(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 107534664 B
(45)授权公告日 2021.06.04

(21)申请号 201680023067.4
(22)申请日 2016.04.28
(65)同一申请的已公布的文献号
申请公布号 CN 107534664 A
(43)申请公布日 2018.01.02
(30)优先权数据
14/699420 2015.04.29 US
(85)PCT国际申请进入国家阶段日
2017.10.20
(86)PCT国际申请的申请数据
PCT/US2016/029728 2016.04.28
(87)PCT国际申请的公布数据
WO2016/176422 EN 2016.11.03

(73)专利权人 慧与发展有限责任合伙企业
地址 美国德克萨斯州
(72)发明人 C.埃斯戴勒
(74)专利代理机构 北京市金杜律师事务所 11256
代理人 王茂华

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/069(2021.01)
(56)对比文件
US 2011247055 A1,2011.10.06
US 2014047510 A1,2014.02.13
审查员 汪婷静

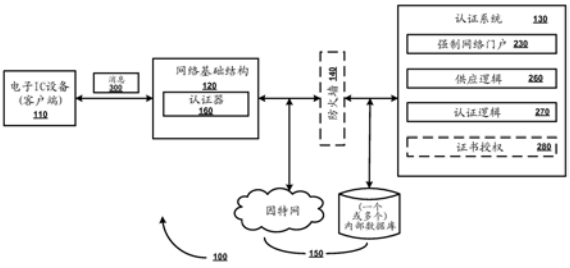
权利要求书2页 说明书10页 附图8页

(54)发明名称

针对使能IEEE 802.1X的网络的多因素授权

(57)摘要

本公开公开了用于提供针对使能IEEE 802.1x的网络的多因素授权的系统和方法。具体地,网络设备经由网络认证协议来认证客户端设备以获得对网络中的网络资源的访问。网络设备然后检测设备隔离触发器,其指示客户端设备的当前用户是未经认证用户的增加的可疑级别。响应于设备隔离触发器,网络设备临时将客户端设备从已认证状态放置到隔离状态直到特定工作流程被当前用户完成。不管先前成功的用户和/或设备认证,客户端设备在隔离状态中时对网络资源具有受限的访问。



CN 107534664 B

1.一种包括指令的非瞬时计算机可读介质,所述指令在由一个或多个硬件处理器执行时引起包括以下各项的操作的执行:

经由网络认证协议来认证客户端设备以获得对网络中的网络资源的访问,其中经由所述网络认证协议认证所述客户端设备包括:

从所述客户端设备接收设备证书,其中在基于从所述客户端设备接收到有效用户凭证而与所述网络的先前的成功用户认证时,所述设备证书已经被发给所述客户端设备;以及

基于所述设备证书的有效性来认证所述客户端设备,以将所述客户端设备放置到已认证状态,而不要求所述设备的用户输入其网络凭证以用于认证;

在所述客户端设备处于所述已认证状态期间,检测设备隔离触发器,其指示客户端设备的当前用户是未经认证用户的增加的可疑级别;以及

响应于设备隔离触发器,临时将客户端设备从所述已认证状态放置到隔离状态直到特定工作流程被当前用户完成,其中不管先前成功的用户和/或设备认证,客户端设备在隔离状态中时对网络资源具有受限的访问。

2.根据权利要求1所述的介质,进一步包括:

发起多因素认证,其要求客户端设备的当前用户完成特定工作流程来确认当前用户的身份。

3.根据权利要求1所述的介质,进一步包括:

响应于由当前用户进行的特定工作流程的完成,将客户端设备从隔离状态放置到已认证状态;以及

响应于由当前用户进行的特定工作流程的失败,将客户端设备从隔离状态放置到未经认证状态,其中客户端设备在未经认证状态中时对网络资源具有受限的访问或不能访问网络资源。

4.根据权利要求1所述的介质,其中网络认证协议遵从IEEE802.1X标准。

5.根据权利要求1所述的介质,其中设备隔离触发器包括预定义时间间隔的流逝。

6.根据权利要求1所述的介质,其中设备隔离触发器包括客户端设备的姿势或地理位置的改变。

7.根据权利要求1所述的介质,其中设备隔离触发器包括阈值数目的连续失败的密码尝试。

8.根据权利要求1所述的介质,其中仅针对网络中的已认证客户端设备的子集发起特定工作流程,并且其中针对子集中的每个已认证客户端设备触发由网络策略定义的特定设备隔离触发器。

9.一种认证系统,包括:

至少一个设备,其包括硬件处理器;

系统被配置成执行包括以下各项的操作:

经由网络认证协议来认证客户端设备以获得对网络中的网络资源的访问,其中认证所述客户端设备包括:

从所述客户端设备接收设备证书,其中在基于从所述客户端设备接收到有效用户凭证而与所述网络的先前的成功用户认证时,所述设备证书已经被发给所述客户端设备;以及

基于所述设备证书的有效性来认证所述客户端设备,以将所述客户端设备放置到已认

证状态，而不要求所述设备的用户输入其网络凭证以用于认证；

在所述客户端设备处于所述已认证状态期间，检测设备隔离触发器，其指示客户端设备的当前用户是未经认证用户的增加的可疑级别；以及

响应于设备隔离触发器，临时将客户端设备从所述已认证状态放置到隔离状态直到特定工作流程被当前用户完成，其中不管先前成功的用户和/或设备认证，客户端设备在隔离状态中时对网络资源具有受限的访问。

10.根据权利要求9所述的系统，进一步包括：

发起多因素认证，其要求客户端设备的当前用户完成特定工作流程来确认当前用户的身份。

11.根据权利要求9所述的系统，进一步包括：

响应于由当前用户进行的特定工作流程的完成，将客户端设备从隔离状态放置到已认证状态；以及

响应于由当前用户进行的特定工作流程的失败，将客户端设备从隔离状态放置到未经认证状态，其中客户端设备在未经认证状态中时对网络资源具有受限的访问或不能访问网络资源。

12.根据权利要求9所述的系统，其中网络认证协议遵从IEEE802.1X标准。

13.根据权利要求9所述的系统，其中设备隔离触发器包括预定义时间间隔的流逝。

14.根据权利要求9所述的系统，其中设备隔离触发器包括客户端设备的姿势或地理位置的改变。

15.根据权利要求9所述的系统，其中设备隔离触发器包括阈值数目的连续失败的密码尝试。

16.根据权利要求9所述的系统，其中仅针对网络中的已认证客户端设备的子集发起特定工作流程，并且其中针对子集中的每个已认证客户端设备触发由网络策略定义的特定设备隔离触发器。

针对使能IEEE 802.1X的网络的多因素授权

技术领域

[0001] 本公开的实施例涉及网络认证。特别地，本公开的实施例描述用于提供针对使能IEEE 802.1x的网络的多因素授权的系统和方法。

背景技术

[0002] 目前，当客户端设备连接到使能IEEE 802.1x的网络或者被供应对使能IEEE 802.1x的网络的访问时，客户端设备将在所有后续认证尝试时透明地连接到该网络。透明访问可经由诸如高速缓存的凭证、设备证书等的技术来递送。例如，先前已经根据IEEE 802.1x协议认证的客户端设备可在不需要任何附加用户输入的情况下向认证服务器呈现设备凭证。

[0003] 然而，不存在使网络基础结构对在客户端设备后面的用户授权的方法。因此，网络访问仅由防止其他用户误用客户端设备和不适当地访问网络资源的本地密码策略来保护。如果非法用户在客户端设备被本地密码锁定之前获得对客户端设备的访问，或者如果非法用户盗取客户端设备的本地密码，则非法用户将能够获得与客户端设备的所有者相同的对网络资源的访问。

[0004] 为了解决上面的忧虑，网络管理员可以配置要求网络用户以频繁间隔改变他们的网络凭证的网络策略。因此，网络基础结构暴露可以被限于密码轮换策略的程度。然而，此类网络策略常常应用于所有网络用户并且对合法的网络用户产生极大的不便和负担。

[0005] 因此，合期望的是在使能IEEE 802.1x的网络中具有附加的安全保护以实现至少两个目的。第一，非法获得对先前认证的客户端设备的占有的用户将不能接收对网络资源的认证。第二，附加的安全保护不会向适当地认证的客户端设备的合法用户添加过度的负担。

[0006] 详细描述

[0007] 在以下描述中，呈现若干具体细节以提供透彻理解。虽然本公开的背景针对网络认证，然而，相关领域中的技术人员将认识到，在本文中公开的概念和技术可以在没有具体细节中的一个或多个的情况下或者结合其他组件等来实践。在其他实例中，未详细地示出或描述公知的实现或操作以避免使在本文中公开的各种示例的各方面模糊。应当理解，本公开涵盖落在本公开的精神和范围内的所有修改、等同和替代。

