(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104813328 A
(43)申请公布日 2015.07.29

(21)申请号 201380061134.8
(22)申请日 2013.12.21
(30)优先权数据
13/726,167 2012.12.23 US
(85)PCT国际申请进入国家阶段日
2015.05.22
(86)PCT国际申请的申请数据
PCT/US2013/077340 2013.12.21
(87)PCT国际申请的公布数据
WO2014/100781 EN 2014.06.26
(71)申请人 迈克菲公司
地址 美国加利福尼亚
(72)发明人 V·E·冯博克恩 P·戈埃尔
S·施雷克 N·M·史密斯
(74)专利代理机构 永新专利商标代理有限公司
72002
代理人 王英 张立达
(51)Int.Cl.
G06F 21/50(2006.01)
G06F 15/16(2006.01)

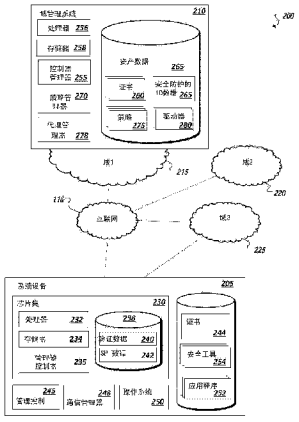
权利要求书3页 说明书21页 附图13页

(54)发明名称

受信容器

(57)摘要

使用计算设备的安全防护的微控制器推导出对于计算设备与特定域的配对是唯一的安全标识符。在所述计算设备的安全防护的存储器中识别与所述计算设备的属性相对应的安全态势数据。在安全防护的容器中将所述安全标识符和安全态势发送至所述特定域的管理设备。所述特定域能够利用在所述安全防护的容器中的信息来验证所述计算设备并且确定将被执行的与所述计算设备和所述特定域的交互有关的安全任务。



CN 104813328 A

1. 一种方法，包括：

使用计算设备的安全防护的微控制器推导对于所述计算设备与特定域的配对是唯一的安全标识符；

在所述计算设备的安全防护的存储器中识别与所述计算设备的属性相对应的安全态势数据；以及

在安全防护的容器中将所述安全标识符和安全态势发送至所述特定域的管理设备。

2. 根据权利要求 1 所述的方法，其中，通过安全通信信道将所述安全防护的容器发送至所述特定域。

3. 根据权利要求 2 所述的方法，还包括：

与所述特定域协商以建立安全信道。

4. 根据权利要求 3 所述的方法，其中，协商所述安全信道包括密钥交换协议。

5. 根据权利要求 4 所述的方法，其中，所述密钥交换协议是 SIGMA 密钥交换协议。

6. 根据权利要求 1 所述的方法，还包括：

在所述计算设备处验证所述特定域；以及

基于所述特定域的所述验证，将安全应用编程接口（API）提供给由所述安全微控制器执行的管理控制器。

7. 根据权利要求 6 所述的方法，还包括从所述特定域接收证书，其中所述特定域至少部分地基于所接收的证书而被验证。

8. 根据权利要求 1 所述的方法，还包括：

使用所述安全防护的微控制器推导对于所述计算设备与第二域的配对是唯一的第二安全标识符；

在所述计算设备的安全防护的存储器中识别与所述计算设备的属性相对应的安全态势数据；以及

将所述第二安全标识符和所述安全态势数据的至少一部分发送至所述第二域。

9. 根据权利要求 1 所述的方法，其中，所述安全防护的微控制器独立于所述计算设备的操作系统，并且由所述安全防护的微控制器推导的安全标识符的值对于所述操作系统是隐蔽的。

10. 根据权利要求 1 所述的方法，还包括使用所述安全微控制器收集所述安全态势数据的至少一部分。

11. 一种方法，包括：

在特定域与特定计算设备之间建立安全连接；

从所述特定计算设备接收所述特定计算设备的安全标识符，所述安全标识符是由所述特定计算设备的安全防护的微控制器根据存储在所述特定计算设备的安全存储器中的验证数据而推导出的；

接收所述特定计算设备的绑定到特定安全标识符的安全态势数据，安全态势识别所述特定计算设备的属性；以及

执行与所述特定计算设备和所述特定域的交互相关的安全任务。

12. 根据权利要求 11 所述的方法，其中，所述安全任务包括将安全策略应用于所述特定计算设备。

13. 根据权利要求 11 所述的方法，其中，所述安全任务包括基于所述安全态势数据来识别与所述特定计算设备相对应的驱动器。

14. 根据权利要求 11 所述的方法，其中，所述安全任务包括经过所述安全微控制器将代理加载到所述特定计算设备上。

15. 根据权利要求 11 所述的方法，将用于所述特定域的验证的域标识符提供给所述特定计算设备。

16. 根据权利要求 11 所述的方法，还包括：

从第二计算设备接收所述第二计算设备的安全标识符，所述第二计算设备的所述安全标识符是由所述第二计算设备的安全防护的微控制器根据存储在所述第二计算设备的安全存储器中的验证数据而推导出的；

接收所述第二计算设备的绑定到所述第二安全标识符的第二安全态势数据，所述第二安全态势数据识别所述第二计算设备的属性；以及

执行与所述第二计算设备和所述特定域的交互有关的安全任务。

17. 至少一种机器可访问存储介质，具有存储于其上的指令，所述指令在机器上执行时使所述机器执行下列操作：

使用计算设备的安全防护的微控制器推导对于所述计算设备与特定域的配对是唯一的安全标识符；

在所述计算设备的安全防护的存储器中识别与所述计算设备的属性相对应的安全态势数据；以及

在安全防护的容器中将所述安全标识符和安全态势发送至所述特定域的管理设备。

18. 根据权利要求 17 所述的存储介质，其中，所述安全标识符是基于所述计算设备的存储在所述安全防护的微控制器的安全存储器中的安全的、永久的硬件标识符来推导出的。

19. 根据权利要求 18 所述的存储介质，其中，推导所述安全标识符包括对所述硬件标识符与所述特定域的域标识符进行哈希处理。

20. 根据权利要求 18 所述的存储介质，其中，所述硬件标识符对于所述安全防护的微控制器是私密的。

21. 根据权利要求 17 所述的存储介质，其中，所述安全标识符是基于由所述特定域通过安全通信信道在所述安全防护的存储器上提供的种子来进行推导的，其中，所述种子对于所述特定域内的所述计算设备是唯一的。

22. 根据权利要求 21 所述的存储介质，其中，推导所述安全标识符包括：

将安全防护的存储器中的所述种子识别为与所述特定域相对应；以及

根据所述种子生成一次性密码，其中，所述特定域根据所述一次性密码来推导所述种子，以针对所述计算设备进行验证。

23. 根据权利要求 17 所述的存储介质，其中，所述安全态势数据包括所述计算设备的启动策略。

24. 根据权利要求 17 所述的存储介质，其中，所述属性包括所述计算设备的硬件配置。

25. 根据权利要求 17 所述的存储介质，其中，所述属性包括所述计算设备的使用状态。

26. 根据权利要求 17 所述的存储介质，其中，所述属性包括安装在所述计算设备上的

软件。

27. 根据权利要求 26 所述的存储介质，其中，所述属性包括安装在所述计算设备上的操作系统。

28. 至少一种机器可访问存储介质，具有存储于其上的指令，所述指令在机器上执行时使所述机器执行以下操作：

参与特定域与特定计算设备之间的安全连接；

从所述特定计算设备接收所述特定计算设备的安全标识符，所述安全标识符是由所述特定计算设备的安全防护的微控制器根据存储在所述特定计算设备的安全存储器中的验证数据而推导出的；

接收所述特定计算设备的绑定到所述特定安全标识符的安全态势数据，其中，安全态势识别所述特定计算设备的属性；以及

执行与所述特定计算设备和所述特定域的交互有关的安全任务。

29. 一种系统，包括：

系统处理器设备；

对于所述系统处理器设备能够访问的系统存储器；

安全管理控制器存储器，其与所述系统处理器和所述系统存储器隔离并且存储：

永久的验证数据；以及

与计算设备的属性相对应的安全态势数据；

安全管理微控制器；以及

管理引擎，适于在由所述管理微控制器执行时执行以下操作：

根据所述验证数据推导安全标识符，所述安全标识符对于所述计算设备与特定域的配对是唯一的；以及

在安全防护的容器中将所述安全标识符和安全态势发送至所述特定域的管理设备。

受信容器

技术领域

[0001] 本公开总体上涉及计算机管理领域，并且更具体地涉及基于硬件的计算机安全管理。

背景技术

[0002] 现代企业和网络内的计算机系统管理能够包括使用用于发现该网络中的各自子系统的属性的工具和技术。安全任务和管理能够例如通过针对网络中的设备分配和实施安全策略来执行。例如，能够基于设备的已知属性将策略分配给特定设备。进而，获得对于网络中的各种设备的访问和/或与其进行通信可以包括基于软件的工具，其被配置为能够在不同的操作系统与设备之间传送各种数据。进而，可以将基于软件的代理安装在系统内的各种设备上，以便为管理者提供在该设备上进行检查、控制并且执行包括安全相关任务的任务的能力。传统上，经过主机设备的操作系统来安装基于软件的代理，并且该操作系统在代理是活动时启动且能够经过该代理与利用和执行任务的管理服务进行通信。在这样的情况下，可以取决于主机设备的操作系统的存在（和可操作性）和/或所安装的代理的存在和可操作性（和安全）来考虑主机设备的管理。

附图说明

[0003] 图 1 是根据至少一个实施例的示例计算系统的简化示意图，该示例计算系统包括具有基于硬件的管理控制器的系统设备；

[0004] 图 2 是根据至少一个实施例的示例计算系统的简化框图，该示例计算系统包括适于与该系统内的一个或多个系统设备上的基于硬件的管理控制器交互的示例域管理器；

[0005] 图 3 是根据至少一个实施例说明示例系统设备与多个不同域之间的交互的简化框图；

[0006] 图 4A-4C 是根据至少一个实施例说明在示例域管理器与具有基于硬件的管理控制器的示例系统设备之间的示例交互的简化流程图；

[0007] 图 5A 是根据至少一个实施例说明在具有基于硬件的管理控制器的示例系统设备与多个示例域管理器之间的交互的简化流程图；

[0008] 图 5B 是根据至少一个实施例说明示例系统设备的安全标识符的生成的简化框图；

[0009] 图 6A 是根据至少一个实施例说明在示例系统设备与示例域管理器之间的示例安全信道的协商的简化流程图；

[0010] 图 6B 是根据至少一个实施例说明在具有基于硬件的管理控制器的示例系统设备与多个示例域管理器之间的交互的简化流程图；

[0011] 图 7A 是根据至少一个实施例说明在示例域管理器与具有基于硬件的管理控制器的示例系统设备之间的交互的简化流程图；

[0012] 图 7B 是根据至少一个实施例说明示例安全容器的简化框图；

[0013] 图 8A-8F 是根据至少一个实施例说明用于管理具有基于硬件的管理控制器的一个或多个系统设备的示例技术的简化流程图。

[0014] 在各附图中类似的附图标号和标记指代类似的元件。

具体实施方式

[0015] 图 1 是说明示例计算环境 100 的简化框图，该示例计算环境 100 包括能够与各种计算系统、网络、或环境（或“域”）（例如，108、110、112、115）交互的多个系统设备（例如，102、105、106、118、120、122、128、130、132、135）。一些系统设备能够包括安全防护的基于硬件的管理控制器（例如、125a-125i），其允许用于系统设备的安全识别符的安全生成和通信，该安全识别符能够在通过包括诸如互联网（例如 116）的广域网的一个或多个网络在该安全防护的基于硬件的管理控制器（例如，125a-125i）与诸如域 108、110、112、115 的服务的后端服务之间的硬件到硬件的通信和事务处理（例如，规避系统设备的操作系统控制）中使用。在一些实现中，硬件到硬件的通信可以经由独立于系统设备（例如，102、105、106、118、120、122、128、130、132、135）的操作系统或者在该操控系统的控制以外的信道在带外发生。

[0016] 域（例如，108、110、112、115）可以包括计算网络、系统和环境，例如私人家庭网络（例如 108）、电子商务系统、搜索引擎系统、社交媒体系统、商业或零售业机构的网络（例如，互联网接入点、WiFi 热点等等）以及企业网络（例如 115）等其他示例。一些系统设备（例如、102、105、106）可以同时在多个不同的域（例如 108、110、112、115）之间迁移并且在这些域内操作，在一些情况下，这些域包括多个环境。可以针对单个系统设备生成多个安全标识符，每个安全标识符对于系统设备与特定域的配对是唯一的。此外，域（例如 108、110、112、115）的后端服务器可以提供有用于协商安全标识符的通信以及针对该系统设备共同验证该域的功能，以确保只有受信实体能够与该系统设备的敏感的基于硬件的控制（例如，管理控制器）直接通信，等等。在一些实现中，每个域（例如 108、110、112、115）可以包括各自的管理系统，其包括用于识别基于硬件的管理控制器（例如，125a-125i）以及与系统设备（例如，102、105、106、118、120、122、128、130、132、135）的管理控制器进行接口连接和通信的功能，以从该设备获得设备信息并且基于所接收的设备信息来执行安全和其他设备管理任务。

[0017] 在一些实现中，管理控制器（例如，125a-125i）可以存在于系统设备（例如，102、105、106、118、120、122、128、130、132、135）的母板或芯片集上并且被实施在独立于系统设备的中央处理单元 (CPU)（和任何操作系统）的微控制器或专用处理器上。管理服务器可以从而经过其各自的管理控制器与系统设备进行带内或带外通信。在一些实例中，管理服务器可以提供应用编程接口 (API)，其适于允许系统设备的管理控制器与管理服务器进行接口连接并且接收和响应该管理服务器的指令和请求。这样的管理服务和任务可以包括在特定网络或域上的系统设备之间协商通信协议并且建立设备间关联性。管理服务器可以附加地或可替换地包括系统安全相关 API，管理服务器 170、175 经过系统设备的管理控制器 108 执行针对网络 110、115 的安全相关任务。

[0018] 在一些实现中，可以基于针对相对应的系统设备的安全识别符的提供来建立基于硬件的 API。例如，安全识别符能够用作唯一地识别和验证家庭网络域 108 中的特定系统

设备（例如 102、105、118、122、120）的基础。安全的硬件到硬件通信可以接着在家庭网络域 108 上的系统设备（例如 102、105、118、122、120）之间被使能，这允许设备之间的各种不同交互。例如，根据在发明名称为“Hardware Management Interface”的美国专利申请号 No. 13/725,722 以及发明名称为“Hardware Management Interface”的美国专利申请序列号 No. 13/726,132（两者全部内容均通过引用结合在此）中描述的原理和示例，经过这样的基于硬件的管理控制器和管理系统可以使能交互、特征、互操作和任务。在另一示例中，企业系统域 115 可以包括各种系统设备（例如，102、106、128、130、132、135）。企业系统域 115 可以利用针对每个系统设备生成的唯一安全标识符来验证和唯一地识别设备以及针对每个设备应该调整的安全策略。域可以利用安全标识符和基于硬件的 API（例如，经过安全标识符验证的）以使得能够基于设备的安全防护的验证来提供服务。

[0019] 一般而言，“服务器”、“客户端”、“计算设备”、“网络元件”、“主机”、“系统类型系统实体”以及“系统”，包括示例计算环境 100（例如，102、105、106、118、120、122、128、130、132、135 等等）中的系统设备，可以包括可操作为接收、传输、处理、存储或管理与计算环境 100 相关联的数据和信息的电子计算设备。如在本文档中使用的，术语“计算机”、“处理器设备”或“处理设备”意在包含任何合适的处理设备。例如，示出为计算环境 100 内的单个设备的元件可以使用诸如包括多个服务器计算机的服务器池的多个计算设备和处理器来实现。进而，计算设备中的任一个、全部或一些可以适于执行任何操作系统，包括 Linux、UNIX、Microsoft Windows、Apple OS、Apple iOS、Google Android、Windows Server 等等，以及适于虚拟化特定操作系统（包括定制和专有操作系统）的执行的虚拟机。

[0020] 用户、端点或客户端计算设备可以包括传统的和移动计算设备，包括个人计算机、膝上型计算机、平板计算机、智能手机、个人数字助理、特色手机、手持视频游戏机、台式计算机、互联网电视以及被设计为与人类用户进行接口连接并且能够通过一个或多个网络（例如 108、110、112、115、116）与其他设备进行通信的其他设备。计算机辅助或者“智能”器具可以包括家用和工业设备以及包括计算机处理器并且由该计算机处理器、其他硬件和/或由计算机处理器执行的一个或多个软件程序控制、监控、辅助、补充或者以其它方式增强该设备的功能的机器。计算机辅助器具可以包括各种各样的计算机辅助机器和产品，包括冰箱、洗衣机、汽车、HVAC 系统、工业机器、烤箱、安全系统等等。

