(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 101331735 B
(45)授权公告日 2012.07.18

(21)申请号 200680047306.6
(22)申请日 2006.12.13
(30)优先权数据
11/305,646 2005.12.16 US
(85)PCT申请进入国家阶段日
2008.06.16
(86)PCT申请的申请数据
PCT/EP2006/069651 2006.12.13
(87)PCT申请的公布数据
WO2007/068715 EN 2007.06.21
(73)专利权人 国际商业机器公司
地址 美国纽约
(72)发明人 本杰明·B·哈蒙 希瑟·M·欣顿
安东尼·S·莫兰
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 黄小临
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
WO 01/11451 A1,2001.02.15,
US 5875296 A,1999.02.23, 全文.
审查员 潘斌

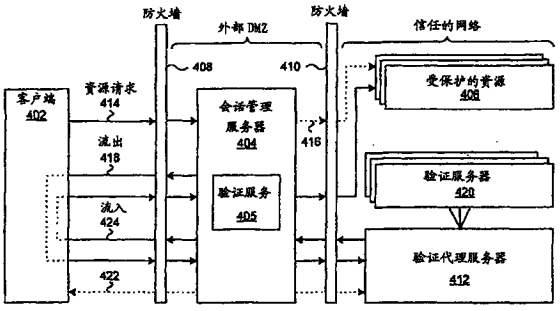
权利要求书 2 页 说明书 10 页 附图 7 页

(54)发明名称

用于扩展验证方法的方法和系统

(57)摘要

给出了用于管理用户的验证证书的方法。会话管理服务器对于包括受保护资源的域对用户执行会话管理。会话管理服务器接收要访问受保护资源的请求,该受保护资源要求已经对于第一类验证上下文而生成的验证证书。响应于确定已经对于第二类验证上下文生成了用户的验证证书,会话管理服务器向验证代理服务器发送包含了用户的验证证书和用于第一类验证上下文的指示符。会话管理服务器随后接收第二消息,该第二消息包含指示已经用于对于第一类验证上下文生成了用户的更新后的验证证书。



CN 101331735 B

1. 一种用于在数据处理系统内管理用户的验证证书的计算机实现的方法，该方法包括：

在会话管理服务器处从客户端接收代表用户访问受保护资源的请求，其中所述会话管理服务器执行对于包括所述受保护资源的域的、关于用户的会话管理，并且其中对所述受保护资源的访问需要已经为第一类验证上下文而生成的验证证书；

响应于所述会话管理服务器确定所述用户的验证证书指示已经为第二类验证上下文生成了验证证书，将第一消息从所述会话管理服务器发送到验证代理服务器，其中，所述第一消息包含所述用户的验证证书和用于所述第一类验证上下文的指示符；以及

在所述会话管理服务器处从所述验证代理服务器接收第二消息，其中所述第二消息包含用户的更新后的验证证书，并且其中，所述更新后的验证证书指示已经为所述第一类验证上下文生成了所述更新后的验证证书。