附图说明

[0008] 通过参考用于说明本公开的实施例的以下描述和随附各图，可以最好地理解本公开。

[0009] 图1是图示根据本公开的实施例的支持IEEE 802.1x认证的示例性网络环境的框图。

[0010] 图2A-2B示出根据本公开的实施例的支持设备凭证供应的示例性网络基础结构。

[0011] 图3是图示根据本公开的实施例的用于在使能IEEE 802.1x的网络中的多因素授

权的示例性网络环境的框图。

[0012] 图4A-4B是图示根据本公开的实施例的涉及在使能IEEE 802.1x的网络中的多因素授权的示例性网络通信交换的序列图。

[0013] 图5是图示根据本公开的实施例的用于在使能IEEE 802.1x的网络中提供多因素授权的过程的流程图。

[0014] 图6是图示根据本公开的实施例的用于在使能IEEE 802.1x的网络中提供多因素授权的系统的框图。

[0015] 概述

[0016] 本公开的实施例涉及网络认证。特别地，本公开的实施例描述用于在使能IEEE 802.1x的网络中提供多因素授权的系统和方法。

[0017] 利用本文中提供的解决方案，网络设备经由网络认证协议来认证客户端设备以获得对网络中的网络资源的访问。网络设备然后检测设备隔离(quarantine)触发器。可以以预定义间隔(例如一周一次、一月一次、一季度一次、一学期一次等)或按需基于客户端设备的当前用户是未经认证用户的增加的可疑级别的指示、或二者的组合来触发设备隔离触发器。响应于设备隔离触发器，网络设备临时将客户端设备从已认证状态放置到隔离状态直到特定工作流程被当前用户完成。不管先前成功的用户和/或设备认证，客户端设备在隔离状态中时对网络资源具有受限的访问。

[0018] 接下来，网络设备发起多因素认证，其要求客户端设备的当前用户完成特定工作流程来确认当前用户的身份。响应于由当前用户进行的特定工作流程的完成，网络设备将客户端设备从隔离状态放置到已认证状态。响应于由当前用户进行的特定工作流程的失败，网络设备将客户端设备从隔离状态放置到未经认证状态。客户端设备在未经认证状态中时对网络资源具有受限的访问或不能访问网络资源。

[0019] 在一些实施例中，仅针对网络中的已认证客户端设备的子集发起特定工作流程。此外，针对子集中的每个已认证客户端设备触发由网络策略定义的特定设备隔离触发器。

[0020] 客户端设备凭证供应

[0021] 图1是图示根据本公开的实施例的支持IEEE 802.1x认证的示例性网络环境的框图。图2A-2B示出根据本公开的实施例的支持设备凭证供应的示例性网络基础结构。

[0022] 根据本公开的该实施例，网络100是具有根据标题为“基于端口的网络访问控制”(2010)的电气与电子工程师协会(IEEE)802.1X的基于端口的网络访问控制的局域网(LAN)。此类访问控制被适配成提供防备电子设备获得对各种网络资源150(例如因特网、内部数据库等)的未授权访问的安全性。

[0023] 更具体地，根据IEEE 802.1X标准的认证包含在(i)设法加入网络100的电子设备(例如客户端设备110)与(ii)形成网络100的某些组件(即网络基础结构120和认证系统130)之间的通信。如所示的，可以安置可选的防火墙140以使认证系统130与可公开访问的服务隔离。然而，将不关于下面描述的操作流程讨论防火墙140。

[0024] 如所图示的，网络基础结构120是被适配成支持认证系统130和客户端设备110之间的通信的电子设备的集合。此外，网络基础结构120被适配成最初限制对网络资源150的访问直到客户端设备110的身份已经被认证。规划网络基础结构120的组件可依赖所选的网络架构而变化。

[0025] 例如，如在网络100是无线局域网(WLAN)的图2A中所示的，网络基础结构120包括通过互连220耦合至控制器210的接入点(AP)200。在本文中，AP 200被配置成与例如在其覆盖范围区内的无线电子设备(诸如客户端设备110)建立通信。控制器210被配置成监视由AP 200从客户端设备110接收的消息并且确定要将什么“角色”分配给客户端设备110。换言之，控制器210向客户端设备110分配具体角色(例如网络访问级别)，其可部分或完全地限制客户端设备110对网络资源150的访问直到客户端设备110的身份已经被认证。作为示例，控制器210可通过将某些消息从客户端设备110重定向到认证系统130支持的强制网络门户实例230来限制对网络资源150的访问。

[0026] 替代地，如在网络100是支持与客户端设备110的有线连通性的局域网(LAN)的图2B中所示的，网络基础结构120包括一个或多个数据传送设备，诸如可管理的交换机240(例如802.1X交换机)和路由器250，它们也为客户端设备110确定特定角色。在客户端设备110第一次尝试加入网络100的情况下，可管理的交换机240将客户端设备110分配到供应角色，其可触发某些消息从客户端110到强制网络门户实例230的重定向直到客户端设备110的身份已经被认证。

[0027] 参考回图1，在已经与客户端设备110建立通信路径之后，网络基础结构120内的电子设备，诸如控制器210或交换机/路由器240和250(在下文中一般被称为“认证器”160)，可执行设备指纹识别。“设备指纹识别”包含监视由客户端设备110传输的初始消息以确定客户端设备110是否先前已被认证。

[0028] 一个类型的“设备指纹识别”包含分析DHCP发现消息的DHCP选项字段内的内容。客户端设备110在为了获得用于在网络100上使用的因特网协议(IP)地址的努力中广播DHCP发现消息。在许多情况下，DHCP选项字段内的内容暗示设备的类型，其可帮助认证器160确定客户端设备110是否应该被放置到供应角色中。

[0029] 更具体地，如果认证器160因为设备类型不可辨认而不能够识别客户端设备110的身份，则客户端设备110被放置到供应角色中，这限制其对网络资源150的访问并且在一些情况下可能因为针对对网络资源150的访问的后续请求而触发与强制网络门户实例230的通信。

[0030] 另一个类型的“设备指纹识别”可以包含认证器160获得对客户端设备110的媒体访问控制(MAC)地址的访问。这可通过从源自客户端设备110的信令提取源MAC地址来完成。将控制设备110的MAC地址与针对先前已认证的设备存储的MAC地址相比较。如果客户端设备110的MAC地址未能匹配所存储的MAC地址中的任何MAC地址，则认证器160将客户端设备110放置到供应角色中。

[0031] 设想针对先前认证的客户端设备存储的MAC地址可被包含在MAC表内，所述MAC表被以由网络管理员选择的周期性来更新。因此，如果在预定的时间段内不存在来自客户端设备中的一个的活动，则从MAC表移除该设备的MAC地址。

[0032] 又一类型的“设备指纹识别”可以包含认证器160比较在客户端设备110和认证系统130之间的初始消息交换期间提供的用户名。可将由控制设备110提供的用户名与被先前认证的电子设备使用并存储在网络基础结构120和/或认证系统130内的有效用户名相比较。

[0033] 一旦客户端设备110已被分配供应角色，即设备基本上被限制(或阻止)访问网络

资源150，认证器160就可以将来自设备110的任何消息重定向到位于认证系统130中的强制网络门户实例230。经重定向的消息用于客户端设备110还没有被认证的那些情况，其在一些情况下可能是由于缺少向客户端设备110供应唯一设备凭证。

[0034] 作为说明性示例，响应于来自被放置于供应角色中的客户端设备110的消息300(例如HTTP 得到请求消息)，认证器160将该消息重定向到由认证系统130提供的强制网络门户实例230。认证系统130内的供应逻辑260分析该消息以确定客户端设备110的类型并且推断其能力。

[0035] 多因素授权

[0036] A.客户端设备管理(Onboarding)过程。

[0037] 图3是图示根据本公开的实施例的用于在使能IEEE 802.1x的网络中的多因素授权的示例性网络环境的框图。图3至少包括客户端设备320、多个接入点(诸如AP 330、AP 332、AP 334……)、网络控制器340和认证服务器350。

[0038] 每个AP(例如AP 330、AP 332、AP 334……)向零个或更多客户端设备提供网络服务。具体地，每个AP在特定无线通信信道上操作并且在该特定无线通信信道上与其客户端设备通信。

[0039] 网络控制器340一般指的是管理其他网络设备(诸如无线接入点)的控制设备。网络控制器340可以操纵对射频功率、无线信道、无线认证、和/或安全性的自动调整。

