(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 102438014 A
(43)申请公布日 2012.05.02

(21)申请号 201110373318.0

(22)申请日 2011.11.22

(30)优先权数据
2010246354 2010.11.22 AU
12/965445 2010.12.10 US

(71)申请人 微软公司
地址 美国华盛顿州

(72)发明人 M. F. 诺瓦克 P. J. 利奇
朱力强 P. J. 米勒 A. 汉加努
曾毅 J. D. 维加斯
K. M. 肖尔特

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李舒 刘鹏

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

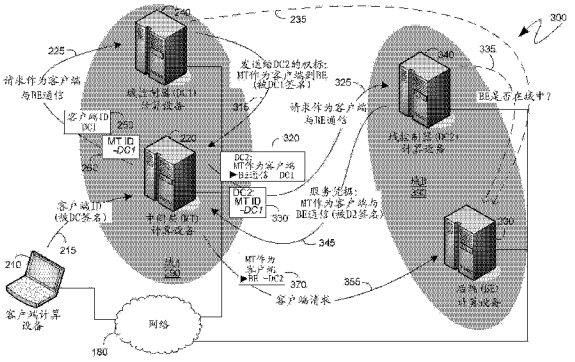
权利要求书 2 页 说明书 13 页 附图 6 页

(54)发明名称

后端受限委托模型

(57)摘要

本发明提供了一种用于委托的方法和系统。在可良好扩展的系统的背景下，客户端可以与中间层通信，中间层然后又可以与后端层通信，从而代表客户端访问信息和资源。每个单独的后端可以建立起限定哪个计算设备可以委托给该后端的策略。与该特定后端位于相同管理域内的域控制器可以执行所述策略。当中间层请求委托给后端时，该请求所指向的域控制器可以应用该策略，或者如果域控制器位于与目标后端不同的域中，则其可以将中间层指向不同域中的域控制器，并且可以签名与不同域控制器通信时中间层可以利用的相关信息。



CN 102438014 A

1. 一种用于实现委托的方法，包括以下步骤：

接收指定目标（230）的委托请求；

检查该目标（230）与执行计算机可执行指令的计算设备是否位于相同域中；

识别包含委托给目标（230）的要求的一个或多个策略；

确定是否满足所识别的一个或多个策略；

生成包含来自委托请求的信息的签名权标；以及

生成允许该委托请求的签名服务凭据；

其中如果所述检查揭示该目标（230）并非位于该域中，则执行用于实现生成签名权标的该计算机可执行指令；以及

其中进一步如果所述检查揭示该目标（230）位于该域中，则执行用于实现识别、确定和生成签名服务凭据的计算机可执行指令。

2. 根据权利要求 1 所述的方法，其中该一个或多个策略中的至少一个策略是由所述目标建立并控制的。

3. 根据权利要求 1 所述的方法，其中该签名权标和签名服务凭据指向另一个域。

4. 根据权利要求 1 所述的方法，其中所述确定还包括请求与所述要求相关联的附加信息。

5. 根据权利要求 1 所述的方法，还包括以下步骤：接收签名的标识，验证签名并且如果验证成功则签名该接收到的标识。

6. 根据权利要求 5 所述的方法，还包括以下步骤：

将如果验证成功则被签名的接收到的标识指向另一域。

7. 一种或多种计算机可读介质，包括用于执行权利要求 1 所述的步骤的计算机可执行指令。

8. 一种系统，包括：

客户端计算设备（210）；

后端层计算设备，包括第一后端计算设备（230）；

中间层计算设备（220），包括用于执行以下步骤的计算机可执行指令：

向第一域控制器计算设备提供中间层计算设备（220）设法作为客户端计算设备（210）与第一后端计算设备（230）通信的指示；

向第一域控制器计算设备提供中间层计算设备（220）的标识；

如果第一后端计算设备（230）和域控制器计算设备均在相同域中，则接收指示该中间层计算设备（220）可以作为客户端计算设备（210）与第一后端计算设备（230）通信的服务凭据；

将所述服务凭据呈现给第一后端计算设备（230）；

如果第一后端计算设备（230）与第一域控制器计算设备位于不同的域中，则接收指示该中间层计算设备（220）设法作为客户端计算设备（210）与第一后端计算设备（230）通信的权标；并且

将该权标呈现给第二域控制器计算设备；并且

该第一域控制器计算设备包括执行以下步骤的计算机可执行指令：

检查第一后端计算设备（230）是否位于还包括第一域控制器计算设备的域中；

识别包含用于委托给该第一后端计算设备（230）的要求的一个或多个策略；

确定中间层计算设备（220）是否满足所述要求；

生成、签名并且传送权标；以及

生成、签名并且传送服务凭据；

其中如果所述检查揭示该第一后端计算设备（230）并非位于该域中，则执行用于实现所述生成、签名并发送权标的计算机可执行指令；以及

其中进一步如果所述检查揭示该第一后端计算设备（230）位于该域中，则执行用于实现所述识别、确定和生成、签名并传送该已签名服务凭据的计算机可执行指令。

9. 根据权利要求 8 所述的系统，其中所述一个或多个策略中的至少一个策略是由第一后端计算设备建立并控制的。

10. 根据权利要求 8 所述的系统，其中该后端层计算设备除了第一后端计算设备还包括第二后端计算设备；其中另外该中间层计算设备还包括其他计算机可执行指令，以用于：作为客户端计算设备与第二后端计算设备通信；聚集从后端计算设备和第二后端计算设备接收的信息；并且将所聚集的信息提供给客户端计算设备。

后端受限委托模型

背景技术

[0001] 在最简单的形式中，客户端与服务器之间的网络通信包括从客户端到服务器的请求，该请求可以专门由该服务器应答并返回到客户端。尽管这种系统确实简单，但是其可能扩展性不好，并且其可能不允许呼叫者在单个信道上同时与多个服务交互，例如文件存储服务、数据库存储服务以及电子邮件服务。为了使客户端仍然能够与单个服务器通信，但又要允许服务器扩展其能力，采用了分层结构。在分层结构中，客户端可以将其请求传送给充当中间层的服务器。该中间层服务器自身不必包括响应客户端请求所需的相关信息。取而代之，该中间层服务器可以向后并参考（reference）作为后端服务器层一部分的一个或多个服务器，以便获得客户端所请求的信息。在获得所述信息之后，中间层服务器继而可以响应该客户端。从客户端的角度来看，单个通信端点（即中间层）可以提供对潜在的无限数量数据和其他信息源的访问。

[0002] 为了使得中间层服务器能够响应客户端的请求，可以允许该中间层服务器代表客户端从后端服务器层获得信息。从安全角度出发，可能有害的是，允许中间层服务器作为客户端与不在后端服务器层中的其他服务器通信。客户端可以向中间层服务器提供其密码或者长期证书（credential）或其他认证信息，并且中间层服务器然后可以作为客户端通过提供该认证信息与任何服务器通信，上述这种设置典型地被称作“不受限委托”，因为将客户端的角色委托给（delegate to）中间层服务器并不受中间层可与哪个服务器进行通信的限制。

[0003] 针对该不受限委托的安全问题的一个解决方案是一种典型地称作“受限委托”的委托模型，其中实施（put in place）了一种策略，该策略限制与代表或作为客户端的中间层服务器通信的后端层服务器。典型地，受限委托模型通过域控制器操作，该域控制器将参考一个或多个相应的策略并确定是否将允许中间层服务器代表或作为客户端与一个或多个后端层服务器通信。例如，在客户端向中间层服务器提供了其认证信息之后，中间层服务器可以从域控制器请求代表并作为客户端对后端层中的一个或多个服务器行动（act）的权利。参考一个或多个相关策略的域控制器可以确定是否准许中间层服务器的请求，并且如果它允许中间层服务器的请求，则域控制器可以向中间层服务器提供服务凭据或者其他信息集合，中间层服务器可以将其呈现给一个或多个后端层服务器，从而指示域控制器已经认为该中间层服务器在与所述后端层服务器通信过程中代表并作为客户端来行动是可接受的。

[0004] 遗憾的是，受限委托难以跨越联网的计算设备的多个域而实现。更具体地讲，在一个域中的后端层服务器不一定信赖另一不同域（例如包括该中间层服务器的域）的域控制器。取而代之，所述包括中间层服务器的域的域控制器既能够直接地也能够经由中间层服务器和后端层服务器间接地与所述包括后端层服务器的域的域控制器通信，并且向第二个域控制器提供足够的信息以使其能够确定的确允许中间层服务器委托给一个或多个后端层服务器。这种模型可能难以实现，因为它需要多个域控制器或者多个域的管理员的协作。此外，这种模型将对委托的限制集中于域策略是否允许中间层服务器委托给（delegate

to）一个或多个后端层服务器。

发明内容

[0005] 在一个实施例中，中间层计算设备对于作为后端层一部分的一个或多个服务器计算设备的委托不是通过域策略是否允许该中间层计算设备委托给该一个或多个后端层计算设备来确定的，而是通过所述一个或多个后端层计算设备中的每一个的相应策略是否允许中间层计算设备委托给（delegate to）它来确定的。因此，降低了域管理员的作用，且取而代之，相关策略的决策作出可以由后端层计算设备的系统管理员来执行，该系统管理员可能对于由这样的后端层计算设备提供的服务更为熟悉。

[0006] 在另一个实施例中，域控制器计算设备在从中间层计算设备接收委托给一个或多个后端层计算设备的请求时可以考虑所述一个或多个后端层计算设备是否位于域控制器的域内。如果该后端层计算设备位于域控制器的域内，则域控制器计算设备可以向中间层计算设备提供服务凭据或者其他信息集合，中间层计算设备可以将其呈现给该一个或多个后端层计算设备，从而使该中间层计算设备能够作为客户端计算设备并代表其行动。然而，如果后端层计算设备并未位于域控制器的域内，则该域控制器计算设备可以改为向中间层计算设备提供权标（token）或者其他信息集合，中间层计算设备可以将其呈现给不同域的另一个域控制器计算设备，从而针对该另一不同域中的后端层计算设备作为客户端计算设备并代表其行动。

