
身份数据 113
订户身份编号 505
安全服务器 140
客户端服务器 141
验证请求 173
身份数据 113
访问属性 449

图23

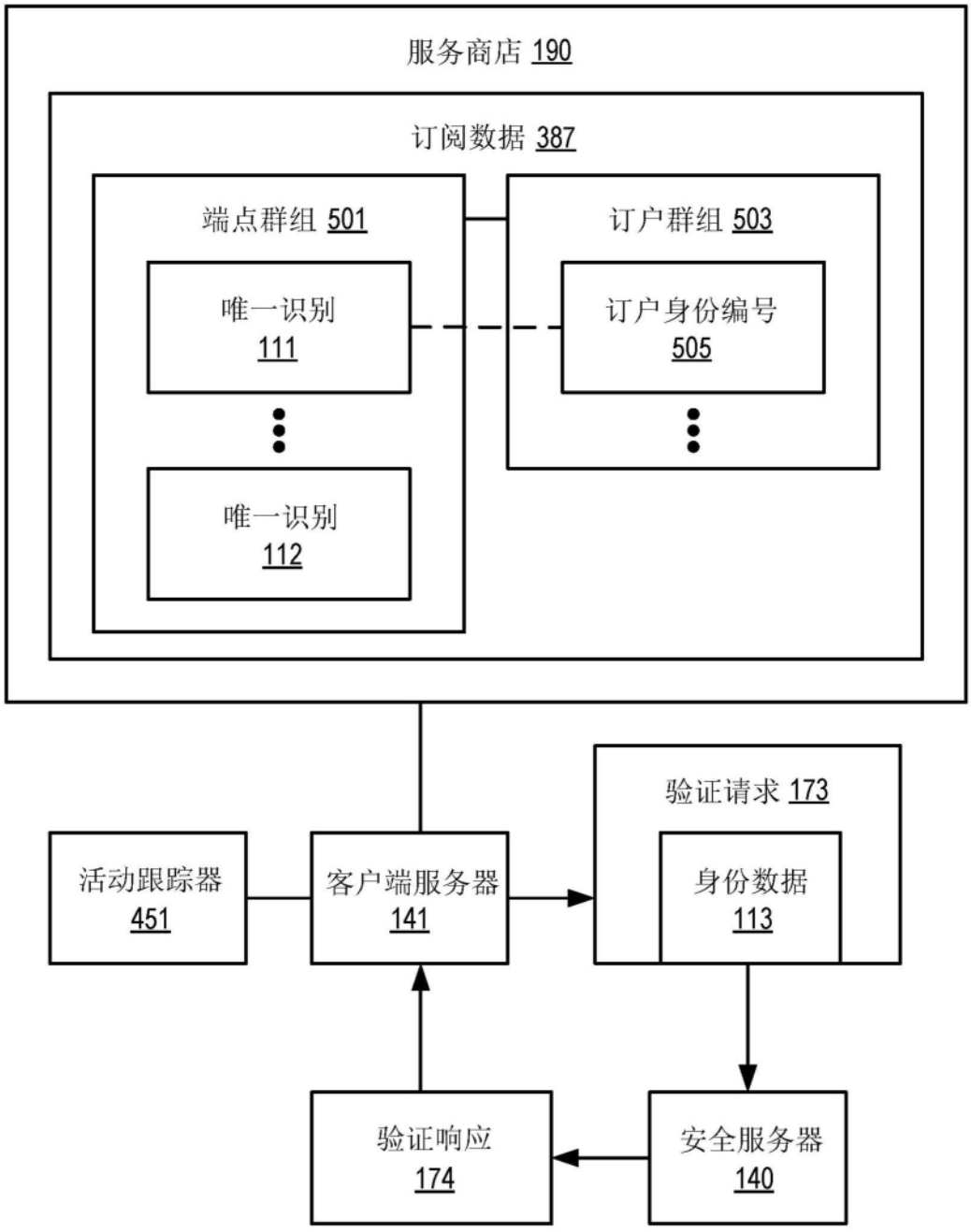

服务商店 190
订阅数据 387
端点群组 501
唯一识别 111
唯一识别 112
订户群组 503
订户身份编号 505
验证请求 173
身份数据 113
活动跟踪器 451
客户端服务器 141
验证响应 174
安全服务器 140