[0040] 客户端设备320可与企业用户或访客用户相关联。网络管理员可以配置为企业用户准许与访客用户不同的对网络资源的访问的网络策略。

[0041] 认证服务器350一般提供应用用来认证凭证的网络服务，所述凭证诸如用户名和密码。当客户端设备(例如客户端设备320)提交凭证的有效集合时，它接收到它随后可以用来访问各种服务的密码证书380。认证通常被用作授权、隐私性以及不可否认性的基础，所述授权是是否可向特定用户或过程准许特权的确定，所述隐私性使信息免于变得为非参与者所知。

[0042] 在一些实施例中，认证服务器350是远程认证拨入用户服务(RADIUS)。RADIUS一般指的是在传输时使用UDP在应用层中运行的客户端/服务器协议。RADIUS常常用作遵从IEEE 802.1X协议的认证过程的后端。

[0043] 例如，当客户端设备320最初尝试访问网络资源时，客户端设备320向网络发送请求。该请求可被AP 320接收，该AP 320将其转发给网络控制器340。网络控制器340确定客户端设备320还没有被网络所认证，并且因此将客户端设备320重定向到认证门户360，所述认证门户360是web浏览器中提示的网站，以使得客户端设备320的用户可以输入他/她的网络凭证(诸如，用户名370和密码375)来用于认证。用户输入然后被发送给认证服务器350，所述认证服务器350查找其认证数据库并且决定向用户准许或拒绝网络访问。如果认证服务器350决定向客户端设备320的用户准许网络访问，则认证服务器350将向客户端设备320发出证书380。在对网络的后续请求中，客户端设备320将呈现接收到的证书380以使得网络控制器340将不会在客户端设备320的初始认证之后使客户端设备320重定向到认证网站(例如强制网络门户360)。

[0044] 在一些实施例中，当客户端设备320的用户呈现用于网络授权的用户名和密码凭证时，网络认证系统将识别到用户正使用弱的认证机制，并且因此将使用户重定向到安全

web认证门户360，在那里客户端设备320的用户被询问用户名370和密码375。在网络认证系统接收到有效用户凭证时，证书380将被发给客户端设备320。证书380可以被本地安装在客户端设备320上并且随着后续网络请求呈现给网络。此外，可以在客户端设备320被盗取的用户报告中撤销证书380。

[0045] B.多因素认证(MFA)。

[0046] 多因素认证(MFA)一般指的是计算机访问控制，其中用户可能经由成功地呈现若干个分离的认证阶段而通过。该多个因素包括但不限于知识因素、占有因素、内在因素等。知识因素要求用户证明他/她的秘密的知识以便认证例如密码、个人标识号(PIN)、一个或多个秘密的问题等。

[0047] 占有因素要求用户证明对体现秘密的密钥的占有。例如，可以使用不具有到客户端设备的连接的断开的令牌来动态地生成令牌。用户将在显示器中查看断开的令牌并且在多因素认证页面390中手动输入作为附加认证信息395的令牌。在一些实施例中，连接的令牌可以被物理连接到客户端设备并且自动地传输数据。连接的令牌包括多个不同的类型，包括但不限于卡读取器、无线标签和USB令牌。

[0048] 内在因素一般指的是与用户相关联的因素。内在因素通常包含生物特征认证，例如指纹读取器、视网膜扫描仪、语音识别等。

[0049] 常规地，MFA被用在web服务器认证中而不是与网络认证无缝整合的透明过程中。MFA与网络认证的简单组合要求利用每个网络认证请求来完成多因素认证工作流程。尽管该方法增加了安全级别，但是它向网络中客户端设备的用户提出了一个重要的可用性问题。根据本公开的实施例，网络仅向已认证客户端设备的由于违反由网络管理员定义的各种安全策略而被认为可疑的子集选择性地触发MFA。

[0050] C.具有周期性的MFA的两层认证架构。

[0051] 图4A-4B是图示涉及在使能IEEE 802.1x的网络中的多因素授权的示例性网络通信交换的序列图。图4A-4B至少包括在网络中互连的客户端设备400、AP 405、网络控制器410和认证服务器415。如下面更详细解释的，在该过程期间，已经经由IEEE 802.1x网络认证协议通过或者用户名和密码或者有效的设备证书成功地认证了客户端设备400。然而，当网络检测特定触发器时，将客户端设备400从已认证状态放置到隔离状态。客户端设备400的当前用户然后被要求完成特定工作流程以验证他/她的身份。

[0052] 此后，如果当前用户已完成该特定工作流程，则认证服务器415将会将客户端设备400从隔离状态放回到已认证状态。另一方面，如果当前用户未能完成该特定工作流程，则认证服务器415将会将客户端设备400从隔离状态放回到未经认证状态，尽管客户端设备400正在呈现用于网络访问的有效凭证和/或设备证书。

[0053] 具体地，在时间点t1处，客户端设备400最初被放置于未经认证状态420中。然后，在时间点t2处，客户端设备400将其凭证信息430发送给AP 405，所述AP 405将凭证信息430转发给网络控制器410。网络控制器410然后将会将凭证信息430转发给后端认证服务器415。特别地，网络控制器410可能通过将用户重定向到与认证服务器415相关联的认证门户来这么做，在所述认证门户处用户可以输入凭证信息430。在接收到凭证信息430时，认证服务器415将执行认证过程。如果被成功认证，则客户端设备400被发设备证书435。在时间点t3处，认证服务器415将用于客户端设备400的设备证书435发送给网络控制器410，所述网

络控制器410经由AP 405将该设备证书435转发给客户端设备400。在时间点t4处，客户端设备400接收设备证书435。在时间点t5处，用户将设备证书435安装在客户端设备400上并且此后客户端设备400与认证服务器415一起重新开始设备管理过程并且在呈现新安装的设备证书435以及成功认证时过渡到已认证状态425。

[0054] 认证服务器415可能周期性地要求被放置于已认证状态425中的客户端设备400利用设备证书440执行自动重新认证。具体地，客户端设备400将被要求向网络呈现有效的设备证书以便保持在已认证状态425中。这些通信改变可以发生不利用设备用户的知识的后台过程中。

[0055] 在一些实施例中，在时间点t7处，网络基础结构可以向认证服务器415通知一个或多个设备隔离触发器445被检测。因此，客户端设备400被立即放置于隔离状态428中。此后，在客户端设备400处于隔离状态428中的时间段期间，客户端设备400对网络资源的访问被临时暂停或限制。值得注意的是，即使客户端设备400拥有有效的设备证书并且将设备证书呈现给网络，其对网络资源的访问也仍被暂停或限制。在一些实施例中，可以以固定间隔(例如每周一次、每月一次、每季度一次、每学期一次等)来触发该设备隔离触发器445。在一些实施例中，网络可能检测到客户端设备400的姿势或地理位置已改变，这提升了客户端设备400的当前用户的可疑级别。因此，网络激活设备隔离触发器445。在一些实施例中，网络的策略引擎可能检测到几个连续失败的密码认证尝试。因此，网络将激活设备隔离触发器445。

[0056] 此类设备隔离触发器445也将触发多因素认证过程450。因此，在时间点t9处，认证服务器415向网络发送多因素认证请求450。客户端设备400在时间点t10处接收多因素认证请求450。要注意，这也可以通过将客户端设备400的用户重定向到用于附加认证信息的用户输入的多因素认证web页面来完成。例如，在时间点t11处，可向客户端设备400的用户呈现指令以遵循指定的工作流程455以便获得用于将客户端设备400从隔离状态428释放所必需的附加认证信息。

[0057] 工作流程455被设计成验证客户端设备400的当前用户的身份。它可以结合用于用户标识的任何现有的或新的技术。例如，在一些实施例中，可能要求用户以回答一组问题。在一些实施例中，可能要求用户执行一系列任务来取回令牌。在一些实施例中，可能要求用户向某一位置或人(例如接待处或IT帮助台)报告以用于身份验证。

[0058] 在时间点t12处，客户端设备400获取附加授权信息460并且将其传输给AP 405。AP 405将附加授权信息460转发给网络控制器410，所述网络控制器410将其转发给认证服务器415。

[0059] 在时间点t13处，基于从客户端设备400接收到的附加授权信息460，认证服务器415确定是准许还是拒绝由客户端设备400进行的网络访问。例如，在图4A中，认证服务器415确定附加授权信息460足够允许客户端设备400的当前用户的标识，并且因此向客户端设备400准许访问。具体地，认证服务器415可以经由网络控制器410和AP 405向客户端设备400传输访问准许消息。而且，认证服务器415将会将客户端设备400从隔离状态428放置回到已认证状态425。此后，利用先前由认证服务器415发给客户端设备400的有效的设备证书，客户端设备400将继续能够访问网络资源。