2. 如权利要求 1 所述的方法，还包括：

将所述更新后的验证证书与用户的预先存在的会话相关联，而不需要为用户建立新的会话。

3. 如权利要求 1 所述的方法，还包括：

在接收到所述更新后的验证证书后，从所述会话管理服务器发送所述代表用户访问所述受保护资源的请求。

4. 如权利要求 1 所述的方法，还包括：

由所述会话管理服务器从所述要访问受保护资源的请求中提取所述受保护资源的统一资源标识符 (URI)；以及

基于所提取的 URI 执行查找操作，以获得所述第一类验证上下文。

5. 如权利要求 1 所述的方法，还包括：

由所述会话管理服务器从可配置的信息中检索所述验证代理服务器的 URI；以及

对于来自所述会话管理服务器的每个请求，使用所检索的所述验证代理服务器的 URI 来获得更新后的证书。

6. 如权利要求 1 所述的方法，还包括：

由所述验证代理服务器从可配置的信息中检索所述会话管理服务器的 URI；以及

对于来自所述验证代理服务器的每个响应，使用所检索的所述会话管理服务器的 URI 来返回更新后的证书。

7. 如权利要求 1 所述的方法，还包括：

由所述验证代理服务器从所述第一消息提取用于所述第一类验证上下文的指示符；以及

基于所提取的用于所述第一类验证上下文的指示符执行查找操作以确定要采用的验证方法，来更新所述用户的验证证书。

8. 如权利要求 7 所述的方法，还包括：

由所述验证代理服务器将所述验证证书发送到所确定的验证方法。

9. 一种用于在数据处理系统内管理用户的验证证书的装置，该装置包括：

用于在会话管理服务器处从客户端接收代表用户访问受保护资源的请求的部件，其中所述会话管理服务器执行对于包括所述受保护资源的域的、关于用户的会话管理，并且其

中对所述受保护资源的访问需要已经为第一类验证上下文而生成的验证证书；

用于响应于所述会话管理服务器确定所述用户的验证证书指示已经为第二类验证上下文生成了验证证书、将第一消息从所述会话管理服务器发送到验证代理服务器的部件，其中，所述第一消息包含所述用户的验证证书和用于所述第一类验证上下文的指示符；以及

用于在所述会话管理服务器处从所述验证代理服务器接收第二消息的部件，其中所述第二消息包含用户的更新后的验证证书，并且其中，所述更新后的验证证书指示已经为所述第一类验证上下文生成了所述更新后的验证证书。

10. 如权利要求 9 所述的装置，还包括：

用于将所述更新后的验证证书与用户的预先存在的会话相关联而不需要为用户建立新的会话的部件。

11. 如权利要求 9 所述的装置，还包括：

用于在接收到所述更新后的验证证书后、从所述会话管理服务器发送所述代表用户访问所述受保护资源请求的部件。

12. 如权利要求 9 所述的装置，还包括：

用于由所述会话管理服务器从所述要访问受保护资源的请求中提取所述受保护资源的统一资源标识符 (URI) 的部件；以及

用于基于所提取的 URI 执行查找操作以获得所述第一类验证上下文的部件。

13. 如权利要求 9 所述的装置，还包括：

用于由所述会话管理服务器从可配置的信息中检索所述验证代理服务器的 URI 的部件；以及

用于对于来自所述会话管理服务器的每个请求使用所检索的所述验证代理服务器的 URI 来获得更新后的证书的部件。

14. 如权利要求 9 所述的装置，还包括：

用于由所述验证代理服务器从可配置的信息中检索所述会话管理服务器的 URI 的部件；以及

用于对于来自所述验证代理服务器的每个响应使用所检索的所述会话管理服务器的 URI 来返回更新后的证书的部件。

15. 如权利要求 9 所述的装置，还包括：

用于由所述验证代理服务器从所述第一消息提取用于所述第一类验证上下文的指示符的部件；以及

用于基于所提取的所述第一类验证上下文的指示符执行查找操作以确定要采用的验证方法来更新所述用户的验证证书的部件。

16. 如权利要求 15 所述的装置，还包括：

用于由所述验证代理服务器将所述验证证书发送到所确定的验证方法的部件。

用于扩展验证方法的方法和系统

技术领域

[0001] 本发明涉及改进的数据处理系统，并且具体地，涉及用于多计算机数据传送的方法和装置。更具体地，本发明导向于计算机系统内的验证方法。

[0002] 背景技术

[0003] 电子商务网站和网络应用代表用户在计算机网络上执行各种业务。出于安全目的，用户必须经常通过验证处理以便证明用户的标识确实达到适当的级别。在基于电子商务网络的环境下，计算机系统经常将验证服务实现为用于访问网站的前门或哨门 (sentry gate) 的形式。这些验证服务位于应用的前面，即，在用户和应用之间，以确保用户在获得对任何资源的访问之前被验证。可以将这些验证服务实现为网络服务器插件、反向代理 (reverse proxy) 或其他类似技术。