图24

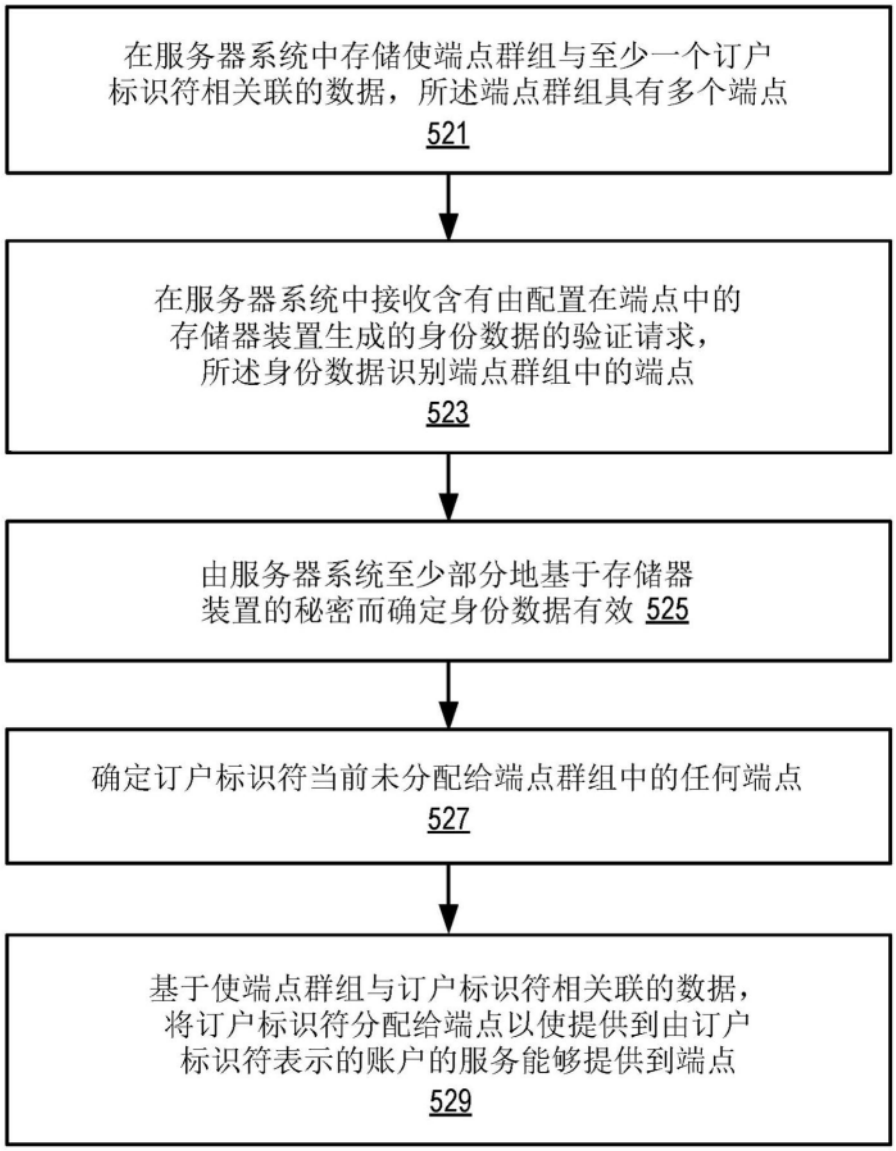

在服务器系统中存储使端点群组与至少一个订户标识符相关联的数据，所述端点群组具有多个端点
521
在服务器系统中接收含有由配置在端点中的存储器装置生成的身份数据的验证请求，所述身份数据识别端点群组中的端点
523
由服务器系统至少部分地基于存储器装置的秘密而确定身份数据有效 525
确定订户标识符当前未分配给端点群组中的任何端点
527
基于使端点群组与订户标识符相关联的数据，将订户标识符分配给端点以使提供到由订户标识符表示的账户的服务能够提供到端点
529