[0060] 在如图4B中图示的另一示例中，认证服务器415确定附加授权信息460未能标识客

户端设备400的合法用户，并且因此向客户端设备400拒绝访问。具体地，认证服务器415可以经由网络控制器410和AP 405将访问拒绝消息传输给客户端设备400。而且，认证服务器415将会将客户端设备400从隔离状态428放置到未经认证状态420。此后，客户端设备400将不再具有对网络资源的任何访问，即使客户端设备400已经安装有先前由认证服务器415发出的有效的设备证书。

[0061] 用于在使能IEEE 802.1x的网络中提供多因素授权的过程

[0062] 图5图示根据本公开的实施例的用于在使能IEEE 802.1x的网络中提供多因素授权的示例性过程。在操作期间，网络设备确定已认证客户端设备满足用于设备隔离触发器的准则(操作500)。设备隔离触发器指示客户端设备的当前用户是未经认证用户的增加的可疑级别。

[0063] 在一些实施例中，设备隔离触发器包括预定义时间间隔的流逝。在一些实施例中，设备隔离触发器包括客户端设备的姿势或地理位置的改变。在一些实施例中，设备隔离触发器包括阈值数目的连续失败的密码尝试。

[0064] 接下来，网络设备将已认证客户端设备放置于隔离状态中并且暂停由已认证客户端设备进行的网络资源访问(操作520)。在这里，网络设备仅临时将客户端设备从已认证状态放置到隔离状态，直到特定工作流程被当前用户完成。当在隔离状态中时，不管先前成功的用户和/或设备认证，客户端设备对网络资源具有受限的访问。

[0065] 然后，网络设备发起要求被隔离的客户端设备用户完成工作流程来确认用户身份的多因素认证过程(操作540)。在一些实施例中，仅针对网络中的已认证客户端设备的子集发起特定工作流程。此外，针对该子集中的每个已认证客户端设备触发由网络策略定义的特定设备隔离触发器。

[0066] 此后，网络设备确定工作流程是否被成功地完成(操作560)。响应于工作流程未被成功地完成，网络设备例如通过将客户端设备从隔离状态放置到未经认证状态来向被隔离的客户端设备拒绝网络资源访问(操作580)。客户端设备在未经认证状态中时对网络资源具有受限的访问或不能访问网络资源。响应于工作流程被成功完成，网络设备例如通过将客户端设备从隔离状态放置到已认证状态来向被隔离的客户端设备准许网络资源访问(操作590)。

[0067] 在一些实施例中，网络设备经由网络认证协议认证客户端设备以获得对网络中的网络资源的访问。网络认证协议可能遵从IEEE 802.1X标准。在一个实施例中，网络设备从客户端设备接收用户凭证信息，并且基于用户凭证信息的有效性来认证客户端设备。在另一实施例中，网络设备从客户端设备接收设备证书，并且基于设备证书的有效性来认证客户端设备。已经在先前的成功认证时将设备证书发给客户端设备。

[0068] 用于在使能IEEE 802.1x的网络中提供多因素授权的系统

[0069] 图6是图示根据本公开的实施例的用于在使能IEEE 802.1x的网络中提供多因素授权的示例性系统的框图。网络设备600至少包括能够或者传输或者接收无线电信号或二者的一个或多个无线电天线610、能够与有线或无线网络通信的网络接口620、能够处理计算指令的处理器630，以及能够存储指令和数据的存储器640。此外，网络设备600进一步包括接收机构650、传输机构660、确定机构670和认证机构680，它们都与网络设备600中的处理器630和/或存储器640通信。网络设备600可以用作客户端系统或服务器系统，或者可以

用作分布式或云计算环境中的客户端和服务器二者。

[0070] 无线电天线610可以是用于接收信令的已知或常规电气组件的任何组合，所述已知或常规电气组件包括但不限于晶体管、电容器、电阻器、复用器、布线、寄存器、二极管或者已知或以后变得已知的任何其他电气组件。

[0071] 网络接口620可以是任何通信接口，其包括但不限于调制解调器、令牌环接口、以太网接口、无线IEEE 802.11接口、蜂窝无线接口、卫星传输接口或者用于耦合网络设备的任何其他接口。

[0072] 处理器630可以包括一个或多个微处理器和/或网络处理器。存储器640可以包括存储组件，诸如动态随机存取存储器(DRAM)、静态随机存取存储器(SRAM)等。特别地，响应于确定机构670确定(1)客户端设备已被认证以访问访客无线网络以及(2)客户端设备位于到特定接入点的紧密物理接近度内二者，存储器640将存储指示客户端设备何时存在认证区的时间戳。

[0073] 接收机构650一般经由网络接口620或无线电天线610从无线客户端接收一个或多个网络消息。所接收的网络消息可以包括但不限于请求和/或响应、信标帧、管理帧、控制路径帧等。具体地，接收机构650可从客户端设备接收用户凭证信息和/或设备证书。

[0074] 传输机构660一般传输消息，其包括但不限于请求和/或响应、信标帧、管理帧、控制路径帧等。

[0075] 确定机构670一般确定已认证客户端设备满足用于设备隔离触发器的准则。设备隔离触发器通常指示客户端设备的当前用户是未经认证用户的增加的可疑级别。

[0076] 在一些实施例中，设备隔离触发器包括预定义时间间隔的流逝。在一些实施例中，设备隔离触发器包括客户端设备的姿势或地理位置的改变。在一些实施例中，设备隔离触发器包括阈值数目的连续失败的密码尝试。

[0077] 认证机构680一般针对无线网络访问来对客户端设备进行认证和/或解除认证。具体地，认证机构680可以经由网络认证协议来认证客户端设备以获得对网络中的网络资源的访问。网络认证协议遵从IEEE 802.1X标准。

[0078] 在一些实施例中，当接收机构650从客户端设备接收到用户凭证信息时，认证机构680基于用户凭证信息的有效性来认证客户端设备。

[0079] 在一些实施例中，当接收机构650从客户端设备接收到设备证书时，认证机构680基于设备证书的有效性来认证客户端设备。在这里，已经在先前的成功认证时将设备证书发给客户端设备。

[0080] 在一些实施例中，响应于确定机构670确定客户端设备满足用于设备隔离触发器的准则，认证机构680临时将客户端设备从已认证状态放置到隔离状态直到特定工作流程被当前用户完成。当在隔离状态中时，不管先前成功的用户和/或设备认证客户端设备都对网络资源具有受限的访问。

[0081] 在一些实施例中，认证机构680发起多因素认证，其要求客户端设备的当前用户完成特定工作流程来确认当前用户的身份。响应于由当前用户进行的特定工作流程的完成，认证机构680将客户端设备从隔离状态放置到已认证状态。响应于由当前用户进行的特定工作流程的失败，认证机构680将客户端设备从隔离状态放置到未经认证状态。客户端设备在未经认证状态中时对网络资源具有受限的访问或不能访问网络资源。

[0082] 在一些实施例中，仅针对网络中的已认证客户端设备的子集发起特定工作流程。此外，针对该子集中的每个已认证客户端设备触发由网络策略定义的特定设备隔离触发器。

[0083] 本公开可以以硬件、软件或者硬件和软件的组合来实现。本公开可以以集中式方式实现在一个计算机系统中，或者以分布式方式实现，其中不同元件跨耦合到网络的若干互连的计算机系统散布。硬件和软件的典型组合可以是具有计算机程序的接入点，所述计算机程序在经加载和执行时控制设备使得它实现本文中描述的方法。

[0084] 本公开还可以以非瞬时方式体现在计算机可读存储介质(例如，可编程电路；半导体存储器，诸如易失性存储器，诸如随机存取存储器“RAM”，或者非易失性存储器，诸如只读存储器、电力支持的RAM、闪存、相变存储器等；硬盘驱动器；光盘驱动器；或者用于接收便携式存储器设备的任何连接器，诸如通用串行总线“USB”闪速驱动器)中，所述计算机可读存储介质包括使能实现本文中描述的方法的所有特征，并且其在加载于计算机系统中时能够实现这些方法。在目前的上下文中，计算机程序意味着指令集的以任何语言、代码或记法的任何表达，所述指令集意图使得具有信息处理能力的系统或者直接地或者在以下中的任一个或二者之后执行特定功能：a)转换成另一个语言、代码或记法；b)以不同的材料形式的再现。

[0085] 如本文中使用的，“网络设备”一般包括被适配成传输和/或接收信令并且处理这样的信令内的信息的设备，诸如站(例如，任何数据处理装置，诸如计算机、蜂窝电话、个人数字助理、平板设备等)、接入点、数据传输设备(诸如网络交换机、路由器、控制器等)等。

[0086] 如本文中使用的，“接入点”(AP)一般指的是用于任何已知或者可能以后变得已知的便捷无线接入技术的接收点。具体地，术语AP不意图限于基于IEEE 802.11的AP。AP一般作为电子设备起作用，所述电子设备被适配成允许无线设备经由各种通信标准连接到有线网络。