[0004] 企业一般希望通过包括因特网的各种网络以用户友好的方式向验证后的用户提供对于受保护资源的安全访问。尽管提供安全验证机制降低了对受保护资源的未授权访问的风险，但是那些验证机制可能成为访问受保护资源的障碍。用户通常希望能够从与一个应用交互改变为与另一应用交互，而不考虑保护支持这些应用的每个具体系统的验证障碍。

[0005] 随着用户变得更老练，他们期望计算机系统协助他们的动作以便减少用户的负担。这种期望也应用于验证处理。用户可能假设一旦他或她已经经过某个计算机系统的验证，则在用户的工作会话期间或者至少对于特定的时间段，该验证应该有效，而不考虑对于用户来说几乎不可见的各种计算机体系界限。企业通常试图在其部署的系统的可操作特性方面满足这些期望，以便不仅安抚用户而且提高用户效率，无论用户效率是与雇员生产量还是与顾客满意度有关。

[0006] 很多计算机系统具有对于不同安全级别的不同类型验证。例如，在成功完成由用户提供正确的用户名与密码的组合的第一级别的验证后，系统可以提供对于网站上的特定一组资源的访问。第二级别的验证可能要求用户给出硬件记号、例如智能卡，其后，为用户提供对于网站上的更严格控制的资源的访问。第三级别的验证可能要求用户提供某种形式的生物学数据，例如通过指纹扫描或视网膜扫描，其后，系统提供对于网站上非常敏感或机密的资源的访问。从一个验证级别向上移动到下一级别的处理被称作“递进验证”或者“被迫再验证”。换句话说，用户按系统要求从一个级别的验证递进到更高级别以便获得对于更敏感资源的访问。

[0007] 可以用公知的验证方法实现验证，但是不容易实现对多种惯用方法的支持。典型的反向代理内的验证方法经常限于支持即开即用 (out-of-the-boxsupported) 的方法、例如相互验证的 SSL（安全套接层），或者各种惯用方法。添加对于新验证方法的支持不是简单的处理，因为典型地在服务器内部内在化 (internalize) 新验证方法。即使在通过外部应用而具有对于添加的新验证方法的支持的那些系统中，该支持的有限之处在于能够基于外部的验证信息为用户建立会话，而不能更新用户的例如当前会话证书 (session credential)，以反映另一验证操作的完成。

[0008] 为了围绕这样的限制而展开工作，当前的解决方案取消了用户的当前会话，并且用在新的会话信息和证书信息中所包括的新验证方法来建立新的会话。一种系统可以尝试以对用户不可见的方式来建立新的会话，从而减少获悉了新会话的用户在该用户不需要这种获悉时的负担。然而，仍然存在的问题是，一般会从用户的原始会话丢失某种程度的状态信息；换句话说，关于从旧会话向新会话的改变，下游应用或受保护资源可能具有某种不可预见的问题。

[0009] 因此，将具有优势的是提供一种方法或系统，其可以将验证方法扩展到可以更新用户证书而不需为用户建立新会话的外部应用，从而获得验证服务或受保护资源出于某种目的所需的更高安全级别。

发明内容

[0010] 给出了用于管理用户的验证证书的方法、系统、计算机程序制品和装置。给出了用于管理用户的验证证书的方法。会话管理服务器对于包括受保护资源的域对用户执行会话管理。会话管理服务器接收要访问受保护资源的请求，该受保护资源要求已经对于第一类验证上下文而生成的验证证书。响应于确定已经对于第二类验证上下文生成了用户的验证证书，会话管理服务器向验 证代理服务器发送包含了用户的验证证书和用于第一类验证上下文的指示符。会话管理服务器随后接收第二消息，该第二消息包含指示已经用于对于第一类验证上下文生成了用户的更新后的验证证书。

