(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102460458 B
(45)授权公告日 2015.10.21

(21)申请号 201080027283.9
(22)申请日 2010.06.16
(30)优先权数据
12/486738 2009.06.17 US
(85)PCT国际申请进入国家阶段日
2011.12.19
(86)PCT国际申请的申请数据
PCT/US2010/038776 2010.06.16
(87)PCT国际申请的公布数据
WO2010/148059 EN 2010.12.23
(73)专利权人 微软技术许可有限责任公司
地址 美国华盛顿州
(72)发明人 V. 萨多夫斯基 S.P. 奥拉里格
C. 寥内蒂 J.R. 哈米尔顿
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 刘红 刘鹏
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
(56)对比文件
US 2006/0123463 A1,2006.06.08,
US 2002/0133713 A1,2002.09.19,
CN 1592206 A,2005.03.09,
US 2006/0123463 A1,2006.06.08,
审查员 张琳

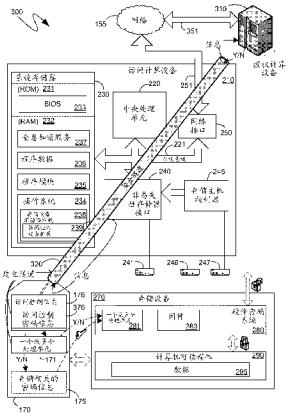
权利要求书3页 说明书17页 附图7页

(54)发明名称

存储设备的远程访问控制

(57)摘要

访问控制设备能够通信地耦合到存储设备并且能够控制对其的访问。访问控制设备能够包括诸如授权实体的身份之类的信息,以允许访问控制设备独立地确定是否提供对相关联存储设备的访问。可选择地,访问控制设备可以包括用于建立至授权计算设备的安全连接的信息,并且访问控制设备可以实施授权计算设备的决定。访问控制设备可以通过指示存储设备执行特定的固件指令来阻止有意义响应数据存储相关的请求来控制访问。访问控制设备也可以包括由存储设备利用来加密和解密数据的存储相关的密码信息。在这样的情况下,访问控制设备能够通过不向存储设备释放存储相关的密码信息来控制访问。



CN 102460458 B

1. 一种访问存储在存储设备（270）上的数据（295）的方法，其中所述存储设备包括至包括访问控制信息（176）的访问控制设备（170）的通信连接，所述方法包括以下步骤：

从所述存储设备（270）接收所述访问控制设备（270）通信地连接到所述存储设备（270）的指示；

通过所述存储设备（270），与所述访问控制设备（170）建立通信连接；

提供识别信息给所述访问控制设备（270）；

从所述访问控制设备接收将被提供给在所述访问控制设备外部的验证计算设备的第一信息；

与所述验证计算设备建立通信连接；

提供第一信息给所述验证计算设备；

从所述验证计算设备接收将被提供给所述访问控制设备的第二信息；以及

提供第二信息给所述访问控制设备；以及

在所述访问控制设备（270）至少部分地因为所提供的识别信息而允许所述存储设备（270）这样做之后，接收对于数据存储相关的请求的有意义响应。

2. 权利要求 1 的方法，其中所述存储设备包括硬件密码系统，并且所述访问控制设备包括存储相关的密码信息；以及其中进一步，接收对于数据存储相关的请求的有意义响应发生在所述访问控制设备给所述存储设备的硬件密码系统提供对于存储相关的密码信息的访问之后。

3. 权利要求 1 的方法，进一步包括从所述访问控制设备接收验证质询的步骤，其中提供识别信息给所述访问控制设备包括给所述访问控制设备提供对于所述验证质询的验证响应。

4. 权利要求 1 的方法，进一步包括以下步骤：

建立至网络的通信连接，以及作为建立至网络的通信连接的一部分，接收授权计算设备的网络地址；其中与所述验证计算设备建立通信连接包括：利用接收到的所述授权计算设备的网络地址，与所述验证计算设备建立网络通信连接。

5. 权利要求 1 的方法，进一步包括以下步骤：实施虚拟处理以充当所述验证计算设备；其中与所述验证计算设备建立通信连接包括与虚拟处理建立通信连接。

6. 一种被配置为访问存储在存储设备上的数据的装置，其中所述存储设备包括至包括访问控制信息（176）的访问控制设备的通信连接，所述装置包括：

第一接收单元，其适于从所述存储设备（270）接收所述访问控制设备（270）通信地连接到所述存储设备（270）的指示；

连接单元，其适于通过所述存储设备（270），与所述访问控制设备（170）建立通信连接；

提供单元，其适于提供识别信息给所述访问控制设备（270）；

第二接收单元，其适于从所述访问控制设备接收将被提供给在所述访问控制设备外部的验证计算设备的第一信息；

建立单元，其适于与所述验证计算设备建立通信连接；

第一提供单元，其适于提供第一信息给所述验证计算设备；

第三接收单元，其适于从所述验证计算设备接收将被提供给所述访问控制设备的第二

信息；以及

第二提供单元，其适于提供第二信息给所述访问控制设备；以及

第四接收单元，其适于，在所述访问控制设备（270）至少部分地因为所提供的识别信息而允许所述存储设备（270）这样做之后，接收对于数据存储相关的请求的有意义响应。

7. 一种访问控制设备（170），其物理地和通信地与存储设备（270）可分离，所述访问控制设备包括：

至少一个通信接口；

至少一个处理单元（171）；以及

由至少一个处理单元（171）可利用来选择性地允许所述存储设备（270）有意义响应数据存储相关的请求的访问控制信息（176）；

其中存储相关的密码信息中的特定密码信息由硬件密码系统可利用来仅解密所述存储设备的加密数据中的部分，所述部分对应于个别用户；其中所述访问控制信息包括个别用户的标识；并且其中进一步，如果所述至少一个处理单元从利用所述访问控制信息所指定的个别用户中的至少一些个别用户接收到验证，所述至少一个处理单元引起所述存储相关的密码信息中的至少一些特定密码信息的供应。

8. 权利要求 7 的访问控制设备，进一步包括由所述存储设备的硬件密码系统可利用来解密由所述存储设备存储的加密数据的存储相关的密码信息；其中所述访问控制信息进一步由至少一个处理单元可利用来选择性地提供存储相关的密码信息给所述存储设备。

9. 权利要求 8 的访问控制设备，进一步包括由所述至少一个处理单元可执行来擦除所述存储相关的密码信息的指令。

10. 权利要求 7 的访问控制设备，其中所述访问控制信息包括一个或多个实体的一个或多个身份，其中对于所述一个或多个实体，所述处理单元将允许所述存储设备有意义响应来自所述一个或多个实体的数据存储相关的请求。

11. 权利要求 7 的访问控制设备，其中所述至少一个处理单元执行包括以下的步骤：

从实体接收身份信息和验证信息；

将接收到的身份信息与访问控制信息相比较；

如果接收到的身份信息被列在所述访问控制信息中，将接收到的验证信息与列在所述访问控制信息中的相应验证信息相比较；以及

如果接收到的验证信息与列在所述访问控制信息中的相应验证信息相匹配，则指示所述存储设备通过执行利用所述数据存储相关的请求所请求的动作来有意义响应所述数据存储相关的请求。

12. 权利要求 7 的访问控制设备，其中所述访问控制信息包括用于与所述访问控制设备外部的授权计算设备建立安全通信隧道的访问控制密码信息。

13. 权利要求 12 的访问控制设备，其中所述至少一个处理单元执行包括以下的步骤：

利用所述访问控制密码信息来与所述授权计算设备建立安全通信隧道；

通过所述安全通信隧道，给所述授权计算设备提供有关与所述加密数据的尝试访问相关联的实体的信息；

通过所述安全通信隧道，从所述授权计算设备接收有关允许所述存储设备有意义响应所述数据存储相关的请求的指示；和

根据从所述授权计算设备接收到的指示，选择性地允许所述存储设备有意义响应所述数据存储相关的请求。

存储设备的远程访问控制

背景技术

[0001] 日益地，计算设备正被用于操作于意图保密的数据和信息以及存储意图保密的数据和信息。这样的数据和信息能够包括政府秘密，但是更有可能包括商业和个人信息，如果这样的信息被恶意方或对手获得的话，那么该信息可能损害到一个或多个个人。这样，已与计算设备的硬件相关联且与计算设备的软件相关联实施了各种安全机制。这样的硬件安全机制的示例包括被设计为基于诸如指纹之类的生物信息来生成安全口令的外设以及对于计算设备的物理访问屏障，诸如键盘锁、通信端口锁等等。与计算设备的软件相关联的安全机制的示例包括各种加密技术以及各种访问控制技术。

[0002] 然而，在完全不是与计算设备直接相关联的活动期间，在一个或多个计算机可读媒体上存储的数据的保护时常失败。例如，当诸如硬盘驱动器之类的包括计算机可读媒体的存储设备的物理装运没有被恰当保护并因此被丢失乃至被盗时，存储在一个或多个计算机可读媒体上的数据可能并且已经受到影响(compromised)。类似地，当包括计算机可读媒体的存储设备无法从主机访问并因此被丢弃了时，存储在一个或多个计算机可读媒体上的数据可能并且已经受到影响。通常，这样的“失败”的存储设备保留以计算设备能够检索和访问的形式存储在其计算机可读媒体上的显著高百分比的数据。

[0003] 为了增强在计算机可读媒体上存储的数据的保护，尤其是在包括这样的媒体的存储设备对于恶意方或对手而言而变成物理上可访问的情况下，研制“全卷(full volume)”加密方法，从而存储在存储设备的计算机可读存储媒体上的实质上所有的数据以加密的形式进行存储，以致于即使恶意方或对手获得了这样的存储设备的物理控制，他们也不大可能在缺乏合适的解密密钥的情况下解密该数据。为了提供更高的性能，在存储设备上存储的数据的加密能够由作为存储设备本身一部分的专用密码硬件来执行，而不给存储和检索这样的数据的计算设备的一个或多个中央处理单元增加负担。

[0004] 除了全卷加密方法之外，其上存储敏感数据的计算机可读存储媒体或整个存储设备以适当方式的物理销毁同样能够增强这样的数据的保护和安全。例如，可能已存储了待保护的数据的计算机可读存储媒体能够物理上被切碎或被暴露于随机的强磁场，使得该数据不是物理上一致的，也不是从计算机可读媒体中物理上可恢复的。可选择地，不是物理上销毁存储设备，而是能够由计算设备根据预定义安全擦除策略多次重写存储在计算机可读存储介质上的敏感数据。不幸地，计算机可读存储媒体和存储设备的物理销毁可能既是昂贵的又是费时的，并且在寻求效率以减少时间和费用时，能够采用可能折衷在这样的媒体上存储的数据的保护和销毁的捷径，从而破坏物理销毁效应。添加进一步低效、诸如政府安全规定之类的各种规定或隐私规定可能施加额外负担，诸如以特定方式进行和记录(document)计算机可读存储媒体的适当销毁的要求。

[0005] 在诸如服务器环境或企业信息技术(IT)环境之类的众多使用情景中，存储设备时常在主机之间移动。在这样的环境中，访问控制执行的形式可能是有用的。不幸地，给存储设备供应(provision)访问控制的形式可能是复杂的，并且可能导致大量额外的硬件组件、开发和后续故障排解成本。

发明内容

[0006] 存储设备能够与在这里被称为“访问控制设备”的物理实体相关联，其中所述实体能够与存储设备的其余部分物理上且通信地相分离。此外，计算设备能够包括计算机可执行指令，这些指令能独立于存储设备而与访问控制设备通信。

[0007] 在一个实施例中，能够为访问控制设备供应密码信息，其中所述信息能够被存储设备的硬件密码系统利用来或直接或间接加密和解密存储在存储设备的计算机可读媒体上的数据。能够进一步供应访问控制设备，使得它仅仅选择性地将其密码信息提供给存储设备的硬件密码系统，并由此允许存储设备提供对存储在其上的数据的选择性访问。结果，甚至在访问控制设备通信地耦合至相关联的存储设备时，访问控制设备也能够通过在满足预定义条件时才将其密码信息释放给存储设备的硬件密码系统来限制对于存储在存储设备上的加密数据的访问。