[0087] 如本文中使用的，术语“互连”或者描述性地用作“被互连”的术语一般被定义为通过信息承载介质所建立的通信路径。“互连”可以是有线互连，其中介质是物理介质(例如，电线、光纤、电缆、总线迹线等)，无线互连(例如，结合无线信令技术的空气)或者这些技术的组合。

[0088] 如本文中使用的，“信息”一般被定义为数据、地址、控制、管理(例如，统计)或其任何组合。对于传输而言，信息可以作为消息来传输，所述消息即以预定格式的位的集合。一个类型的消息，即无线消息，包括具有预定数目的信息位的报头和净荷数据。无线消息可以被放置于如一个或多个分组、帧或信元的格式中。

[0089] 如本文中使用的，“无线局域网”(WLAN)一般指的是通信网络，所述通信网络通过如下来链接两个或更多设备：使用一些无线分发方法(例如，扩频或者正交频分复用无线电)；并且通常通过接入点提供到因特网的连接；并且因此，为用户提供在本地覆盖区域内四处移动且仍然保持连接到网络的移动性。

[0090] 如本文中使用的，术语“机构”一般指的是提供一个或多个功能的系统或设备的组件，包括但不限于软件组件、电子组件、电气组件、机械组件、机电组件等。

[0091] 如本文中使用的，术语“实施例”一般指的是用来作为示例而非限制进行说明的实施例。

[0092] 本领域技术人员将领会到，前述示例和实施例是对本公开的范围而言是示例性的而非限制性的。意图在阅读说明书和研究各图时对本领域技术人员显而易见的对其的所有置换、增强、等同和改进都包括在本公开的真实精神和范围内。因此意图以下所附权利要求书包括如落在本公开的真实精神和范围内的所有这样的修改、置换和等同。

[0093] 虽然已经根据各种实施例描述了本公开，但是本公开不应当被限于仅所描述的那些实施例，而是可以在随附权利要求书的精神和范围内以修改和更改来实践。同样地，在本公开中对标准做出引用的情况下，引用一般是对如可适用于所公开的技术领域的标准的当前版本做出的。然而，在说明书和随附权利要求书的精神和范围内，所描述的实施例可以在标准的后续发展下实践。说明书因此要视为说明性的而非限制性的。

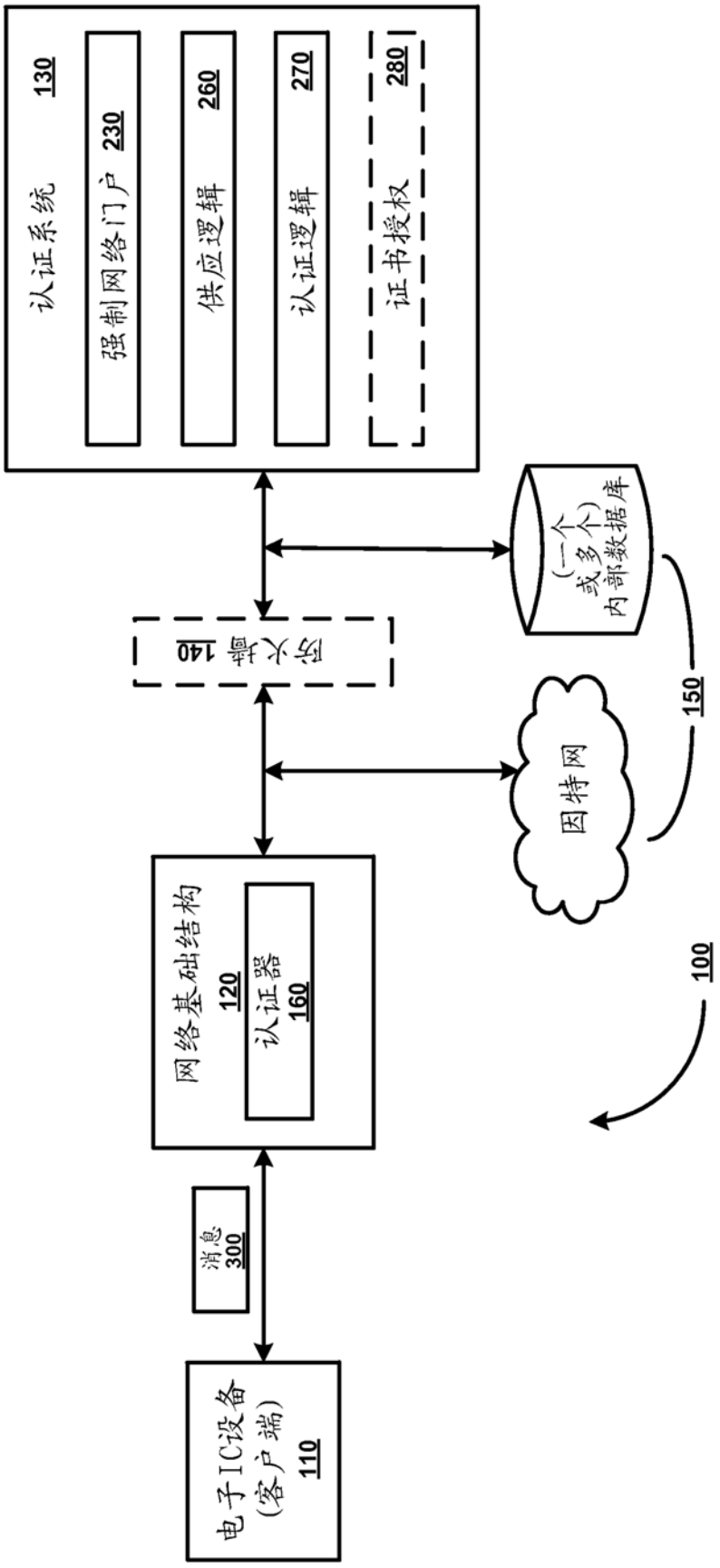

认证系统 130
强制网络门户 230
供应逻辑 260
认证逻辑 270
证书授权 280
(一个或多个)内部数据库
安全域 140
因特网
150
网络基础结构 120
认证器 160
100
消息 300
电子IC设备(客户端) 110

图 1

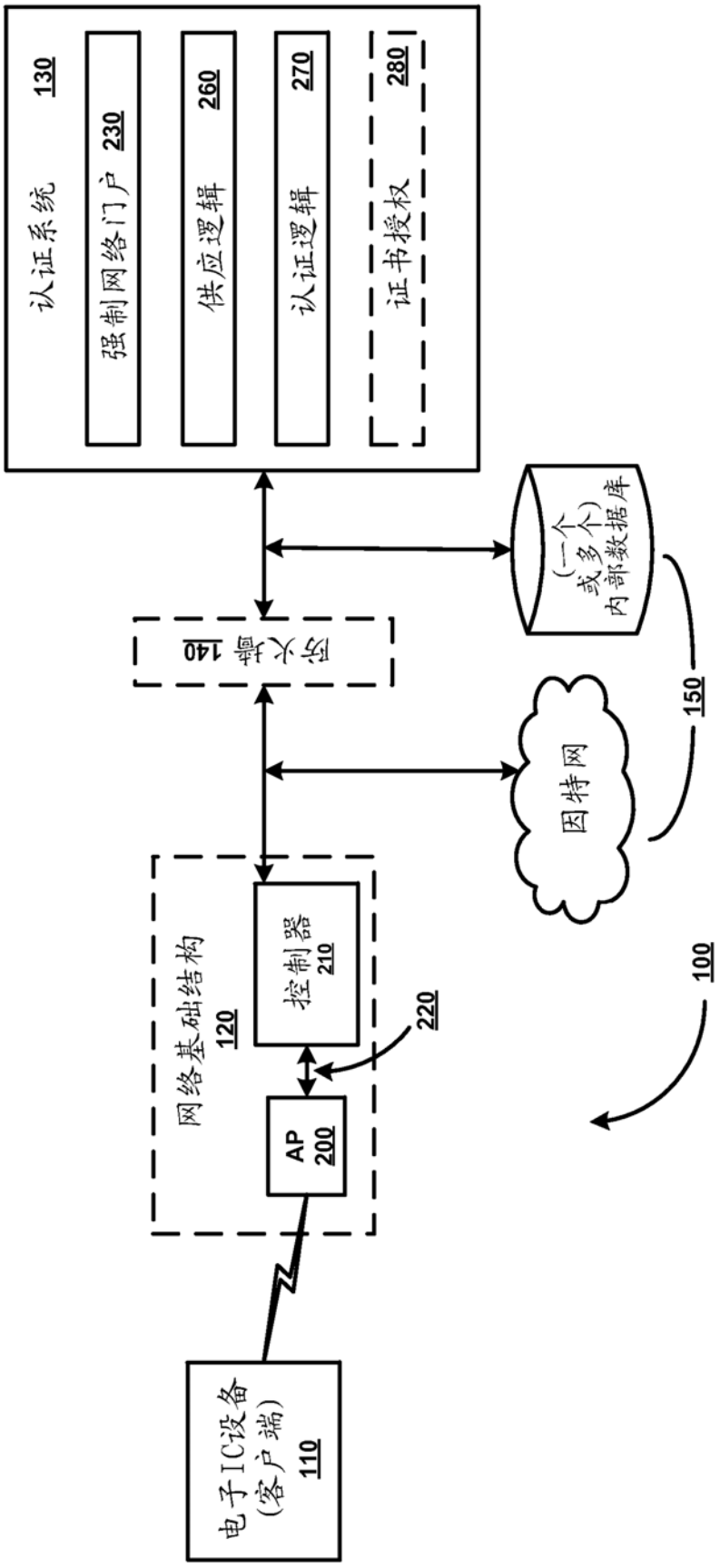

认证系统 130
强制网络门户 230
供应逻辑 260
认证逻辑 270
证书授权 280
(一个或多个)内部数据库
安全部 140
因特网
150
网络基础结构 120
控制器 210
220
AP 200
100
ZZ
电子IC设备(客户端) 110