[0007] 在另一个实施例中，域控制器计算设备可以在提供最终可以用于使得中间层计算设备能够在与一个或多个后端层计算设备通信中作为客户端计算设备并代表其行动的权标、服务凭据或者其他类似数据之前可以验证中间层计算设备或者其他域控制器计算设备。

[0008] 该发明内容以简化形式介绍了下文在具体实施方式中进一步描述的概念的选择。该发明内容不旨在确定所要保护主题的关键特征或者必要特征，也不旨在用于限制所要求保护主题的范围。

[0009] 根据下面参照附图进行的具体实施方式将会清楚本发明的附加特征和优点。

附图说明

[0010] 结合附图可以最佳地理解后面的具体实施方式，在附图中：

图 1 是示例性计算设备的示意图；

图 2 是图示用于使得中间层计算设备能够委托给相同域内的后端层计算设备的示例性通信序列（series）的系统示意图；

图 3 是图示使得中间层计算设备能够委托给不同域中的后端层计算设备的示例性通信序列的系统示意图；

图 4 是图示使得中间层计算设备能够委托给不同域中的后端层计算设备的另一个示例性通信序列的系统示意图；

图 5 是示例性中间层计算设备的示例性操作的流程图；以及

图 6 是示例性域控制器计算设备的示例性操作的流程图。

具体实施方式

[0011] 下面的描述涉及一种委托模型，其中关于中间层计算设备能否委托给后端层计算设备的决策是由后端层计算设备是否将允许中间层计算设备委托给它来确定的。为了实现这种委托模型，在一个实施例中，域控制器计算设备在从中间层计算设备接收委托给后端层计算设备的请求时可以首先确定该后端层计算设备是否位于该域控制器的域中。如果该后端层计算设备位于该域控制器的域中，则该域控制器可以向中间层计算设备提供服务凭据或者其他信息集合，中间层计算设备可以将其呈现给后端层计算设备，从而使得中间层计算设备能够作为客户端计算设备并代表其行动。然而，如果该后端层计算设备不在该域控制器的域中，则该域控制器计算设备可以改为向中间层计算设备提供权标或其他信息集合，中间层计算设备可以将其呈现给不同域的另一域控制器计算设备，从而针对所述另一不同域中的后端层计算设备作为客户端计算设备并代表其行动。按照这种方式，中间层计算设备在其与后端层计算设备通信过程中作为客户端计算设备并代表其行动的能力可能受到由与后端层计算设备相同域的域控制器计算设备所执行（enforce）的策略的控制，并且因此受作为该策略指定者（specifier）的后端层计算设备本身控制。

[0012] 本文中描述的技术参考了特定类型的通信及通信元件，例如“服务凭据”或者“权标”。然而，这样的引用仅被提供用于向数据的集合分配命名，该命名提供获悉由下面的描述详述的过程和决策作出所必需的信息。这样的引用不旨在将所述技术限于经常与术语相关联的特定标准化协议。因此，尽管本领域技术人员可以认识到可以促使特定的、现有的认证和委托协议（例如 Kerberos）执行以下详细描述的元件中的至少一些，但是本文中提供的描述不旨在被限于这样的现有协议，而是同样适用于可以提供并实现下述机制和过程的各个方面的任意消息和数据集合。类似地，本文中描述的技术参考了一个或多个“域控制器”计算设备。这样的参考是为了标记方便并且易于理解，而不旨在将所述技术特别地限于必须执行全套域控制器功能的计算设备。取而代之，本领域技术人员将会认识到，以下参考“域控制器”详细描述的功能可以由任意的可信中央机构（authority）计算设备来执行。因此，本文中采用的术语“域控制器”意指任何可信的中央机构，且术语“域控制器计算设备”意指包括和实现可信中央机构的任何一个或多个计算设备。

[0013] 尽管不需要，但以下描述将处于正被计算设备执行的计算机可执行指令（例如程序模块）的总体背景中。更具体地讲，所述描述将会参考由一个或多个计算设备或外围设备执行的操作的动作和符号表示，除非另外说明。同样地，将会被理解的是，有时被称为计算机可执行的这样的动作和操作包括由以结构化形式表示数据的电信号的处理单元进行的操纵。该操纵转换所述数据或者在存储器的某个位置维护该数据，其按照本领域技术人员很好理解的方式重新配置或者以另外的方式改变计算设备或外围设备的操作。维护数据的数据结构是具有由数据格式限定的特定属性的物理位置。

[0014] 一般而言，程序模块包括执行特定任务或者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，本领域技术人员将会理解，所述计算设备不需限于常规的个人计算机，并且包括其他计算配置，所述计算配置包括手持设备、多处理器系统、基于微处理器或可编程的消费型电子产品、网络PC、微型计算机、大型计算机等。类似的是，所述计算设备不需要限于孤立的计算设备，因为所述机制还可以在通过通信网络链接的分布式计算环境中实践。在分布式计算环境中，程序模块既可以位于本地存储设备中也可以位于远

程存储设备中。

[0015] 参照图 1，图示了一种示例性计算设备 100，其部分包括可以用于并辅助下述方法的硬件元件。示例性计算设备 100 可以包括但不限于一个或多个中央处理单元（CPU）120、系统存储器 130 和将包括系统存储器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意一种，这些总线结构包括利用多种总线架构中任意一种的存储器总线或存储器控制器、外围总线以及本地总线。根据特定的物理实现方式，可以将 CPU 120、系统存储器 130 以及计算设备 100 的其他组件中的一个或多个物理上共同定位，例如定位在单芯片上。在这种情况下，系统总线 121 中的一些或全部可能只不过是单芯片结构内的硅路径，并且其在图 1 中的图示可能只不过是为了图示目的的标记便利。

[0016] 计算设备 100 典型地还包括计算机可读介质，所述介质可以包括可被计算设备 100 访问的任何可用的介质。仅为举例而非限制，计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以用于存储信息的任何方法或技术实现的介质，所述信息例如是计算机可读指令、数据结构、程序模块或者其他数据。计算机存储介质包括但不限于 RAM、ROM、EEPROM、闪存或者其他存储技术、CD-ROM、数字通用盘（DVD）或其他光盘存储、盒式磁带、磁带、磁盘存储或其他磁存储设备、或者可以用于存储所希望的信息并且可被计算设备 100 访问的任何其他介质。通信介质典型地包含计算机可读指令、数据结构、程序模块或者已调制数据信号（例如载波或其他传送机制）中的其他数据，并且包括任何信息递送介质。仅为举例而非限制，通信介质包括有线介质，例如有线网络或者直接有线连接，还包括无线介质，例如声学、RF、红外及其他无线介质。以上介质的任意组合也应包含在计算机可读介质的范围内。

[0017] 当使用通信介质时，该计算设备 100 可以经由与一个或多个远程计算机的逻辑连接而在联网环境中操作。图 1 所描绘的逻辑连接是与网络 180 的通用网络连接 171，该网络可以是局域网（LAN）、诸如因特网之类的广域网（WAN），或者其他网络。计算设备 100 通过网络接口或适配器 170 与通用网络连接 171 连接，该网络接口或适配器 170 又与系统总线 121 连接。在联网的环境中，相对于计算设备 100 描绘的程序模块或者其一部分或外围程序可以被存储在通过该通用网络连接 171 与计算设备 100 通信耦合的一个或多个其他计算设备的存储器中。将理解，所示的网络连接是示例性的，并且可以采用其他方式建立计算设备之间的通信链路。

[0018] 在计算机存储介质中，系统存储器 130 包括易失性和 / 或非易失性存储器形式的计算机存储介质，其包括只读存储器（ROM）131 和随机存取存储器（RAM）132。尤其包含用于引导计算设备 100 的代码的基本输入 / 输出系统 133（BIOS）典型地存储在 ROM 131 中。RAM 132 典型地包含可由处理单元 120 立即访问的和 / 或当前正在运行的数据和 / 或程序模块。作为举例而非限制，图 1 图示了操作系统 134、其他程序模块 135 以及程序数据 136。RAM 132 还可以包含可能与 TPM 150 的操作相关的数据，例如 TCG 事件日志 190。在一个实施例中，TCG 事件日志 190 可以包括自加电以来或其最后一次重启以来由计算设备 100 加载或执行的所有模块的唯一标识；加载或执行的相同模块可以产生当前由 TPM150 在一个或多个 PCR 中维护的值。

[0019] 计算设备 100 还可以包括其他可移除 / 不可移除、易失性 / 非易失性计算机存储

介质。作为举例而非限制，图 1 图示了从不可移除、非易失性介质读取或向其写入的硬盘驱动器 141。可以与示例性计算设备一起使用的其他可移除 / 不可移除、易失性 / 非易失性计算机存储介质包括但不限于盒式磁带、闪存卡、数字通用盘、数字视频带、固态 RAM、固态 ROM 等。硬盘驱动器 141 典型地通过诸如接口 140 之类的不可移除存储器接口连接到系统总线 121。

[0020] 以上讨论并在图 1 中示出的驱动器及其相关联的计算机存储介质为计算设备 100 提供了对计算机可读指令、数据结构、程序模块及其他数据的存储。例如，在图 1 中，硬盘驱动器 141 被图示为存储操作系统 144、其他程序模块 145 以及程序数据 146。注意，这些组件既可以与操作系统 134、其他程序模块 135 和程序数据 136 相同也可以与它们不同。在这里，操作系统 144、其他程序模块 145 和程序数据 146 被赋予了不同的数字以说明至少它们是不同的副本。