图25

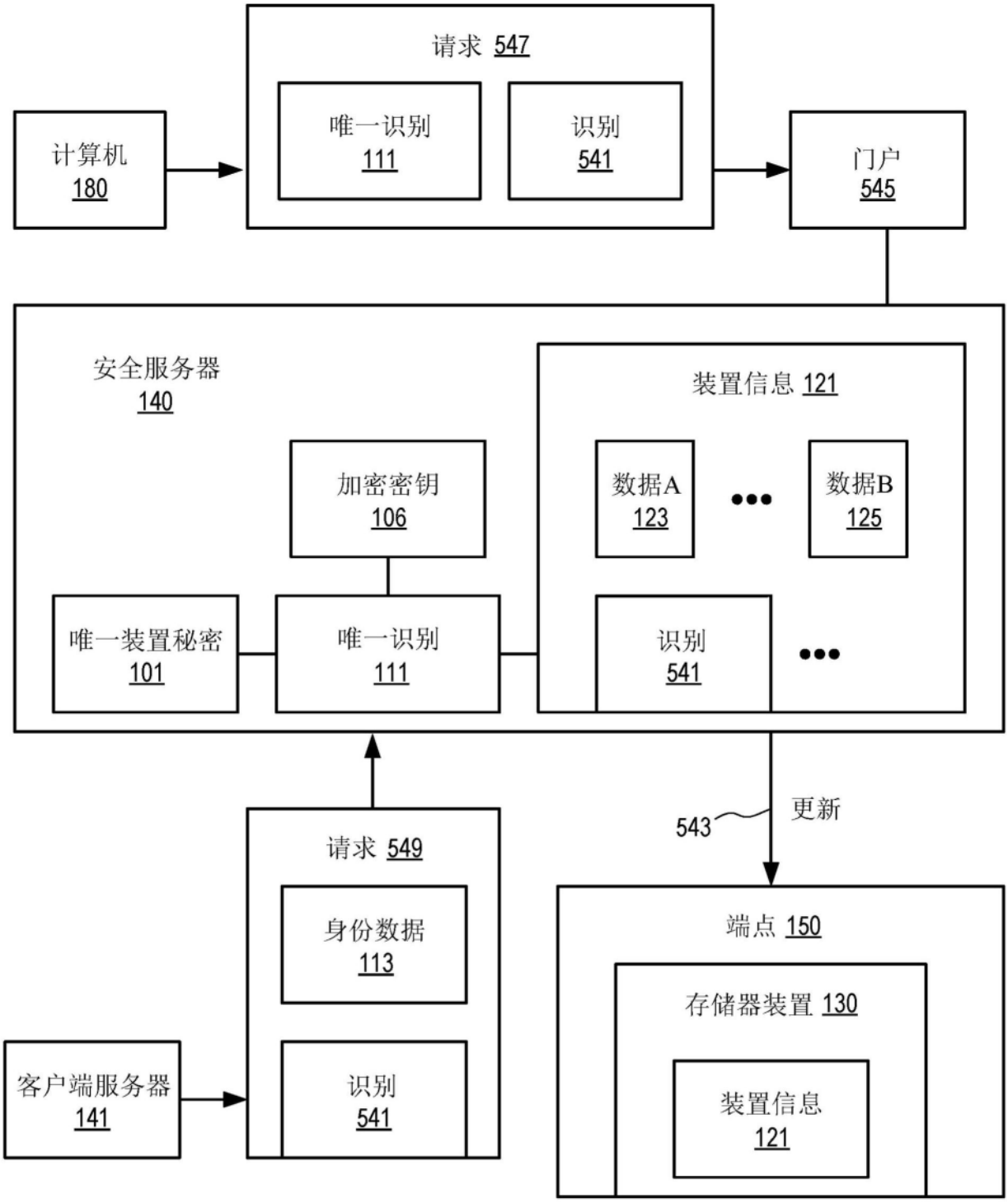

请求 547
唯一识别 111
识别 541
计算机 180
门户 545
安全服务器 140
装置信息 121
加密密钥 106
数据A 123
数据B 125
唯一装置秘密 101
唯一识别 111
识别 541
更新
543
请求 549
身份数据 113
端点 150
存储器装置 130
客户端服务器 141
识别 541
装置信息 121