图 2A

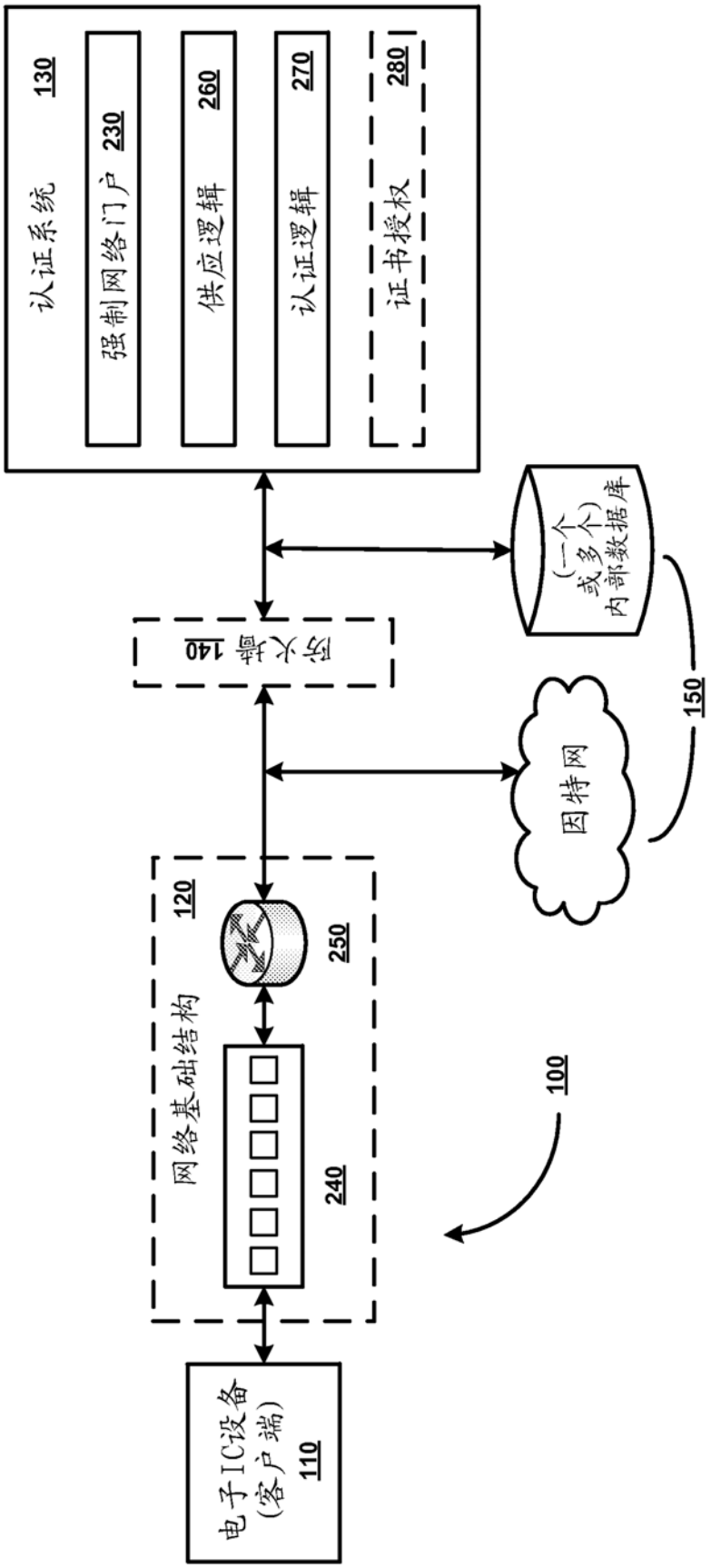

认证系统 130
强制网络门户 230
供应逻辑 260
认证逻辑 270
证书授权 280
(一个或多个)内部数据库
150
因特网
140
网络基础结构 120
250
240
100
电子IC设备(客户端) 110

图 2B

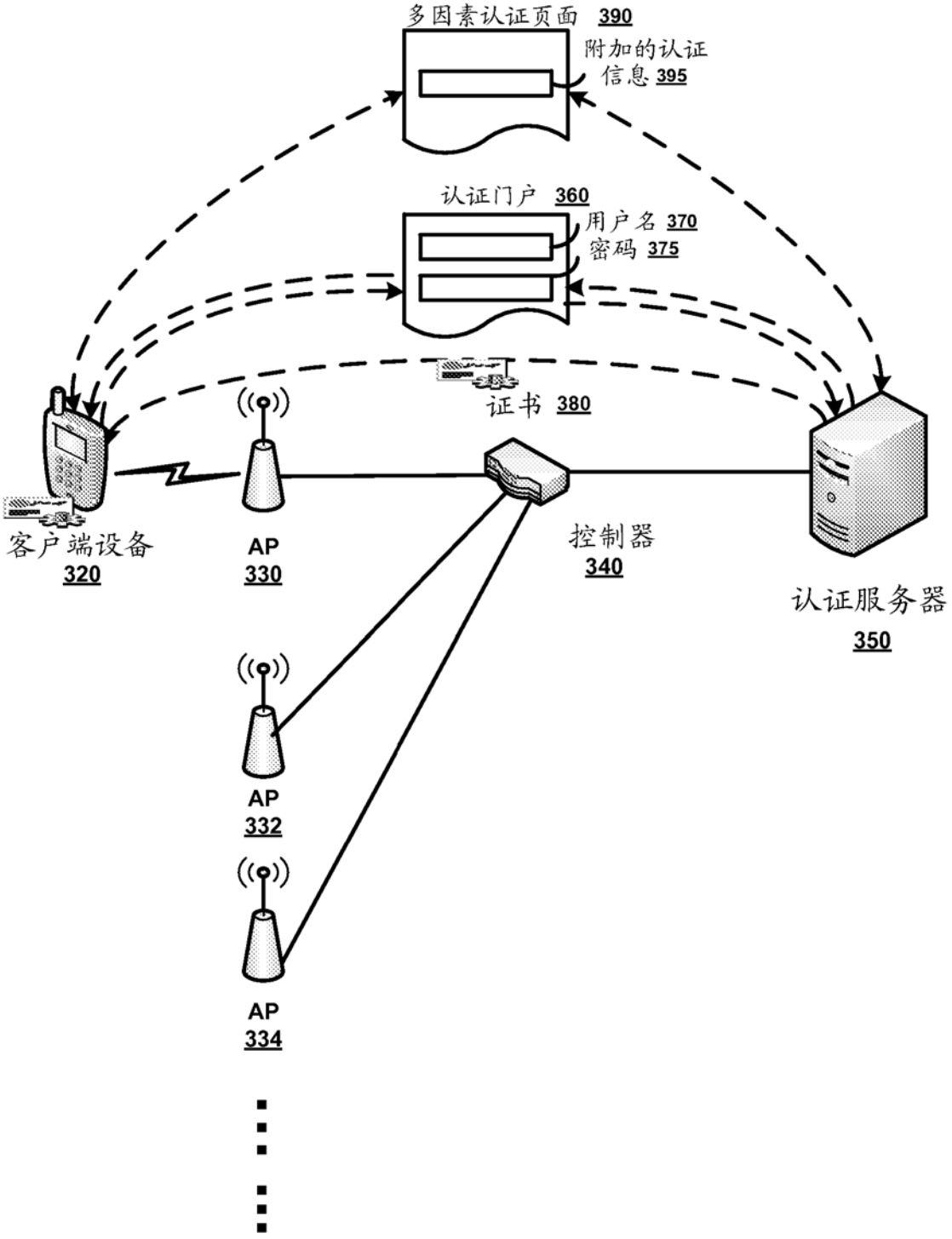

多因素认证页面 390
附加的认证
信息 395
认证门户 360
用户名 370
密码 375
证书 380
客户端设备
320
AP
330
控制器
340
认证服务器
350
AP
332
AP
334