[0021] 转到图 2，其中所示的系统 200 包括四个计算设备，即客户端计算设备 210、中间层计算设备 220、后端计算设备 230 以及域控制器计算设备 240。这些计算设备中的每一个可以采用刚才描述的示例性计算设备 100 的形式，并且可以包括以上参照示例性计算设备 100 所详细描述的组件的一些或全部。图 2 的系统 200 的计算设备被示出为经由通信连接通信地耦合到网络 180。为了图示方便，该网络 180 由单个说明性元件来图示，但是这并不意味着局限于单个网络域或者任何其他类似的网络分区或结构，也不意味着说明也是图 2 系统 200 中所示的域 A 290 外部的网络。取而代之，附图中所用的网络 180 意在表示图中所示系统的计算设备（包括所示的各种域）之间的所有网络通信连接，并且意在表示直接和间接通信连接。因此，例如，图 2 所示的系统 200 图示了一系列的示例性通信，借助这些通信，客户端计算设备 210 可以通过网络 180 与中间层计算设备 220 直接或间接地通信。图 2 的系统 200 还图示了示例性通信序列，借助这些通信序列，中间层计算设备 220 可以同样直接或间接且同样通过网络 180 与域控制器计算设备 240 和后端计算设备 230 通信。因此，尽管将中间层计算设备 220、域控制器计算设备 240 以及后端计算设备 230 全部图示为相同域 A 290 的一部分，但是如先前所指示的，网络 180 意在被认为包括域 A 290，而不意在被认为与域 A 290 分离并远离域 A 290 的网络单元。如以下将要详细描述的，所示的通信图示了委托机制的示例性操作，其可以使得中间层计算设备 220 针对后端层计算设备（例如后端计算设备 230）代表客户端计算设备 210 行动。

[0022] 起初，如图 2 的系统 200 所示，客户端计算设备 210 可以通过经由通信 215 提供能被域控制器计算设备 240 签名的客户端标识符或者其他数据集合向中间层计算设备（例如中间层计算设备 220）认证它自己。例如，在一个实施例中，在开始与中间层计算设备 220 的通信（例如通信 215）之前，客户端计算设备 210 可以首先从域控制器计算设备 240 获得客户端标识符。本领域技术人员会认识到，该域控制器计算设备 240 可以在提供所述客户端标识符之前执行对客户端计算设备 210 的评估。例如，域控制器计算设备 240 可以验证该客户端计算设备 210 是否符合相关的安全设定，例如是否已经安装了最新版本的反恶意软件应用程序，或者作为另一个实例，是否已经为客户端计算设备 210 上驻留的各种操作系统和软件应用程序安装了最新的补丁包。这种信息可以由客户端计算设备 210 提供作为其与域控制器计算设备 240 通信的一部分，并且可以由域控制器计算设备参照例如事件日志来验证，该事件日志可由客户端计算设备 210 以可安全验证方式维护。

[0023] 一旦域控制器计算设备 240 已确定可以允许客户端计算设备 210 与受域控制器计算设备 240 控制并由图 2 阴影区域表示的域 A 290 内的其他计算设备通信，则该域控制器计算设备 240 可以向该客户端计算设备 210 提供客户端标识符或者其他识别数据集合。这种客户端标识符或者其他标识数据可以由域控制器 240 签名，使得域 A 290 内的其他计算设备可以验证其真实性。例如，域 A 290 中其他计算设备中的每一个，例如中间层计算设备 220 和后端计算设备 230，可以访问域控制器计算设备 240 的公钥。因此，如果域控制器计算设备 240 要用其私钥签名该客户端标识符（该私钥对应于域 A 290 内其他计算设备拥有的公钥），则这些其他计算设备中的每一个可以按照本领域技术人员公知的方式参照公钥来验证这种签名。可替代地，与依靠公 / 私钥对不同，所述签名可以利用一个或多个共享对称密钥来执行，该对称密钥在域控制器计算设备 240 与该域（例如域 A 290）内与域控制器计算设备 240 通信的计算设备之间维护。

[0024] 因此，当客户端计算设备 210 经由通信 215 将其客户端标识符传送给中间层计算设备 220 时，中间层计算设备 220 可以利用例如域控制器计算设备 240 的公钥来验证由客户端计算设备 210 在通信 215 中提供的客户端标识符实际上是由域控制器计算设备 240 签名的。在对客户端计算设备 210 进行这种验证之后，中间层计算设备 220 可以接受来自客户端计算设备 210 的请求，并且作为所述请求的一部分，其可以要求客户端计算设备 210 提供一些标识或者认证信息以证明该客户端计算设备 210 的用户被授权访问正请求的信息或资源。如下面进一步详细阐述的，随后中间层计算设备 220 可以利用这种标识和认证信息针对后端层计算设备（例如后端计算设备 230）代表客户端计算设备 210 行动。

[0025] 如前所指示，客户端计算设备 210 的用户所请求的信息或资源可能不必与中间层计算设备 220 协同定位（co-located）。取而代之，中间层计算设备 220 可以充当客户端计算设备 210 的单个通信端点从而做出众多请求中的任意一个，并且然后该中间层计算设备 220 可以与适当的后端层计算设备（例如后端计算设备 230）通信，以访问正被客户端计算设备 210 的用户请求的相关信息或资源。按照这种方式，单个中间层计算设备，例如中间层计算设备 220，可以提供对可能分散（spread out across）在多个后端层计算设备的众多信息或其他资源的访问，尽管为了易于图示，图 2 系统 200 中仅示出了单个后端层计算设备，即后端计算设备 230。

[0026] 在中间层计算设备 220 已经例如参照经由通信 215 传送的客户 ID 验证（validate）了客户端计算设备 210 之后，并且在中间层计算设备 220 已经接收了来自客户端计算设备 210 用户的标识和认证信息之后（此处的通信未在图 2 系统 200 中明确示出以避免图示拥挤），中间层计算设备 220 可以请求被允许与适当的后端层计算设备（例如后端计算设备 230）通信，好像它就是客户端计算设备 210 一样。在一个实施例中，这种请求 225 可以连同域控制器计算设备 240 能用于评价该请求 225 并遵照该请求执行的信息一起被传送到域控制器计算设备 240。例如，如图 2 的系统 200 所示，随着请求 225，中间层计算设备 220 可以提供其经由通信 215 从客户端计算设备 210 接收到的客户端标识符 250，并且该标识符由域控制器计算设备 240 签名。类似地，仍如图所示，随着请求 225，中间层计算设备 220 可以提供它自己的标识符 260，其与客户端标识符 250 一样也由域控制器计算设备 240 签名。

[0027] 在一个实施例中，域控制器计算设备 240 在接收到请求 225 以及标识符 250 和 260

时可以参照标识符 250 和 260 分别验证客户端计算设备 210 和中间层计算设备 220。域控制器计算设备同样可以在确定是否允许中间层计算设备 220 委托给后端计算设备 230 之前，首先确定中间层计算设备 220 希望委托给的后端计算设备 230 实际上是否在域控制器计算设备 240 的域 A 290 内。因此，如图 2 的系统 200 中用虚线 235 表示的，域控制器计算设备 240 可以确定后端计算设备 230 是否位于其域 290 内。如果后端计算设备 230 位于域 A 290 内，则域控制器计算设备 240 可以参考一个或多个策略来确定后端计算设备 230 是否将允许中间层计算设备 220 委托给它。

[0028] 在一个实施例中，可以至少部分地通过可以由后端计算设备 230 自身或者更具体地由后端计算设备 230 的管理员建立的策略来告知域控制器计算设备 240 作出的后端计算设备 230 是否将允许中间层计算设备 220 委托给它的确定。本领域技术人员将可以认识到，允许后端计算设备 230 设置策略不需要引入任何安全风险，或者篡夺域控制器计算设备 240 的功能，因为该后端计算设备 230 可以被信任，以正确地确定它可以信任谁委托给它。不同的是，后端计算设备 230 可以被信任以建立限定其信任其它设备委托给它的准则的策略。

[0029] 在一个实施例中，域控制器计算设备 240 在评估所述一个或多个策略确定后端计算设备 230 是否将允许中间层计算设备 220 委托给它时可以按照与以上参照客户端计算设备 210 描述的相似的方式执行对中间层计算设备 220 的评估。例如，域控制器计算设备 240 可以验证中间层计算设备 220 符合相关的安全设定，例如已经安装了最新版本的抗恶意软件应用程序，或者作为另一个实例，已经为客户端计算设备 210 上驻留的各种操作系统和软件应用程序安装了最新的补丁包。更具体的讲，域控制器计算设备 240 参考的、包括如所指示地可以由后端计算设备 230 建立的策略的所述策略可以指定 ：如果满足某些条件 (包括例如参考刚才描述的相关安全设定的条件)，则后端计算设备 230 将仅允许该中间层计算设备 220 委托给它。然而，相关策略并非仅限于对中间层计算设备 220 安全方面的分析，而是可以基于任何信息或者信息集合 (包括例如正在使用的操作系统的类型、附接的外围设备的类型、计算设备的硬件配置或者任何其他信息或者信息集合之类) 限制被允许委托后端计算设备 230 的计算设备。作为中间层计算设备 220 的标识符 260 的一部分或者作为域控制器计算设备 240 与中间层计算设备 220 之间的后续通信的一部分，这种信息可以由域控制器计算设备 240 从中间层计算设备 220 收集。