[0008] 在另一个实施例中，能够为访问控制设备供应诸如计算设备或用户之类的实体的列表，其中能够允许这些实体访问存储在与访问控制设备相关联的存储设备上的数据。访问控制设备随后能够指示与之相关联的存储设备不有意义响应来自不在列出实体之中的实体的数据存储相关的通信。可选择地，或另外，如果访问控制设备被供应密码信息，那么它能够将其密码信息提供给存储设备的硬件密码系统，并因而仅在寻求访问存储数据的实体在列出的实体之中时才允许存储设备提供对其存储数据的访问。寻求访问存储数据的实体能够通过用户口令、计算设备标识符或其他的能够以诸如在质询 / 响应(challenge/response)验证机制的上下文内的安全上下文来提供的类似信息来识别其自身。

[0009] 在进一步实施例中，访问控制设备能够被供应密码信息，其中密码信息使之能与授权计算设备建立安全通信隧道。寻求访问存储在与访问控制设备相关联的存储设备上的数据的计算设备能够被用于使得访问控制设备能够通过安全隧道与授权计算设备通信。访问控制设备随后能够给授权计算设备提供相关信息，并且仅在授权计算设备指示这样的动作是恰当的时候才能够允许或指示它与之相关联的存储设备提供数据给请求设备。

[0010] 在更进一步实施例中，访问控制设备能够被供应可执行指令，这些可执行指令能够允许访问控制设备更新其自身或被定制成提供客户特定的访问控制逻辑和算法。这样的可执行指令或“脚本小程序(scriptlet)”集合能够在供应期间被提供给访问控制设备，并且能够随后以安全且可靠的方式从外部计算设备进行更新。访问控制设备能够被供应，以致它参考空间和时间之一或这二者而非相关联的存储设备或计算设备来单独地初始化其自身。

[0011] 在还进一步实施例中，访问控制设备能够被供应可执行指令，这些可执行指令能够允许访问控制设备擦除存储在相关联的存储设备上的数据或擦除存储在访问控制设备上的任何密码信息，并从而导致在相关联的存储设备上使用这样的密码信息加密的数据是不可读取且不可访问的。访问控制设备能够基于它自己的确定或基于诸如从授权计算设备远程接收的指令来激活这样的可执行指令。

[0012] 提供这个发明内容部分来以简化的形式介绍下面在详细描述部分中进一步描述的概念的选择。这个发明内容部分并不打算标识所请求保护的主题的访问控制特征或基本特征，也不打算用于限制所请求保护的主题的范围。

[0013] 附加的特征和优点从以下参考附图进行的详细描述中将是明显的。

附图说明

[0014] 以下详细描述当与附图进行结合时可以被最佳地理解，其中：

[0015] 图 1 是示例的供应计算设备和示例的访问控制设备的框图；

[0016] 图 2 是示例的访问计算设备、示例的访问控制设备和示例的存储设备的框图；

[0017] 图 3 是示例的访问计算设备、示例的访问控制设备和示例的存储设备的另一框图；

[0018] 图 4 是在访问控制设备与存储设备之间的示例通信的框图；

[0019] 图 5 是在访问控制设备与存储设备之间的附加的示例通信的框图；

[0020] 图 6 是示例的供应计算设备的示例操作的流程图；和

[0021] 图 7 是示例的访问计算设备的示例操作的流程图。

具体实施方式

[0022] 以下描述涉及存储系统，其包括存储设备以及物理和通信可分离的访问控制设备，其中访问控制设备包含能够由访问控制设备利用来控制何时使得存储设备上存储的数据可用于寻求访问它的实体的访问控制信息。访问控制设备例如通过指示存储设备不有意义响应来自未授权实体的数据存储相关的通信而能够阻止存储设备与这样的非授权实体通信，其中数据存储相关的通信包括请求已经存储在存储设备上的数据的通信以及请求所提供的数据存储在存储设备上的通信。访问控制设备也能够包括密码信息，其选择性供应给存储设备的硬件密码系统能够控制对存储在存储设备上的加密数据的访问。诸如通过使得访问控制设备比较试图访问的实体的身份与预先提供的批准实体的列表，能够由访问控制设备本身提供授权，或者授权也能够由授权计算设备提供，其中授权计算设备能够通信地耦合到访问控制设备并通过访问计算设备提供授权指令给访问控制设备。

[0023] 这里描述的技术集中于但不限于存储设备以及物理和通信可分离的访问控制设备。实际上，下面描述的访问控制机制能够同样地利用单个存储设备内不是注定是可分离的分立组件来实施，尽管在这样的情况下，在访问控制设备与存储设备在物理上被分离时存在的安全优势可能不存在。但是，这样的安全优势是独立于利用下述的访问控制机制所提供的安全性的，并因此没有将下述机制的适用性限于特定的硬件配置。因此，虽然下面的描述参考与物理上可分离的访问控制设备相关联的存储设备，但是这些描述本身的范围并打算被如此限制。

[0024] 另外，虽然不作要求，但是下面的描述将采用诸如程序模块之类的由一个或多个处理单元执行的计算机可执行指令的一般上下文。更具体地，除非另有说明，否则这些描述将参考由一个或多个处理单元执行的动作以及操作的符号表示。这样，将明白：有时被称为计算机执行的这样的动作和操作包括由处理单元对以结构形式表示数据的电信号进行的操纵。这种操纵转换数据或将其保持在存储器中的某些位置上，其以本领域技术人员熟知的方式来重新配置或以其他方式改变处理单元或与之相连的外设的操作。其中保持数据的数据结构是具有利用数据的格式所定义的特定属性的物理位置。

[0025] 一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对

象、组件、数据结构等等。此外，本领域技术人员将意识到：所参考的处理单元不一定限于常规的个人计算处理单元，而包括其他的处理器配置，这包括时常在外设、手持设备、多处理器系统、基于微处理器或可编程的消费电子设备中找到的专用处理器、特定用途处理器、通信处理器、总线处理器、控制器等等。类似地，在以下描述中参考的计算设备不一定限于独立的计算设备，因为这些机制也可以在其中任务由通过通信网络链接的远程处理设备来执行的分布式计算环境中进行实践。在分布式计算环境中，程序模块可以位于本地和远程记忆存储设备二者中。

[0026] 转到图1，示出包括示例的供应计算设备110和示例的访问控制设备170的示例系统100。如将描述的，供应计算设备110能够被用于例如通过给访问控制设备提供能够允许访问控制设备限制对相关联存储设备的访问的信息来供应访问控制设备170。

[0027] 首先转到供应计算设备110，它能够包括但不限于一个或多个中央处理单元(CPU)120、系统总线130以及将包括系统存储器130在内的各种系统组件耦合到处理单元120的系统总线121。系统总线121可以是若干类型的总线结构中的任何一种，其包括使用各种总线或点对点架构中的任何一种的存储器总线或存储器控制器、外设总线以及本地总线。取决于具体的物理实现方式，CPU 120和系统存储器130中的一个或多个能够在物理上共同定位，例如，共同位于单个芯片上。在这样的情况下，一些或所有的系统总线121能够仅仅是单个芯片结构内的硅通道，并且其在图1中的示意可以只是用于说明目的的标记便利。

[0028] 供应计算设备110通常也包括计算机可读媒体，其能够包括任何的能被诸如供应计算设备110之类的计算设备访问的可用媒体，并且包括易失性和非易失性媒体以及可移动和不可移动媒体二者。通过示例而非限制，计算机可读媒体可以包括计算机存储媒体和通信媒体。计算机存储媒体包括采用任何方法或技术实现的用于存储诸如计算机可读指令、数据结构、程序模块或其他数据之类的信息的媒体。计算机存储媒体包括但不限于RAM、ROM、EEPROM、闪存或其他存储技术、CD-ROM、数字多用途碟片(DVD)或其他光盘存储设备、磁带盒、磁带、磁盘存储设备或其他磁存储设备、固态盘(SSD)或其他基于固态的存储设备或任何其他的能够用于存储所需信息并能被诸如供应计算设备110之类的计算设备访问的介质。通信媒体通常在诸如载波之类的调制数据信号或其他的传输机制中包括计算机可读指令、数据结构、程序模块或其他数据，并且包括任何的信息递送媒体。通过示例而非限制，通信媒体包括诸如有线网络或直接线路连接之类的有线媒体以及诸如声学、RF、红外和其他无线媒体之类的无线媒体。上面的任何一个的组合也应被包括在计算机可读媒体的范围之内。

[0029] 系统存储器130包括采用易失性和/或非易失性存储器形式的计算机存储媒体，诸如只读存储器(ROM)131和随机存取存储器(RAM)132。在ROM 431中通常存储基本输入/输出系统133(BIOS)，其包含诸如在启动期间有助于在计算设备100内的各元件之间传送信息的基本例程。RAM 132通常包含由处理单元120立即可访问的和/或由处理单元120目前正对其操作的数据和/或程序模块。通过示例而非限制，图1示出操作系统134、其他程序模块135以及程序数据136。还示出全卷加密服务137，其在一些实施例中可以是操作系统134的一部分。全卷加密服务137能够允许诸如供应计算设备110之类的计算设备提供存储在一个或多个计算机可读存储媒体或其某些部分上的大部分或所有的信息的加密，

其中所述某些部分例如是被计算设备的操作系统 134 或其他存储控制器定义为个别卷的部分。

[0030] 除了可选地包括全卷加密服务 137 之外，供应计算设备 110 的操作系统 134 还可以包括存储设备驱动器堆栈 138。存储设备驱动器堆栈 138 可以包括涉及建立和保持与一个或多个存储设备的通信的计算机可读指令，诸如如下所述的。此外，存储设备驱动器堆栈 138 可以包括访问控制设备扩展 139，其能够包括涉及与诸如访问控制设备 170 之类的访问控制设备建立和保持通信的计算机可执行指令。如果存储设备驱动器堆栈接收到诸如访问控制设备 170 之类的访问控制设备通信地耦合到供应计算设备 110 的指示，那么访问控制设备扩展 139 能够由存储设备驱动器堆栈 138 来请求并由存储设备驱动器堆栈 138 来加载。如下面进一步将描述的，或直接地诸如通过有线或无线通信连接、或通过访问控制设备通信地耦合至的诸如存储设备之类的另一中间设备，诸如访问控制设备 170 之类的访问控制设备能够通信地耦合到诸如供应计算设备 110 之类的计算设备。

[0031] 除了上述的之外，供应计算设备 110 还可以包括存储设备，这包括可移动 / 不可移动、易失性 / 非易失性计算机存储设备。仅通过示例，图 1 示出读取或写入不可移动的非易失性磁媒体的硬盘存储设备 141、146 和 147。其他的能够与示例计算设备一起使用的可移动 / 不可移动、易失性 / 非易失性计算机存储媒体包括但不限于磁带盒、闪存卡、固态驱动器（SSD）和其他基于固态的存储设备、数字多用途碟片、数字录像带、固态 RAM、固态 ROM 等等。硬盘存储设备 141、146 和 147 或这些其他的可移动 / 不可移动、易失性 / 非易失性计算机存储媒体中的任何一个通常通过诸如接口 140 之类的存储器接口或直接地或间接地连接到系统总线 121。在图 1 的示意的示例供应计算设备 110 中，硬盘存储设备 141 被显示为诸如通过供应计算设备 110 内部的物理连接或经由端口暴露的外部连接而直接地被连接到非易失性存储器接口 140，而硬盘存储设备 146 和 147 被显示为被连接到例如诸如廉价设备冗余阵列（Redundant Array of Inexpensive Devices）（RAID）控制器之类的存储主机控制器 145，其中所述控制器随后又能够再次诸如通过物理上在计算设备 100 内部的连接而被连接到接口 140。非易失性存储器接口 140 可以是任何的非易失性存储器接口，这包括但不限于通用串行总线（Universal Serial Bus）（USB）接口、符合 IEEE1394 规范中的任何一个或多个的接口、串行 AT 附件（Serial AT Attachment）（SATA）接口或其他类似的接口。