附图说明

[0011] 现在将仅通过例子，参考附图描述本发明，附图中：

[0012] 图 1A 绘出数据处理系统的典型网络，这些数据处理系统的每个都可以实现本发明；

[0013] 图 1B 绘出在可实现本发明的数据处理系统中可以使用的典型计算机体系；

[0014] 图 2 绘出示出了典型的企业数据处理系统的方框图；

[0015] 图 3 绘出示出了当客户尝试访问服务器处的受保护资源时可以使用的典型验证处理的数据流程图；

[0016] 图 4 绘出示出了用于执行扩展的验证操作的数据处理系统的一部分的方框图；

[0017] 图 5 绘出示出由支持验证操作的会话管理服务器所管理的一些信息的方框图；

[0018] 图 6 绘出示出由支持验证操作的验证代理服务器所管理的一些信息的方框图；

[0019] 图 7 绘出示出了在会话管理服务器到验证代理服务器之间的验证请求消息中可以包含的一些信息的方框图；

[0020] 图 8 绘出示出了在从验证代理服务器到会话管理服务器的验证响应消息中可以包含的一些信息的方框图；

[0021] 图 9 绘出示出了会话管理服务器通过该处理来启动验证操作的处理的流程图；

[0022] 图 10 绘出示出了验证代理服务器通过该处理来管理如所请求的验证操作的处理的流程图；以及

[0023] 图 11 绘出示出了会话管理服务器通过该处理来完成验证操作的处理的流程图。

具体实施方式

[0024] 一般而言，可以包含或涉及本发明的设备包括很多种数据处理技术。因此，作为背景，在更详细描述本发明之前，描述分布式数据处理系统中的硬件和软件组件的典型组织。

[0025] 现在参考附图，图 1A 绘出数据处理系统的典型网络，每个数据处理系统可以实现本发明的一部分。分布式数据处理系统 100 包括网络 101，其是可以用于提供在分布式数据处理系统 100 内的连接在一起的各种设备和计算机之间的通信链接的媒介。网络 101 可以包括诸如有线或光纤电缆的永久连接或者通过电话或无线通信而做出的临时连接。在所示例子中，服务器 102 和 103 与存储单元 104 一起被连接到网络 101。另外，客户端 105-107 也被连接到网络 101。可以由各种计算设备、比如主机、个人计算机、个人数字助理 (PDA) 等来代表客户端 105-107 和服务器 102-103。分布式数据处理系统 100 可以包括未示出的另外的服务器、客户端、路由器、其他设备、以及对等体系。

[0026] 在所示例子中，分布式数据处理系统 100 可以包括具有网络 101 的因特网，代表使用各种协议来相互通信的网络和网关的全世界范围的集合，该各种协议诸如轻量级目录访问协议 (LDAP)、传输控制协议 / 因特网协议 (TCP/IP)、文件传送协议 (FTP)、超文本传输协议 (HTTP)、无线应用协议 (WAP) 等的。当然，分布式数据处理系统 100 还可以包括大量各种网络，诸如，企业内部互联网、局域网 (LAN) 或广域网 (WAN)。例如，服务器 102 直接支持客户端 109 和网络 110，该服务器 102 并入了无线通信链接。网络使能的电话 111 通过无线链接 112 连接到网络 110，并且 PDA 113 通过无线链接 114 连接到网络 110。电话 111 和 PDA 113 也可以经过使用适当的技术、比如蓝牙 TM 无线技术的无线链接在它们自身之间直接传送数据，以建立所谓的个人局域网络 (PAN) 或个人 ad-hoc 网络。以类似的方式，PDA 113 可以经由无线通信链接 116 向 PDA 107 传送数据。

[0027] 可以在各种硬件平台上实现本发明；图 1A 意要作为各种计算环境的例子，并且不意要作为对本发明的体系限制。

[0028] 现在参考图 1B，该图绘出了比如图 1A 所示的、可以在其中实现本发明的数据处理系统的典型计算机体系。数据处理系统 120 包括：与内部系统总线 123 连接的一个或多个中央处理单元 (CPU)122，该内部系统总线 123 与随机存取存储器 (RAM)124、只读存储器 126、以及输入 / 输出适配器 128 互连，该输入 / 输出适配器 128 支持各种 I/O 设备，比如打印机 130、盘单元 132 或其他未示出的设备，比如音频输出系统等。系统总线 123 还连接了提供到通信链接 136 的访问的通信适配器 134。用户接口适配器 148 连接了各种用户设备，比如键盘 140 和鼠标 142，或者未示出的其他设备，比如触摸屏、触针、麦克风等。显示适配器 144 将系统总线 123 连接到显示设备 146。