[0030] 在一个实施例中，域控制器计算设备 240 所参考的用来确定是否允许中间层计算设备 220 委托给后端计算设备 230 的一个或多个策略可以参考中间层计算设备 220 上执行的服务以及物理中间层计算设备 220 本身。在这种实施例中，中间层计算设备 220 的标识符 260 不仅可以包括物理计算设备自身的标识符，还可以包括一个或多个服务的标识符或者在该中间层计算设备 220 上执行并且将要执行委托的其他计算机可执行指令的集合。因此，下面为了说明的目的，对中间层计算设备 220 的标识 (例如标识 260) 的参考意指包括物理设备自身的标识、一个或多个服务的标识或者将要执行委托的其他正在执行的计算机可执行指令、或者其任意组合。

[0031] 基于对所述策略的考虑，如果域控制器计算设备 240 确定后端计算设备 230 将允许中间层计算设备 220 委托给它，则如通信 245 所示，该域控制器计算设备 240 可以提供服务凭据或者其他信息集合，所述服务凭据或信息集合可以被域控制器签名并且可以指示中

间层计算设备 220 将被允许作为客户端计算设备 210 与后端计算设备 230 通信。然后，一旦接收到通信 245，中间层计算设备 220 继续向后端计算设备 230 发出请求，如通信 255 所示，该请求是中间层计算设备先前从客户端计算设备 210 接收来的。如图 2 的系统 200 所示，该通信 255 还可以包括服务凭据 270，该凭据可能已经由中间层计算设备 220 经由通信 245 从域控制器计算设备 240 接收。

[0032] 尽管为了避免图示拥挤，图 2 的系统 200 中并未具体示出，但是后端计算设备 230 可以例如参照域控制器的公钥来评估提供有客户端请求 255 的服务凭据 270，以验证其实际上是适当且正确签名的服务凭据，并且如果后端计算设备 230 这样确定，那么其可以继续与该中间层计算设备 220 通信，好像该中间层计算设备 220 是客户端计算设备 210。同样，后端计算设备 230 可以请求中间层计算设备 220 认证，如同在客户端计算设备 210 与后端计算设备 230 直接通信的情况下被要求将其自身向后端计算设备 230 认证一样。在这样的认证中，后端计算设备 230 可以基于客户端计算设备 210 自身的身份、基于客户端计算设备 210 的单独用户或用户组的身份或者其任意组合来确定是否准许客户端的请求。因此，为了这种认证的目的，中间层计算设备 220 可以从客户端计算设备 210 获得这种信息，并且可以将该信息作为原始通信 255 的一部分或者后续通信的一部分提供给后端计算设备 230。

[0033] 按照这种方式，中间层计算设备 220 可以从后端计算设备 230 获得由客户端计算设备 210 请求的信息和资源，随后该中间层计算设备 220 可以响应于客户端计算设备的原始请求将所述信息和资源返回到客户端计算设备 210。本领域技术人员将会认识到，在域 A 290 内可以添加附加的后端层计算设备，并且可以允许中间层计算设备 220 按照相同方式委托给那些后端层计算设备，从而允许中间层计算设备 220 访问实际上潜在无限数量的信息和资源，同时仍然允许客户端计算机 210（或许是中间层计算设备 220）具有用于访问所述信息和那些资源的单独通信参考。此外，当前描述的机制可以被以递归方式利用，其中例如后端计算设备 230 又能充当中间层计算设备并且可以委托给另外不同的后端计算设备。这种另外的委托可以根据本文中描述的机制执行，并且可以基于可以以类似方式评估的可独立设定的策略。

[0034] 如前所述，尽管图 2 的示例性系统 200 仅图示了单个后端计算设备 230，但本文中提供的描述同样适用于单个中间层计算设备与多个后端层计算设备之间的通信，其中中间层计算设备充当客户端计算设备的聚合器。例如，如果客户端计算设备 210 想要请求遍布多个后端层计算设备（包括例如后端计算设备 230 和其他后端层计算设备）的信息，则中间层计算设备 220 可以按照与上述相同的方式委托给这种其他后端层计算设备，并且这将在下面进行更详细的描述。中间层计算设备 220 然后可以从所述多个后端层计算设备获得相关信息，该后端层计算设备可以包括图 2 所示并且在本说明书中参考的后端计算设备 230，并且该后端层计算设备在将客户端计算设备 210 的信息呈现给客户端计算设备 210 作为对这种设备做出的请求的响应之前，可以收集并汇集客户端计算设备 210 的这种信息。

[0035] 在其他实施例中，为了响应客户端计算设备 210 的请求，中间层计算设备 220 需要代表客户端计算设备 210 委托给的后端计算设备 230 可能不必位于相同的域，例如域 A 290 内。转到图 3，其中所示的系统 300 图示了一种多域系统，其中域控制器计算设备 240 和中间层计算设备 220 保持在域 A 290 中，但是中间层计算设备 220 需要委托给的后端计算设备 230 可以为域 B 390 的一部分，该域可以具有它自己的域控制器计算设备 340。为了将域

A 290 的域控制器计算设备 240 与域 B 390 的域控制器计算设备 340 区分开，图 3 中将用简写标记“DC1”来参考域 A 290 的域控制器 240，并且图 3 中用简写标记“DC2”来表示域 B 390 的域控制器 340。此外，先前图 2 中所示的相同通信和元件在图 3 的系统 300 中保留它们的相同的数字标识符。

[0036] 因此，如从图 3 的系统 300 可以看出，客户端计算设备 210 仍可以按照前述方式与中间层计算设备 220 通信，并且中间层计算设备 220 仍可以也按照前述方式与域控制器计算设备 240 通信。然而，当经由前述的通信 225 从中间层计算设备 220 接收作为客户端计算设备 210 与后端计算设备 230 通信的请求时，域控制器计算设备 240 同样如前所述那样可以首先确定(如虚线 235 所示)该后端计算设备 230 与域控制器计算设备 240 是否位于相同的域，即域 A 290 中。在图 3 的系统 300 表示的特定实例中，可以看到，该后端计算设备 230 与域控制器计算设备 240 不在相同的域内。

[0037] 因此，该域控制器计算设备 240 并非评估策略以确定后端计算设备 230 是否将允许中间层计算设备 220 委托给它，而是改为可以经由通信 315 向中间层计算设备 220 提供可以被域控制器计算设备 240 签名的权标或者其他信息集合。这种权标或者其他信息集合可以使中间层计算设备 220 能够将其委托请求指向不同的域控制器计算设备，例如在图 3 所示实例中的域控制器计算设备 340。因此，在一个实施例中，经由通信 315 提供的权标可以指向域控制器计算设备 340。

[0038] 当接收到由通信 315 提供的权标时，中间层计算设备 220 可以向域 B 390 中的域控制器计算设备 340 发送请求 325，该请求可与先前描述的请求 225 类似。然而，尽管前述请求 225 还包含均要由域控制器计算设备 240 签名的客户端标识符 250 和中间层标识符 260，但是中间层计算设备 220 已指向域控制器计算设备 340 的请求 325 可以包含通过通信 315 接收的权标 320（该权标可以是前述的权标），并且还可以包含被域控制器计算设备 240 签名的中间层计算设备 220 的标识符 330。在一个实施例中，与经由通信 315 提供的权标 320 类似，中间层计算设备 220 的标识符 330 同样可以指向域控制器计算设备 340。在这种实施例中，或者作为通信 315 的一部分，或者作为与通信 315 一起发生的通信的一部分，中间层计算设备 220 可以从域控制器计算设备 240 请求或者另外接收被域控制器计算设备 240 签名且指向域控制器计算设备 340 的标识符 330。此外，在一个实施例中，可以将权标 320 和标识符 330 经由可替代路径(包括例如从域控制器计算设备 240 直接提供或者其他可替代路径)传送到域控制器计算设备 340。

[0039] 当域控制器计算设备 340 接收请求 325 时，其首先可以按照与前面针对域控制器计算设备 240 所述类似的方式确定该请求 325 所参考的后端计算设备 230 与域控制器计算设备 340 是否位于相同的域中，即图 3 所示的说明性系统 300 中的域 B 390 中。和前面一样，这种确定在图 3 中用虚线 335 图示。在本实例中，因为后端计算设备 230 与域控制器设备 340 位于相同的域中，即域 B 390 中，所以域控制器计算设备 340 可以继续通过例如参考一个或多个策略来确定后端计算设备 230 是否将允许中间层计算设备 220 委托给它。

[0040] 在执行这种确定的过程中，域控制器计算设备 340 可以首先验证由中间层计算设备 220 提供的作为请求 325 一部分的权标 320 和中间层标识符 330 正确地被域控制器计算设备 240 签名。例如，域控制器计算设备 340 可以参照其可以访问的域控制器计算设备 240 的公钥做出这种确定。一旦域控制器计算设备 340 已经执行这种验证，则其可以查阅一个

或多个策略来确定例如后端计算设备 230 是否允许中间层计算设备 220 委托给它。如前所述，由域控制器计算设备 340 查阅的策略可以包括后端计算设备 230 建立的策略，这是因为后端计算设备 230 可以被信任以建立定义其信任谁委托给它的策略。还如前所述，由域控制器计算设备 340 查阅的策略实际上可以参考中间层计算设备 220 的任何方面，包括例如正由中间层计算设备 220 执行的操作系统、中间层计算设备 220 的硬件，以及中间层计算设备 220 的安全属性，例如是否已经应用了最新的补丁包以及是否使用了最新版本的抗恶意软件。这样的信息可以包含在中间层计算设备 220 可经由通信 325 提供给域控制器计算设备 340 的中间层标识符 330 中，或者可替代地，这样的信息可以经由域控制器计算设备 340 与中间层计算设备 220 之间的、结合通信 325 执行的另外的通信交换来提供。