图26

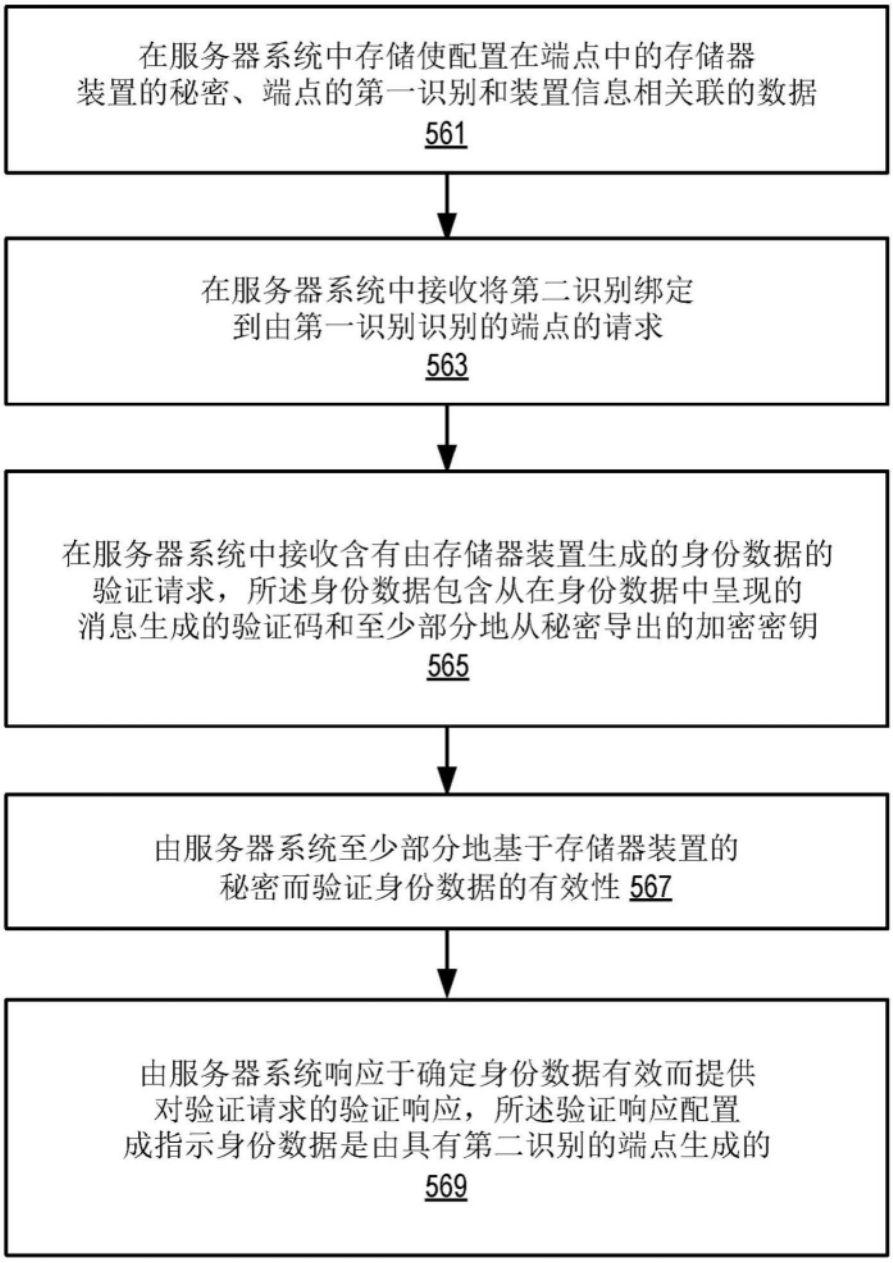

在服务器系统中存储使配置在端点中的存储器装置的秘密、端点的第一识别和装置信息相关联的数据
561
在服务器系统中接收将第二识别绑定到由第一识别识别的端点的请求
563
在服务器系统中接收含有由存储器装置生成的身份数据的验证请求，所述身份数据包含从在身份数据中呈现的消息生成的验证码和至少部分地从秘密导出的加密密钥
565
由服务器系统至少部分地基于存储器装置的秘密而验证身份数据的有效性 567
由服务器系统响应于确定身份数据有效而提供对验证请求的验证响应，所述验证响应配置成指示身份数据是由具有第二识别的端点生成的
569