[0021] 虽然图 1 描述为包含多个元件或者与多个元件相关联，但是并非图 1 的计算环境 100 内说明的所有元件都会在本公开的每个替代实现中使用。此外，结合图 1 的示例描述的元件中的一个或多个可以位于计算环境 100 外部，而在其他实例中，某些元件可以被包括在其他所描述的元件以及未在所说明的实现中描述的其他元件的一个或多个内或者作为其一部分。进而，图 1 中说明的某些元件可以与其他组件组合，并且用于除了在本文描述的那些目的以外的可替换的或附加的目的。

[0022] 检测、识别、跟踪和管理计算系统中的资产（asset）传统上已经成为系统管理者面对的重大挑战。连接到网络的单个未知的、缺乏了解的或者缺乏监控的设备会潜在地将整个系统暴露于各种安全威胁和攻击，包括恶意软件、未授权的数据访问、流氓用户等等。在一些实例中，代理（例如 140a、140b）可以被安装在系统设备（例如 130、132）上以辅助管理者查看系统设备的属性，容易地检测网络上的设备且与其进行通信，并且在系统设备上实施特定的安全策略。然而，未受管理的设备（即，不拥有安装的代理的设备）会保持在

管理系统的通信、控制和监控之外，该管理系统被设计为使能设备间通信和操作、在设备进入和离开网络时检测该设备、对各种设备应用策略以及在网络上实施安全，这些功能由于不能有效地与这样的未受管理的设备进行通信而受到阻碍。进而，在一些设备上安装代理会是困难的，代理的提供受到非常缺乏关于未受管理的设备的信息的损害。此外，在一些实例中，未受管理的设备不是能够集成到网络中并且能够整体上有益于用户或网络，而是能够被发送到隔离检查的或者管理的子网络直到管理者更加仔细地检查该未受管理的设备，在其上安装代理等等。此外，由于越来越多的设备变得“智能”，因为它们日益受到计算处理器的控制，包括网络通信适配器并且能够与其他系统进行通信，因此，潜在地未受管理的设备的范围在持续增加。

[0023] 此外，安全管理会涉及包括利用各种平台和操作系统的设备的各种各样的系统设备的管理。在本公开中描述的系统中的至少一些，例如图 1 和图 2 的系统，可以包括在一些情况中能够解决上述问题以及在本文没有明确描述的其他问题的功能。例如，为了提供跨各种系统设备平台的这一级别的功能支持，可以经过示例管理控制器（例如 125a-125i）在操作系统之下的硬件中提供功能。例如，可以一致地跨各种硬件平台（例如结合能够在各种各样的系统设备中利用的芯片集家族）来实现这样的管理控制器功能。安全和受信的 API 可以基于硬件提供有远程可访问能力，使得即使在缺少代理或其他这样的组件的情况下，仍然能够一致且可靠地访问安全数据和操作。

[0024] 虽然在设备与域之间的硬件 API 的特性和能力会改变并且演化以实现潜在无穷的各种任务并且提供无穷的潜在特征阵列，但是植根于或者基于硬件的系统设备的身份能够用作这样的设备能够被构建在其上的原子单元。在一些实例中，除了提供用于生成系统设备的安全标识符的功能以外，管理控制器能够进一步使能远程服务器访问其他受信身份信息。例如，转至图 2 的示例，简化框图 200 示出了包括示例系统设备 205 和特定域 215 的域管理系统 210 的计算环境。特定域 215 可以是系统设备 205 可以与其交互的若干域（例如 220、225）之一。每个域可以实现利用与域 215 的域管理系统 210 类似的原理的域管理系统。进而，在一些实例中，系统设备 205 可以例如通过连接到由域（例如 225）控制或与其相关联的私人网络，或者可替换地至少部分地通过诸如互联网 116 的公共网络，来与域进行直接交互。

[0025] 在一个示例实现中，系统设备 205 可以包括芯片集 230，其包括诸如中央处理单元 (CPU) 的处理器 232 以及存储器 234，该存储器 234 例如是包括由 CPU 利用并且对于系统设备 205 的操作系统（例如，250）可存取的系统存储器的存储器。在一些示例中，芯片集 230 可以附加地包括管理微控制器 235，其可以提供安全防护的处理功能以执行在操作系统的控制和指令以外（或者之下）的管理任务。在一些实现中，示例管理微控制器 235 可以运行提供低功率、带外管理控制器的少量内核操作系统。在一些实现中，可以提供由管理微控制器 235 访问并且利用的安全防护的存储器 238，以执行包括生成系统设备 205 的安全标识符的设备管理活动。安全防护的存储器 238 可以与系统存储器分离并且作为一个示例可以被体现为芯片集 230 的闪存组件，等等。安全防护的存储器 238 可以包括由管理微控制器 235 使用的验证数据 240 以生成用于该系统设备 205 的安全 ID，并且在一些实例中，可以包括安全 ID 本身。在一些实现中，安全防护的存储器 238 可以附加地包括描述系统设备 205 的属性的安全态势数据 242，其被安全地保持并且不受设备 205 的用户、操作系统 250 或者

其他实体（包括恶意软件和可能访问设备的系统存储器和/或操作系统250的黑客）的改变、控制或操控。附加地，安全防护的存储器238可以额外地包括、存储或指向由管理微控制器执行的指令和软件（例如245）以提供管理控制器的功能，包括安全ID和安全态势数据242的生成和管理等等。

[0026] 除了安全防护的处理和存储器设施以外，系统设备205还可以包括通信管理器248，其可以用于实现管理控制器和域与它们各自的域管理系统之间的安全防护的通信信道。在一些实现中，通信管理器248可以与管理微控制器235结合实现以允许管理微控制器访问网络，同时系统设备205的操作系统是不活动的、缺席的等等。因此，管理微控制器235可以直接访问系统设备的网络接口。在一些实现中，管理微控制器可以运行完全独立的带外通信信道（例如通过专用TCP/IP栈），允许微控制器检查并且接收未由CPU处理的分组，并且在CPU对其进行访问之前检查进站和/或出站业务。有效地，两个逻辑网络连接可以被维持在设备205的单个物理联网连接器上，一个经过CPU（例如232）在带内，而另一个经过管理微控制器235在带外。通信管理器248中的网络滤波器可以用于例如基于端口数目，可编程地将业务重新指向主机操作系统接口或者管理微控制器235处的管理控制器的接口。独立的网络通信信道可以允许管理微控制器235（以及使用管理微控制器实现的管理控制器）执行可以一直潜在地有效发生而与操作系统的状态无关的各种通信和远程管理功能。

[0027] 管理微控制器235可以利用独立和/或专用网络通信信道以通过一个或多个网络（例如，116、域215的网络等等）与包括域（例如215、220、225）的管理系统（例如210）的外部系统进行通信。系统设备的管理控制器和域管理系统（例如210）可以结合它们的交互、会话、API等等而进行共同验证。在一个示例实现中，一个或多个证书（例如244）可以被保持为与证书颁发机构相对应，该证书颁发机构将该证书颁发给域（用于经过它们各自的域管理系统使用），证明该域是合法的、受信的并且满足用于使授权的域在该证书下合格的阈值，以与基于硬件的管理控制器进行接口连接和通信。在一些实现中，这样的证书可以是特定于管理控制器的特定品牌、型号或实现的。在将敏感信息传送到域管理系统之前，管理控制器可以检验相对应的域管理系统拥有证书（例如260）的副本，或者仍然是证书的授权拥有者（例如，基于对证书的颁发机构的查询）。管理控制器可以顺次提供系统设备的安全标识符以在该域处验证系统设备。

[0028] 在一些实例中，证书（例如244）可以与安全态势数据242、验证数据240和其他信息一起被维持在管理控制器可存取的存储器（例如238）上。管理控制器可存取的存储器（例如238）也可以由管理微控制器写入。在一些实现中，管理控制器可存取的存储器（例如238）可以是非易失性的受保护存储器，因为系统设备205的其他硬件组件和系统设备205的操作系统250不能够存取该存储器238，从而确保存储在安全防护的存储器238中的信息的完整性和保密性。进而，除了受保护的管理控制器可访问的存储器（例如238）以外，在一些实现中，管理微控制器235附加地存取系统存储器（例如234），允许管理控制器访问关于系统设备205的属性的附加信息，例如系统设备的应用程序（例如252）、在该设备上部署的安全工具和应对措施（例如254）、系统设备的活动和历史、用于该设备的地理位置信息、系统设备的用户概况、由该设备使用或连接到该设备的网络，等等。在一些实现中，这样的信息可以用于生成安全地包含在系统设备205的硬件内的安全态势数据242。进

而，在一些示例中，管理控制器还可以被配置为管理代理、软件更新、安全工具和其他程序、特征和数据在该系统设备上的提供，以增强该设备的功能和安全，等等。

[0029] 示例域管理系统 210 可以在域的计算设备、服务器和设施中实现，以管理与连接到该域并且参与该域的系统设备的基于硬件的管理控制器的交互。例如，示例域管理系统 210 可以包括一个或多个处理器 256、多个存储器元件 258 之一，以及诸如控制器管理器 255、资产管理器 270、策略管理器 272 和代理管理器 278 等其他潜在组件的其他工具和组件。控制器管理器 255 可以提供用于识别、验证和管理与试图结合设备与域（例如 215）的交互而利用基于硬件的管理控制器的一个或多个系统设备（例如 205）的会话的功能。例如，控制器管理器 255 可以管理域（例如 215）与系统设备（例如 205）的共同验证，例如使已经由受信的颁发机构颁发证书的系统设备合法化，并且接受和管理来自该系统设备的安全标识符和其他信息。进而，控制器管理器 255 可以管理已经与其进行通信的系统设备，包括使用基于硬件的管理控制器参与域的那些系统设备。例如，控制器管理器 255 可以维持将安全防护的 ID 映射到利用基于硬件的管理控制器的单独系统设备的安全标识符数据。

[0030] 资产数据 265 也可以被保持或者对于示例设备管理系统 210 可用，资产数据描述包括在该域中或者被识别为访问该域的多个资产的属性，该域包括具有基于硬件的管理控制器（例如 205）的系统设备。资产数据可以从各种源进行收集，包括单独资产上安装的代理、资产的扫描（例如，通过各种安全工具、本地和 / 或基于网络的扫描仪等等），以及经由与利用基于硬件的管理控制器的资产的通信而接收的安全态势数据和其他属性数据。资产可以包括系统设备、网络、应用程序、数据结构以及利用、包括在和 / 或管理域的系统的人类用户。进而，客户端系统设备的安全标识符可以被与资产数据 265 中的概况维持在一起和 / 或被映射到该概况。

[0031] 除了提供用于将策略动态地分配给特定系统设备并且实施这些策略的功能的策略管理器 270 以外，在一些实现中，策略管理器 270 还可以包括用于定义新策略、修改现有策略、建立用于将策略应用到特定系统设备（例如，基于所检测的设备的属性）的规则和标准等等的功能。策略管理器 270 可以与部署在网络内的一个或多个安全工具协同操作并且可以在系统设备本身上进行本地操作。例如，一些安全工具可以被部署为远离系统设备，以允许策略实施远离目标系统设备、应用程序或人发生，从而允许安全实施而无需将策略（或实施）推向目标本身。这例如在移入和移出受监控的网络的移动设备，以及未受管理的设备（例如不包括能够实施重要的安全策略的代理或者其他本地安全工具的设备）的安全实施中会是有用的。这样的安全工具可以例如包括防火墙、网络网关、邮件网关、主机入侵保护 (HIP) 工具、网络入侵保护 (NIP) 工具、防恶意软件工具、数据丢失防止 (DLP) 工具、系统攻击管理器、系统策略遵守管理器、资产临界工具、入侵检测系统 (IDS)、入侵保护系统 (IPS) 和 / 或安全信息管理 (SIM) 工具等等。无论如何，经过运行、加载或者以其它方式与系统设备直接进行接口连接的安全工具，安全实施在目标系统设备本地上也是可能的。在一些实例中，安全工具还可以为管理控制器提供用于直接在目标设备处实施策略的接口。例如，在一些示例中，部署在系统设备上的代理可以用作安全实施工具，例如，根据应用于特定系统设备的一个或多个安全策略本地地阻止该设备处的特定活动、将策略指令传递给特定系统设备上的其他安全工具。

[0032] 包括在资产数据 265 中的属性信息可以用于确定将被应用于各个资产的策略

275。可以提供策略管理器 270，管理策略 275 在域（例如 215）内的开发和实施。在一些实例中，可以基于资产数据，针对各个资产来调整策略。在其他实例中，预先开发的策略可以基于资产数据而被匹配到资产。策略 275 可以包括安全和遵守策略，以及用于管理和控制域的其他策略。例如，基于对策略 275 的遵守，可以执行对数据、应用程序、服务和域的其他资源的访问、安全任务、审查、扫描、应对措施部署、更新和其他动作，等等。进而，对于利用基于硬件的管理控制器的系统设备资产，策略实施会试图影响管理控制器以执行这样的任务。作为一个示例，可以从系统设备获得信息，允许域管理系统 210 识别针对该系统设备的驱动器，该驱动器可以被下载或者以其它方式识别和访问以允许域管理系统 210 更好地与系统设备通信并且协调与该系统设备的通信以及在该系统设备与该域内的其他计算设备之间的通信。

[0033] 在另一示例中，域管理系统可以包括代理管理器 278，其适于辅助代理加载在该域内的各种资产上。在一些实现中，代理管理器 278 可以用于经过基于硬件的管理控制器将代理加载在系统设备上。该代理随后可以用于辅助管理和识别系统设备。在一些实现中，代理管理器 278 可以辅助加载永久代理至系统设备上，而在其他示例中，可以加载例如与系统设备（例如 205）与域 215 之间的给定会话相对应的暂时的、可解除的代理。

[0034] 代理的加载仅是能够经过与受信域管理系统进行接口连接的基于硬件的管理控制器安全和有效地执行以改善域和系统设备两者的安全性、可操作性和特征集的潜在无穷的任务和服务之一。实际上，受管理的系统设备（例如已经具有代理的设备）自身可以通过提供基于硬件的管理控制器而得到改善。例如，当端点由于重新成像、操作系统重新安装、硬件更新（新的磁盘或新的网卡）或简单地卸载代理等等而改变时，识别系统和安装新的相对应的替代代理的能力可以基于系统设备的基于其安全防护的 ID 的重新识别。这也可以有益于在第三方域（例如，客户环境）内或者在云中提供器具，因为能够可靠且一致地检验系统设备的身份。此外，在执行涉及该设备的任何敏感任务之前，确保该设备在引导阶段处于已知状态可以提供表示该设备的信任水平的附加数据点。在其他附加示例中，“欺骗端点”袭击会通过挑战正在报告的代理数据的有效性而威胁损害端点系统设备的完整性。通过经过基于硬件的管理控制器生成的基于硬件的安全 ID，这一整个类型的问题由于可靠地检验系统设备的身份的能力而被排除。

[0035] 进而，基于值得信任的安全态势数据（例如，242）可以推断系统设备的安全状态，以有助于在允许特定资产访问网络之前细化其对环境造成的风险的评估。作为另一示例，可以通过借助根植于硬件的值得信任的安全 ID 数据以代替（或作为补充）其他诸如 IP 地址、MAC 地址等等的较不持续或具有欺骗性的标识符来改善网络监控器（例如防火墙、入侵检测系统、入侵防止系统和其他安全工具）。在其他示例和优势中，在主处理器、系统存储器、操作系统等等不可用或不可操作时，经过管理控制器的一些实现的安全联网能力，可以实现对于安全态势数据和安全存储器（例如 238）的其他资源的带外网络访问，允许附加的特征和服务，包括支持和诊断任务的性能。

[0036] 进而，在存储于系统设备处的安全态势数据中描述的属性信息可以被传送至使用管理控制器的验证的域管理系统。这样的信息可以包括识别系统设备以及该系统设备上的计算设备的类型的信息，允许管理系统识别和 / 或取回对应于该系统设备的设备驱动器。在一个示例中，属性信息可以包括该系统设备的计算设备和 / 或该系统设备本身的品牌、

型号和制造商的标识。属性信息还可以包括固件、操作系统和由该系统设备的计算设备使用的其他软件的标识，包括版本信息。使用属性信息，管理系统（例如使用控制器管理器）可以识别为设备驱动器提供服务的源（包括远程源）、更新以及用于系统设备和/或其计算设备的其他信息。这样的信息随后可以用于执行各种安全相关任务并且改善与系统设备的事务处理。

[0037] 转到图 3 的示例，所示的简化框图说明了单个系统设备 205 可以维持并且提供多个唯一的安全 ID（例如 305、310），每个安全 ID 与系统设备 205 和不同的各自域（例如 210、220）的特定配对相对应并且对于该配对是唯一的。系统设备 205，经过基于硬件的管理控制器 302，可以生成或识别对应于特定域的安全 ID 并且将该安全 ID（例如 305、310），在该设备 205 的操作系统的访问和控制以外，传输至该域，例如传输至该域的域管理系统，等等。该域随后可以根据该安全 ID 验证和识别该设备。