[0041] 如果域控制器计算设备 340 基于上述评估确定应当允许中间层计算设备 220 委托给后端计算设备 230，则域控制器计算设备可以经由图 3 所示的通信 345 提供服务凭据或者其他信息集合，所述服务凭据或信息集合可以被域控制器计算设备 340 签名并且可以使得中间层计算设备 220 能够委托给后端计算设备 230。如前所述，然后中间层计算设备 220 可以向后端计算设备 230 发出请求，该请求最初是由客户端计算设备 210 向中间层计算设备 220 发出的，如通信 355 所示。此外，请求 355 可以包括可能已经从域控制器计算设备 340 经由通信 345 提供的服务凭据 370。

[0042] 如前所述，当接收到请求 355 时，后端计算设备 230 可以评估该服务凭据 370 并且验证其被包括后端计算设备 230 的域（例如图 3 所示的图示实例中的域 B 390）的域控制器计算设备 340 正确地签名。如果后端计算设备 230 验证了该服务凭据 370，则其可以继续与中间层计算设备 220 通信，如同该中间层计算设备 220 就是客户端计算设备 210。按照这种方式，中间层计算设备 220 可以代表客户端计算设备 210 从后端计算设备 230 获得信息和资源，并且然后可以响应于由客户端计算设备 210 指向中间层计算设备 220 的请求将该信息和那些资源回呈给客户端计算设备 210。

[0043] 在某些情形下，中间层计算设备 220 在最终能够委托给后端层计算设备（例如后端计算设备 230）之前可能需要与超过两个域中的域控制器计算设备通信。在这种情况下，该域控制器计算设备的操作，并且甚至是整个系统的操作可以按照与上述类似的方式进行。转到图 4，图中所示的系统 400 提供了这种系统以及其中所示的各种元件的操作和通信的一个说明性实例。可以看出，中间层计算设备 220 在试图委托给后端计算设备 230 时，首先可以经由通信 225 联系域控制器计算设备 240，并且该域控制器计算设备 240 可以基于虚线 235 所示的评估来确定后端计算设备 230 并非位于域控制器计算设备 240 的域内，即图 4 的示例性系统 400 中的域 A 290 内。因此，和前面描述的一样，域控制器计算设备 240 可以经由例如通信 315 向中间层计算设备 220 提供到另一域控制器计算设备的权标。然后，还如前所述，中间层计算设备 220 可以经由通信 325 向不同域（即图 4 所示的示例性系统 400 中的域 B 390）中的这种域控制器计算设备 340 提供该权标 320 以及中间层标识符 330。

[0044] 然而，在图 4 的示例性系统 400 中，中间层计算设备 220 设法委托给的后端计算设备 230 不是域 B 390 的一部分。取而代之，在一个实施例中，域 B 390 可以仅仅是“更接近”具有后端计算设备 230 的域，例如图 4 所示示例性系统 400 中的域 C 490。该域 B 390 的域控制器计算设备 340 可能已被域控制器计算设备 240 选定（当发送给它的权标已经生成并被提供给中间层计算设备 220 时），这是因为域控制器计算设备 240 相信域 B 390“更接近”

后端计算设备 230。在一个实施例中，在选择下一域控制器计算设备时，域控制器计算设备 240 至少可以确保所述提名（referral）最终不会回送到自己身上。转回到图 4 的所示系统 400，如图 4 中虚线 335 所示的域控制器计算设备 340 所作出的关于后端计算设备 230 是否位于其域内的确定可以揭示出后端计算设备 230 实际上与域控制器计算设备 340 并非位于相同域，即域 B 390 中。因此，按照与以上参照域控制器计算设备 240 所述类似的方式，域控制器计算设备 340 可以向中间层计算设备 220 提供响应 345，从而将该域控制器计算设备 340 签名的权标提供给中间层计算设备 220，该权标指示中间层计算设备 220 在其与后端计算设备 230 的通信过程中设法充当客户端计算设备 210。如前所述，在一个实施例中，经由通信 345 提供的权标可以指向另一特定的域控制器计算设备，例如域 C 490 中的域控制器计算设备 440。如前面一样，为了区分图 4 所示的域控制器计算设备，图 4 中将使用简写标记“DC3”来参考域控制器计算设备 440。

[0045] 中间层计算设备 220 在从域控制器计算设备 340 接收到通信 345 时可以像前面一样将作为客户端计算设备 210 与后端计算设备 230 通信的请求 425 指向到由该通信 345 指定的其他域控制器计算设备，例如在图 4 所示的示例性系统 400 中为域控制器计算设备 440。该请求 425 可以包括已经通过通信 345 从域控制器计算设备 340 接收的权标 420，以及中间层标识符 430。在一个实施例中，为了获得由域控制器计算设备 340 签名的中间层标识符 430，中间层计算设备 220 可以请求域控制器计算设备 340 基于中间层计算设备 220 作为请求 325 的一部分提供给域控制器计算设备 340 的中间层标识符 330 生成这种标识符 430。如果域控制器计算设备 340 信任该域控制器计算设备 240，则域控制器计算设备 340 可以通过自己签名中间层标识符 330 中先前已经被域控制器计算设备 240 签名的信息来生成中间层标识符 430。和前面一样，在一个实施例中，可以特别将中间层标识符 430 和权标 420 指向到域控制器计算设备 440。

[0046] 然后，该域控制器计算设备 440 可以按照与先前关于域控制器计算设备 240 和域控制器计算设备 340 所述类似的方式继续工作。具体讲，如虚线 435 所示，域控制器计算设备 440 可以验证后端计算设备 230 实际上是否与域控制器计算设备 440 位于相同域内，即图 4 的示例性系统 400 中的域 C 490，这被识别为请求 425 的一部分。在图 4 所示实例中，因为后端计算设备 230 位于与域控制器计算设备 440 相同的域中，所以该域控制器计算设备 440 可以继续参考包括例如后端计算设备 230 建立的策略在内的一个或多个策略以确定后端计算设备 230 是否将允许中间层计算设备 220 委托给它。如前所指示，域控制器计算设备 440 查阅的策略可以参考由中间层计算设备 220 的诸多方面，并且有关这些方面的信息可以包含在中间层计算设备 220 经由通信 425 可提供给域控制器计算设备 440 的中间层标识符 430 中，或者可替代地可以经由域控制器计算设备 440 与中间层计算设备 220 之间结合通信 425 执行的另外的通信交换来提供这样的信息。

[0047] 和前面一样，如果域控制器计算设备 440 确定将允许中间层计算设备 220 委托给后端计算设备 230，则域控制器计算设备 440 可以经由通信 445 将可被域控制器计算设备 440 签名并且可以使得中间层计算设备 220 能够作为客户端计算设备 210 与后端计算设备 230 通信的服务凭据返回中间层计算设备 220。随后，同样如前所述，中间层计算设备 220 可以向后端计算设备 230 发出适当的请求，如通信 455 所示，并且可以包括域控制器计算设备 440 经由通信 445 提供的服务凭据 470。此外，尽管仅跨经一个、两个和三个域进行了图示，

但是本领域技术人员可以理解，本文中所述的机制同样适用于跨经任何数量的域或其他类似分区。

[0048] 转到图 5，图中所示的流程图 500 图示了根据上述机制可由中间层计算设备执行的示例性步骤序列。起初，在步骤 510 处，可以接收指向作为后端层计算设备一部分的信息或资源的客户请求。发出请求的客户端计算设备也可以例如通过提供标识符、权标或者可能已经被域控制器计算设备签名的其他类似信息来认证自己。在步骤 520 处，可以验证所提供的信息，例如通过使用域控制器计算设备的公钥。如果在步骤 520 处认证失败，则所述处理继续到步骤 570，此时可以报错。相关处理可以然后在步骤 580 处结束。

[0049] 然而，可替代地，如果在步骤 520 处客户端认证成功，则在步骤 530 处可以将均能被域控制器计算设备签名的由客户端计算设备提供的信息以及有关中间层计算设备的其他信息连同允许作为客户端计算设备与后端层计算设备通信的请求一起提供给域控制器计算设备。响应于步骤 530 处信息的提供，在步骤 540 处可以接收到可被域控制器签名的服务凭据或者其他类似的信息集合。如果在步骤 540 处接收到所述服务凭据，则所述处理可继续到步骤 550，并且可以将所述服务凭据提供给适当的后端层计算设备，从而代表其请求已在 510 处被接收的客户端计算设备与后端层计算设备建立通信。尽管这种通信可以按照本领域技术人员公知的方式进行，与本说明书相关的处理然后在步骤 580 处结束。然而，如果在步骤 540 处未接收到服务凭据，则所述处理可继续到步骤 560，取代服务凭据，可以接收到权标或者其他信息集合，该权标或信息集合可以将作为客户端计算设备与后端层计算设备通信的请求指向到不同的域控制器计算设备。如果在步骤 560 处接收到所述权标，则所述处理可返回步骤 530，并且可以将请求指向到另一个不同的域控制器计算设备。可替代地，如果在步骤 560 处未接收到权标并且在步骤 540 处未接收到服务凭据，则所述处理继续到步骤 570，可向客户端报告相应错误。按照这种方式，中间层计算设备可以继续请求获得一个或多个域控制器计算设备的允许以与后端层计算设备通信，直到请求到达与后端层计算设备位于相同域中的域控制器计算设备为止，该域控制器计算设备然后作出有关一个或多个相关策略是否指示后端层计算设备将允许中间层计算设备委托给它的决定。