图 3

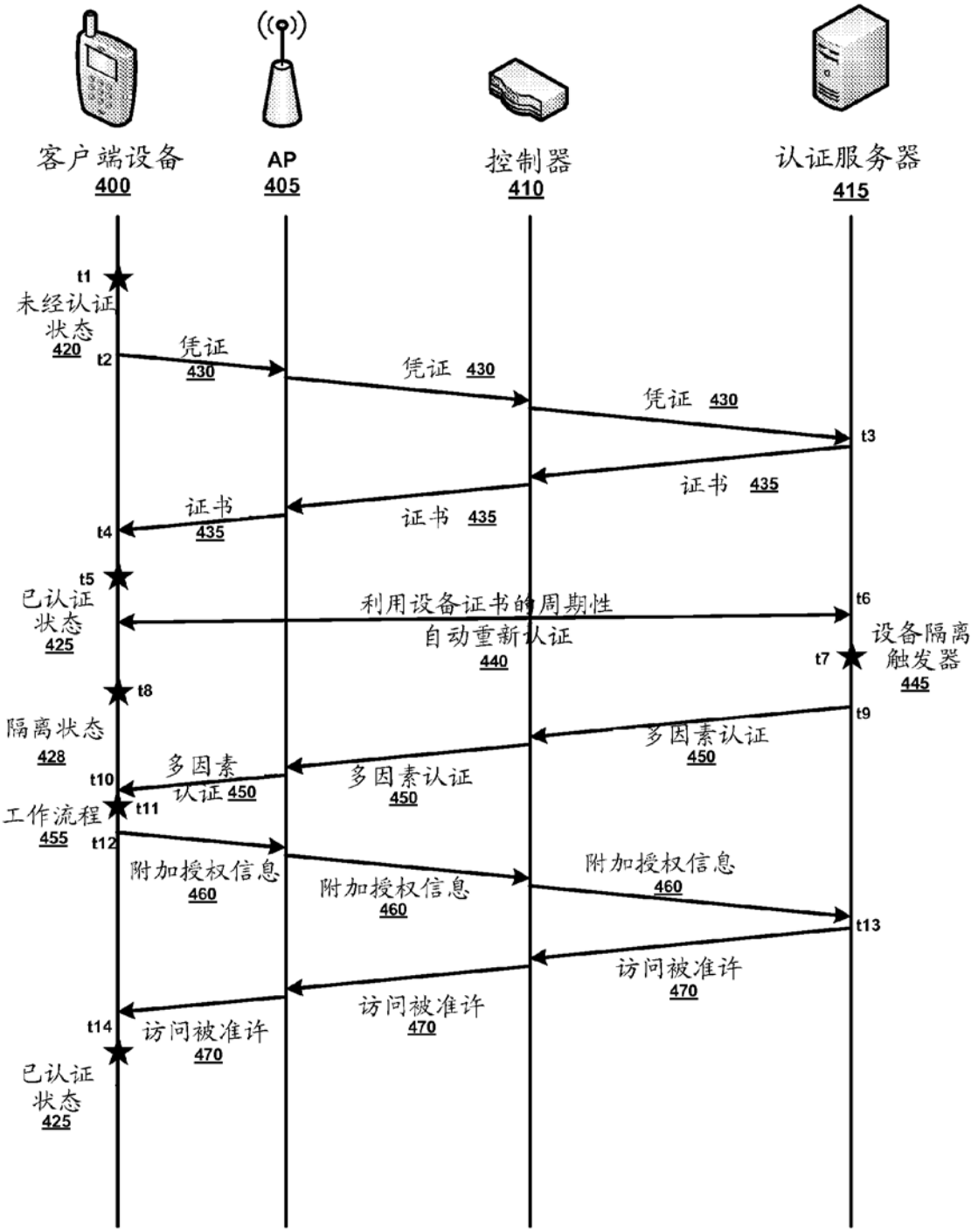

客户端设备
400
AP
405
控制器
410
认证服务器
415
t1
未经认证状态
420
t2
凭证
430
凭证 430
凭证 430
t3
证书 435
证书 435
证书
435
t4
t5
已认证状态
425
利用设备证书的周期性
自动重新认证
440
t6
设备隔离触发器
445
t7
t8
隔离状态
428
t9
多因素认证
450
多因素认证
450
多因素认证 450
t10
t11
工作流程
455
t12
附加授权信息
460
附加授权信息
460
附加授权信息
460
t13
访问被准许
470
访问被准许
470
访问被准许
470
t14
已认证状态
425

图 4A

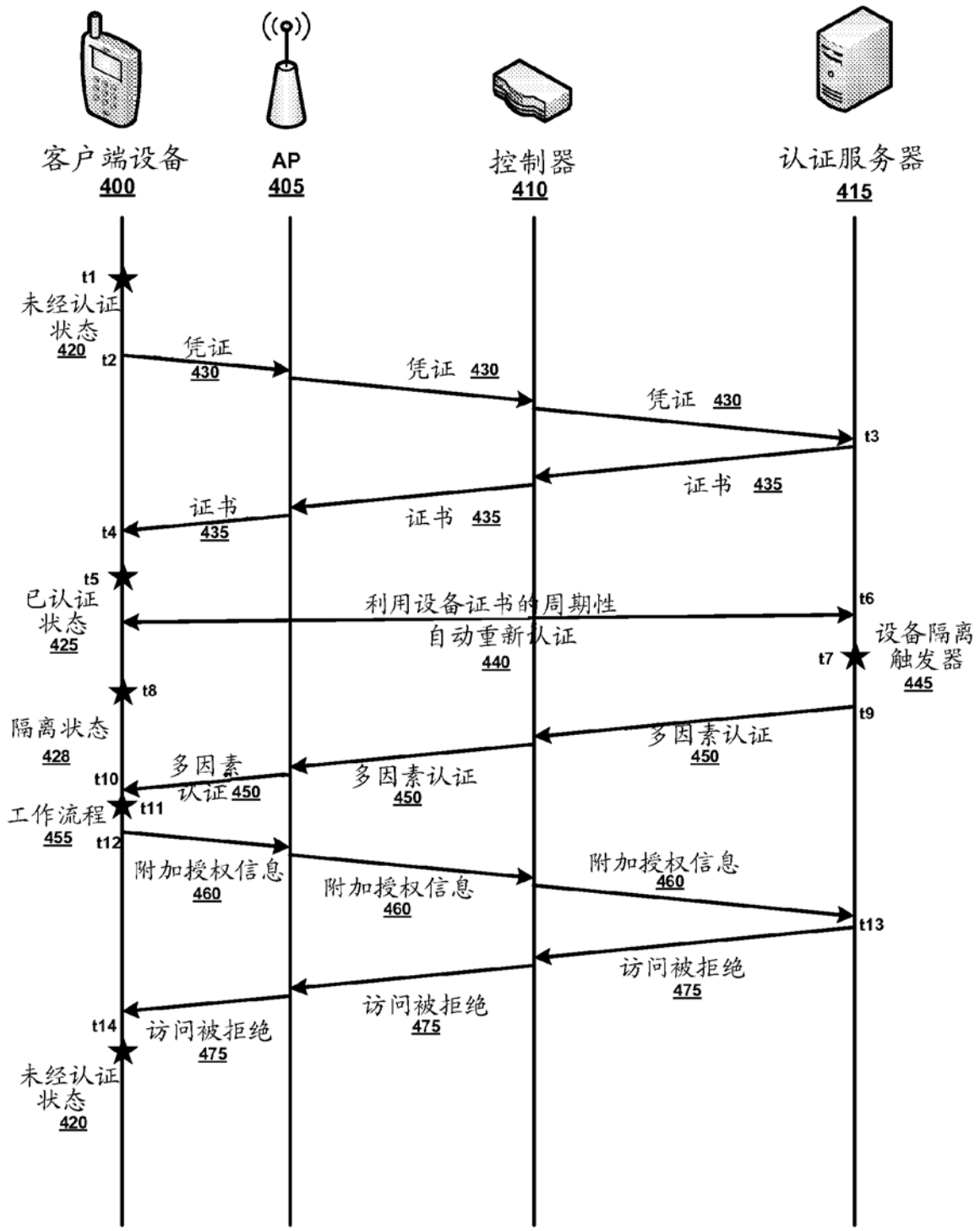

客户端设备
400
AP
405
控制器
410
认证服务器
415
t1
未经认证状态
420
凭证
430
t2
凭证 430
凭证 430
t3
证书 435
证书
435
证书 435
t4
t5
已认证状态
425
利用设备证书的周期性
自动重新认证
440
t6
设备隔离触发器
445
t7
t8
隔离状态
428
t9
多因素认证
450
多因素
认证 450
多因素认证
450
t10
t11
工作流程
455
t12
附加授权信息
460
附加授权信息
460
附加授权信息
460
t13
访问被拒绝
475
访问被拒绝
475
访问被拒绝
475
t14
未经认证状态
420