[0038] 转至图 4A-4C 的示例，所说明的示例流程图 400a-c 示出了生成和使用用于示例系统设备的安全 ID 的示例技术。在图 4A 中，系统设备的特定软件 410，例如在该系统设备的操作系统内的应用程序，可以利用域（例如，在域接口 415 处）请求事务处理 422。该域可以利用域管理器（在此被称为“域管理系统”）420 以请求 424 该系统是否能够例如经过该系统设备的安全的基于硬件的管理控制器（例如 405）提供受信的、基于硬件的安全 ID。请求 424 也可以指导系统设备提供安全 ID，以在该域处验证系统设备。在图 4A 的特定示例中，系统设备将拒绝该请求 424 的响应 425 返回至域。

[0039] 可以由于各种因素导致拒绝（例如 425）。在一些实例中，该域可能不具有由系统设备（例如，使用管理控制器 405）承认的有效证书，以表明该域是用于与管理控制器 405 通信、提供和/或共享系统设备的安全 ID、与该域共享安全态势数据等等的值得信任的伙伴。在另一示例中，系统设备可能未配备有与该域及其请求 424 兼容的管理控制器。在又一些示例中，涉及系统设备的管理控制器和域的安全会话可能是用户指导的。例如，响应于接收到请求 424，在系统设备上会对用户呈现用户界面，以请求准许该管理控制器 405 在系统设备与域之间建立安全的硬件到硬件通信。在这样的实例中，用户可以自由地选择拒绝该域具有与系统设备的管理控制器进行接口连接的特权。在这样的实例中，系统设备可以试图参与与该域的传统会话（例如事务处理 428），而无需管理控制器 405 的辅助或特征以及使用管理控制器 405 和域管理器 420 建立的安全会话。

[0040] 在图 4A 的示例中，响应于对于建立与域管理器 420 的安全会话的拒绝，域管理器 420 可以使一组策略应用于 426 系统设备。该组策略可以是用于没有（或不能够）提供安全 ID 的增强的识别服务以及使用兼容的管理控制器的安全防护的通信信道的任何这样的系统设备或者系统设备的类似型号的缺省策略。这样的策略可以包括导致系统设备的用户享受对于该域、其服务、数据、促销等等的简化水平的访问的安全策略、电子商务策略等等。在一些实例中，系统设备的所请求的事务处理（例如，422 处）可以取决于有效的安全 ID 的交换、导致由该域对所请求的事务处理的拒绝的拒绝 425。在其他示例中，例如在图 4A 中说明的示例，所请求的事务处理仍然可以被执行（例如 428），尽管在事务处理 428 期间将拒绝和更加严格的策略 426（诸如更加限制性的安全策略）应用于系统设备。

[0041] 转至图 4B 的示例，将另一事务处理请求从系统设备的软件 410 转发至域 415，再次导致对于来自系统设备的安全 ID 的请求 432。在这一示例中，例如，响应于用户准许在系统

设备处与该域的安全会话，设备软件 410 可以查询（例如在 434 处）管理控制器 405 以确定安全 ID 对于请求的域是否是可用的。在一个示例实现中，安全 ID 可以基于从该域接收到的种子数据，其中管理控制器将附加的验证数据与该种子数据组合，或者应用在基于硬件的管理控制器 405 处安全地受信和执行的特定算法以基于该种子数据生成安全 ID。在一些实例中，安全 ID 可以是对于该域与系统设备的配对是唯一的一次性密码的形式。在图 4B 的示例中，管理控制器可以确定对于请求的域不存在种子并且将这一结果（例如在 435 处）传送至系统设备软件。在一些实例中，这可以表明在系统设备与域之间还没有建立配对。

[0042] 如图 4B 的示例所示的，系统设备可以向该域告知（例如在 436 处）：还没有从该域接收到种子，但是期望与该域的安全会话。使用管理控制器 405 的系统设备接着可以与该域协商 438 安全防护的交换协议以便有利于域种子到系统设备的管理控制器 405 的安全和秘密传送，避免该种子对于该系统设备的操作系统以及第三方欺骗者可识别，等等。在一些实现中，为了向该系统设备共同验证域（例如域的域管理器 420），域管理器 405 可以使用所协商的安全信道（例如建立于 438 处），结合域特定的种子 443（例如在 442 处发送的）附加地将域证书（例如由受信的证书颁发机构颁发）发送 440 至系统设备。安全信道还可以用于将对于系统设备与域的配对是唯一的域种子 443 提供给系统设备的管理控制器 405。因此，在将种子 443 提供 442 给管理控制器 405 之后，种子 443 的副本可以被永久地存储在域管理器 420 和管理控制器 405 的每一个上。种子 443 可以作为对于该域的验证数据而存储在管理控制器 405 的安全存储器中。管理控制器接着可以使用种子 443 以基于管理控制器能够传送至域管理器的该种子来生成一次性密码。一次性密码的形式可以在管理控制器 405 与域管理器 420 之间协商并达成一致。在一个示例中，可以通过对种子 443 和域标识符（例如四个字节的域 ID）的组合进行连结或哈希处理来生成一次性密码。域 ID 可以例如包括在传送 440 至管理控制器 405 的证书中。在另一示例中，一次性密码可以基于系统时钟值与种子的哈希或连结处理。

[0043] 一旦接收到一次性密码（或者在管理控制器 405 处由种子生成的其它安全 ID），该域可以基于该一次性密码检验参与与该域的会话的系统设备是种子所传输到的相同系统设备。基于系统设备的标识和验证，由管理控制器传送的任何安全态势数据以及以其它方式从系统设备收集的属性信息，可以在系统设备与域管理器之间的事务处理 448 期间由域管理器 420 将策略应用 446 于系统设备。在一些实现中，在域处系统设备经由基于域种子（例如 443）的安全 ID 的验证可以导致更加容许的策略应用 446 于该域中的系统设备，在一些示例中，增强了在与该域的事务处理会话 448 期间对于系统设备可用的访问、许可、服务和特征。

[0044] 转至图 4C 的示例，表示系统设备与该域之间的后续事务处理。在这一示例中，系统设备上提供的域种子 443 保持被存储在管理控制器 405 的安全防护的存储器中以及域管理器 420 的存储器中。附加的验证数据也可以被存储在管理控制器 405 的安全防护的存储器中，诸如与种子 443 相对应的域的域 ID。可以由系统设备请求 450 事务处理，由域管理器 420 触发对于系统设备的安全 ID 的请求 452。在一些实例中，用户可以提供有选项以从事与该域的安全防护的会话，而在其他实例中，用户可以指示：在提供种子 443 之后，与该域的未来会话应该被自动安全防护而无需直接用户批准，等等。进而，可以针对种子是否已经

被提供用于请求的域来查询 454 管理控制器 405。管理控制器 405 可以通过识别安全防护的存储器中的种子 443 并且回复 455 已经提供该种子 443 来响应该查询 454。管理控制器 405 和域管理器 420 可以再次协商和建立（例如在 456 处）用于传送系统设备的安全 ID 的安全防护的信道。或者，可以识别和应用先前协商的安全通信协议以在管理控制器 405 与域管理器 420 之间建立安全的通信信道。附加地，为了针对系统设备验证域管理器，管理控制器 405 可以例如通过确定证书是否来自有效的证书颁发机构并且确定该域是否保留证书的有效持有者（例如通过检查批准的或者可选地由证书颁发机构识别的恶意域的列表等等），来重新检验 458 该域的域证书。

[0045] 一旦验证发出请求的域管理器 420 和建立 438 安全防护的通信信道，管理控制器可以基于种子 443 生成一次性密码的实例并且将该一次性密码传送 460 至域管理器 420。域管理器 420 也可以独立地生成一次性密码并且将其与从管理控制器 405 接收（在 460 处）的一次性密码进行比较，以验证管理控制器 405 确实是在该域与其具有预先存在的关系（例如，如在图 4B 的示例中建立的）的系统设备上先前生成和提供的种子（例如 443）之一的持有者。因此，在管理控制器 405 与域管理器 420 之间建立的安全会话期间，域管理器 420 可以识别（或重新识别）与由基于种子的安全 ID（例如一次性密码）识别的系统设备相对应的安全策略，并且在利用系统设备完成的事务处理 464 期间将该安全策略应用 462 于该系统设备。

[0046] 在一些实现中，多个不同的种子（包括种子 443）可以被存储在管理控制器 405 的安全存储器上，每个种子对应于管理控制器 405 的系统设备与各自域的特定配对。在一些实现中，安全防护的存储器中的种子（以及其他验证数据）无法被篡改或修改并且可以在存储器中持久，以便无惧系统清理、操作系统安装以及影响系统设备的其他存储器的类似情况。然而，为了保护用户的隐私，用户可以使管理控制器重置或删除安全存储器中的种子以及其他验证数据，包括安全存储器中的全部安全 ID、验证数据和其他标识符的完全重置。例如，在出售或者以其它方式处置系统设备时，用户会希望擦除基于硬件的安全 ID 以便另一用户无法使用由前一用户使用的先前的安全 ID，以在特定域内验证与前一用户相关联的概况，等等。

[0047] 管理控制器可以使用和生成其他类型的安全 ID。作为另一示例，如在图 5A-5B 的简化框图中说明的，可以可替换地由系统设备的永久硬件标识符（例如 525），而不是由该域提供并且与管理控制器结合地存储的种子的集合，来生成一个或多个安全 ID。例如，转至图 5A 的简化流程图 500a，系统设备（例如经过系统设备操作系统和运行在该操作系统上的应用程序以及其他设备软件 510）可以请求与域 A 之间的事务处理或会话（例如与域 A 的接口 515 进行接口连接）。域 A 的域管理器 520 可以用于试图建立利用系统设备的管理控制器 505 的功能的安全会话。例如，域管理器 520 可以请求 535 来自系统设备的安全 ID 以验证（以及潜在地重新识别）系统设备。如在图 4A-4C 的示例中，用户可以被提供有并且给予允许与该域建立安全会话以及设置针对该会话的规则和 / 或偏好的选项。例如，用户可以设置用于建立什么样的安全态势数据和数据类型能够与请求的域共享（例如，在一些情况下，基于该域的特定身份，改变共享的数据量）、建立管理控制器 505 是否可以自动试图加入与域（或者用户识别的域的子集）的安全会话（例如通过跳过用户验证步骤）的规则、偏好或参数。

[0048] 进而，如在图 4A-4C 的示例中，可以针对管理控制器与域管理器之间的通信（并且在系统设备的操作系统的控制和解释以外）建立 538 安全通信信道。进而，管理控制器 505 可以提供有 540 域 A 的域证书以验证域管理器 520 作为安全会话的值得信任的伙伴（例如在先前示例中）。在一些实例中，域证书可以与安全通信信道的协商和构建（例如 538）相结合地被传递 540 至管理控制器 505。在图 5A 的示例中，管理控制器 505 可以识别域证书中该域的信息。在一些实例中，域证书可以包括唯一地识别该域的数据。管理控制器 505 可以使用管理控制器的安全（和秘密）的硬件标识符 525，连同域标识符一起生成对于管理控制器 505（以及相对应的系统设备）与域管理器（以及相对应的域）的配对唯一的安全 ID。在一些实例中，安全 ID 可以经过安全硬件标识符 525 和域标识符的哈希处理来得到，等等。

[0049] 一旦根据硬件 ID 525 推导出安全 ID，如在其他示例中，管理控制器 505 随后可以将安全 ID 返回 545 至域管理器，以在该域处识别和验证管理控制器（和系统设备）。域管理器 520 随后可以确定该安全 ID 是之前已经在该域处被接收还是该域内的新的安全 ID。在安全 ID 匹配之前接收的安全 ID 的实例中，域管理器 520 可以识别与安全 ID 相对应的预先生成的概况和概况数据，并且基于安全 ID 将系统设备与该概况重新相关联。在安全 ID 被确定为域 A 的新的安全 ID 的实例中，域管理器 520 可以生成与新的安全 ID 相对应的概况记录。类似技术可以应用于结合图 4A-4C 描述的示例实现。概况记录可以用于收集和存储描述与管理控制器 505 和安全 ID 相关联的设备（和 / 或用户）的安全相关属性的安全数据。其他属性也可以被记录在概况记录中并且与安全 ID 相关联，例如包括对应于系统设备在该域中的交互和事务处理并且在该系统设备在该域中的交互和事务处理期间收集（例如，使用管理控制器 505）的会话信息、用户概况信息、浏览历史、账户信息等等。按照这一方式，域管理器可以基于安全和值得信任的安全 ID 来可靠地识别特定系统设备在该域内的使用。如在其他示例中，在管理控制器与域管理器 520 之间的安全会话内，域管理器 520 随后可以确定针对该系统设备的属性调整的安全策略（和其他策略）并且在事务处理 550 中将这些策略应用 548 于系统设备。

[0050] 转至图 5B，所示的简化框图 500b 说明涉及示例管理控制器 505 的组件和交互。在这一特定示例实现中，管理控制器 505 可以包括管理微控制器，其具有对于该管理微控制器可访问的，但是与系统设备的其他元件（诸如 CPU、操作系统等）隔离的安全管理微控制器只读存储器 572。管理微控制器存储器 572 可以包括嵌入在系统设备的硬件中的熔丝密钥 (fuse key)575 或另一永久标识符。这样的永久硬件 ID 可以在系统设备芯片集的制造期间设置并且对于该系统设备是唯一且私密的。在一些实例中，为了辅助保护系统设备的用户的隐私，可以从熔丝密钥值 575 推导出单独的私密的硬件 ID 576。在一些实例中，硬件 ID 576 是存储在管理控制器 505（例如，其基于永久熔丝密钥值）的闪存中并且可以被推导出，使得其是全局唯一的。在又一些示例中，可以针对单个设备生成多个硬件 ID 576。例如，在与域和提供多个不同服务（例如电子邮件、ID 管理、内容提供商、在线零售、社交网络等）的服务提供商的交互中，多个不同的硬件 ID 可以用于生成针对单个设备 - 域配对的多个安全 ID，每个安全 ID 与该设备 - 域配对的特定服务或上下文配对。这可以有助于防止用户或设备数据在域的多个服务之间交叉关联。

[0051] 在一些实例中，由硬件熔丝密钥 575 推导出的硬件 ID 576 可以在生成在建立与域

的安全会话中使用的安全ID时使用。在其他实现中，可以从硬件ID 576推导出另一基于硬件的标识符或根ID 578。例如，根ID 578可以是存储在管理微控制器的闪存（例如574）中的永久标识符。在一些实现中，根ID 578可以被重置并且根据需要由用户替代以生成由相同的硬件ID推导出的新的根ID 578。例如，虽然根ID 578可以避免由用户、操作系统和相对应的应用程序、第三方等等操控或篡改，但是为了保护隐私，用户无论怎样可以被允许选择删除根ID和提示使用管理控制器生成新的不同的根ID的选项。应该理解，在一些实现中，由新的根ID推导出的安全ID将不同于由先前的根ID推导出的安全ID。因此，用户可以通过重置根ID并且从而以由其推导出新的安全ID的新的根ID替代先前的根ID，来手动地将他们的系统设备与由各种域维持的并且与由先前根ID推导出的先前的安全ID值相关联的先前概况解除关联。

[0052] 如在图5B的示例中示出的，证书584也可以被维持在管理微控制器的闪存上。证书584可以是将域管理器授权并且验证为与基于硬件的管理控制器（例如505）通信的受信伙伴的受信证书颁发机构的根证书582的副本。例如，响应于所接收的并且结合管理控制器与域管理器的共同验证与特定的域相关联的域证书（例如580），证书584的副本可以结合域管理器的验证使用，在管理控制器与域管理器之间建立安全连接（例如，使用安全交换协议）等等。例如，管理控制器可以利用证书584来检验从域管理器接收到的域证书（例如580）。示例域证书580可以包括序列号585、域唯一标识符586、证书类型字段、证书的公钥590、证书颁发机构的签名592，以及可以结合相对应的域管理器的识别和验证使用的潜在附加的数据。

[0053] 如在图5B的示例中进一步示出的，在一些实现中，（管理控制器的）管理微控制器可以接收域证书并且处理域证书580以识别该域的域标识符586值。相同的域标识符586可以被包括在从该域接收的每个域证书（或者由该域使用的用于传送该域标识符的其他消息）中。管理微控制器随后可以根据该域标识符和根ID推导出特定于系统设备与域的配对的唯一的安全ID 595。例如，安全ID 595可以例如经过对域标识符和根ID值进行哈希处理而将域标识符与根ID进行组合来推导。在这一特定示例中，不是将各种域种子的集合存储在管理微控制器的安全闪存574中，而是将单个根ID（或者，在一些替代实现中是硬件ID 576）存储在闪存574中，从而在每次系统设备试图建立（以及重新建立）与给定域的安全会话时推导并且重新推导出相同的域特定的安全ID，管理微控制器访问和利用永久的根ID 578和域ID 586输入的相同组合。