[0050] 参照图 6，图中所示的流程图 600 图示了根据以上详细描述的机制可以由域控制器计算设备执行的示例性步骤序列。起初，在步骤 610 处，可以从中间层计算设备接收到作为客户端计算设备与后端层计算设备通信的请求。然后所述处理可继续到步骤 620，此时可以确定在步骤 610 中接收到的请求中指定的后端层计算设备与执行流程图 600 各个步骤的计算设备是否位于相同的域中。如果在步骤 620 处确定后端层计算设备并非位于相同域中，则所述处理可继续到步骤 660，此时可以生成权标或者其他信息集合，并且将该权标或信息集合传送给步骤 610 中从其接收请求的中间层计算设备。在步骤 660 处生成并传送的权标或者其他信息集合可以包括将中间层计算设备指向到另一域控制器的信息，还可以包括通知该另一域控制器所述中间层计算设备正在设法充当客户端计算设备与后端层计算设备进行通信的信息。此外，如以上详细描述的，在步骤 660 处生成并传送的信息还可以包括可以被域控制器计算设备签名的中间层计算设备的标识，其包括例如各种配置信息。如图所示，相关处理在步骤 670 处结束。

[0051] 可替代地，如果在步骤 620 处确定步骤 610 处接收到的请求所被指向到的后端层计算设备实际上位于相同域内，则所述处理可继续到步骤 630，此时可以对一个或多个策略

进行评估以确定后端层计算设备是否允许发出步骤 610 处接收到的请求的中间层计算设备委托给它。如前所述，可以参照已经被相关后端层计算设备限定并由其提供的一个或多个策略来做出在步骤 630 处的决定。此外，同样如前所述，步骤 630 处的决定可以包括确定请求的中间层计算设备是否符合由相关策略建立的任何因素，包括例如涉及中间层计算设备硬件或软件配置的因素。同样，步骤 630 处的决定可以包括确定中间层计算设备在步骤 610 处提供的信息是否被域控制器计算设备正确签名并且指示中间层计算设备符合相关策略参考的因素。可替代地，同样如前所述，步骤 630 处的确定可以包括为了确定中间层计算设备是否符合相关策略参考的因素而与中间层计算设备进行的其他通信，然而为了便于说明，这些附加的通信并未在图 6 的流程图 600 中具体示出。

[0052] 如果在步骤 630 处确定了允许中间层计算设备委托给后端层计算设备，则所述处理可继续到步骤 640，此时可以生成准许中间层计算设备在客户端计算设备与后端层计算设备的通信中充当该客户端计算设备的服务凭据或其他信息，并且将该服务凭据或信息传送给中间层计算设备。相关处理然后可继续到步骤 670。可替代地，如果在步骤 630 处确定相关策略不允许中间层计算设备委托给后端层计算设备，则所述处理可继续到步骤 650，此时可以向中间层计算设备报错。相关处理然后可以在步骤 670 处结束。

[0053] 通过以上的描述可以看出，提供了一种如由被委托的计算设备来告知一个计算设备要委托给另一计算设备的能力的委托机制。考虑到本文中描述的主题的许多可能的变化，我们要求保护可能落入所附权利要求及其等价物范围内的所有这样的实施例作为我们的发明。

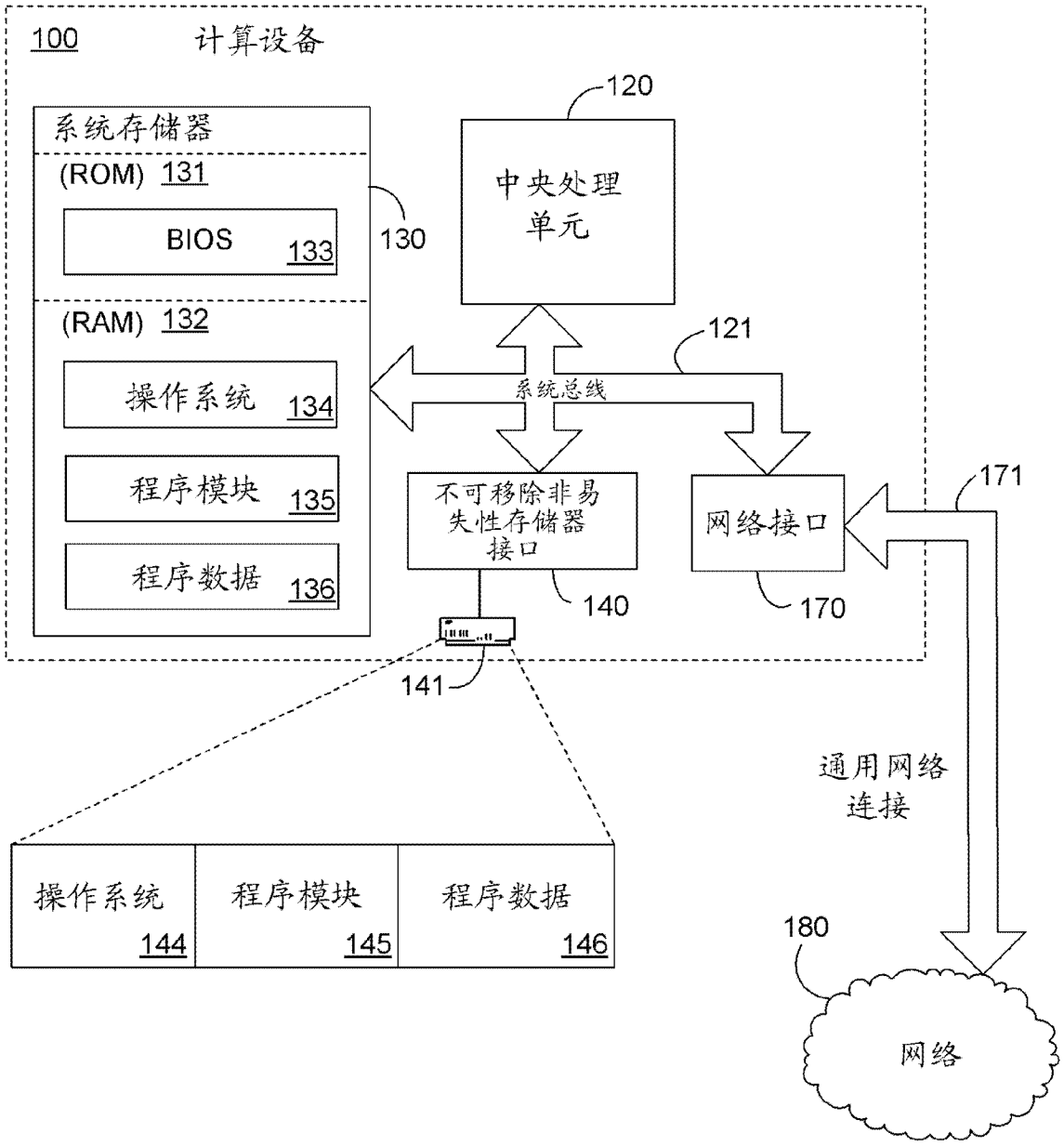

100
计算设备
120
中央处理单元
系统存储器
(ROM) 131
BIOS 133
130
(RAM) 132
操作系统 134
程序模块 135
程序数据 136
121
系统总线
不可移除非易失性存储器接口
140
网络接口
170
171
141
通用网络连接
操作系统 144
程序模块 145
程序数据 146
180
网络

图 1

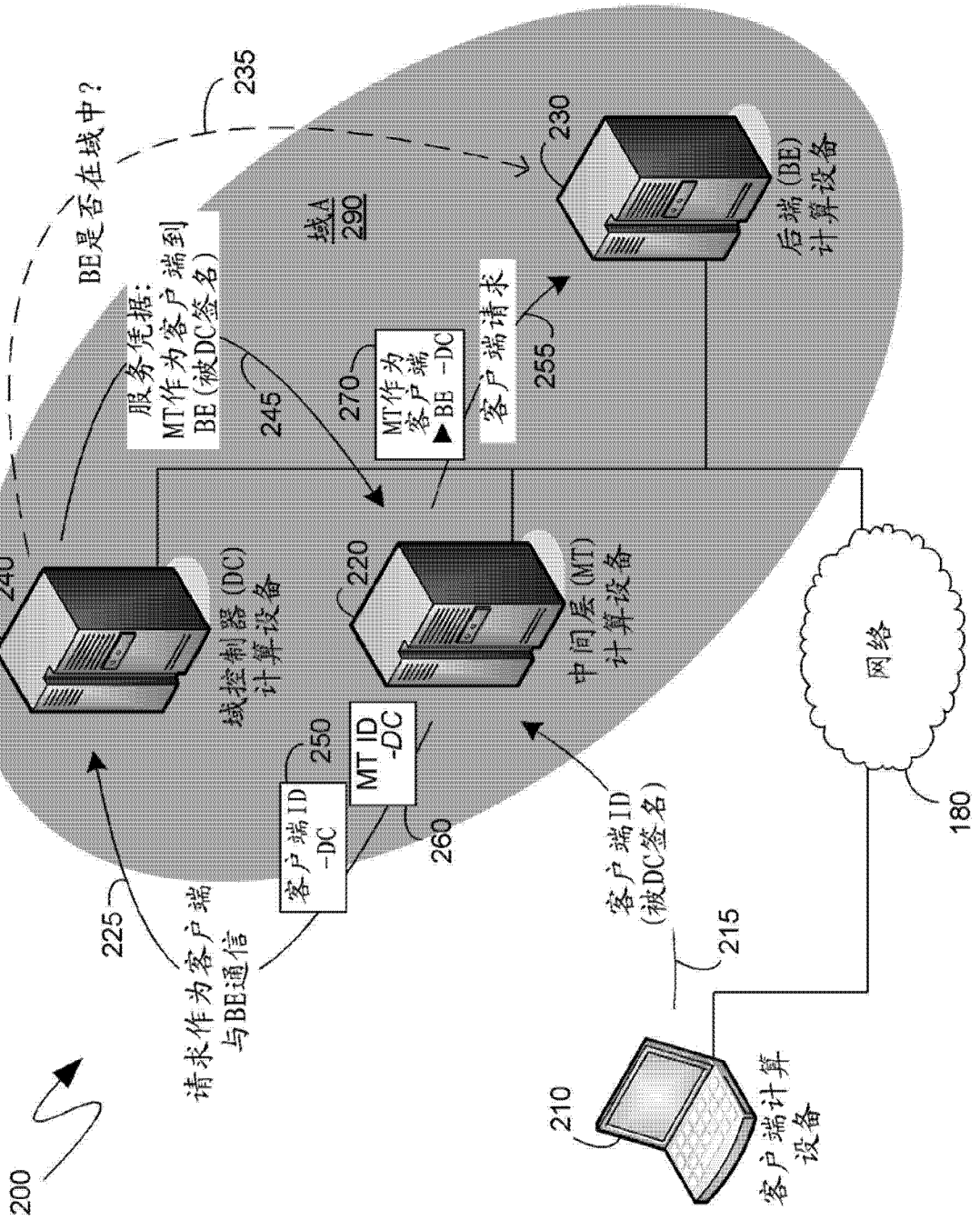

200
请求作为客户端与BE通信
225
客户端ID -DC
250
MT ID -DC
260
客户端ID (被DC签名)
215
210
客户端计算设备
域控制器(DC)计算设备
240
中间层(MT)计算设备
220
网络
180
后端(BE)计算设备
230
域A 290
BE是否在域中?
235
服务凭据: MT作为客户端到BE(被DC签名)
245
MT作为客户端▲BE -DC
270
客户端请求
255