[0032] 供应计算设备 110 可以操作在使用至一个或多个远程计算设备的逻辑连接的联网环境中。为了说明简单起见，在图 1 中将供应计算设备 110 显示为连接到不限于任何特定的网络或联网协议的网络 155。图 1 所示的逻辑连接是通用网络连接 151，其可以是局域网（LAN）、广域网（WAN）或其他网络。供应计算设备 110 通过网络接口或适配器 150 而连接到通用网络连接 151，其中网络接口或适配器 150 又连接到系统总线 121。在联网环境中，相对于供应计算设备 110 或其部分或外设描述的程序模块可以存储在通过通用网络连接 151 而通信地耦合到供应计算设备 110 的一个或多个其他计算设备的存储器中。例如，诸如在下面更详细描述的授权计算设备能够充当其动作在下面进行描述的一些或所有的计算机可执行指令的主机。将意识到：所显示的网络连接是示例性的，并且可以使用在计算设备之间建立通信链接的其他手段。

[0033] 与以下描述相关的是：供应计算设备 110 能够通信地耦合到访问控制设备，诸如

图 1 所示的访问控制设备 170。访问控制设备 170 能够直接地、通信地被耦合到供应计算设备 110，这包括通过有线或无线连接进行耦合，或者访问控制设备能够通过访问控制设备直接地与之通信地耦合的存储设备而被间接地、通信地耦合至供应计算设备。在图 1 的系统 100 中，访问控制设备 170 被显示为诸如通过非易失性存储器接口 140 而直接地、通信地耦合到供应计算设备 110。图 1 的虚线指示：访问控制设备 170 能够可移动地、通信地耦合至供应计算设备 110。在一个实施例中，为了制造效率，访问控制设备 170 能够符合标准的存储卡规范，并因此，例如，能够采用与任何其他这样的符合相同规范的存储卡相同的方式、诸如通过通信地连接至供应计算设备的内部存储卡读取器或外部存储卡读取器外设而通信地耦合到供应计算设备 110。

[0034] 访问控制设备 170 能够包括一个或多个处理单元 171，其能够包括能够基于输入集合来调节其输出的控制器或其他组件。如在下面将进一步描述的，访问控制设备 170 的处理单元 171 能够用于执行涉及确定是否允许和启用相关联的存储设备来向存储设备通信地连接至的访问计算设备提供数据或存储该访问计算设备中的数据的动作。

[0035] 在执行与这样的守门(gate-keeping)有关的动作中，访问控制设备 170 的处理单元 171 能够利用能够由供应计算设备 110 提供的访问控制信息 176，如在系统 100 中所示的。在一个实施例中，访问控制信息 176 可以包括能够被允许来访问利用访问控制设备 170 的密码信息加密的数据的实体的列表，并因此，当访问控制设备确定这样的实体正在请求访问时，访问控制设备能够启用相关联的存储设备来允许请求实体访问。例如，访问控制信息 176 能够包括诸如媒体访问控制(MAC)地址、全球名称(WWN)或其他唯一设备或实体标识符之类的标识符的列表。访问控制信息 176 也可以包括实体的口令，以致这些实体能够被要求在访问控制设备释放密码信息之前通过提供其口令来向访问控制设备 170 证明其身份。其他的包括基于类似的质询 / 响应模板的密码机制同样能够被利用来向访问控制设备 170 提供寻求访问利用访问控制设备 170 通信地耦合至的存储设备所存储的数据的那些实体的验证。

[0036] 在一个实施例中，访问控制设备 170 能够进一步包括存储相关的密码信息 175，其中存储设备能够使用该密码信息来加密将要存储在这样的存储设备的存储媒体上的数据和解密已经存储在存储媒体上的加密数据。这样，访问控制设备 170 能够利用存储相关的密码信息 175 通过不提供密码信息给存储设备来控制对存储设备的数据的访问，直至访问控制设备已确定请求访问存储设备及其数据的实体是由访问控制信息 176 指示为被允许访问的实体之一。其中访问控制信息 176 包括可接受实体的列表或对其而言访问将被拒绝的实体的列表的实施例在其中能够访问数据的实体受到限制并且是相对静态的家庭或小型商务环境内是特别有用的。

[0037] 然而，在替换实施例中，在确定是否允许对访问控制设备通信地耦合至的存储设备的访问时，访问控制设备能够参考访问控制设备 170 外部的计算设备，诸如授权计算设备。在这样的实施例中，访问控制设备 170 能够依赖授权计算设备来指示它何时它应该或者不应该允许访问。如本领域技术人员将认识到的，这样的实施例在其中能够被允许来访问某些数据的实体可能经常变化的企业环境内可能是有用的。此外，如下面进一步将描述的，其中访问控制设备 170 参考另一计算设备的实施例能够与通常由企业实施的现有访问控制技术相结合。

[0038] 在上述的实施例中，由供应计算设备 110 提供给访问控制设备 170 的访问控制信息 176 能够包括关于与授权计算设备建立安全通信的信息。例如，访问控制信息 176 能够包括诸如授权计算设备的公共访问控制的密码信息，或者包括其他的访问控制设备 170 能够从中协商共享秘密的这样的信息或其他的用来提供与授权计算设备的安全通信的这样的密码工具。访问控制信息 176 也可以包括授权计算设备的标识，诸如授权计算设备的域名服务器（DNS）名称或其网络地址。在下面进一步描述的替换实施例中，这样的识别信息反而能够被提供给寻求访问在访问控制设备 170 通信地耦合至的存储设备上的数据的计算设备。

[0039] 如在系统 100 中所示的，在一个实施例中，供应计算设备 110 的操作系统 134 能够利用存储设备驱动器堆栈 138 来与访问控制设备 170 通信。更特别地，如所示的，当存储设备驱动器堆栈检测到访问控制设备 170 的存在时，存储设备驱动器堆栈 138 能够调用或以其他方式加载访问控制设备扩展 139。访问控制设备扩展 139 随后能够处理与访问控制设备 170 的通信，这包括访问控制信息 176 的供应。在一个实施例中，如所显示的，可能是程序模块 135 的一部分的诸如安全相关程序之类的一个或多个程序能够提供访问控制信息 176 给访问控制设备扩展 139 并从访问控制设备扩展 139 提供访问控制信息 176 给访问控制设备 170，其中如上所示的，访问控制信息 176 可以包括对其将授予访问的实体的列表，或者也如上所示的，访问控制信息 176 可以包括用于建立和保持至访问控制设备 170 外部的授权计算设备的安全通信连接的包括密码信息在内的信息。

[0040] 诸如通过访问控制设备扩展 139，供应计算设备 110 能够为访问控制设备 170 供应访问控制信息 176 并且也可选地为访问控制设备供应存储相关的密码信息 175。存储相关的密码信息 175 以及相关联的通信在系统 100 中利用虚线来显示，以指示它们是可选的。如果访问控制设备 170 从存储设备中通信地断开，存储相关的密码信息 175 的缺少可能导致存储在这样的存储设备的存储媒体上的加密数据是不可访问的。因此，如果存储设备物理上被丢失或被盗，访问控制设备 170 从这样的存储设备中的通信断开能够提供附加保护层，并且这也能够充当存储在这样的存储设备的存储媒体上的加密数据的密码擦除或销毁的证据。

[0041] 在一个实施例中，存储相关的密码信息 175 能够包括“物理访问控制”，其可以是能够被用作以本领域技术人员熟知的方对加密和解密操作进行的访问控制的一系列比特。因此，如在下面的描述中利用的术语“物理访问控制”旨在指示被用作密码访问控制的数据的集合，其中所述数据从诸如访问控制设备 170 之类的物理可移动源中进行提供并被存储在该源上。这样的物理访问控制用于与“逻辑访问控制”形成对比，其中“逻辑访问控制”不是物理上与其上存储利用这样的访问控制加密的数据的媒体可分离的。

[0042] 由供应计算设备 110 可选地供应给访问控制设备 170 的存储相关的密码信息 175 能够由供应计算设备的多个子系统中的任何一个通过访问控制设备扩展 139 来提供。例如，除了使用逻辑访问控制之外，全卷加密服务 137 还能够运用其现有功能来生成物理访问控制，并将其作为存储相关的密码信息 175 的至少一部分提供给访问控制设备 170。可选择地，物理访问控制或其他的存储相关的密码信息 175 能够利用诸如可能存在于存储主机控制器 145 或其他的存储接口上的硬件之类的专用硬件来生成。作为还一个替换方案，存储相关的密码信息 175 能够从 BIOS 133 被提供给访问控制设备 170。

[0043] 为了保持提供给访问控制设备 170 的可选的存储相关的密码信息 175 的安全性和保密性，这样的信息能够由供应计算设备 110 以最小化诸如通过在供应计算设备 110 上运行的恶意计算机可执行指令而被对手获得这样的信息的可能性的方式来提供。因此，在一个实施例中，提供给访问控制设备 170 的存储相关的密码信息 175 能够在供应计算设备 110 的启动完成之前被提供，并且所提供的信息也能够在供应计算设备的启动完成之前从供应计算设备中删除。由于恶意的计算机可执行指令通常不能在主机计算设备的启动完成之前通过在供应计算设备 110 的启动完成之前向访问控制设备 170 提供以及随后丢弃存储相关的密码信息 175 来操作，所以能够保护所提供的信息免受随后有可能在供应计算设备上运行的任何恶意计算机可执行指令的损害。

[0044] 例如，BIOS 133 能够检测通信地连接到供应计算设备 110 的接口的访问控制设备 170 的存在，并且能够在启动供应计算设备上的任何其他的处理、例如包括启动操作系统 134 的运行之前提供存储相关的密码信息 175 给访问控制设备 170。类似地，在首次初始化控制器并且如果不是操作系统 134 的启动开始之前也至少是在操作系统 134 的启动完成之前，存储主机控制器 145 能够检测访问控制设备 170 的存在。然后，控制器 145 同样能够将存储相关的密码信息 175 提供给访问控制设备 170，并且能够在任何恶意的计算机可执行指令能够运行在供应计算设备 110 上之前丢弃它。作为另一个替换方案，由于全卷加密服务 137 可能已包括被设计成保护其逻辑访问控制免受在供应计算设备 110 上运行的恶意计算机可执行指令损害的机制，所以全卷加密服务 137 能够使用这些机制来安全地为访问控制设备 170 供应存储相关的密码信息 175，并且随后丢弃它，以便进一步减小它将在供应计算设备 110 上被发现的可能性。在这样的实施例中，上面参考访问控制设备扩展 139 所述的至少一些功能能够在操作系统 134 的外部、诸如由 BIOS 133 或存储主机控制器 145 来实现。

[0045] 一旦已由供应计算设备 110 供应了访问控制设备 170，那么访问控制设备 170 能够从供应计算设备 110 通信地且可选地、物理地断开，并且随后能够与存储设备一起被利用来允许存储设备存储加密数据和访问已存储在这样的存储设备的计算机可读媒体上的加密数据。

[0046] 转到图 2，显示包括访问计算设备 210、访问控制设备 170 以及访问控制设备能够通信地耦合至的示例存储设备 270 的系统 200。如下面进一步描述的，访问控制设备 170 与示例存储设备 270 之间的通信耦合可以是但不一定是物理耦合。示例存储设备 270 能够代表被显示为通信地耦合至访问计算设备 210 的存储设备 241、246 或 247 中的任何一个或多个。访问计算设备 210 可以是与上面具体描述的供应计算设备 110 不同的计算设备，或者它可以是相同的计算设备，例如，诸如由管理员和用户使用的计算设备，其中管理员能够将该计算设备用作供应计算设备，而用户能够将其用作访问计算设备。因此，为了便于参考和说明，供应计算设备 210 的各元件与计算设备 110 的类似元件不同地进行编号，但是其功能可以是相似的乃至相同的。因此，CPU 220、系统总线 221、系统存储器 230、可选的非易失性存储器接口 240 以及存储主机控制器 245 全部类似于先前描述的 CPU 120、系统总线 121、系统存储器 130、接口 140 以及存储主机控制器 145。类似地，具有 BIOS 233 的 ROM 231 以及具有包括存储设备驱动器堆栈 238 与访问控制设备扩展 239 的操作系统 234、程序模块 235、程序数据 236 和全卷加密服务 237 的 RAM 232 也类似于上述的 ROM 131、BIOS 133、RAM

132、操作系统 134、存储设备驱动器堆栈 138、访问控制设备扩展 139、程序模块 135、程序数据 136 以及全卷加密服务 137。然而，访问控制设备 170 可以是上面详述的相同的访问控制设备。