[0029] 本领域普通技术人员将认识到，图 1B 中的硬件可以取决于系统实现而改变。例如，系统可以具有诸如基于 Intel®Pentium®的处理器和数字信号处理器 (DSP) 的一个或多个处理器，以及一种或多种易失性和非易失性存储器。除了图 1B 中所示的硬件以外或者替换图 1B 中所示的硬件，还可以使用其他外围设备。所示例子不意味着暗示关于本发明的体系限制。

[0030] 除了能够在各种硬件平台上实现以外，也可以在各种软件环境下实现本发明。典型的操作系统可以用于控制每个数据处理系统内的程序执行。例如，一个设备可以运行 Unix®操作系统，而另一设备包含简单的 Java®运行时间环境。代表性的计算机平台可以

包括浏览器，这是用于访问各种格式的超文本文档的公知软件应用，该各种格式的超文本文档诸如图形文件、文字处理文件、可扩展标记语言 (XML)、超文本标记语言 (HTML)、手持设备标记语言 (HDML)、无线标记语言 (WML) 和各种其它格式和类型的文件。

[0031] 如关于图 1A 和 1B 所述，可以在各种硬件和软件平台上实现本发明。尽管更具体地，本发明导向于改进的数据处理环境。在更详细描述本发明之前，描述典型的数据处理环境的一些方面。

[0032] 在此对附图的描述可以涉及由客户端设备或客户端设备的用户做出的某些动作。本领域普通技术人员将理解，去往客户端的响应和 / 或来自客户端的请求有时候由用户发起，并且其他时候经常由客户端代表该客户端的用户来自动发起。因此，当在附图的描述中提到客户端或者客户端的用户时，应当理解，可互换地使用术语“客户端”和“用户”，而不会严重影响所述处理的意思。

[0033] 下文中可以将某些计算任务描述为由功能单元执行。功能单元可以由例程、子例程、处理、子处理、进程、功能、方法、面向对象的对象、软件模块、小程序、插件、ActiveX™ 控制、脚本或用于执行计算任务的固件或软件的一些其他组件来表示。

[0034] 在此对附图的描述可以涉及各种组件之间的信息交换，并且该信息交换可以被描述为经由消息、例如跟随了响应消息的请求消息的交换来实现的。应当注意，当合适时，可以经由诸如消息、方法调用、远程进程调用、事件信号或其他机制的各种数据交换机制来等效地实现计算组件间的信息交换，该信息交换可以包括同步或异步的请求 / 响应交换。

[0035] 现在参考图 2，方框图绘出典型的企业数据处理系统。而图 1A 绘出具有客户端和服务器的典型数据处理系统，相反，图 2 示出与某些服务器侧实体有关的网络内的客户端，该某些服务器侧实体可以用于支持对于访问资源的客户端请求。如在典型的计算环境中，企业域 200 例如通过网络 208 使用客户端 206 上的浏览器应用 204 来主管 (host) 用户 202 可以访问的资源；计算机网络可以是因特网、企业内部互联网或其他网络，如图 1A 所示。

[0036] 企业域 200 支持多个服务器。应用服务器 210 通过基于网络的应用或其他类型后端应用、包括传统应用 (legacy application)，来支持受控制的资源和 / 或未控制的资源。反向代理服务器 214、或者简称代理服务器 214 执行用于企业域 200 的广阔范围的功能。例如，代理服务器 214 可以缓存网页以便镜像 (mirror) 来自应用服务器的内容。可以分别通过输入数据流过滤器 216 和输出数据流过滤器 218 来处理流入和流出的数据流，以便根据在各种策略中所指定的目标或条件或根据所采用的软件模块的配置来对流入的请求和流出的响应执行各种处理任务。