图 2

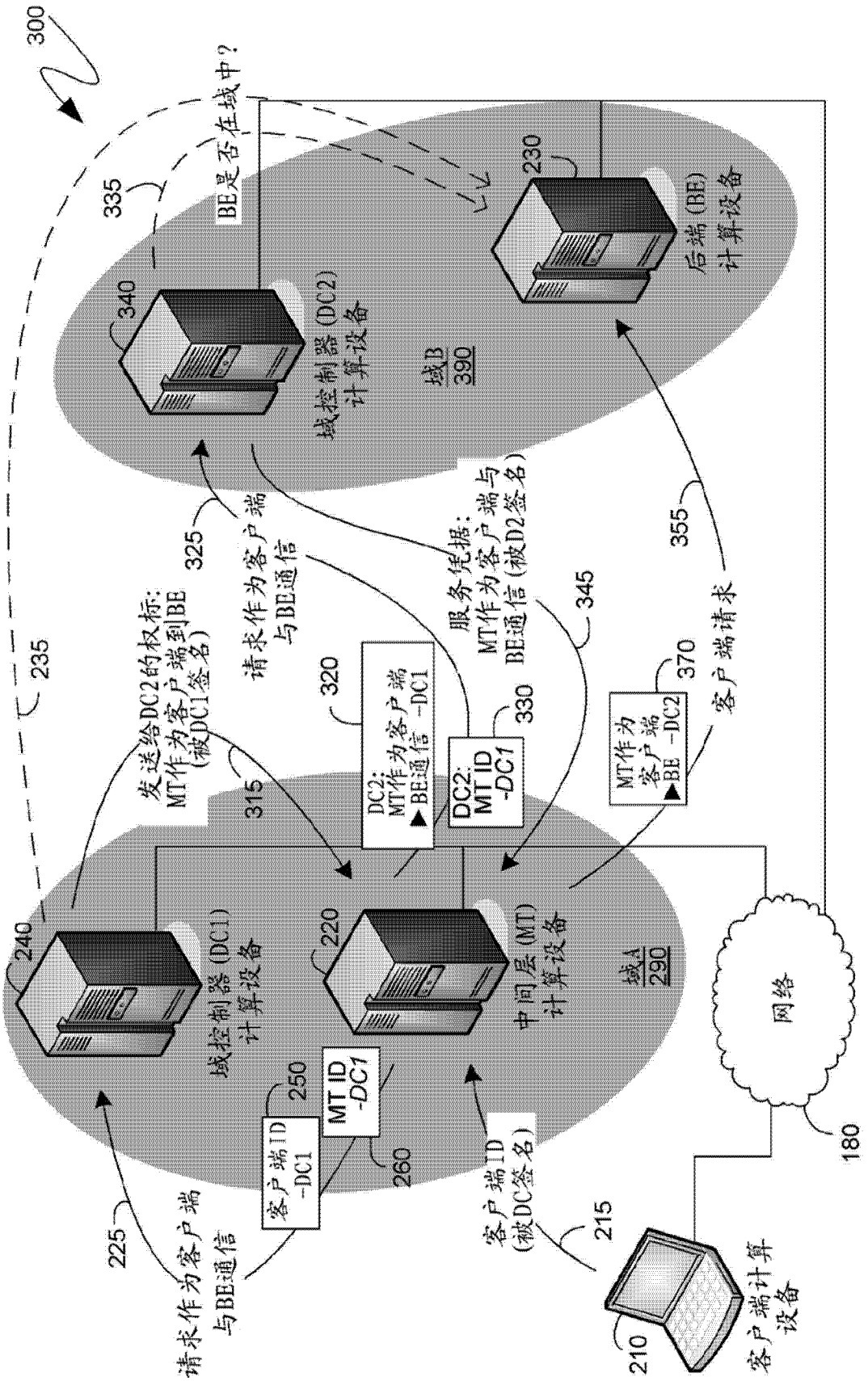

300
BE是否在域中?
335
340
域控制器(DC2)
计算设备
域B
390
230
后端(BE)
计算设备
325
请求作为客户端
与BE通信
355
235
发送给DC2的权标:
MT作为客户端到BE
(被DC1签名)
315
320
DC2:
MT作为客户端
▲BE通信 -DC1
DC2:
MT ID
-DC1
330
服务凭据:
MT作为客户端与
BE通信(被D2签名)
345
MT作为
客户端
▲BE -DC2
370
客户端请求
240
域控制器(DC1)
计算设备
220
中间层(MT)
计算设备
域A
290
网络
250
客户端ID
-DC1
MT ID
-DC1
260
225
请求作为客户端
与BE通信
客户端ID
(被DC签名)
215
180
210
客户端计算
设备

图 3

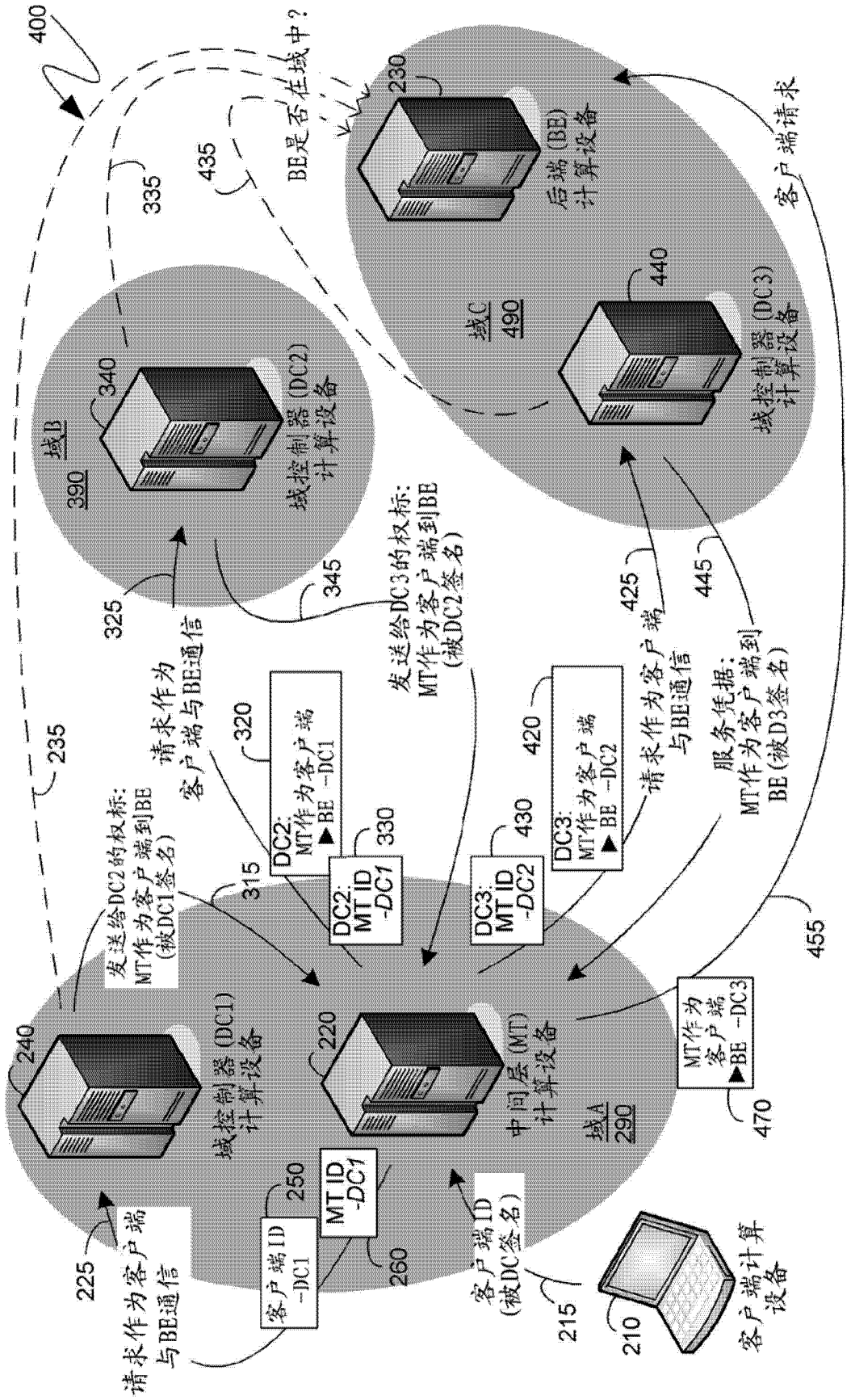

400
BE是否在域中？
435
335
客户端请求
455
域C
490
后端（BE）
计算设备
230
域控制器（DC3）
计算设备
440
域B
390
域控制器（DC2）
计算设备
340
325
345
发送给DC3的权标：
MT作为客户端到BE
（被DC2签名）
425
445
请求作为客户端
与BE通信
服务凭据：
MT作为客户端到
BE（被D3签名）
235
发送给DC2的权标：
MT作为客户端到BE
（被DC1签名）
请求作为
客户端与BE通信
320
DC2：
MT作为客户端
▲BE -DC1
315
DC2：
MT ID
-DC1
330
DC3：
MT ID
-DC2
430
420
DC3：
MT作为客户端
▲BE -DC2
请求作为客户端
与BE通信
域控制器（DC1）
计算设备
240
220
中间层（MT）
计算设备
域A
290
MT作为
客户端
▲BE -DC3
470
225
请求作为客户端
与BE通信
客户端ID
-DC1
250
MT ID
-DC1
260
客户端ID
（被DC签名）
215
210
客户端计算
设备