[0047] 转到图 2 的系统 200 的存储设备 270，该存储设备 270 能够以与上述的存储设备 141、146 和 147 之中的任何一个相同的方式来使用，并且能够替换或充当上述的存储设备 141、146 和 147 之中的任何一个，其中存储设备的类似物在图 2 中被示意为存储设备 241、246 和 247。实际上，如利用其附近的图形布局所示的，存储设备 270 旨在更详细地代表通信地耦合至访问计算设备 210 的存储设备 241、246 和 247 中的任何一个或多个。

[0048] 存储设备 270 能够包括一个或多个计算机可读媒体 290，其能够包括不可移动的非易失性磁媒体、不可移动的非易失性的基于固态的存储媒体或其他的可移动 / 不可移动、易失性 / 非易失性计算机存储媒体，其包括上述中的任何一个。存储设备 270 的计算机可读媒体 290 能够由计算设备利用来存储用于这样的计算设备的计算机可读指令、数据结构、程序模块和其他数据。例如，存储设备 270 的计算机可读媒体 290 被说明为存储数据 295，其中该数据可以是当由存储设备 270 提供时为用于访问计算设备 210 的操作系统 234、其他程序模块 235 或程序数据 236 中的一些或全部的基础的数据。

[0049] 除了计算机可读媒体 290 之外，示例的存储设备 270 也能够可选地包括硬件密码系统 280，该密码系统能够加密被提供给存储设备 270 的数据以便存储在计算机可读媒体 290 上，并且能够解密从计算机可读媒体中读取的随后将被提供给访问计算设备 210 的数据。这样，硬件密码系统 280 能够执行其密码功能，而不给访问计算设备 210 的 CPU 220 或其他元件增加负担，其在一个实施例中以与任何其他存储设备相同的方式对待存储设备 270 而不考虑数据加密和解密。更进一步，如果访问计算设备 210 不包括诸如全卷加密服务 237 之类的相关密码元件，那么相关联的访问控制设备 170 的存储相关的密码信息 175 能够由硬件密码系统 280 来管理。硬件密码系统 280 在图 2 中利用虚线来说明，以指示它是可选组件，这非常类似于访问控制设备 170 的存储相关的密码信息 175。

[0050] 然而，虽然存储设备 270 的硬件密码系统 280 可以是可选的，但是无论是否存在硬件密码系统，诸如一个或多个处理单元 281 和固件 283 之类的被显示成子组件的其他组件可能存在。更具体地，在一个实施例中，例如，处理单元 281 和固件 283 能够为存储设备 270 提供独立处理至少诸如各种维护和通信任务之类的基本指令的能力。然而，在另一个实施例中，处理单元 281 和固件 283 至少部分地能够被用于执行密码功能，诸如提供给存储设备的数据的加密以及从计算机可读媒体 290 中读取的数据的解密。在这样的实施例中，处理单元 281 和固件 283 至少部分地能够被认为是硬件密码系统 280 的一部分。此外，如同访问控制设备 170 的处理单元 171 一样，存储设备 270 的处理单元 281 可以包括能够基于输入集合来调节其输出的控制器或其他组件。

[0051] 在其中存在访问控制设备 170 的存储相关的密码信息 175 的实施例中，存储相关的密码信息 175 能够被存储设备 270 的硬件密码系统 280 参考，并且能够通知由存储设备 270 的硬件密码系统 280 执行的加密和解密。在一个实施例中，例如，硬件密码系统 280 能够参考访问控制设备 170 的存储相关的密码信息 175 以及诸如在访问计算设备 210 上运行的全卷加密服务 237 或另一个类似的密码系统所提供的附加的密码信息来执行其密码功能。

[0052] 诸如以上面详述的方式可能先前已供应的访问控制设备 170 能够通信地连接至存储设备 270，如利用图 2 的虚线双向通信箭头所示的。如下面将进一步描述的，访问控制设备 170 与存储设备 270 之间这样的通信连接可以是有线的或无线的，并且可以是直接或间接的，例如通过访问计算设备 210。

[0053] 访问计算设备 210 能够通过向存储设备发送恰当的读取命令来尝试访问存储设备 270 的数据 295。如果访问控制设备 170 还没有通信地连接到存储设备 270，该存储设备能够在一个实施例中通知访问计算设备 210 :它不能提供对数据 295 的访问。然而，在替换实施例中，访问控制设备 170 的缺少能够允许以常规方式来使用存储设备 270。如果访问控制设备 170 包括存储相关的密码信息 175，那么在这样的实施例中，如果访问控制设备没有通信地耦合到存储设备，存储设备能够通知访问计算设备 210 :它不能访问数据 295（在这样的实施例中，该数据将采用加密的形式），这是因为存储设备的硬件密码系统 280 为了对加密数据进行解密而需要的存储相关的密码信息 175 是不可获得的。另一方面，如果访问控制设备 170 已通信地耦合到存储设备 270，那么访问控制设备能够确定或接收有关是否允许存储设备 270 给访问计算设备 210 提供对数据 295 的访问的确定。这样的访问能够通过诸如由处理单元 281 执行被访问控制设备 170 通知或调用并操作来拒绝访问计算设备 210 访问数据 295 的指令来拒绝。这样的访问能够附加地或可选择地通过拒绝访问对加密数据进行解密所需的存储相关的密码信息 175 来拒绝。

[0054] 存储设备 270 能够将正在使用合适的存储相关的通信协议实施访问控制的访问控制设备 170 的存在通知访问计算设备。如下面将进一步描述的，存储设备 270 能够将错误消息返回给访问计算设备 210，以响应其尝试访问存储在存储设备的存储媒体 290 上的数据 295。这样的错误消息能够向访问计算设备 210 指示通信地耦合的访问控制设备 170 的存在。响应于能够由被操作系统 234 加载来与存储设备 270 通信的存储设备驱动器堆栈 238 接收的这样的错误消息，存储设备驱动器堆栈 238 能够调用访问控制设备扩展 239 或以其他方式导致访问控制设备扩展 239 被加载，其中该扩展随后能够允许访问计算设备 210 与访问控制设备 170 通信。访问控制设备扩展 239 能够被实现为动态加载的库模块 (Dynamically Loaded Library module)(DLL)、预加载例程或任何其他的运行时绑定可执行计算机代码。

[0055] 在诸如利用图 2 的系统 200 所示的实施例中，访问计算设备 210 的访问控制设备扩展 239 能够与访问控制设备 170 通信并提供信息给访问控制设备 170，以使得访问控制设备的处理单元 171 能够基于为访问控制设备供应的访问控制信息 176 来做出访问控制决定。例如，由访问控制设备 170 请求并被提供给访问控制设备 170 的信息能够包括访问计算设备 210 或存储设备 270 的识别信息。这样的识别信息能够允许访问控制设备 170 诸如基于访问控制信息 176 来确定是否访问计算设备 210 和存储设备 270 是批准的实体。以这样的方式，对数据 295 的访问能够仅限于特定的访问计算设备 210，诸如在安全区域中或没有 WAN 接入的那些计算设备。作为另一示例，由于可靠性和性能原因，诸如与上述的存储主机控制器 145 相类似的存储主机控制器 245 之类的控制器的制造商可以要求只有特定类型的存储设备与其控制器一起使用。在这样的情况下，采用访问控制信息 176 的形式，能够为访问控制设备 170 供应相关联的存储设备 270 能够被允许来与之互操作的一个或多个控制器的一个或多个标识符。或者，可选择地，能够为访问控制设备 170 供应诸如存储设备 270

之类的特定存储设备以及诸如访问计算设备 210 的存储主机控制器 245 之类的特定控制器的标识符，其中特定存储设备和特定控制器被允许彼此互操作。即使存储设备和访问计算设备个别地是批准的实体，如由访问控制信息 176 所指定的，通过核实存储设备 270 通信地连接到恰当的访问计算设备 210，能够采用这样的方式来限制对数据 295 的访问。

[0056] 在另一个实施例中，访问控制设备 170 能够包括多组存储相关的密码信息 175，使得参考存储相关的密码信息以及所提供的对其的访问能够独立地解密能够以加密状态存储的存储设备 270 内的数据 295 的个别分区或其他分段。在这样的实施例中，由访问计算设备提供的信息能够包括用户识别信息，例如用户名和口令，其能够被访问控制设备 170 的处理单元 171 用来确定用户是否恰当地验证了它们自己并在由访问控制信息 176 保持的批准列表上。对于特定用户来说，访问控制信息 176 能够指定 ：能够提供给存储设备 270 的存储相关的密码信息 175 只解密诸如能够利用授权用户访问的计算机可读媒体 290 中的预格式化分区来定义的加密数据的一部分。对于多用户或分时访问计算设备 210 来说，这样的实施例可能是有用的。

[0057] 如在系统 200 中所示的，依照由供应计算设备 110 为访问控制设备供应的访问控制信息 176，能够由访问控制设备 170 的处理单元 171 考虑由访问计算设备 210 提供的信息，并且访问控制设备的处理单元能够基于这样的考虑来确定是允许还是不允许存储设备 270 有意义响应来自访问计算设备的数据存储相关的通信，并从而或允许或不允许访问计算设备 210 读取在计算机可读媒体 290 上的数据 295 或在计算机可读媒体 290 上写入附加数据。在一个实施例中，如上所示，是允许还是不允许存储设备 270 有意义响应数据存储相关的通信的确定能够通过访问控制设备 170 的处理单元 171 指示存储设备 270 的处理单元 281 执行来自固件 283 的恰当指令来实现。例如，如果处理单元 171 确定不应允许访问计算设备 210 在存储设备 270 上存储数据或从存储设备 270 读取数据，处理单元 171 能够指示处理单元 281 执行来自固件 283 的指令，其中这些指令通知访问计算设备 210 ：或将数据写入计算机可读媒体 290 或读取已经存储于其上的数据 295 的其请求正被拒绝。此外，从固件 283 执行的指令能够为访问计算设备 210 提供拒绝理由的指示，诸如恰当的错误代码。在也如上所述的另一个实施例中，是否允许存储设备 270 有意义响应数据存储相关的通信的确定能够通过以下来实现 ：访问控制设备 170 的处理单元 171 释放或者不释放存储相关的密码信息 175 给存储设备 270 的硬件密码系统 280 的处理单元 281，并从而允许或者不允许硬件密码系统 280 解密（以加密形式存储的）数据 295 且从而给访问计算设备 210 提供对这样的数据的访问。由访问控制设备 170 提供的这样的访问控制可以是对访问禁用的补充，其中访问禁用可以通过以下来完成 ：从存储设备 270 中通信地断开包括存储相关的密码信息 175 的访问控制设备 170，并从而通信地中断任何的给存储设备提供必要的存储相关的密码信息以允许存储设备访问存储在其上的加密数据的能力。

[0058] 在诸如利用图 3 的系统 300 所示的另一个实施例中，访问控制设备 170 能够不基于诸如利用访问控制信息 176 所通知的它自己的确定而基于访问控制设备 170 能够通信地耦合至的授权计算设备 310 的确定来允许或不允许存储设备 270 有意义响应来自访问计算设备 210 的数据存储相关的通信。转到图 3，系统 300 被显示成包括系统 200 的访问计算设备 210、访问控制设备 170 和存储设备 270。然而，另外，系统 300 也包括授权计算设备 310，该授权计算设备能够例如经由访问计算设备和授权计算设备二者分别与之保持独立的网

络连接 251 和 351 的网络 155 而通信地耦合至访问计算设备 210。

[0059] 在利用系统 300 所示的实施例中，访问控制设备 170 能够具有访问控制密码信息 376 作为访问控制信息 176 的一部分，其中该访问控制密码信息 376 能够被利用来通过访问计算设备 210 建立至授权计算设备 310 的安全通信隧道 320。如前所述，当访问计算设备 210 尝试访问存储在存储设备 270 上的数据 295 时，存储设备能够将访问控制设备 170 的存在通知访问计算设备，而这又可能导致访问计算设备的操作系统 234 的存储设备驱动器堆栈 238 加载访问控制设备扩展 239 或导致访问控制设备扩展 239 被执行，其中访问控制设备扩展 239 可以允许在访问计算设备与访问控制设备之间的通信。通过那些通信，访问控制设备 170 能够请求访问计算设备 210 的访问控制设备扩展 239 将来自访问控制设备的消息递送到授权计算设备 310 以及相反地将来自授权计算设备的消息提供给访问控制设备。以这样的方式，访问控制设备 170 能够与授权计算设备 310 建立安全通信隧道 320。