[0037] 会话管理单元 220 管理如由代理服务器 214 识别的会话标识符、缓存的证书或与会话有关的其他信息。基于网络的应用典型地利用各种手段来帮助用户输入验证信息，该验证信息通常为 HTML 表单内的用户名 / 密码组合。在图 2 所示的例子中，在客户端 206 可以具有对资源的访问之前，可以要求对用户 202 进行验证，这之后，为客户端 206 建立会话。在可替换的实施例中，在向用户提供对域 200 上的资源的访问之前不进行验证和授权操作；可能不需随附的验证操作来创建用户会话。

[0038] 上述企业域 200 内的实体表示许多计算环境内的典型的实体。然而，许多企业域具有用于控制对于受保护计算资源的访问的安全特征。计算资源可以是应用、对象、文档、网页、文件、可执行的代码模块、或一些其他的计算资源或通信类资源。如果发请求的客户

端或发请求的用户被验证和 / 或授权，受保护的或受控制的资源是仅可访问或可检索的资源 ；在一些情况下，经过验证的用户是默认被授权的用户。验证服务器 222 可以支持各种验证机 制，比如用户名 / 密码、X.509 证书或安全记号 ；多个验证服务器可以专用于专门的验证方法。授权服务器 224 可以使用授权数据库 226，其包含如下信息，诸如访问控制列表 228、授权策略 230、关于用户组或角色的信息 232、以及关于特定管理组内的管理用户的信息 234。使用该信息，授权服务器 224 响应于来自客户端 206 的请求，向代理服务器 214 提供对于是否应该允许继续具体请求、例如是否应该准许对受控制的资源访问的指示。应当注意，可以与各种验证和授权应用联合地实现本发明，并且在此描述的本发明的实施例不应被理解为将本发明的范围限制于验证和授权服务的配置。

[0039] 现在参考图 3，数据流程图图示了当客户端试图访问服务器处的受保护资源时可以使用的典型的验证处理。如所示，位于客户端工作站 300 处的用户通过在客户端工作站上执行的用户的网络浏览器，来寻求经过计算机网络对服务器 302 上的受保护资源的访问。受保护资源可以由仅能够由被验证和授权的用户来访问的统一资源定位符 (URL)、或者更具体地统一资源标识符 (URI) 来标识。

[0040] 当用户请求服务器侧的受保护资源、比如域“ibm.com”内的网页时，开始处理 (步骤 304)。在联网的环境下，术语“服务器侧”和“客户端侧”分别指网络环境中的服务器或客户端处的动作或实体。网络浏览器 (或相关应用或小程序) 生成 HTTP 请求，该 HTTP 请求被发送到主管域“ibm.com”的网络服务器 (步骤 306)。术语“请求”和“响应”应该被理解为包括适合于具体操作中所涉及的信息、诸如消息、通信协议信息或其他有关信息的传送的数据格式化。

[0041] 服务器确定没有客户端的有效会话 (步骤 308)，因此服务器通过向客户端发送某种类型的验证询问 (challenge) 来要求用户进行验证处理 (步骤 310)。验证询问可以是各种格式的，比如 HTML 表单。然后用户提供所请求或所需要的信息 (步骤 312)、比如用户标识符和相关密码，或者客户端可以自动返回某种信息、比如数字证书。

[0042] 向服务器发送验证响应消息 (步骤 314)，此时，服务器例如通过在检索先前所提交的注册信息并将所呈现的验证信息与用户所存储的信息相匹配来验证用户或客户端 (步骤 316)。假设验证成功，则为被验证的用户或客户端建立有效会话。