图 4B

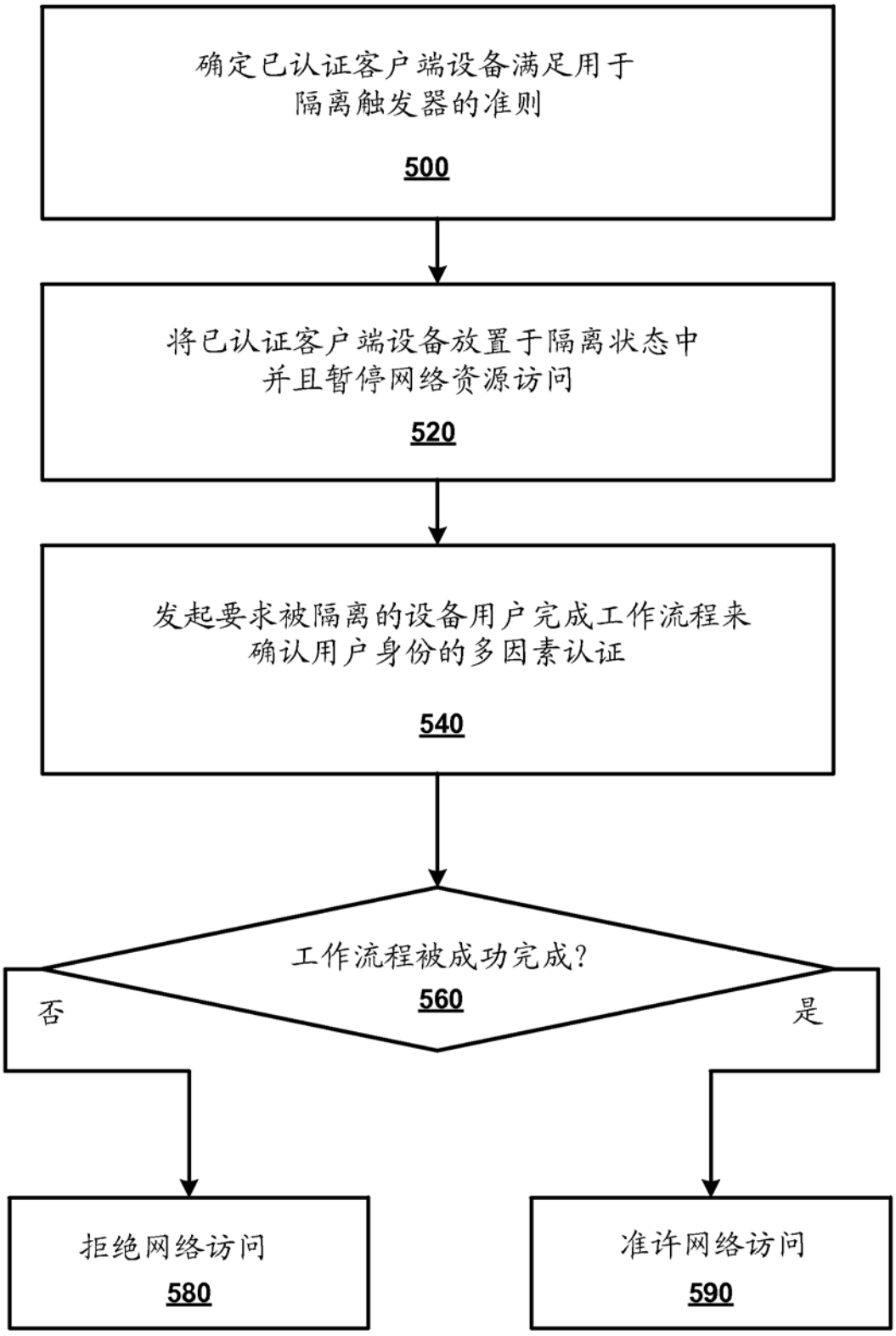

确定已认证客户端设备满足用于
隔离触发器的准则
500
将已认证客户端设备放置于隔离状态中
并且暂停网络资源访问
520
发起要求被隔离的设备用户完成工作流程来
确认用户身份的多因素认证
540
工作流程被成功完成?
560
否
是
拒绝网络访问
580
准许网络访问
590

图 5

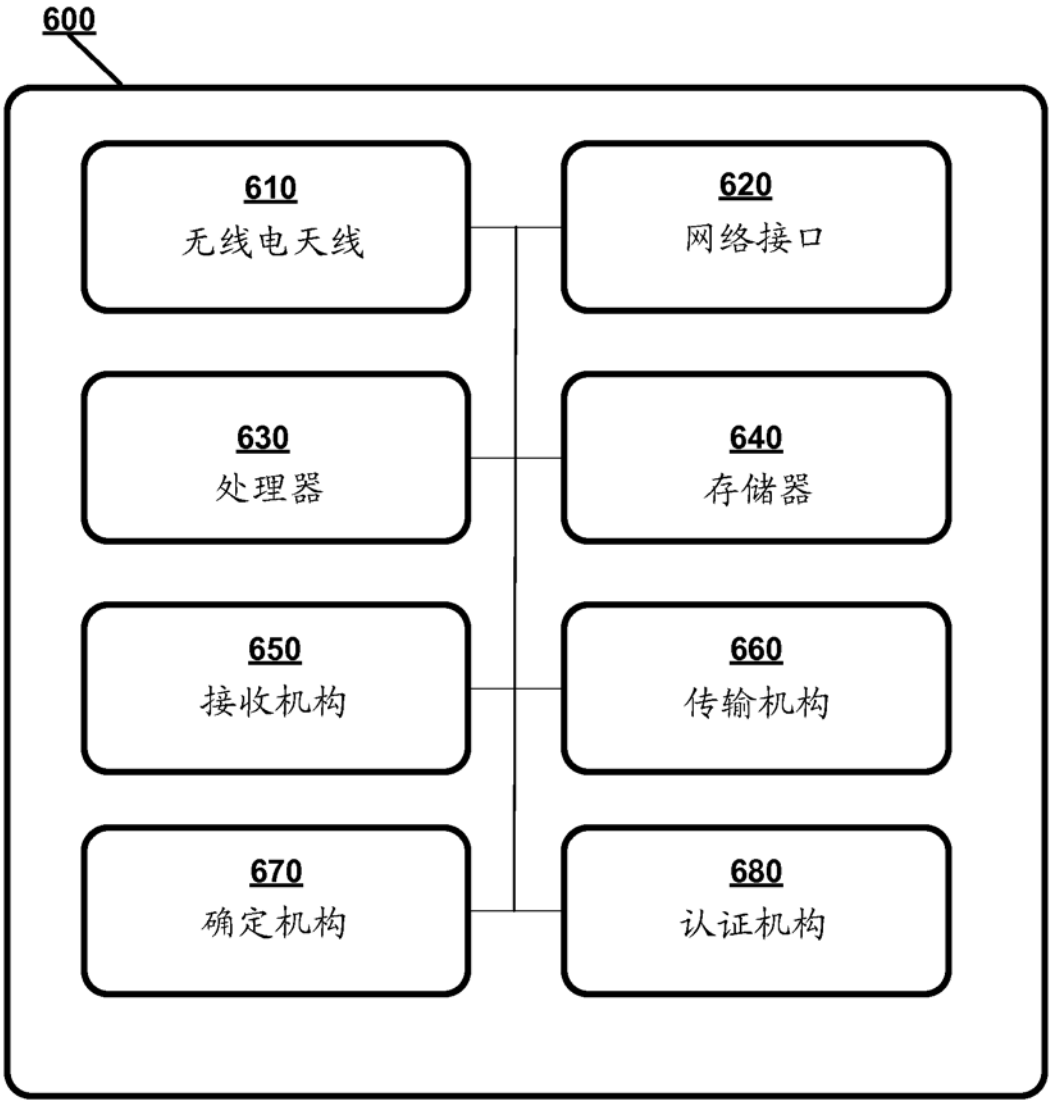

600
610
无线电天线
620
网络接口
630
处理器
640
存储器
650
接收机构
660
传输机构
670
确定机构
680
认证机构

图 6