[0060] 为了将来自访问控制设备 170 的消息提供给授权计算设备 310，访问控制设备扩展 239 能够请求：访问计算设备 210 的网络接口 250 建立至授权计算设备的通信连接。在一个实施例中，授权计算设备 310 的诸如其网络地址或 DNS 名称之类的位置能够被提供给访问控制设备扩展 239，并由此从访问控制设备 170 的访问控制信息 176 中被提供给网络接口 250。在替换实施例中，授权计算设备 310 的位置可能已为访问计算设备 210 所知。例如，通常，当诸如访问计算设备 210 之类的计算设备与网络 155 建立网络连接 251 时，为该计算设备提供某些网络信息，例如，其包括 DNS 服务器的地址以及服务于该计算设备的路由器的地址。以同样的方式，根据上述实施例，能够为诸如访问计算设备 210 之类的计算设备提供用于诸如授权计算设备 310 之类的授权计算设备的网络地址或其他位置信息，其中授权计算设备能够服务于网络 155 上或该计算设备已连接至的该网络的相同部分上的计算设备。

[0061] 访问控制密码信息 376 可以包括授权计算设备 310 的公共访问密钥、在授权计算设备与访问控制设备 170 之间共享的秘密或能够允许访问控制设备 170 与授权计算设备 310 诸如通过包括与点对点隧道协议（PPTP）或层 2 隧道协议（L2TP）相似或相同的协议的标准隧道机制来建立安全通信隧道 320 的任何类似的密码信息。正如本领域技术人员所知的，这样的隧道机制可以依赖于各种安全证书诸如共享口令或访问控制的交换，或者它们能够依赖于由诸如 Kerberos 或 RADIUS 服务器之类的独立验证器提供的安全证书，其中的任一或所有的证书可能已作为访问控制密码信息 376 被提供给访问控制设备 170。利用安全隧道 320，尽管消息由访问计算设备 210 中继并因此对于在访问计算设备上运行的组件和处理是可见的事实，但是这样的组件和处理不能明白这样的消息的内容，并因此不能导致访问控制设备 170 提供存储相关的密码信息 175，此时授权计算设备 310 将不以其他方式指示这样的存储相关的密码信息的供应是适当的。如前所示，能够包括用于建立安全通信隧道 320 的证书和其他信息的访问控制密码信息 376 可能在供应期间已由供应计算设备 110 提供给访问控制设备 170。

[0062] 在一个实施例中，授权计算设备 310 能够与现有的访问控制技术和方法诸如网络访问保护（Network Access Protection）（NAP）、网络准入控制（Network Admission Control）（NAC）、安全网络访问（Secure Network Access）（SNA）或其他类似技术相结合。例如，现有 NAP 服务器计算设备可能已知道如利用更新的反恶意软件、所应用的操作系统

更新以及其他类似信息量化的计算设备的安全性。如利用现有 NAP 服务器计算设备所确定的可能不满足安全阈值等级的计算设备同样能够向授权计算设备 310 进行识别，并且授权计算设备能够指示访问控制设备 170 不提供存储相关的密码信息 175 给通信地耦合至这样的计算设备的存储设备。

[0063] 因此，如图 3 所示，通过与在访问计算设备 210 上运行的存储设备驱动器堆栈 238 中的访问控制设备扩展 239 进行的通信，访问控制设备 170 仍能够获悉与访问控制设备当前通信耦合至的访问计算设备与存储设备 270 相关联的具体信息。如前所示，这样的信息可以包括使用访问计算设备 210 的用户、访问计算设备本身、存储主机控制器 245、存储设备 270 的身份以及其他信息，其中所述信息能够由访问控制设备 170 通过安全隧道 320 提供给授权计算设备 310。基于如此提供的信息以及诸如上述的 NAP 信息之类的可能可用于它的其他信息，授权计算设备 310 能够确定是否允许存储设备 270 对来自访问计算设备 210 的数据存储相关的通信提供有意义响应。如所示的，从授权计算设备 310 至访问控制设备 170 的指令能够通过安全隧道 320 来接收。在一个实施例中，来自授权计算设备 310 的指令能够由访问控制设备 170 的处理单元 171 来接收，并且如上所述，处理单元能够指示存储设备 270 的处理单元 281 执行来自固件 283 的恰当指令，以便或有意义响应来自访问计算设备 210 的数据存储相关的通信或者使用来自访问计算设备 210 的存储相关的通信或请求的适当的错误或其他拒绝来响应。在另一个实施例中，来自授权计算设备 310 的指令能够由访问控制设备 170 的处理单元 171 来接收，并且也如上所述，处理单元能够向存储设备 270 的处理单元 281 或提供或拒绝存储相关的密码信息 175，以允许或阻止存储设备 270 有意义响应来自访问计算设备 210 的数据存储相关的通信。

[0064] 在一个实施例中，不运行在与访问计算设备 210 相隔开的独立计算设备上，在授权计算设备 310 上运行的授权处理反而能够运行在访问计算设备的保护空间内。在这样的实施例中，授权计算设备 310 可以是虚拟机或在访问计算设备 210 上运行的其他受保护的独立处理。因为在上述的实施例中访问计算设备 210 运送消息给授权计算设备 310 以及从授权计算设备 310 中运送消息，所以授权计算设备反而能够通过在访问计算设备上执行计算机可执行指令来实现而无需改变访问控制设备 170。

[0065] 转到图 4，更详细示出和描述在访问控制设备 170 与存储设备 270 之间的通信连接，诸如在图 2 和 3 中利用虚的通信箭头所示出的。在一个实施例中，如利用系统 400 所示的，存储设备 270 能够不仅包括先前描述的硬件密码系统 280 和计算机可读媒体 290，而且还能够包括访问控制设备接口 410。仅通过示例，访问控制设备接口 410 可以是存储设备 270 上的插槽或连接器，以致访问控制设备 170 能够物理上被插入访问控制设备接口 410 或以其他方式被连接到访问控制设备接口 410，以致在被插入或被连接时，访问控制设备 170 实质上并不改变存储设备 270 的尺寸。在这样的情况下，存储设备 270 能够被诸如访问计算设备 210 之类的计算设备使用，如上详细描述的，如同任何其他的相似类型的存储设备在没有访问控制设备的情况下一样。例如，如果存储设备 270 被设计成符合标准硬盘驱动器大小，那么访问计算设备 210 能够使用访问控制设备 170 物理上连接至的存储设备 270 作为内部硬盘驱动器，并且访问控制设备的存在或缺乏将不改变存储设备 270 的物理尺寸来禁止这样的使用。

[0066] 作为另一个示例，访问控制设备 170 能够采用诸如通常用于蜂窝电话的全球移动

通信系统(GSM)用户身份模块(SIM)的形式。在这样的情况下,访问控制设备接口 410 可以是通常又被包括在蜂窝电话内的 GSM SIM 接口。因为访问控制设备 170 以及访问控制设备接口 410 的物理形状因子二者能够被广泛应用并因此是便宜的,所以这样的实施例能够提供成本优势。

[0067] 作为还一个示例,访问控制设备 170 能够包括常见的连接器,诸如通用串行总线(USB)连接器,而相应的访问控制设备接口 410 同样能够如此。与上述的 GSM SIM 实施例一样,USB 连接器同样由于其普遍性而提供成本优势。在这样的实施例中,下述的访问控制设备 170 与硬件密码系统 280 之间的通信能够经由众所周知的 USB 通信协议来执行。

[0068] 但是,访问控制设备 170 不一定需要被物理连接到存储设备 270 以便通信地连接至该存储设备。上述的实施例提供在访问控制设备 170 与存储设备 270 之间的物理连接,以避免通过存储设备的常见类型接口来发送任何的指令或密码信息 175 给处理单元 281。以这样方式,访问控制设备 170 和存储设备 271 的硬件设计能够确保由处理单元 171 提供的指令或存储相关的密码信息 175 不能被外部实体获得。

[0069] 在替换实施例中,尽管由处理单元 171 提供给处理单元 281 的指令以及存储相关的密码信息 175 之中的至少一些通过存储设备 270 的外部通信接口进行传送,但是这些指令和信息也能够得到保护。因而,如系统 450 中所示的,尽管访问控制设备 170 与存储设备 270 的物理分离,但是也能够在访问控制设备 170 与存储设备 270 之间经由访问计算设备 210 来建立通信连接。如所示的,系统 450 能够包括访问计算设备 210、访问控制设备 170 以及存储设备 270,其中访问控制设备和存储设备独立地连接到访问计算设备。尽管示出系统 450,其中访问计算设备 210、访问控制设备 170 和存储设备 270 被显示成分离的物理实体,但是不要求这样的物理分离。例如,存储设备 270 能够诸如采用内部硬盘驱动器的形式被内部连接到访问计算设备 210。访问控制设备 170 转而能够被连接至访问计算设备 210 的外部接口,诸如流行的外设或存储接口,这包括有线和无线接口在内。在这样的实施例中,访问控制设备 170 与存储设备 270 之间的通信能够由访问计算设备 210 中的存储设备驱动器堆栈 238 中继,其中访问计算设备能够通过它自己的机制并通过访问控制设备扩展 239 与访问控制设备和存储设备二者通信。

[0070] 转到图 5,参考系统 500 利用更多特异性示出在访问计算设备 210 与访问控制设备 170 之间的示例通信交换。如图 5 所示,系统 500 能够包括与上面具体描述的系统 200 和 300 相同的基本组件,这包括访问控制设备 170、存储设备 270、访问计算设备 210 以及可选地包括授权计算设备 310。初始地,如利用通信 510 所示的,例如,访问计算设备 210 以及更特别地访问计算设备的操作系统 234 (未显示)中的存储设备驱动器堆栈 238 能够诸如通过发出读取请求、初始化请求或其他类似的访问请求而提出存储设备 270 的数据存储相关的请求。响应于数据存储相关的请求 510,存储设备能够提供包括错误代码的错误通信 520。正如本领域技术人员将知道的,诸如将由存储设备驱动器堆栈 238 执行的与存储设备的通信能够采用错误代码的形式提供错误通信,其中每一个代码指示存储设备 270 的部分上的特定错误或错误的类型。在一个实施例中,错误代码能够由存储设备 270 作为通信 520 的一部分被提供给存储设备驱动器堆栈 238,其中通信 520 能够指示存储设备通信地耦合至访问控制设备 170,并且能够进一步指示因为通信耦合的访问控制设备尚未授权存储设备 270 对数据存储请求 510 有意义地提供响应而导致访问数据 295 的尝试失败,其中例

如，诸如通过指示处理单元 281 这样做或通过提供解密请求数据所需要的存储相关的密码信息 175 来有意义提供响应。

[0071] 响应于这样的错误代码，如利用动作 530 所示的，存储设备驱动器堆栈 238 能够加载访问控制设备扩展 239 或导致访问控制设备扩展 239 被加载或以其他方式被执行。如前所示，访问控制设备扩展 239 能够包括被配置成包括当访问控制设备诸如通过存储设备而仅仅间接通信地耦合至计算设备时与诸如访问控制设备 170 之类的这样的访问控制设备通信的计算机可执行指令。一旦访问控制设备扩展 239 被加载，那么它能够将诸如通信 540 之类的通信引导到访问控制设备 170。在一个实施例中，通信 540 能够包括诸如将传统地被引导到存储设备 270 的写入命令，但是写入命令能够指定地址或地址范围，其中所述地址或地址范围能够向存储设备指示该通信被引导到访问控制设备 170。因而，如图 5 所示，来自访问控制设备扩展 239 的通信 540 能够最初地被提供给存储设备 270，并且基于所指定的地址或地址范围，存储设备随后能够进一步将通信 540 提供给访问控制设备 170。