[0054] 返回至图5A的示例，如以上指出的，基于硬件的ID 525（例如作为示例的硬件ID 576或根ID 578）可以用于推导出多个安全ID，每个安全ID对应于各自的域。例如，系统设备可以与第二域，域B（例如经由域接口528）交互（例如，在552处）。域B的域管理器530可以请求555安全会话以及系统设备的安全ID，允许用户指定是否期望与域B的这样的会话。如在先前的示例中，例如基于域B的域证书，与第二域管理器530的验证一起，可以协商558安全交换协议和连接。在一些实现中，每个域（例如域A和B）的域证书可以通过共同的证书颁发机构来提供，例如负责识别针对与包括管理控制器的芯片集的特定品牌、型号和/或制造商等的兼容性和值得信任程度满足阈值的伙伴域的证书颁发机构。

[0055] 继续图5A的示例，如在与域A的会话的情况下，管理控制器505可以利用来自域证书的信息（例如唯一的域标识符（例如586））连同硬件ID525一起来推导出与系统设备

和域 B 的配对相对应的安全 ID。该安全 ID 随后可以通过安全通信信道被传送 565 至域管理器 530。域管理器 530 可以将所接收的安全 ID 映射到由域管理器维持的概况并且识别针对该系统设备（或者针对通常利用管理控制器来建立与域的安全会话的系统设备）调整的策略，该策略可以在包括事务处理 570 的会话期间应用 568 于该系统设备。

[0056] 在一些实现中，系统设备，经过管理控制器 505，可以同时参与与多个不同的域（例如，域 A 和 B）的多个安全会话。类似地，在结合图 4A-4C 的示例描述的基于种子的实现中，可以使用管理控制器来管理多个同时发生的会话。在一些实现中，管理控制器可以维持识别会话的会话数据、该会话的安全通信参数（例如，使用的交换协议、使用的密钥和加密方案等等）、该会话中涉及的域（连同验证状态、域标识符等等），以及用于跟踪该域、会话以及要在该会话期间使用的相应安全 ID 的其他数据。

[0057] 应该了解到，在一些实现中，管理控制器可以被配置为根据多个不同的协议和方案推导出安全 ID。例如，在一些实现中，管理控制器可以被配置为既基于接收自域的种子数据来推导出安全 ID（例如，如在图 4A-4C 的示例中）又根据基于硬件的硬件 ID 数据来推导出安全 ID（例如，如在图 5A-5B 的示例中）。例如，用于在基于硬件 ID 的安全 ID 中使用的根 ID（例如 578）以及种子（例如 443）两者可以由安全闪存中的管理微控制器存储并维持（例如 574）。实际上，在一些实现中，根 ID（或其他硬件 ID）可以与种子数据一起使用来推导出一次性密码或者与一些域使用的其他安全 ID。例如，种子数据可以被用作域标识符并且被哈希处理或者以其它方式与硬件 ID 相组合以生成安全 ID。在一些实例中，管理控制器可以例如根据请求的域的身份或者该域对于安全 ID 的请求来识别出要将哪一个安全 ID 格式应用于请求的域。

[0058] 如在图 4B-5B 的上面示例中指出的，可以在系统设备的管理控制器与域的域管理器之间协商和建立安全通信信道。在一些实例中，用于建立安全通信信道的交换协议的协商可以包括识别该域的证书和其他数据的传递，该证书和其他数据由系统设备在验证与系统设备的基于硬件的管理控制器进行交互的域管理器时使用。在一些示例实现中，基于密钥的加密可以用于确保域管理器与管理控制器之间的通信。进而，在一些实现中，安全密钥交换协议可以附加地用于安全地交换在加密信道中使用的密钥。信道可以被安全防护以隐藏安全 ID、种子、验证数据、安全态势数据和传输自管理控制器或者从系统设备的其他组件、处理器、应用程序、操作系统等传送至管理控制器的其他信息。按照这一方式，由管理控制器传输至该域的数据可以被保护免受用户、应用程序或试图故意或者以其它方式危害由管理控制器维护的数据的合法性的其他实体的操控或影响。

[0059] 在一些实现中，可以利用密钥交换协议，该密钥交换协议允许结合在管理控制器与域管理器之间的安全通信信道的建立的共同验证和安全密钥交换。在一些实现中，可以使用既安全（例如，根据中间人、未知密钥共享、身份错误绑定和其他攻击）又维持至少一方（例如在该示例中是管理控制器）的身份的隐私的协议。在一个示例实现中，可以利用 SIGMA 密钥交换协议或经过符号和 mac 机制以及 Diffie-Hellamn 交换元件建立私密共享密钥的其他协议来在管理控制器与域管理器之间建立加密的通信信道。例如，转至图 6 的示例，所示的简化流程图 600 说明了在管理控制器 605 与域管理器 615 之间的示例 SIGMA 交换，允许在系统设备的软件 610 的影响以外的安全 ID 的协商。在图 6 的示例中，系统设备软件 610 提供 625 公开值 S1。在一些实例中，值 S1 可以包括管理控制器 605 的公开基 g^x。

作为响应，域管理器 615 可以发送 630S2，确认对于安全 ID 的请求并且包括 :g^y，B，$SIG_B(g^x, g^y)$，$MAC_{Km}(B)$，其中 g^y 是域管理器的公开基，B 是域管理器的公开密钥，$SIG_B(g^x, g^y)$ 是 g^x 和 g^x 的签名，以及 $MAC_{Km}(B)$ 是 B 的 mac。作为响应，管理控制器 605 可以发送 S3，其包括 A，$SIG_A(g^y, g^x)$，$MAC_{Km}(A)$，以及在一些实例中，使用域管理器的密钥 B 加密的安全 ID。

[0060] 在一些实现中，管理控制器（例如 605）与域管理器（例如 615）之间的通信可以用于推导出与系统设备和相对应的域的配对相对应的安全 ID。如在以上示例中，安全 ID 可以用于提供管理控制器的设备在该域内的基于硬件的验证。例如，在图 6B 的示例中，所示的简化流程图 600b 包括示例设备的示例管理控制器 605 和设备软件 610，连同适于经过管理控制器 605 接受基于硬件的设备验证的域的各自域接口（620、628）和域管理器（615、630）。例如，可以将事务处理请求 632 从设备发送至域，其发起 SIGMA 握手（例如在 635 处）。作为响应，域管理器 640 可以将 S2 值在该握手中传输至管理控制器 605。附加地，域“基础名称”值，或者域标识符可以被包括在或被附加于唯一地识别该域的 S2 的传输 640 中。管理控制器可以接收 S2 值并识别域标识符并且试图至少部分地基于域标识符来检验域的真实性。此外，如在图 5A-5B 的示例中，管理控制器 605 可以使用永久的硬件 ID 并且使用域标识符和硬件 ID 625 推导出 642 用于该设备的安全 ID。所推导的安全 ID 对于该设备与域的配对是唯一的。在一些实例中，密钥推导函数可以用于推导该安全 ID。

[0061] 在推导出安全 ID 之后，管理控制器 605 可以通过传输 S3645 来响应 SIGMA S2 通信 640。在这一示例中，管理控制器 605 可以使安全 ID 包括在通信 645 中。域管理器 620 可以接收通信 645 以完成 SIGMA 协商并且获得由管理控制器 605 推导出的安全 ID。也可以由管理控制器传递其他信息以用于检验设备的身份，例如该设备的品牌、型号、版本等。进而，基于该设备的基于硬件的验证，可以通过域将安全策略应用于 648 设备，并且可以在设备与域之间完成一个或多个事务处理 650。附加地，由域特定的基础名称（例如在 640 处）推导出的会话密钥可以用于将客户端设备与域的配对绑定到事务处理 650，提供另一层安全，允许客户端设备和域检验整个事务处理中其他方的身份。

[0062] 如在图 5A-5B 的示例中，在初始推导并且与域管理器共享硬件 ID 推导的安全 ID 之后，后续的事务处理可以使安全 ID 被重新推导以针对域管理器重新验证该设备。例如，如图 6B 所示，可以将后续事务处理请求 652 从相同设备发送至相同域。可以再次发起 655SIGMA 协商。作为响应，域管理器可以为配对特定的 ID 提供 S2 响应 660。例如，配对特定的响应可以包括来自其原始 S2 响应的相同域标识符（例如 640）。管理控制器可以根据标识符识别该域并且将由 SIGMA 协商产生的会话归属于该域。在其它实例中，配对标识符可以包括推导出的安全 ID（例如，在 645 处接收）。在这样的实例中，将多租户隐私连同每一方对于事务处理 680 都是真实的保证一起提供给客户端设备和域二者。例如，管理控制器可以针对所接收的安全 ID（例如 660 的“PAIRING_ID”）执行密钥推导操作，以推导出原始域标识符（例如，接收于 640 处）。在其他实例中，原始域标识符可以被包括在或者附加于 S2 响应中，其将安全标识符结合为配对标识符基本名称，以辅助管理控制器检验该域是安全 ID 的合法持有者（例如，基于管理控制器 605 根据重新提供的域标识符来重新推导 655 安全 ID）。在任一实例中，管理控制器 605 可以确认域的身份（例如，在该域知道该安全 ID 的基础上）。在一些情况下，管理控制器可以通过将重新推导的安全 ID 经过 SIGMA 协商的完成传递回（在 670 处）到域管理器 615 来重新检验其身份。域管理器 615 可以识别

来自 SIGMA 消息 670 的安全 ID 并且查询数据库或其他结构以查看该安全 ID 是否是已知的安全 ID。在这一示例中，域管理器 615 可以识别出该安全 ID 对应于该设备，重新验证该设备，并且将安全策略重新应用于该设备。进而，域管理器 615 可以应用由该设备在先前事务处理（例如 650）期间收集的信息以细化在后续事务处理（例如 680）中应用于 675 该设备的策略，并且基于映射到该设备的并且由该系统设备的安全 ID 索引的先前收集的信息来调整服务、产品和用户体验产物。附加地，除了应用以上原理的其他示例和实现以外，由配对的标识符基本名称推导出的事务处理 680 的会话密钥可以用于将事务处理 680 绑定于客户端设备与该域的配对。

[0063] 现在转至图 7A 的示例，所示的简化流程图 700a 说明了基于硬件的管理控制器涉及到安全态势数据和描述系统设备的属性的其他数据的安全通信和管理中。例如，如在先前示例中，响应于系统设备试图发起 725 与该域的一个或多个事务处理（例如，在域接口 715 处），域管理器 720 可以试图经过对于该系统设备的安全 ID 的请求 730 来发起与该系统设备的安全会话。安全通信会话可以被建立 735 并且可以结合该域的验证来检验 740 该域的证书。使用类似于图 4A-5B 的示例中的任一个（或其组合）的方案以及其他方案，可以通过管理控制器 705 推导出安全 ID 并且将其传输 745 至域管理器 720。在图 7A 的示例中，一旦建立了与域管理器 720 的安全连接，管理控制器 705 可以就附加地在安全信道上将安全态势数据 750 的至少一部分传递 755 至域管理器 720。在一些实现中，可以将安全态势数据 750 的该部分与安全 ID 一起作为安全容器结构进行传输，允许该域更加直接地识别该安全态势数据并且将其绑定至经过安全 ID 识别的系统设备概况。

[0064] 安全态势数据 750 可以包括描述系统设备的属性的各种数据。在一些实例中，安全态势数据 750 可以描述系统设备的永久属性，例如芯片集的型号和制造商的标识符、系统设备的身份、系统设备、类型等等以及其他信息。在一些示例中，这样的永久属性可以被预先加载到管理控制器的安全存储器上（例如，在制造商处）。其他数据可以描述系统设备的更加动态的属性。例如，管理控制器可以访问和查询系统存储器、系统设备的外围设备、系统设备的其他处理器、系统设备的操作系统以及用于识别和收集系统设备的其他属性的其他系统设备实体。这样收集的属性也可以被添加到并且包括在安全态势数据中。附加地，管理控制器 705 可以附加地监控和识别该系统设备的属性的更新和变化并且捕获安全态势数据中的这些变化。

[0065] 如同维持在管理控制器的安全存储器中的种子、根 ID 以及其他验证数据一样，描述系统设备的各种属性的安全态势数据可以与用户、操作系统、第三方等等的控制或影响隔离，从而提供安全和值得信任的资源库或容器，用于记录在和系统设备与其进行交互的域共享时有用的该系统设备的属性。共享（例如在 755 处）安全态势数据可以允许域管理器更好地识别系统设备的各方面，影响诸如安全策略的哪些策略可应用于该设备并且允许域管理器更好地调整策略到涉及系统设备和域的事务处理的应用 760。这样的事务处理可以不仅包括基于软件的事务处理（例如 765）而且还包括硬件到硬件的事务处理，例如在管理控制器 705 与域管理器 720 之间的事务处理。

[0066] 转至图 7B，示出了根据一个示例实现的示例受信安全容器 770。安全容器可以将该域中的系统设备的安全 ID 与安全态势数据的集合 780 进行打包，以便传输至域管理器，用于例如在安全会话的开始时，或者在域与管理控制器之间提供 API 时，将系统设备引入

到域管理器时使用。在一个示例实现中，安全态势数据 780 的集合可以描述一个或多个系统设备属性，例如系统设备的引导策略、用于系统设备的 OEM 公钥哈希等等。实际上，各种安全态势属性可以被包括在由管理控制器维持的安全态势数据中，并且能够与一个或多个域管理器共享。例如，操作系统类型、版本、批次等等可以被识别并且连同安装在系统设备上的应用程序一起被维持在安全态势数据中。在一些实例中，安全态势数据也可以识别在系统设备上部署的应对措施和安全工具。也可以收集（例如从系统设备上收集这样的数据的其他传感器）用户概况的识别、使用历史和统计数据、行为信息以及描述系统设备的用户的其他信息。附加地，安全概况数据可以描述包括收集自该设备的地理位置信息（例如，从系统设备的全球定位系统组件）、可以被识别的设备的当前操作状态（例如，设备是否开 / 关、电池 / 充电水平等等）、设备的模式（例如，从例如设备的加速度计或其他组件收集的设备如何被使用）的属性。

[0067] 包括在安全态势数据中的一些属性可以是高度设备依赖的。例如，诸如汽车的功能板计算机的系统设备可以包括描述如由该计算机监控的汽车的功能和状态的信息。类似的状态信息可以由包括在智能器具的芯片集中的管理控制器收集。如应该理解的，可以被潜在地收集并维持在安全态势数据中的属性数据的类型可以如日益种类丰富的智能设备、个人计算设备、外围设备以及包括联网和计算机处理能力的其它设备那样变化和多样化。

[0068] 由管理控制器 705 共享的安全态势数据的部分和类型可以在域之间改变。在一些实例中，管理控制器可以识别由域请求的最小量的信息并且仅仅提供这一最小量的信息。除了安全态势数据的初始集合（例如，被封装在受信安全容器 770 中）以外，管理控制器 705 可以利用安全会话以基于该域与系统设备之间的交互的类型，将基于需要或请求的附加安全态势数据传输至该域。例如，涉及系统设备的由域提供的特定服务的消费的事务处理可以请求包括在安全态势数据中的有关该系统设备的特定类型的信息。

[0069] 安全态势数据可以提供与域对于系统设备的安全评估有关的系统设备的属性的最新且值得信任的说明。基于如在安全态势数据中传送的设备的属性，域可以更好地理解系统设备的攻击和安全概况，允许域更加准确和全面地应用安全策略并且采取预防措施来考虑系统设备的安全概况的弱点（或长处）。实际上，虽然在一些实例中，系统设备与域之间的安全会话会导致更宽松的策略应用于系统设备，但是在其他实例中，一旦从系统设备接收到表明关键弱点或其他令人担心的属性的安全态势数据，域就可以实际上基于该安全态势数据来将更加严格的策略应用于与该系统设备的交互。

[0070] 图 8A-8F 是示出示例技术的简化流程图 800a-f，涉及试图与域进行事务处理的计算设备的基于硬件的管理控制器。在图 8A 的示例中，计算设备试图 802 访问特定的域，并且基于与该域的初始通信来接收 804 来自特定域的请求（例如，来自特定域的域管理器）以参与与该域的安全会话。随后可以识别 806 提供在管理控制器的安全存储器上的域种子。在一些实例中，种子的识别 806 可以与来自特定域的种子的接收同时进行，而在其他实例中，可能已经在与特定域的先前事务处理中接收了种子，并且可以在管理控制器的安全存储器中识别先前提供的种子。种子会是安全的，因为其仅仅由管理控制器在系统设备处可访问，使得种子值的值对于系统设备的操作系统、中央处理器和其他更多可访问的组件是隐蔽的。