图27

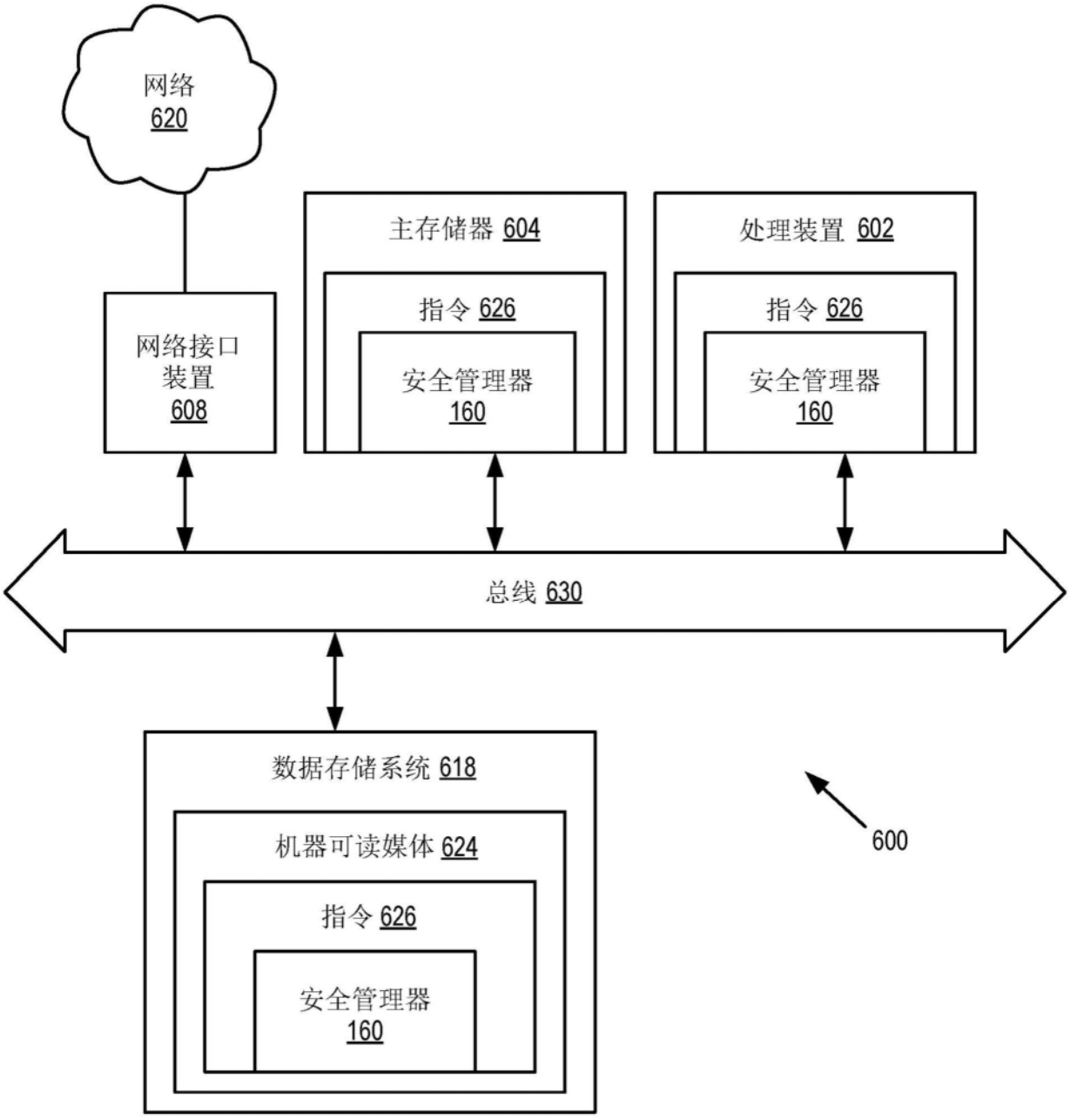

网络
620
主存储器 604
指令 626
安全管理器
160
处理装置 602
指令 626
安全管理器
160
网络接口
装置
608
总线 630
数据存储系统 618
机器可读媒体 624
指令 626
安全管理器
160
600

图28