[0072] 访问控制设备 170 能够提供响应通信 550，其中响应通信 550 诸如通过最初由访问控制设备提供给存储设备 270 并且随后从存储设备提供给存储设备驱动器堆栈 238 而能够被反向递送到访问控制设备扩展 239。存储设备驱动器堆栈 238 随后能够依据响应 550 的接收而将它辨认为适合于访问控制设备扩展 239 的响应，并且它能够将访问控制设备扩展引导至该响应。如上所述，在一些实施例中，诸如响应 550 之类的响应能够请求访问控制设备扩展 239 将某些可能已被包括在响应 550 中的数据转发给授权计算设备 310。在这样的情况下，例如，访问控制设备扩展 239 能够请求在访问计算设备 210 上运行的相关网络处理与网络接口 250 一起建立至授权计算设备 310 的通信连接，如利用请求 560 所指示的。访问控制设备扩展 239 从而能够提供数据给访问控制设备 170 和授权计算设备 310 以及从访问控制设备 170 和授权计算设备 310 提供数据，从而允许访问控制设备和授权计算设备建立安全通信隧道 320。

[0073] 转到图 6，流程图 600 提供诸如能够由图 1 的系统 100 中示出并在上面具体描述的示例供应计算设备 110 执行的访问控制设备 170 的示例供应的进一步说明。如从流程图 600 中能够看出的，初始地，在步骤 610，能够启动诸如访问控制设备 170 之类的访问控制设备的供应。步骤 610 的供应启动可以是自动启动，诸如响应于通信地耦合至供应计算设备的访问控制设备的检测，或者诸如通过能够由在供应计算设备上运行的一个或多个处理呈现的合适用户界面，它可以是手动或用户启动的供应。随后，在步骤 620，能够作出有关是否被供应的访问控制设备将与授权计算设备一起进行利用或者是否它将在独立基础上执行访问控制决定的确定。如果在步骤 620 确定被供应的访问控制设备将不与授权计算设备一起使用，那么在步骤 630，能够为访问控制设备供应访问控制信息，其中该访问控制信息能够包括诸如用户、计算设备、存储设备、存储主机控制器或其组合之类的能够被授予对访问控制设备通信地耦合至的存储设备的数据相关能力的访问的那些实体的标识。可选择地，如果在步骤 620 确定被供应的访问控制设备将与授权计算设备一起使用，那么在步骤 640 能够为访问控制设备供应包括访问控制密码信息的访问控制信息，其中所述信息能够允许访问控制设备诸如以上面详细描述的方式通过访问计算设备与授权计算设备建立安全通信隧道。

[0074] 无论是在步骤 630 为独立的访问控制操作供应访问控制设备还是在步骤 640 为与

授权计算设备进行的交互供应访问控制设备，在这两种情况中，处理能够继续进行可选的步骤650，其中该步骤借助于虚边界而被显示为可选的，其中在该步骤中能够为访问控制设备供应存储相关的密码信息，而密码信息能够由访问控制设备通信地耦合至的存储设备用于加密或解密所存储的数据或将被存储在存储设备上的数据。在一个实施例中，在步骤650上存储相关的密码信息的供应能够为访问控制设备供应多组例如物理访问控制，使得与访问控制设备通信的每一个后续存储设备能够获取下一个物理访问控制并将其标记为在使用。以这样的方式，单个访问控制设备能够被多个存储设备共享或与之一起进行使用。如所示的，一旦存储相关的密码信息在步骤650可选地被供应给访问控制设备，相关处理能够在步骤660结束。

[0075] 转到图7，显示进一步说明诸如上面具体描述的示例的访问计算设备210之类的访问计算设备的示例操作的流程图700。转到流程图700，初始地，如所示的，在步骤705，访问计算设备能够向访问计算设备通信地耦合的存储设备发出数据存储相关的请求，诸如访问请求。响应于步骤705上这样的数据存储相关的请求，访问计算设备能够在步骤710接收指示正被访问的存储设备通信地耦合至访问控制设备的错误。如果在步骤710没有接收到这样的错误，那么访问计算设备能够在步骤715开始以传统方式使用该存储设备。相关的处理随后能够在步骤760结束。

[0076] 如果在步骤710访问计算设备接收到来自存储设备的指示存储设备通信地耦合到访问控制设备的错误，那么访问计算设备在步骤720能够加载访问控制设备扩展，并且如前所述，使用访问控制设备扩展与访问控制设备通信。在步骤725，能够作出有关访问控制设备是否正在请求信息的确定。如果访问控制设备正在请求信息，那么在步骤730能够提供被请求的信息。如前所述，如此请求的信息能够包括访问计算设备的身份、使用这样的计算设备的用户、访问存储设备的存储主机控制器的身份以及存储设备本身的身份。也如前所述，这样的身份能够诸如通过口令或其他的安全机制来验证，并且在这样的情况下，在步骤730提供的请求信息能够包括那些口令或对于可能已由访问控制设备在步骤725提供的质询进行的其他响应。一旦在步骤730提供了请求的信息，则处理能够返回到步骤725，以等待来自访问控制设备的进一步信息请求。

[0077] 如果在步骤725访问控制设备没有请求任何信息，那么处理能够继续至步骤735，并且能够确定访问控制设备是否已请求至授权计算设备的连接。如果在步骤735这样的连接没有被请求，那么相关处理能够在步骤760结束。然而，如果在步骤735这样的连接被请求，那么在步骤740，请求计算设备能够诸如以上面详细描述的方式与授权计算设备建立连接。随后，在步骤745，能够由访问计算设备执行在访问控制设备与授权计算设备之间的数据交换，也如上所述。

[0078] 在步骤750，能够进行检查，以确定访问控制设备是否已请求结束与授权计算设备的连接。如果没有提出这样的请求，那么处理能够返回到步骤745，并且能够继续在访问控制设备与授权计算设备之间交换数据。然而，如果在步骤750访问控制设备请求结束与授权计算设备的连接，那么在步骤755，该连接可以被结束并且相关处理能够在步骤760结束。

[0079] 如从上面的描述中能够明白的，已提供了能够控制对存储设备的访问的访问控制设备。鉴于在这里描述的主题的许多可能的变型，我们宣称可能落入以下权利要求书及其

等价物的范围内的所有这样的实施例为我们的发明。

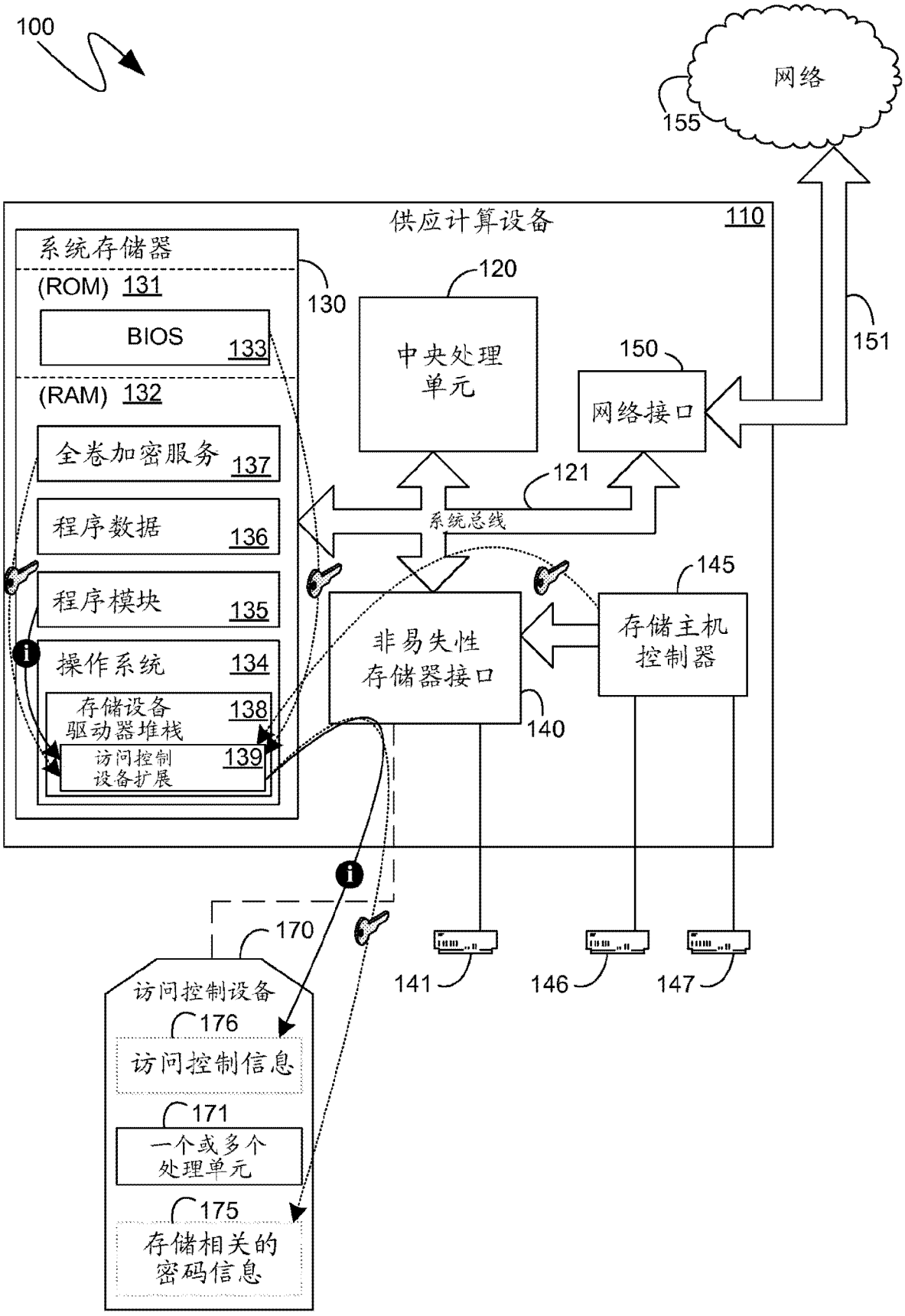

100
网络
155
供应计算设备
110
系统存储器
(ROM) 131
BIOS 133
(RAM) 132
全卷加密服务 137
程序数据 136
程序模块 135
操作系统 134
存储设备驱动器堆栈 138
访问控制设备扩展 139
130
120
中央处理单元
150
网络接口
151
121
系统总线
145
非易失性存储器接口
存储主机控制器
140
141
146
147
170
访问控制设备
176
访问控制信息
171
一个或多个处理单元
175
存储相关的密码信息