[0071] 管理控制器可以根据种子推导出 808 一次性密码。所推导的一次性密码可以是能

够由特定域解构以识别私密种子并且从而验证该计算设备是在其上初始提供种子的同一设备的密码。在一些实例中，可以基于种子和对于管理控制器和特定域两者均已知的另一值，例如域的标识符、设备的标识符、系统时钟值、计数器值、日期或代码字等等的组合（例如，哈希处理），来推导出一次性密码。在一些实现中，在每次系统设备试图加入与特定域的安全会话时，能够根据种子生成不同的一次性密码。该一次性密码在系统设备与该域之间建立的安全连接上进行传送并且用于 810 验证该域中的系统设备。在一些情况中，能够通过管理控制器与特定的域来建立安全连接，包括例如经过特定域的域证书与管理控制器的共享而进行的特定域的验证。在一些实现中，可以将诸如 SIGMA 密钥交换协议的密钥交换协议包括在安全通信信道的建立中。

[0072] 转至图 8B，从特定域的角度来看，例如在特定域的域管理器处，可以识别 812 系统设备访问特定域的企图，例如提示将被发送 814 至系统设备的对于参与与该特定域的安全防护的会话的请求。可以例如通过在特定域与系统设备之间建立的安全通信信道来接收 816 一次性密码，该一次性密码由系统设备根据提供在系统设备的安全存储器上的特定域的种子推导出。特定域可以基于一次性密码来验证 818 该系统设备。在一些实例中，验证 818 可以包括特定域解构一次性密码以识别基础域种子。在其他实例中，特定域还根据该种子推导出一次性密码（对于特定域和系统设备两者是已知的）并且将由该系统设备接收的一次性密码与由特定域（例如域管理器）独立推导出的一次性密码进行比较。

[0073] 在已经验证 818 系统设备参与与特定域的安全会话以后，该特定域随后可以继续与该系统设备进行通信并且执行涉及该系统设备的基于硬件的管理控制器的事务处理。附加地，基于系统设备允许与管理控制器进行接口连接，特定域可以例如基于经过安全会话建立的增强的信任水平，将诸如安全或者其他策略的特定策略在会话期间应用于（例如 820）系统设备。在一些实例中，可以在安全会话中（或在系统设备的验证期间）从管理控制器接收安全态势数据或者描述系统设备的属性的其他数据，并且应用于系统设备的策略可以基于所描述的属性或者被调整为考虑所描述的属性。可以认为由管理控制器传送的属性比由系统设备的更易于操控、欺骗等等的其他非基于硬件的组件传输的属性数据更值得信任。

[0074] 转至图 8C 的示例，系统设备可以试图 822 访问特定域并且接收 824 来自该域的对于参与与该域的安全会话的请求。例如，可以结合来自特定域的域证书的接收，接收 825 该特定域的域标识符。在一些实现中，可以结合特定域与系统设备之间的安全通信信道的协商（例如，在密钥交换中），接收域证书。进而，可以在系统设备的管理控制器的安全存储器中识别 826 永久的硬件标识符。硬件标识符可以是仅仅对于管理控制器可访问的私密值并且避免由系统设备的中央处理器、操作系统和其他元件操控。在一些实现中，硬件标识符可以基于永久嵌入在设备的硬件中的标识符并且在设备的制造期间设定，例如熔丝密钥。管理控制器可以根据域标识符和硬件标识符，例如经过域标识符和硬件标识符的哈希处理，推导出 828 安全标识符。安全标识符可以对于系统设备与特定域的配对是唯一的并且可以对于系统设备的其他元件是隐蔽和受保护的。管理控制器随后可以例如在系统设备与特定域之间的安全通信信道上将安全标识符传送 830 至特定域。安全标识符对于管理控制器和特定域可以是私密的，从而确保对于特定域来说，该安全标识符是真实可信的。进而，其他数据也可以连同安全标识符一起传输以辅助特定域识别系统设备并且与该系统设备一起

工作。在其他示例中，这样的数据可以包括安全态势数据和描述系统设备的属性的其他数据。

[0075] 转至图 8D 的示例，从特定域的观点出发（例如特定域的域管理器处），可以识别 842 系统设备访问该域的企图，提出要被发送 844 至系统设备的请求，以要求参与与该特定域的安全会话。例如，响应于系统设备接受参与安全会话的请求，也可以将域标识符传送 846 至系统设备。结合系统设备处特定域（或域管理器）的验证和 / 或系统设备与特定域之间的安全通信信道的建立，可以在发送至系统设备的域证书中传输域标识符。随后可以例如在安全通信信道上从系统设备接收 848 安全标识符，根据维持在系统设备的安全存储器中的域标识符和永久硬件标识符推导出该安全标识符。诸如安全态势数据的其他数据也可以被接收并且与安全标识符（并且从而与系统设备）相关联。基于安全标识符（以及其他数据，例如安全态势数据），特定域可以识别与系统设备相关或者可应用于该系统设备的策略。这样的策略可以应用于 850 涉及系统设备与特定域的事务处理，并且可以包括安全策略、电子商务策略、数据访问策略、规则遵守策略等等。

[0076] 现在转至图 8E 的示例，如上所述，结合管理控制器的系统设备与特定的被验证的域之间的安全会话，管理控制器可以用于提供安全态势数据。这样的安全态势数据可以连同验证数据，例如域种子、硬件标识符、安全标识符等等，一起被维持在管理控制器的安全存储器中，以避免数据被用户、应用程序、恶意软件、第三方以及可能从将不正确或虚假数据提供给特定域中受益的其他实体操控。可以由管理控制器根据存储在安全存储器中的验证数据来推导出 852 安全标识符，该安全标识符与系统设备和各自的域的配对相对应。系统设备可以潜在地推导出用于与多个不同的域的配对的安全标识符。进而，各种技术可以用于生成安全标识符，包括采用上述示例实现的原理的技术。

[0077] 除了安全标识符以外，管理控制器可以识别 854 和访问描述系统设备的属性的安全态势数据。在一些实例中，安全态势数据可以由管理控制器安全地收集并且包括描述在系统设备上部署的启动策略、加密密钥和协议、安全工具和应对措施、在系统设备上安装并且运行的操作系统和应用程序、系统设备的硬件规格和配置、系统设备的当前使用状态、系统设备的地理定位，以及可以被收集的描述系统设备、其软件、硬件、网络、用户等等的操作和状态的各种其他数据。在一些实现中，可以将安全态势数据的一部分与安全标识符一起打包以便被安全传递（例如 856）至特定域。在一些实例中，可以提供安全容器以传递安全标识符和安全态势数据中允许特定域与管理控制器且顺次与系统设备进行接口连接并且利用管理控制器且顺次该系统设备的其他功能的那一部分。因此，可以将安全标识符和安全态势数据安全地传输 856 至特定域，用于由特定域在识别和验证该域上的系统设备时使用，并且用于各种附加的潜在用途。附加的安全态势数据也可以在管理控制器与该域之间的会话期间经过安全连接共享。

[0078] 转至图 8F，从特定域的角度而言，可以利用具有管理控制器的系统设备建立 860 安全通信信道。在一些实例中，特定域与管理控制器协商安全通信信道。在一些示例中，可以利用管理控制器的带外通信信道与特定域进行通信。可以通过该安全信道从系统设备接收 862 硬件推导的安全标识符。附加地，也可以从系统设备接收安全态势数据，该安全态势数据也由基于硬件的管理控制器管理和维持。实际上，在一些实现中，安全标识符和安全态势数据可以经过安全通信信道在安全容器中一起进行发送。特定域可以处理安全标识符以

验证系统设备并且在一些实例中，识别对应于系统设备的相关联的概况。特定域可以进一步处理安全态势数据以识别系统设备的与特定域的一个或多个策略或规则相关的一个或多个属性。系统设备随后可以顺次基于所接收的安全标识符和/或安全态势数据来执行866一个或多个安全相关任务。在许多其他示例中，这样的任务可以包括代理经由管理控制器在系统设备上的安装。例如，设备信息可以被识别，该设备信息允许特定域识别和访问一个或多个驱动器以用于与系统设备进行更好的通信，并且协调系统设备与该域中的一个或多个其他设备之间的通信。

[0079] 虽然已经根据特定实现和基本相关联的方法描述了本公开，但是这些实现和方法的替代和组合排列对于本领域技术人员来说是明显的。例如，在本文描述的动作可以按照与所描述的顺序不同的顺序执行并且仍然实现所期望的结果。作为一个示例，在附图中描绘的过程并不一定要求所示的特定顺序或连续的顺序以实现所期望的结果。所说明的系统和工具可以类似地采取替代的架构、组件和模块来实现类似的结果和功能。例如，在特定实现中，多任务、并行处理和基于云的解决方案会是有益的。

[0080] 在本说明书中描述的主题和操作的实施例可以被实现在数字电子电路或计算机软件、固件或硬件中，包括在本说明书中公开的结构和它们的结构等同物，或者它们中的一个或多个的组合。在本说明书中描述的主题的实施例可以被实现为一个或多个计算机程序，即，在计算机存储介质上编码的，由一个或多个处理器设备执行或控制其操作的计算机程序指令的一个或多个模块。替代地或者附加地，程序指令可以被编码在人工生成的传播信号上，例如，机器生成的电、光或电磁信号上，其被生成用于对信息进行编码以传输至合适的接收器装置，用于由数据处理装置执行。计算机存储介质可以是，或者被包括在计算机可读存储设备、计算机可读存储基板、随机或串行存取存储器阵列或设备，或者它们或其他示例中的一个或多个的组合。计算机存储介质也可以是，或者被包括在一个或多个分离的物理组件或介质（例如，多个CD、磁盘或其他存储设备）中，包括分布式软件环境或云计算环境。

[0081] 包括核心和接入网络的网络，该接入网络包括无线接入网络，可以包括一个或多个网络元件。网络元件可以包括各种类型的路由器、交换机、网关、桥、负载均衡器、防火墙、服务器、内联服务节点、代理、处理器、模块或者可用于在网络环境中交换信息的任何其他合适的设备、组件、元件或对象。网络元件可以包括合适的处理器、存储器元件、硬件和/或软件以支持（或者以其它方式执行）与使用用于屏蔽管理功能的处理器相关联的活动，如在本文中说明的。而且，网络元件可以包括有利于其操作的任何合适的组件、模块、接口或对象。这可以包括允许数据或信息的有效交换的合适算法和通信协议。

[0082] 虽然本说明书包含许多具体的实现细节，但是这些不应该被视为对本发明或所请求保护的范围的限制，相反是作为特定于具体发明的具体实施例的特征的描述。在不同实施例的上下文中在本说明书中描述的特定特征也可以在单个实施例中被组合地实现。相反，在单个实施例的上下文中描述的各种特征也可以在多个实施例中分开或以任何合适的子组合实现。而且，虽然特征在以上被描述为以特定组合工作并且甚至被初始这样地请求保护，但是在一些情况下可以将来自请求保护的组合的一个或多个特征从该组合中去除，并且所请求保护的组合可以指向子组合或子组合的变形。

[0083] 一般而言，本公开的主题包括能够执行诸如使用计算设备的安全防护的微控制器

来推导对于计算设备与特定域的配对是唯一的安全标识符，以及在计算设备的安全防护的存储器中识别与该计算设备的属性相对应的安全态势数据的方法、软件、计算机可执行指令和系统。可以将安全标识符和安全态势在安全防护的容器中发送至特定域的管理设备。

[0084] 在一个示例中，可以提供包括系统处理器设备、对于该系统处理器设备可存取的系统存储器、安全管理控制器存储器、安全管理微控制器以及管理引擎的系统。安全管理控制器存储器可以与系统处理器和系统存储器隔离并且存储永久的验证数据和与计算设备的属性相对应的安全态势数据。在由管理微控制器执行时，管理引擎可以适于根据验证数据推导安全标识符，该安全标识符对于计算设备与特定域的配对是唯一的。管理引擎可以进一步适于将安全标识符和安全态势在安全防护的容器中发送至特定域的管理设备。

[0085] 在一些实例中，可以将安全防护的容器通过安全通信信道发送到特定域。使用诸如 SIGMA 密钥交换协议的密钥交换协议，可以例如在特定域与计算设备之间协商安全信道。可以在计算设备处验证特定域并且可以基于特定域的验证来提供由安全微控制器执行的针对管理控制器的安全应用编程接口 (API)。附加地，可以从特定域接收证书并且可以至少部分地基于所接收的证书来验证该特定域。

[0086] 在一些实例中，安全微控制器可以用于推导对于计算设备与第二域的配对是唯一的第二安全标识符，并且可以将第二安全标识符和安全态势数据的至少一部分发送至第二域。安全防护的微控制器可以独立于计算设备的操作系统，并且由安全防护的微控制器推导出的安全标识符的值对于操作系统而言可以是隐蔽的。因而，可以使用安全微控制器来收集安全态势数据的至少一部分。

[0087] 进而，在一些实例中，可以基于存储在安全防护的微控制器的安全存储器中的计算设备的安全的永久的硬件标识符来推导安全标识符，并且推导安全标识符可以包括对硬件标识符与特定域的域标识符进行哈希处理。硬件标识符对于安全防护的微控制器可以是私密的。在其他实例中，可以基于经过安全通信信道由特定域提供在安全防护的存储器上的种子来推导安全标识符，其中该种子对于特定域内的计算设备是唯一的。在这样的示例中，推导安全标识符可以包括将安全防护的存储器中的种子识别为与特定域相对应，并且根据该种子生成一次性密码，其中该特定域根据一次性密码来推导种子以针对计算设备进行验证。进而，安全态势数据可以包括计算设备的启动策略和其他属性。在潜在的许多其他示例中，这样的属性可以包括计算设备的硬件配置、计算设备的使用状态、安装在计算设备上的软件、计算设备的操作系统。

[0088] 在另一一般方面，本公开的主题包括能够执行诸如在特定域与特定计算设备之间建立安全连接以及从特定计算设备接收对于特定域的安全标识符的方法、软件、计算机可执行指令和系统，该安全标识符由特定计算设备的安全防护的微控制器根据存储在特定计算设备的安全存储器中的验证数据来推导。进而，可以接收制约于特定安全标识符的特定计算设备的安全态势数据，该安全态势识别特定计算设备的属性。可以执行与特定计算设备和特定域的交互有关的安全任务。

[0089] 在一些实例中，安全任务可以包括例如将安全策略应用于特定计算设备，基于安全态势数据识别与特定计算设备相对应的驱动器，经过安全微控制器将代理加载到特定计算设备上等等的动作。可以提供域标识符以用于验证特定计算设备处的特定域。附加地，除了其他示例和前述的组合以外，在一些实例中，可以连同第二安全态势数据一起接收用

于第二计算设备的第二安全标识符，并且可以执行与第二计算设备和特定域的交互有关的安全任务。

[0090] 因而，已经描述了主题的具体实施例。其他实施例在所附权利要求的范围内。在一些情况下，在权利要求中引述的动作可以按照不同的顺序执行并且仍然实现期望的结果。此外，在附图中描绘的过程并不一定要求所示的具体顺序或连续顺序以实现期望的结果。