图 4

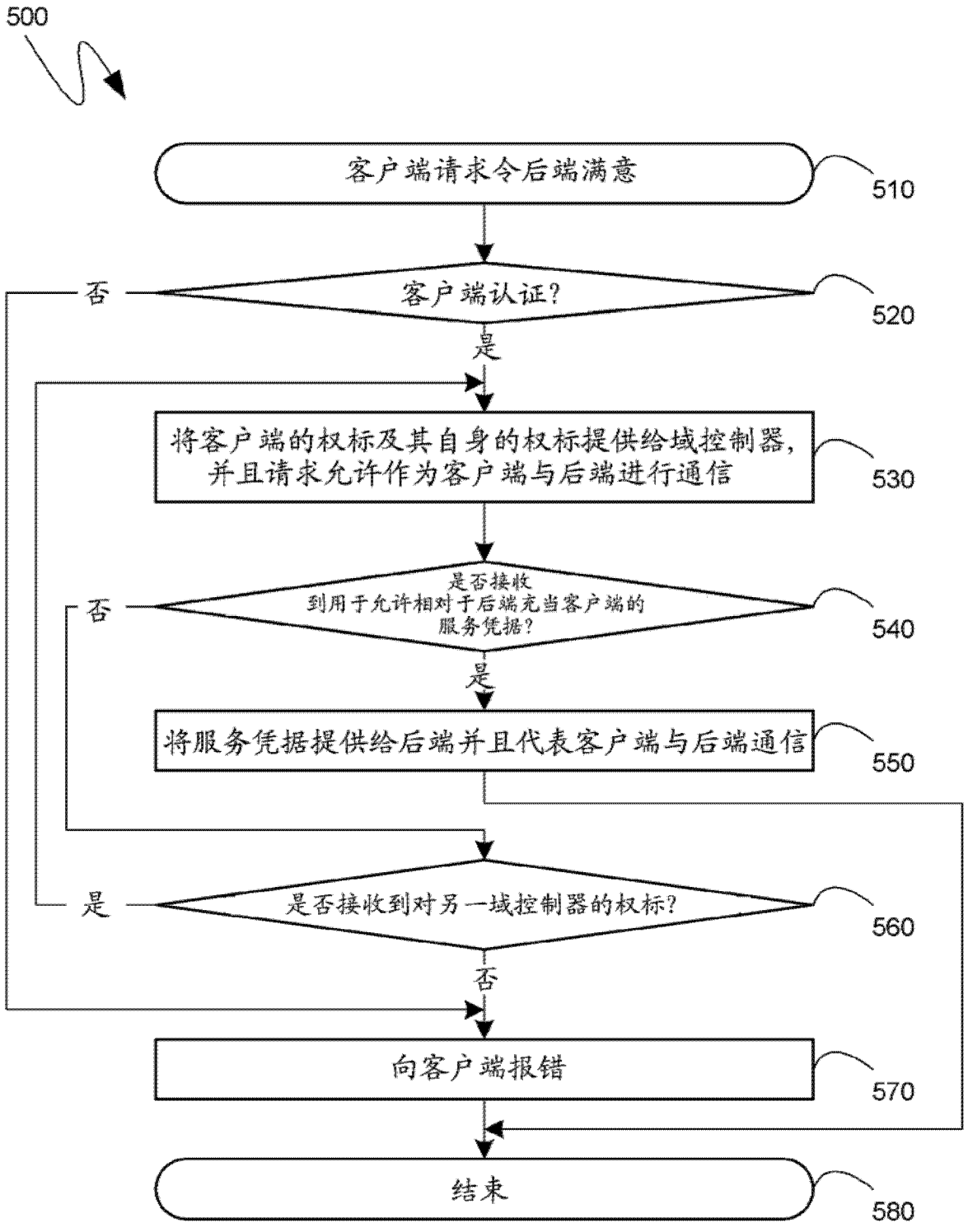

500
客户端请求令后端满意
510
否
客户端认证?
520
是
将客户端的权标及其自身的权标提供给域控制器，并且请求允许作为客户端与后端进行通信
530
否
是否接收到用于允许相对于后端充当客户端的服务凭据?
540
是
将服务凭据提供给后端并且代表客户端与后端通信
550
是
是否接收到对另一域控制器的权标?
560
否
向客户端报错
570
结束
580

图 5

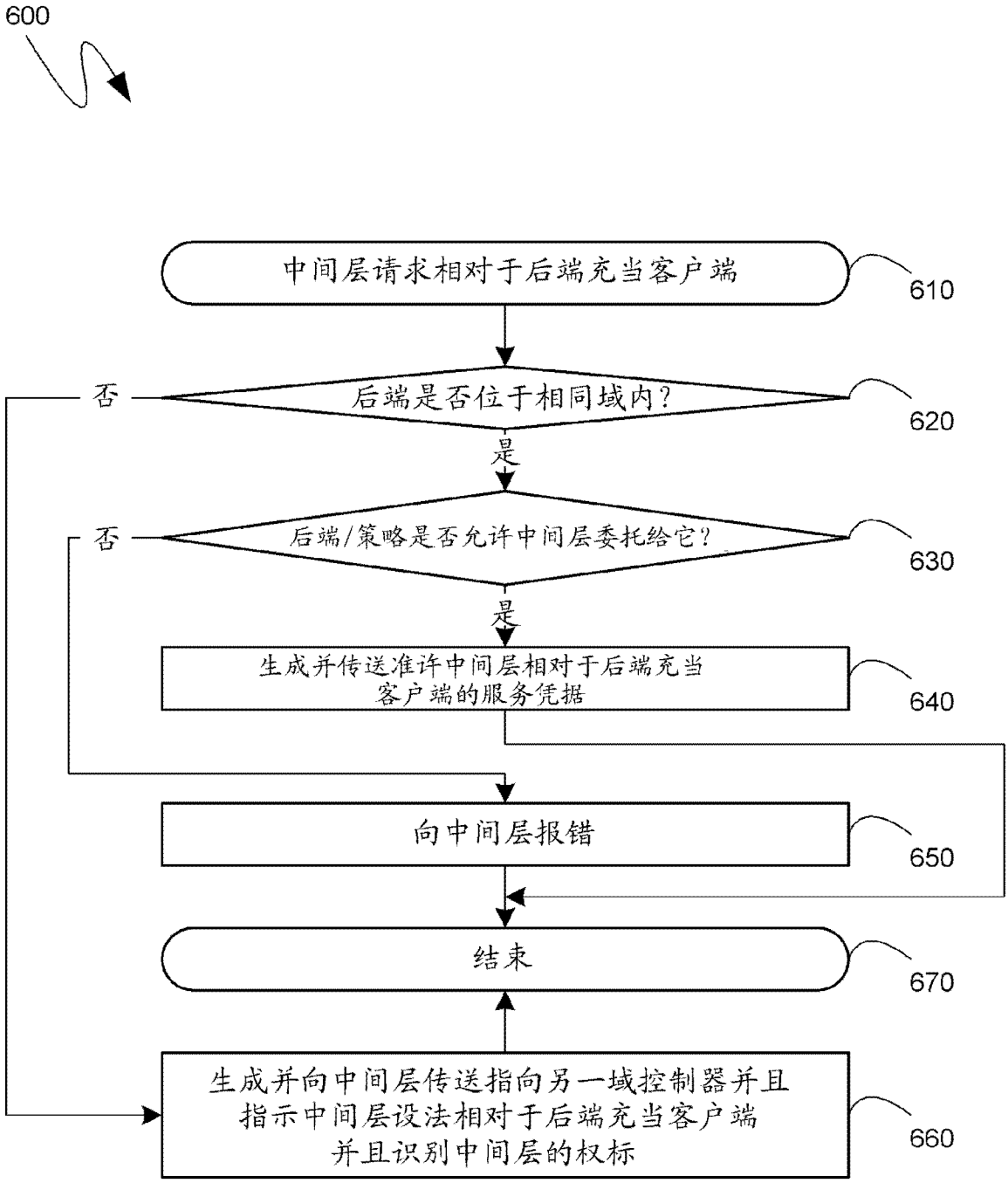

600
中间层请求相对于后端充当客户端
610
后端是否位于相同域内?
否
620
是
后端/策略是否允许中间层委托给它?
否
630
是
生成并传送准许中间层相对于后端充当客户端的服务凭据
640
向中间层报错
650
结束
670
生成并向中间层传送指向另一域控制器并且指示中间层设法相对于后端充当客户端并且识别中间层的权标
660

图 6