图 1

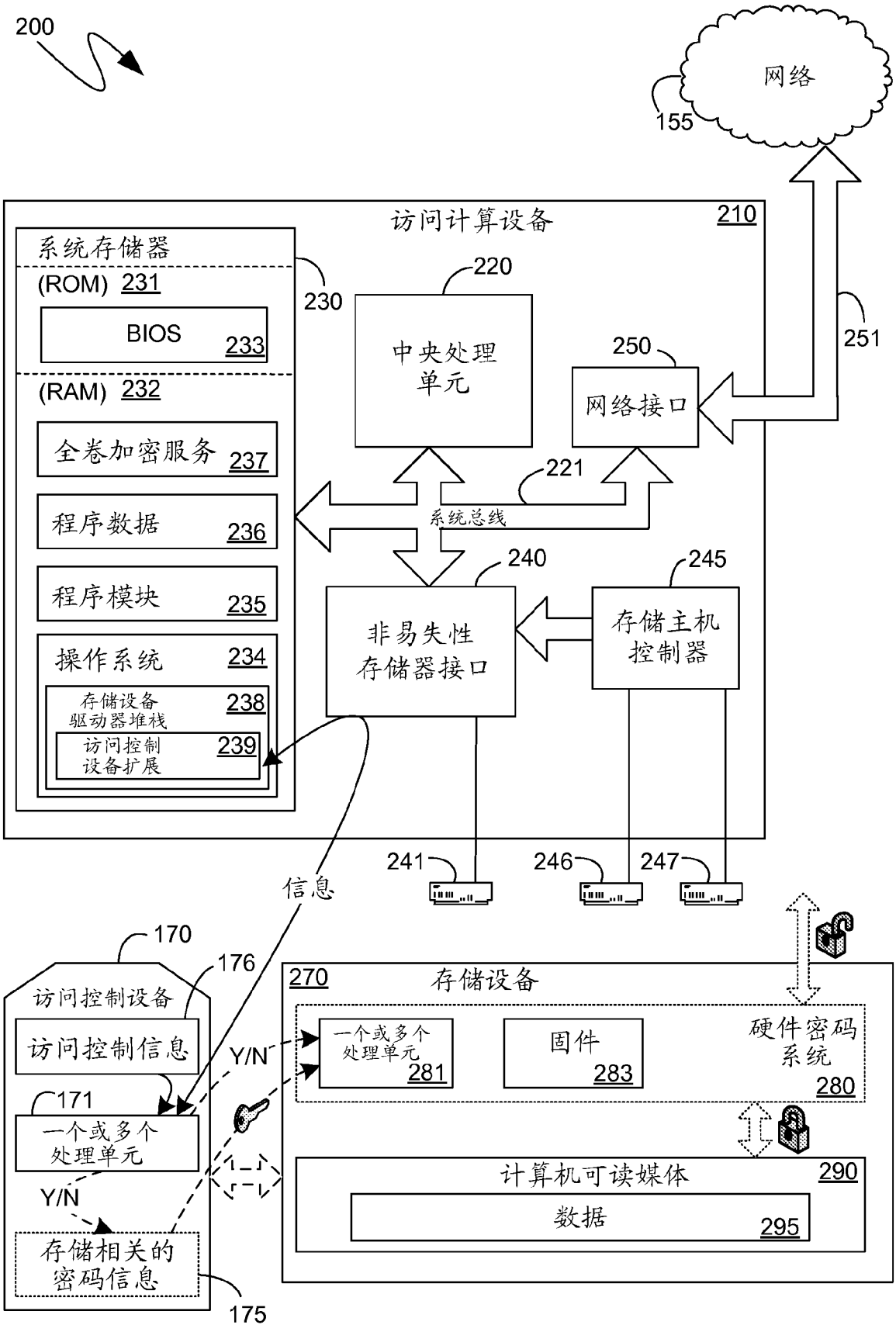

200
网络
155
访问计算设备
210
系统存储器
(ROM) 231
BIOS 233
(RAM) 232
230
全卷加密服务 237
程序数据 236
程序模块 235
操作系统 234
存储设备驱动器堆栈 238
访问控制设备扩展 239
220
中央处理单元
250
网络接口
251
221
系统总线
240
非易失性存储器接口
245
存储主机控制器
241
246
247
信息
170
176
访问控制设备
访问控制信息
171
一个或多个处理单元
Y/N
Y/N
存储相关的密码信息
175
270
存储设备
一个或多个处理单元 281
固件 283
硬件密码系统 280
计算机可读媒体 290
数据 295

图 2

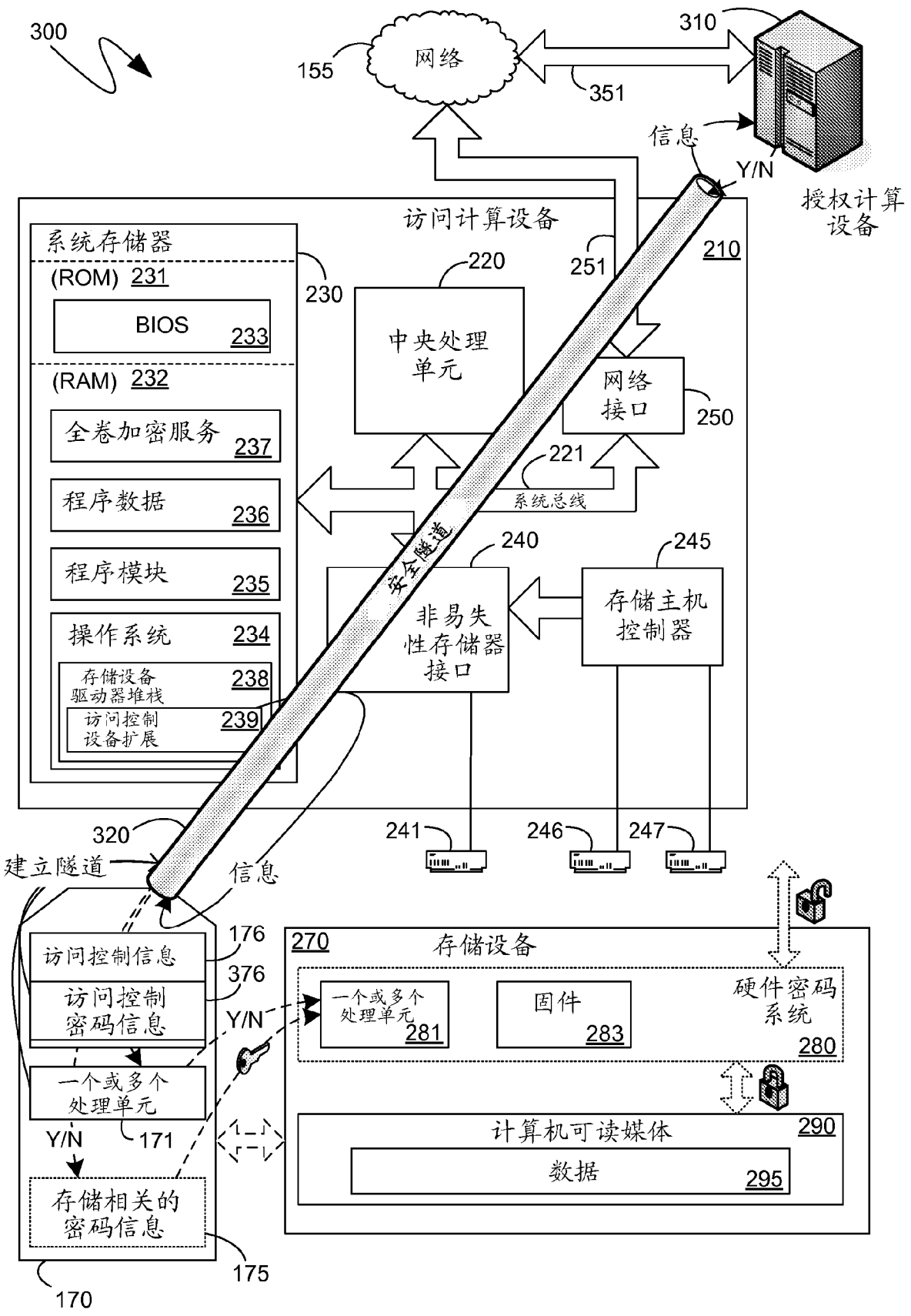

300
网络
155
310
351
信息
Y/N
授权计算设备
访问计算设备
210
系统存储器
(ROM) 231
BIOS 233
(RAM) 232
230
220
251
中央处理单元
网络接口
250
全卷加密服务 237
程序数据 236
程序模块 235
操作系统 234
存储设备驱动器堆栈 238
访问控制设备扩展 239
221
系统总线
安全隧道
240
245
非易失性存储器接口
存储主机控制器
241
246
247
320
建立隧道
信息
176
访问控制信息
376
访问控制密码信息
Y/N
一个或多个处理单元
171
Y/N
存储相关的密码信息
175
170
270
存储设备
一个或多个处理单元 281
固件 283
硬件密码系统 280
计算机可读媒体 290
数据 295

图 3

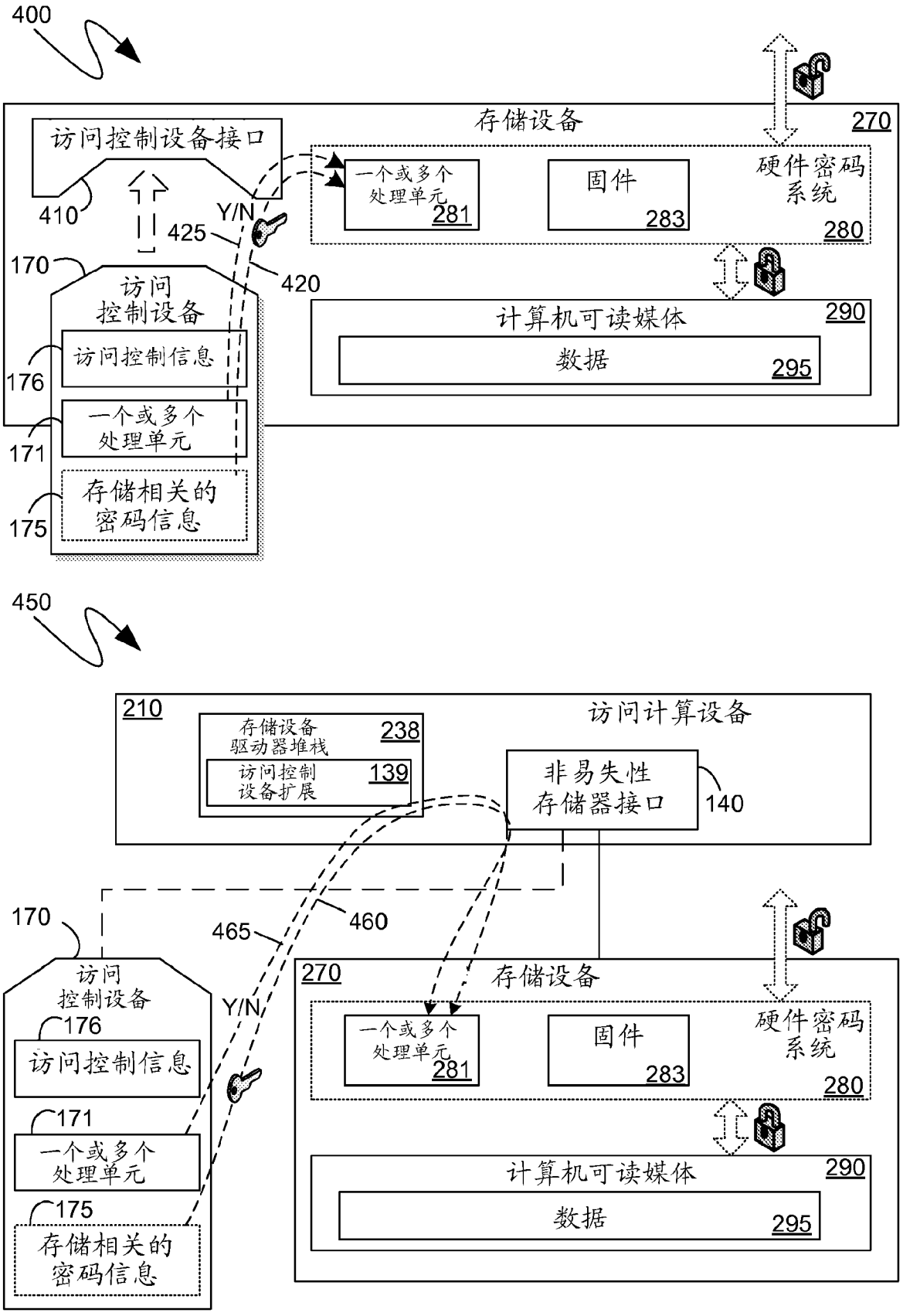

400
存储设备
270
访问控制设备接口
410
425
Y/N
一个或多个处理单元
281
固件
283
硬件密码系统
280
420
170
访问控制设备
访问控制信息
176
一个或多个处理单元
171
存储相关的密码信息
175
计算机可读媒体
290
数据
295
450
210
访问计算设备
存储设备驱动器堆栈
238
访问控制设备扩展
139
非易失性存储器接口
140
460
465
170
访问控制设备
176
访问控制信息
171
一个或多个处理单元
175
存储相关的密码信息
Y/N
270
存储设备
一个或多个处理单元
281
固件
283
硬件密码系统
280
计算机可读媒体
290
数据
295