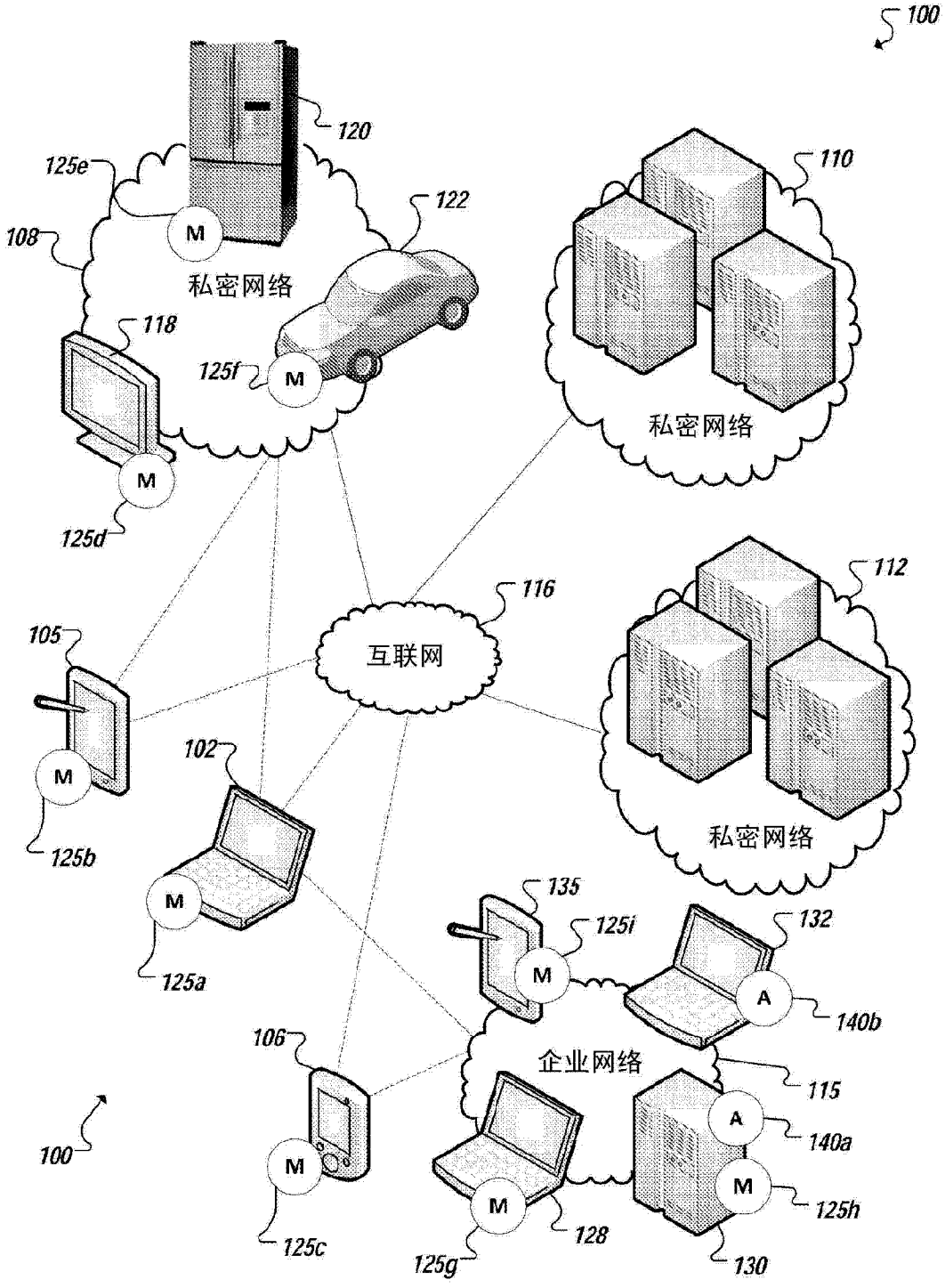

100
120
125e
122
108
M
私密网络
110
118
125f
M
M
私密网络
125d
112
116
105
互联网
M
102
私密网络
125b
M
135
125i
132
125a
M
A
140b
106
企业网络
115
100
A
140a
M
M
125h
M
128
125c
125g
130

图 1

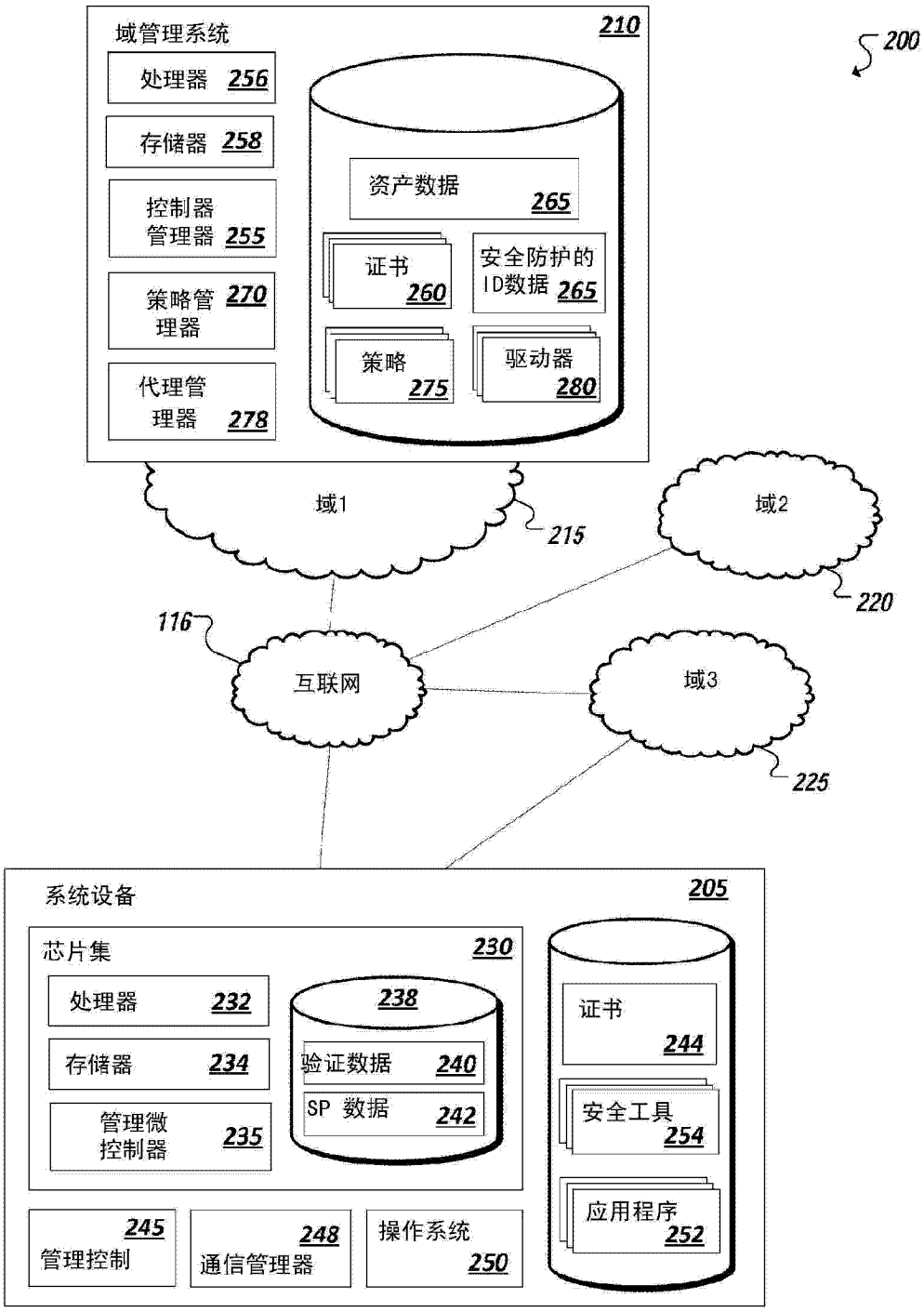

域管理系统
210
200
处理器 256
存储器 258
控制器管理器 255
策略管理器 270
代理管理器 278
资产数据 265
证书 260
安全防护的ID数据 265
策略 275
驱动器 280
域1
215
域2
220
116
互联网
域3
225
系统设备
205
芯片集
230
处理器 232
存储器 234
管理微控制器 235
238
验证数据 240
SP 数据 242
证书 244
安全工具 254
应用程序 252
245
管理控制
248
通信管理器
操作系统 250

图 2

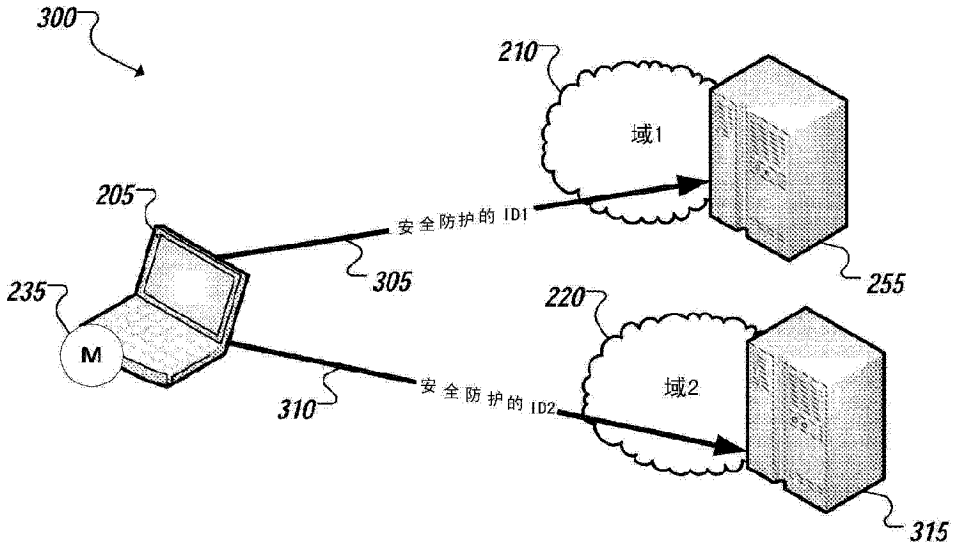

300
210
域1
205
安全防护的 ID1
305
255
235
M
220
域2
310
安全防护的 ID2
315

图 3

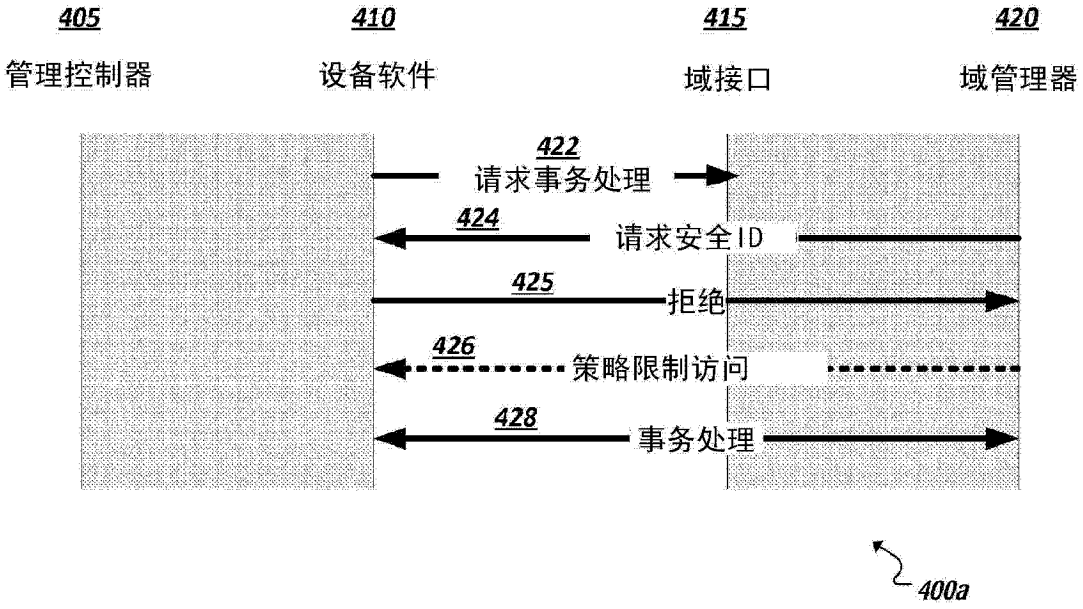

405
管理控制器
410
设备软件
415
域接口
420
域管理器
422
请求事务处理
424
请求安全 ID
425
拒绝
426
策略限制访问
428
事务处理
400a

图 4A

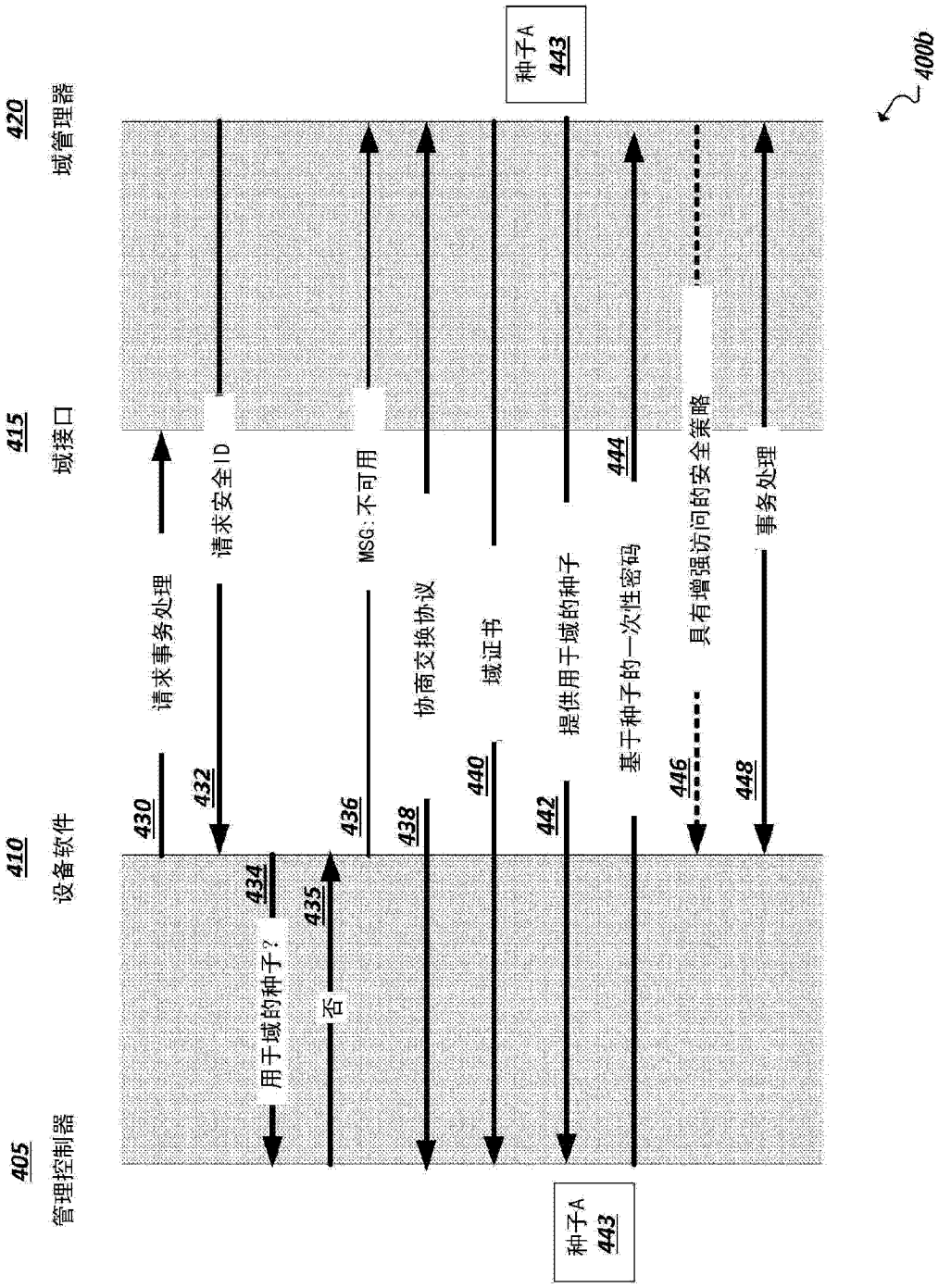

400b
405 管理控制器
410 设备软件
415 域接口
420 域管理器
种子A 443
430 请求事务处理
432 请求安全ID
434 用于域的种子?
435 否
436 MSG:不可用
438 协商交换协议
440 域证书
442 提供用于域的种子
444 基于种子的一次性密码
446 具有增强访问的安全策略
448 事务处理
种子A 443

图 4B

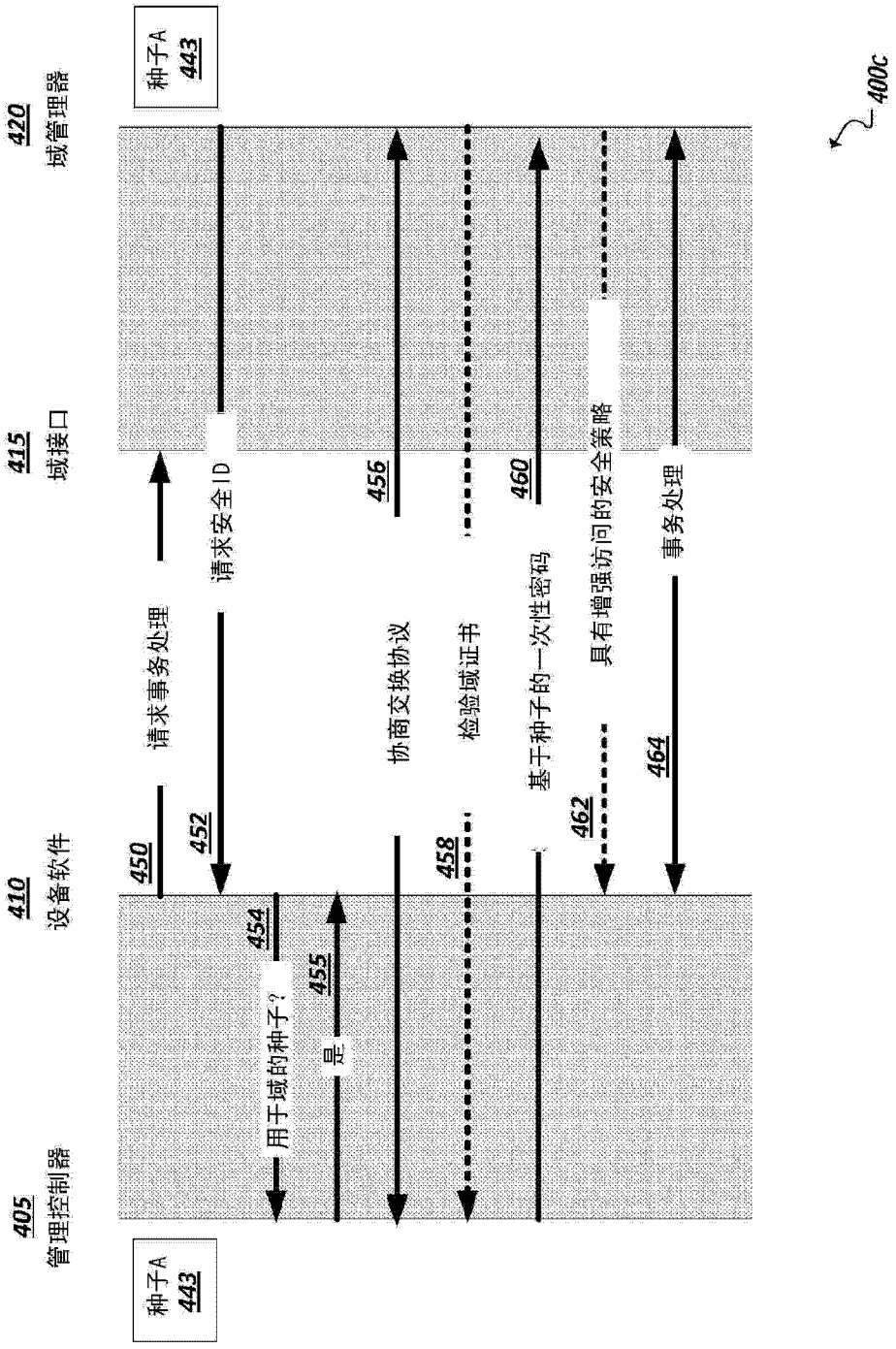

400c
420
域管理器
415
域接口
410
设备软件
405
管理控制器
种子A
443
种子A
443
请求事务处理
请求安全ID
协商交换协议
检验域证书
基于种子的一次性密码
具有增强访问的安全策略
事务处理
用于域的种子?
是
450
452
454
455
456
458
460
462
464

图 4C

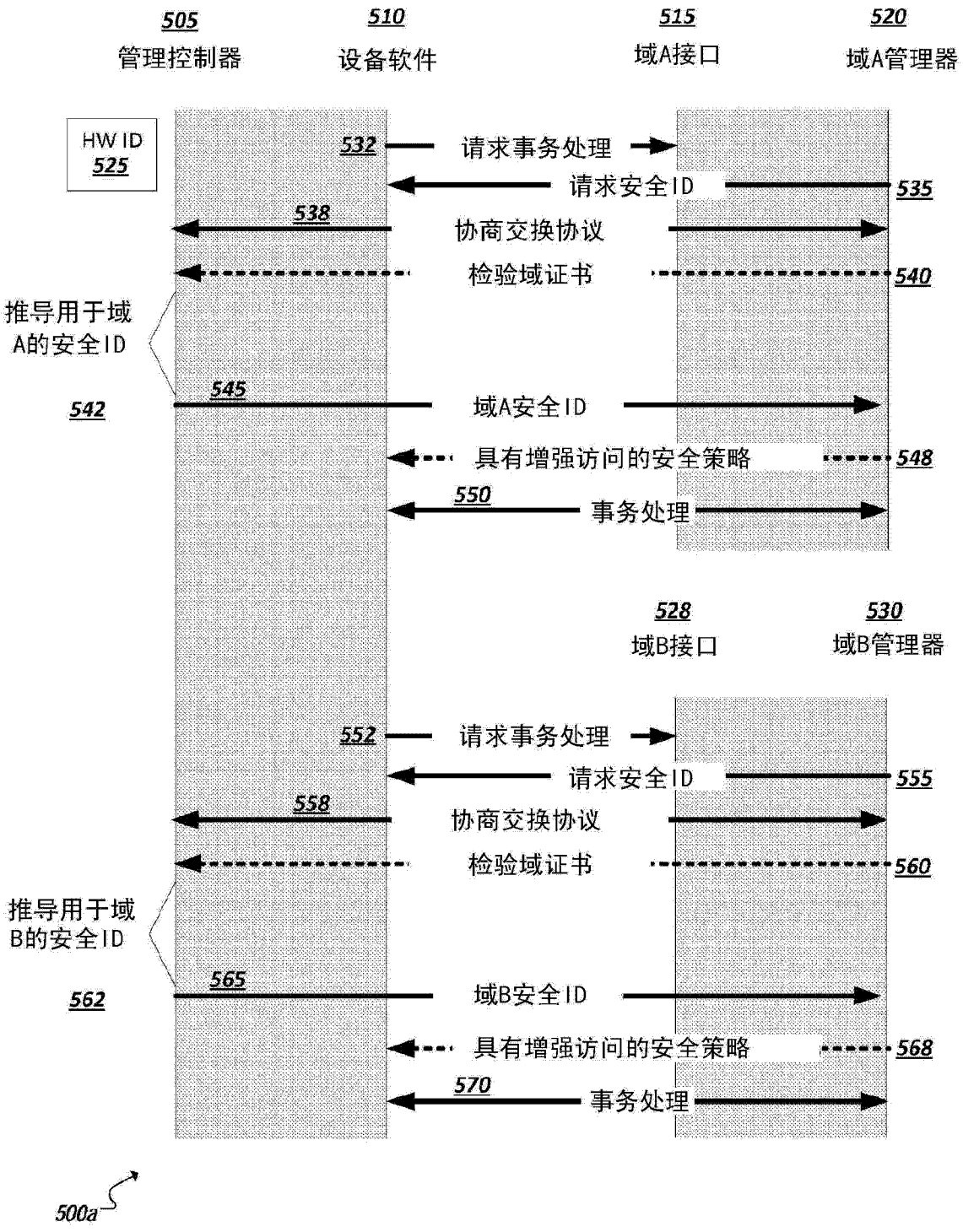

505
管理控制器
510
设备软件
515
域A接口
520
域A管理器
HW ID
525
532
请求事务处理
请求安全ID
535
538
协商交换协议
检验域证书
540
推导用于域
A的安全ID
542
545
域A安全ID
具有增强访问的安全策略
548
550
事务处理
528
域B接口
530
域B管理器
552
请求事务处理
请求安全ID
555
558
协商交换协议
检验域证书
560
推导用于域
B的安全ID
562
565
域B安全ID
具有增强访问的安全策略
568
570
事务处理
500a

图 5A

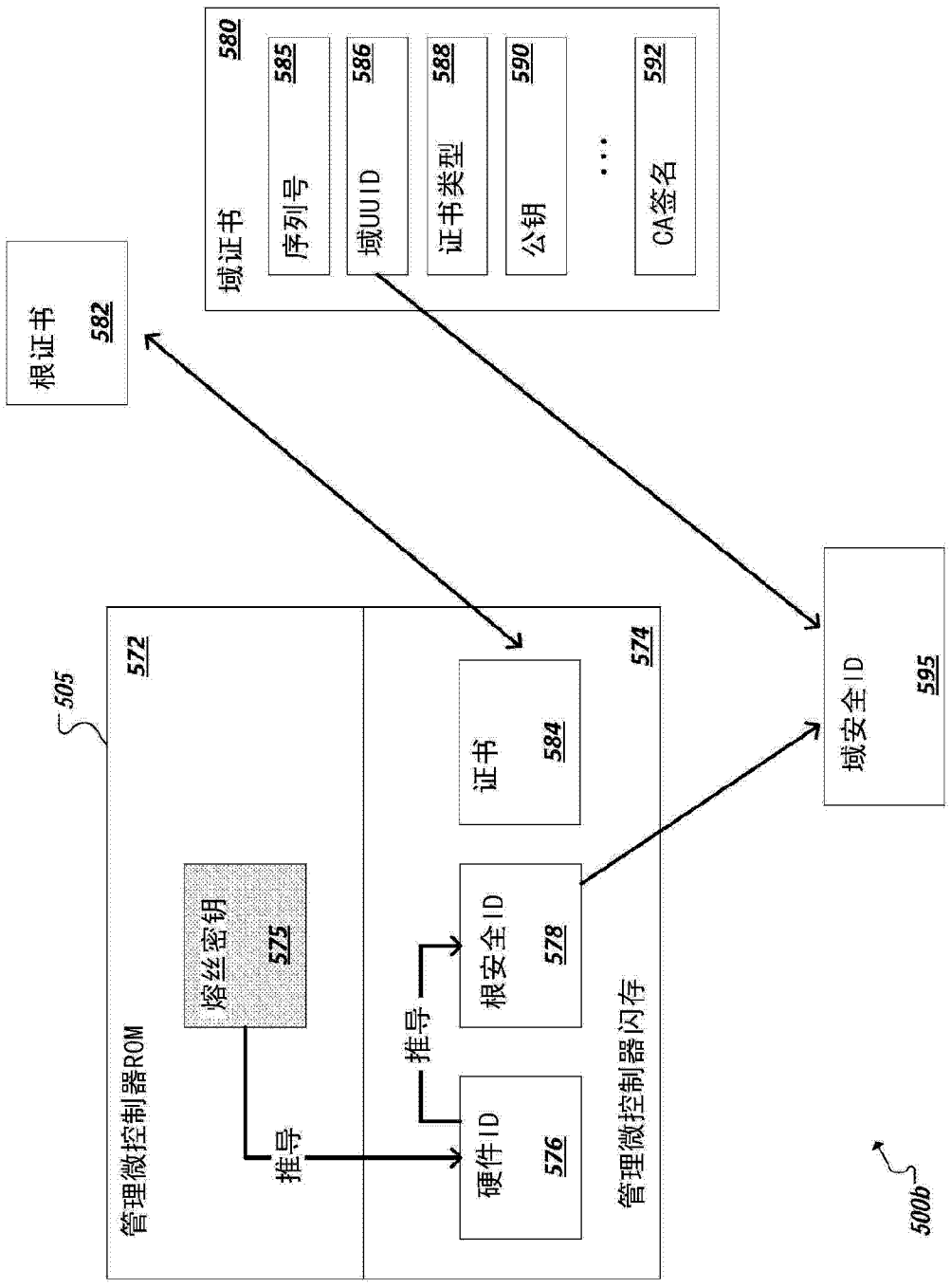

根证书
582
域证书
580
序列号
585
域UUID
586
证书类型
588
公钥
590
...
CA签名
592
505
572
管理微控制器ROM
熔丝密钥
575
推导
574
管理微控制器闪存
证书
584
推导
根安全ID
578
硬件ID
576
域安全ID
595
500b

图 5B

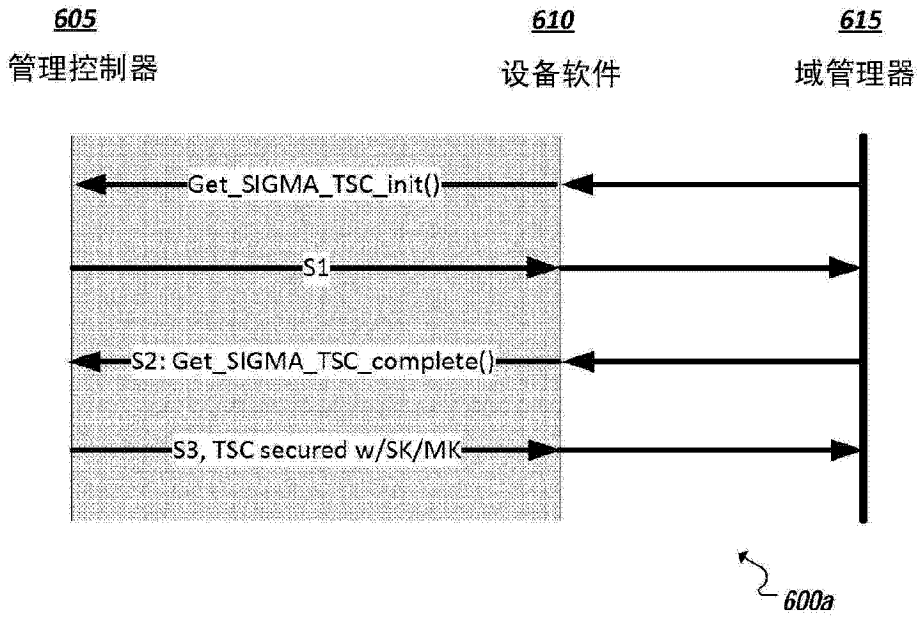

605
管理控制器
610
设备软件
615
域管理器
Get_SIGMA_TSC_init()
S1
S2: Get_SIGMA_TSC_complete()
S3, TSC secured w/SK/MK
600a

图 6A

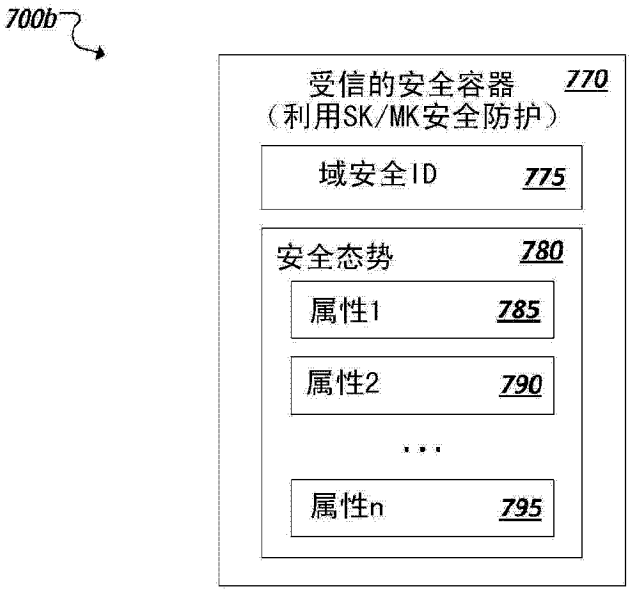

700b
受信的安全容器
（利用SK/MK安全防护）
770
域安全ID
775
安全态势
780
属性1
785
属性2
790
...
属性n
795

图 7B

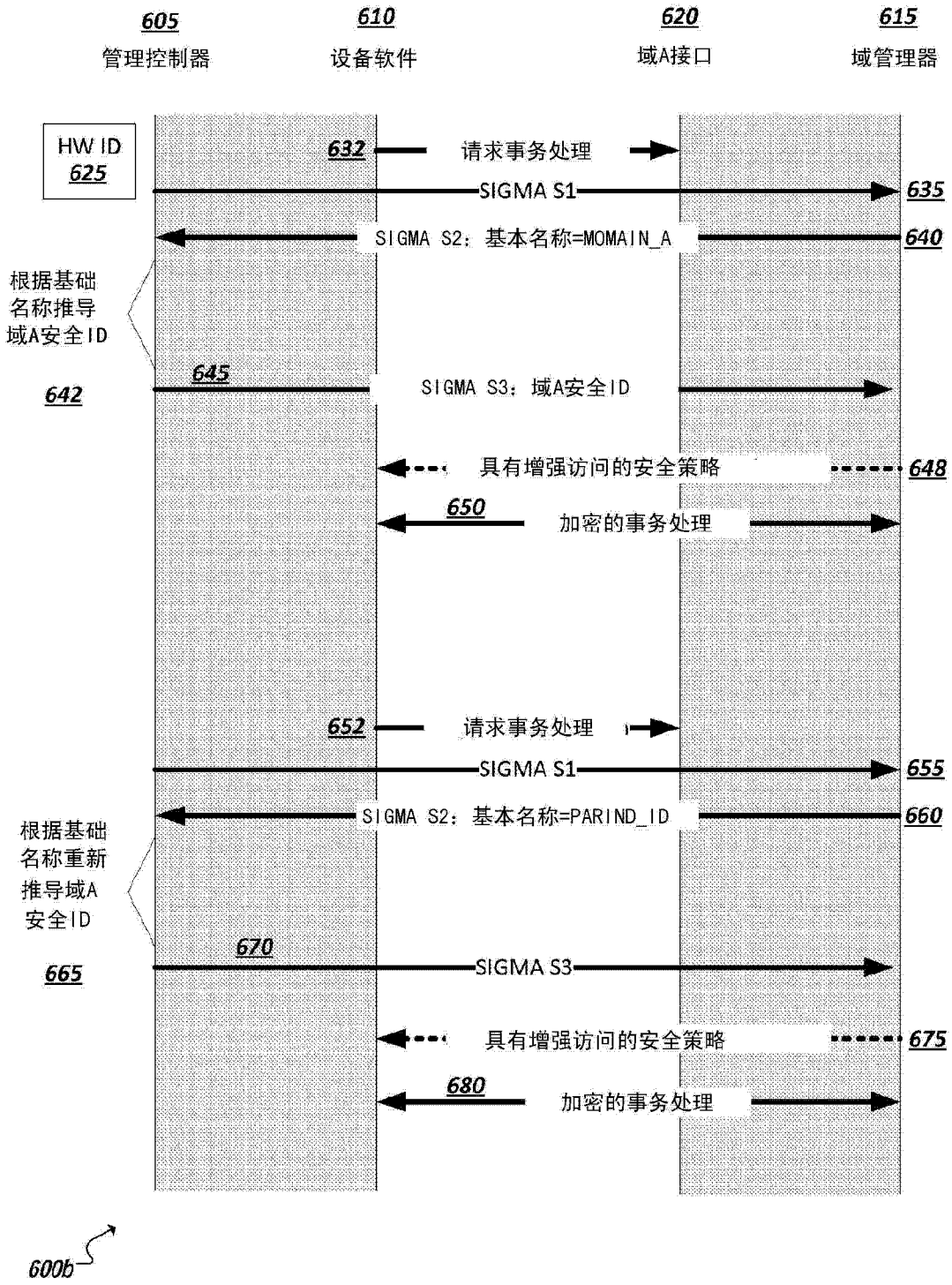

605
管理控制器
610
设备软件
620
域A接口
615
域管理器
HW ID
625
632
请求事务处理
SIGMA S1
635
SIGMA S2：基本名称=MOMAIN_A
640
根据基础
名称推导
域A安全ID
642
645
SIGMA S3：域A安全ID
具有增强访问的安全策略
648
650
加密的事务处理
652
请求事务处理
SIGMA S1
655
SIGMA S2：基本名称=PARIND_ID
660
根据基础
名称重新
推导域A
安全ID
665
670
SIGMA S3
具有增强访问的安全策略
675
680
加密的事务处理
600b