图 4

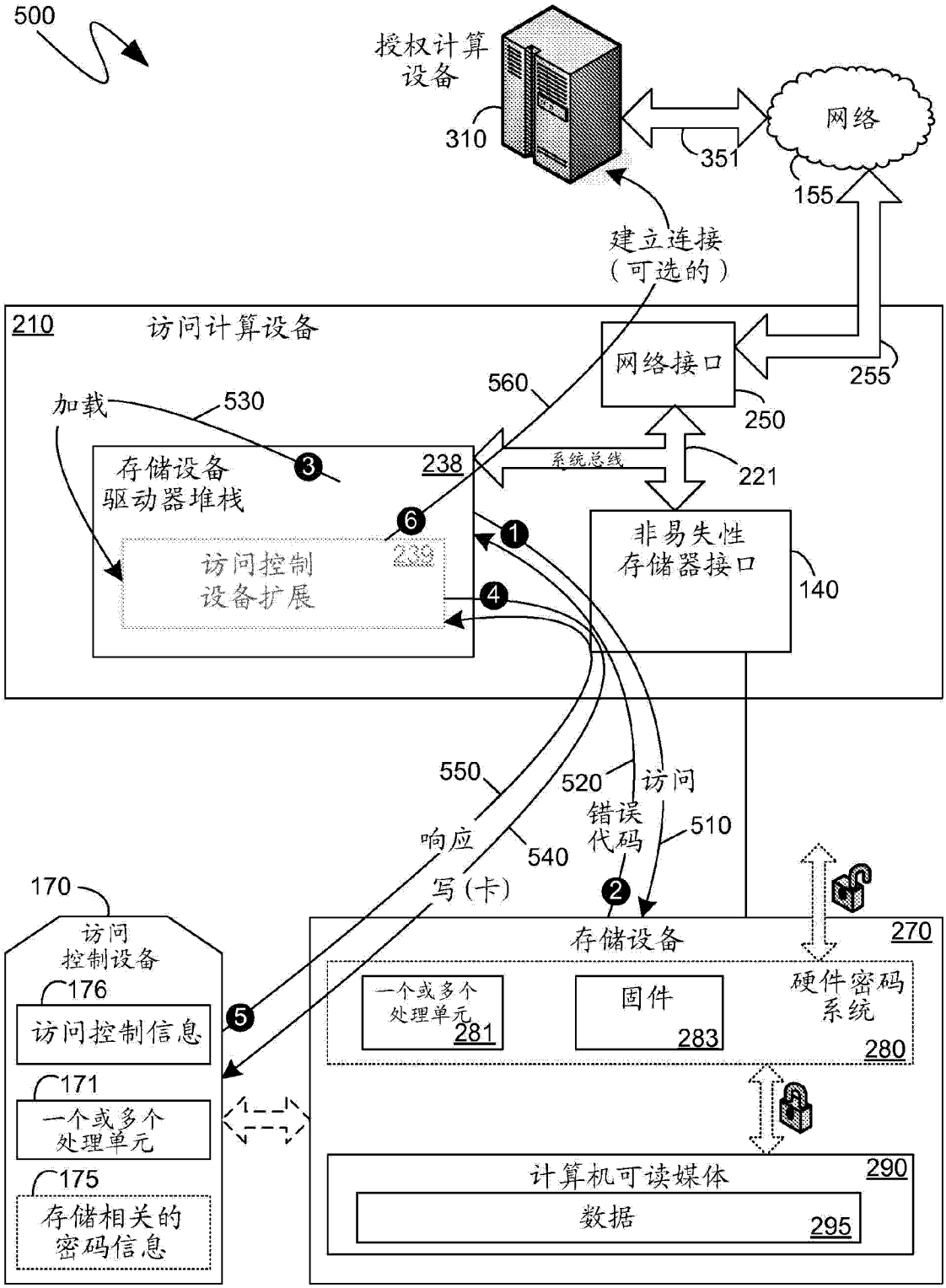

500
授权计算设备
310
网络
351
155
建立连接（可选的）
210
访问计算设备
网络接口
255
560
250
加载
530
存储设备驱动器堆栈
238
系统总线
221
访问控制设备扩展
239
非易失性存储器接口
140
550
520
访问
响应
540
错误代码
510
写（卡）
170
访问控制设备
176
访问控制信息
171
一个或多个处理单元
175
存储相关的密码信息
存储设备
270
一个或多个处理单元
281
固件
283
硬件密码系统
280
计算机可读媒体
290
数据
295

图 5

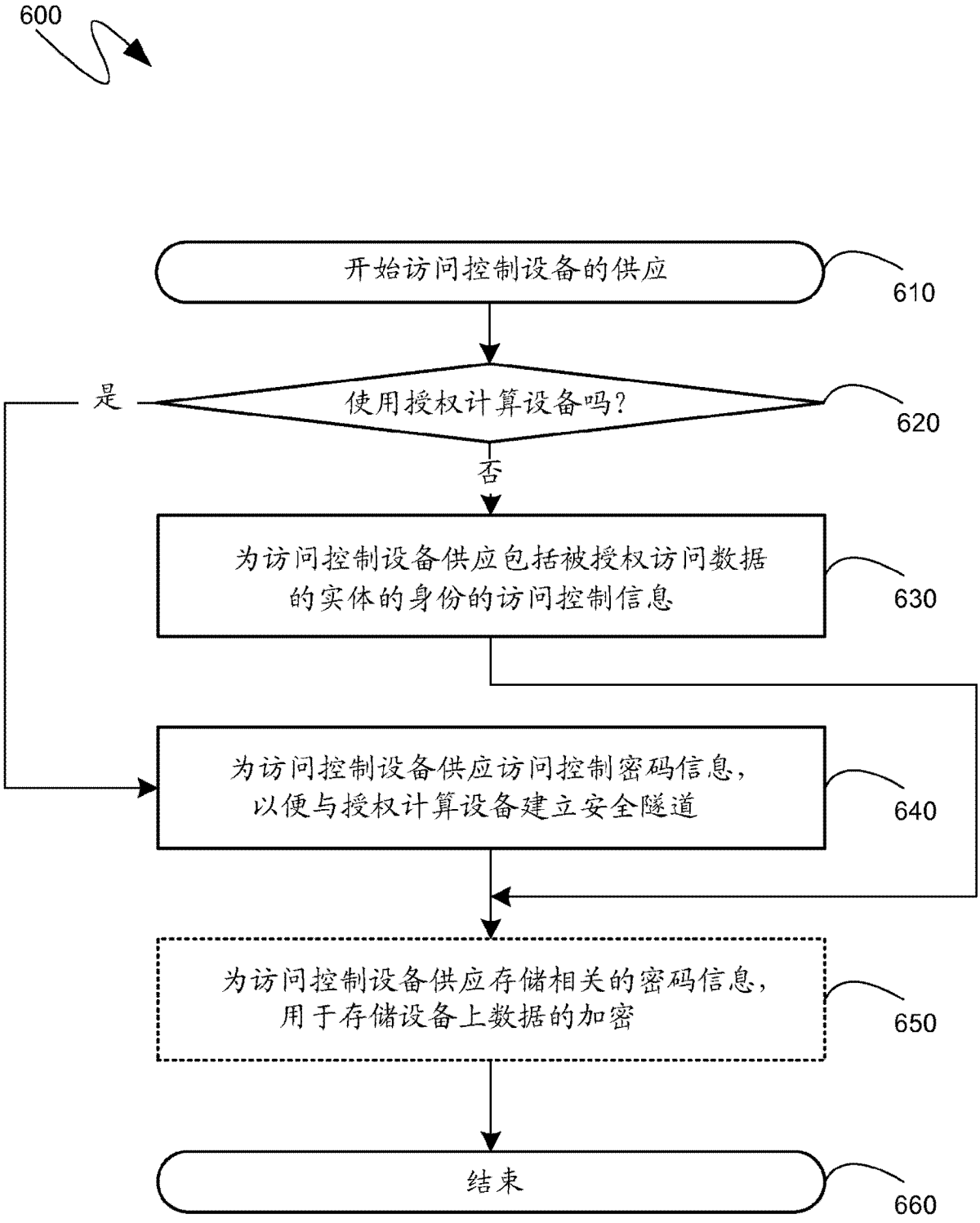

600
开始访问控制设备的供应
610
使用授权计算设备吗?
620
是
否
为访问控制设备供应包括被授权访问数据的实体的身份的访问控制信息
630
为访问控制设备供应访问控制密码信息，以便与授权计算设备建立安全隧道
640
为访问控制设备供应存储相关的密码信息，用于存储设备上数据的加密
650
结束
660

图 6

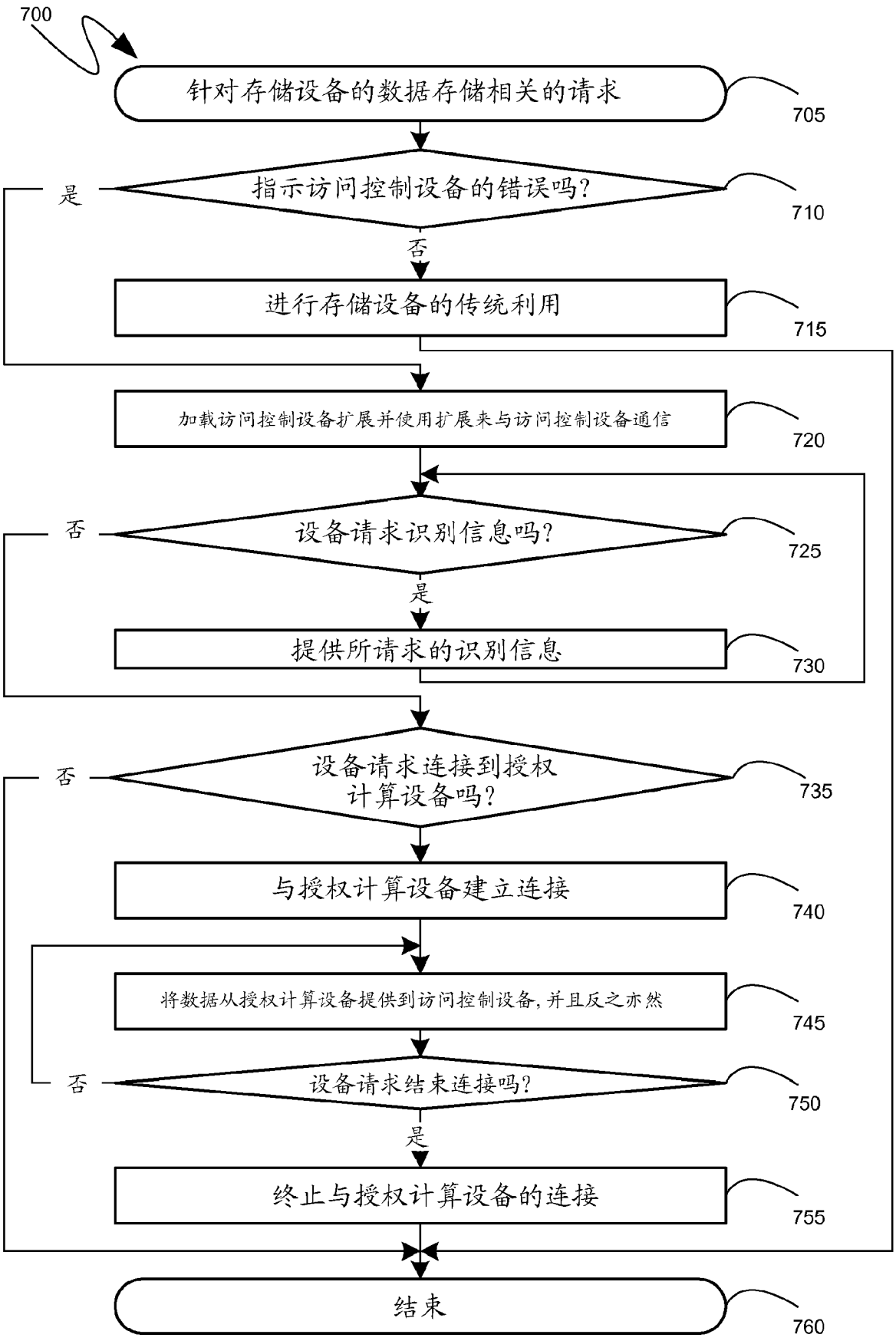

700
针对存储设备的数据存储相关的请求
705
指示访问控制设备的错误吗?
710
是
否
进行存储设备的传统利用
715
加载访问控制设备扩展并使用扩展来与访问控制设备通信
720
设备请求识别信息吗?
725
否
是
提供所请求的识别信息
730
设备请求连接到授权计算设备吗?
735
否
与授权计算设备建立连接
740
将数据从授权计算设备提供到访问控制设备,并且反之亦然
745
设备请求结束连接吗?
750
否
是
终止与授权计算设备的连接
755
结束
760

图 7