图 6B

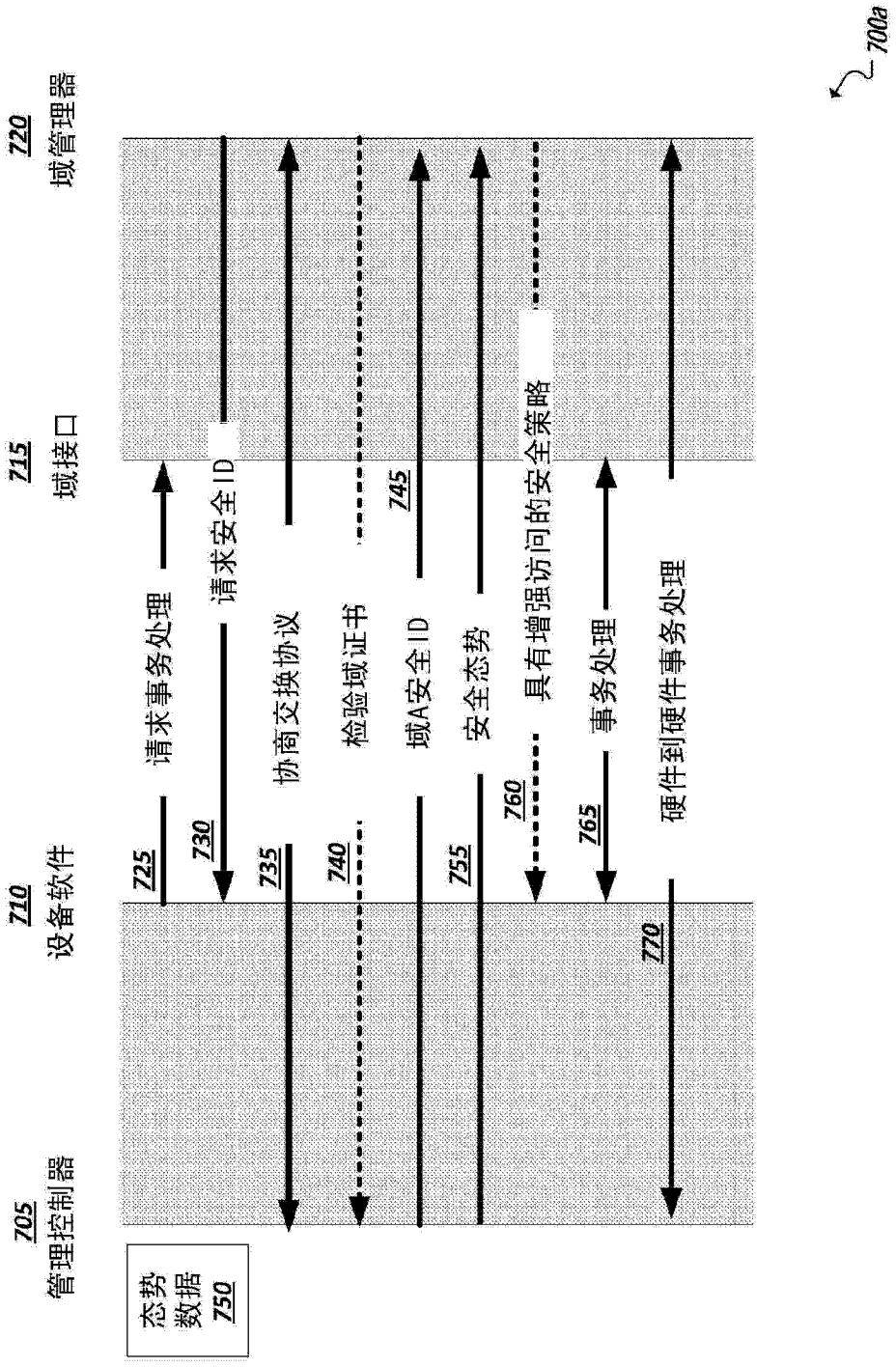

700a
Z20
域管理器
Z15
域接口
Z10
设备软件
Z05
管理控制器
态势数据 Z50
Z25
请求事务处理
Z30
请求安全ID
Z35
协商交换协议
Z40
检验域证书
Z45
域A安全ID
Z55
安全态势
Z60
具有增强访问的安全策略
Z65
事务处理
Z70
硬件到硬件事务处理

图 7A

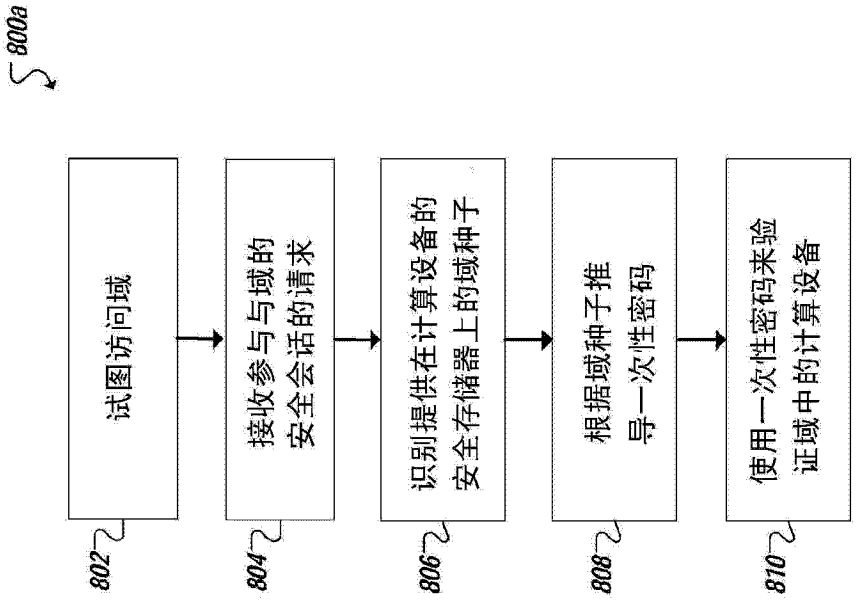

800a
试图访问域
802
接收参与与域的安全会话的请求
804
识别提供在计算设备的安全存储器上的域种子
806
根据域种子推导一次性密码
808
使用一次性密码来验证域中的计算设备
810

图 8A

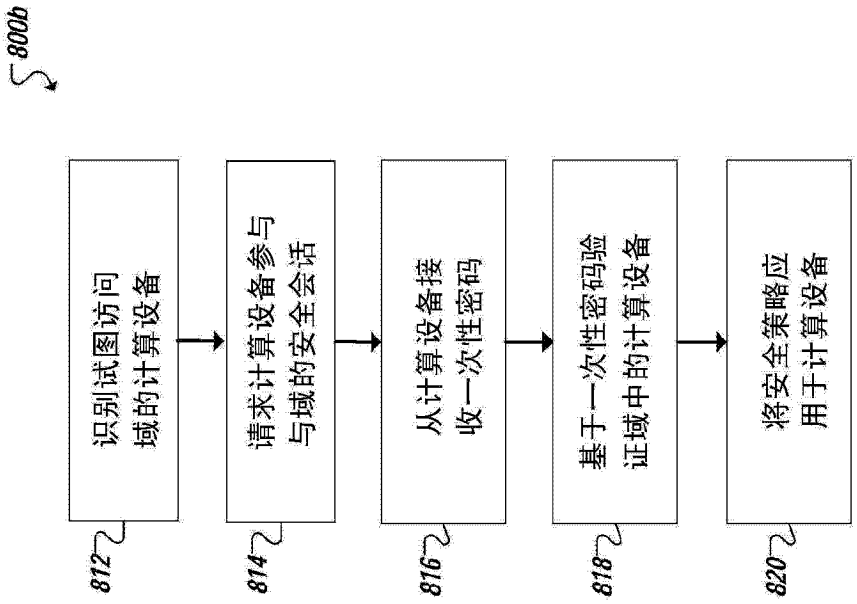

800b
识别试图访问域的计算设备
812
请求计算设备参与与域的安全会话
814
从计算设备接收一次性密码
816
基于一次性密码验证域中的计算设备
818
将安全策略应用于计算设备
820

图 8B

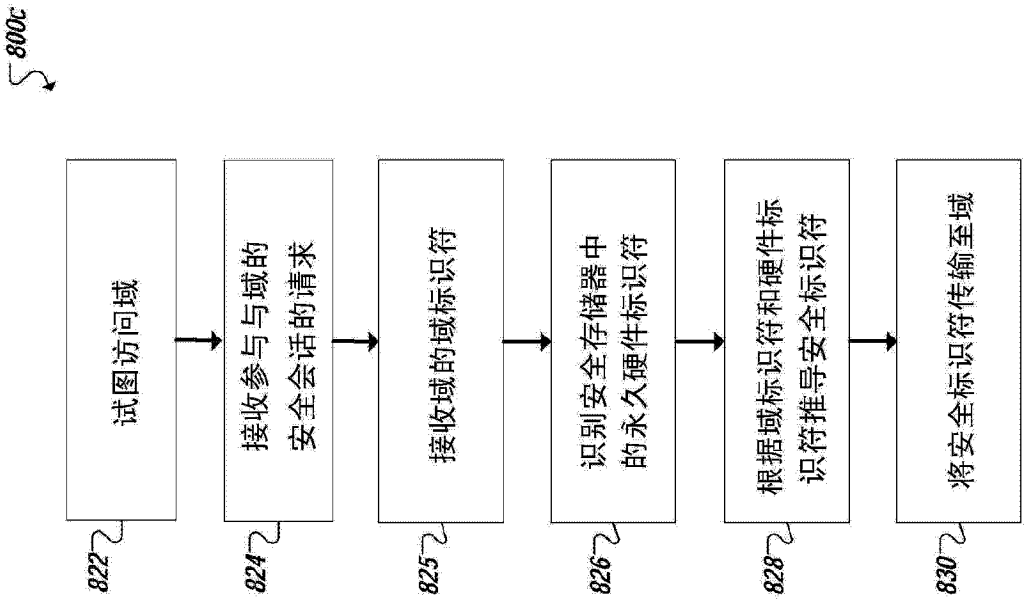

800c
试图访问域
822
接收参与与域的安全会话的请求
824
接收域的域标识符
825
识别安全存储器中的永久硬件标识符
826
根据域标识符和硬件标识符推导安全标识符
828
将安全标识符传输至域
830

图 8C

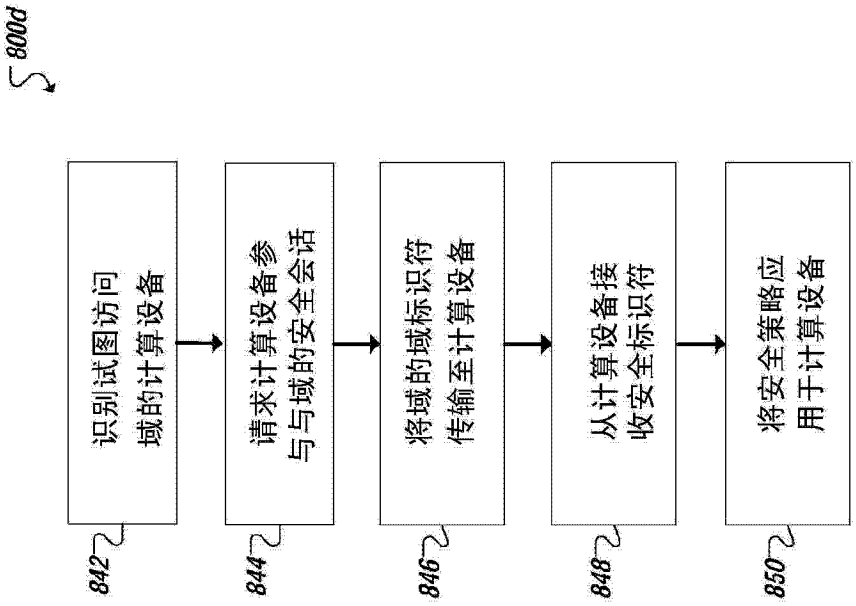

800d
识别试图访问域的计算设备
842
请求计算设备参与与域的安全会话
844
将域的域标识符传输至计算设备
846
从计算设备接收安全标识符
848
将安全策略应用于计算设备
850

图 8D

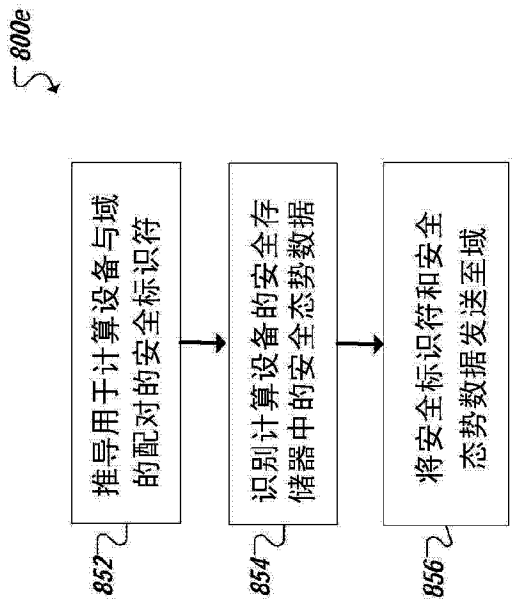

800e
推导用于计算设备与域的配对的安全标识符
识别计算设备的安全存储器中的安全态势数据
将安全标识符和安全态势数据发送至域
852
854
856

图 8E

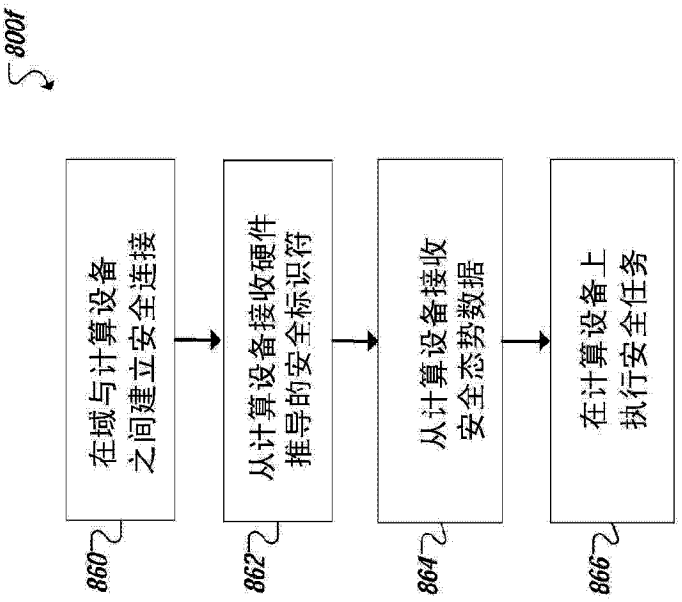

800f
在域与计算设备之间建立安全连接
从计算设备接收硬件推导的安全标识符
从计算设备接收安全态势数据
在计算设备上执行安全任务
860
862
864
866

图 8F