[0043] 然后服务器检索被请求的网页，并将 HTTP 响应消息发送到客户端 (步骤 318)。这时，用户可以通过点击超文本链接来请求浏览器中的“ibm.com”内的另一页面 (步骤 320)，并且浏览器将另一 HTTP 请求消息发送到服务器 (步骤 322)。这时，服务器基于由服务器保持的会话状态信息来识别用户具有有效会话 (步骤 324)。例如，因为用户的客户端返回了 HTTP 请求消息内的会话 ID，因此服务器识别发出请求的用户的适当的会话状态信息。基于所缓存的用户会话信息，服务器例如通过用户的证书的副本的可用性，来确定用户已经被验证 ；然后服务器可以确定，在满足用户的请求之前，不需要执行诸如验证操作的某些操作。服务器在另一 HTTP 响应消息中将所请求的网页发送回客户端 (步骤 326)，从而满足了用户对于受保护资源的原始请求。

[0044] 尽管图 2 绘出了典型的数据处理系统，并且图 3 绘出了当客户端试图访问服务器处的受保护资源时可以使用的典型的验证处理，但是本发明定向为将验证操作扩展到外部应用的改进的验证基础结构，其中该外部应用可以更新用户证书而不需要求为用户建立新

的会话，如其余图所示。

[0045] 现在参考图 4，方框图绘出了根据本发明的实施例的用于执行扩展的验证操作的数据处理系统的一部分。图 4 所示的数据处理系统与图 2 所示的数据处理系统类似。例如，在两图中：客户端 402 与客户端 206 类似；会话管理服务器 404 与代理服务器 214 类似；并且受保护资源 406 可以表示应用服务器 210 和其它类型的受保护资源。

[0046] 优选地，会话管理服务器 404 位于计算的 DMZ（隔离区 (DeMilitarizedzone)）内，以便向会话管理服务器 404 和从会话管理服务器 404 传送的数据必须通过防火墙 408 和 410。会话管理服务器 404 负责关于用户会话的会话管理，其中该用户会话是在包括了受保护资源 406 的安全域中创建的。当可能时，会话管理服务器 404 依靠验证服务 405 来进行验证操作；在验证服务 405 不能进行验证操作的情况下，会话管理服务器 404 依靠验证代理服务器 412，如下更详细说明。

[0047] 会话管理服务器 404 和受保护资源 406 可以存在于信任的网络内，其可以代表例如与图 2 所述的企业域 200 类似的企业域内的计算资源。然而，也可以在其他安全域内主管各种组件、具体为验证代理服务器 412。

[0048] 图 4 图示用于论述验证操作可以处于执行对域的会话管理的会话管理服务器外部的本发明的实施方式的组件，其中，验证操作更新用户的证书而不需为用户建立新的会话。此外，图 4 图示了在客户端 / 用户和支持由客户端 / 用户访问的受保护资源的组件之间的一些数据流。去往会话管理服务器 404 和来自会话管理服务器 404 的示例数据流被图示为通过客户端而被重定向；然而，应当注意，可以通过各种传输的消息以及其他数据传送机制来执行去往会话管理服务器 404 和来自会话管理服务器 404 的数据流，该各种传输的消息是向会话管理服务器 / 从会话管理服务器发送和 / 或转发的，该其他数据传送机制向会话管理服务器推入数据或从会话管理服务器拉出数据。

[0049] 在某个时间点，客户端 402 的用户可能已经经由会话管理服务器 404 完成了验证处理，使得会话管理服务器 404 具有用户的证书；例如当将用户所接收的请求转发或发送到受保护资源 406 时，会话管理服务器 404 使用证书以向用户提供对某些受保护资源 406 的访问。在很多情况下，当会话管理服务器 404 接收要访问受保护资源的请求并确定发出请求的用户的证书足够时，会话管理服务器 404 转发或发送用户的请求而不修改用户的当前证书。

[0050] 然而，在图 4 所示的例子中，当会话管理服务器 404 接收到资源请求 414 时，资源请求 414 不被转发到受保护资源，例如作为假定被转发的请求 416。在此情况下，会话管理服务器 404 识别资源请求 414 是要访问如下受保护资源的请求：该受保护资源需要合适的、有效的、足够的、满足的或可接受的用于在特定验证上下文中的断言 (assertion) 的证书。在所示例子中，会话管理服务器 404 识别用户的当前证书对于由受保护资源所需要的验证上下文来说是不合适的、无效的、不足够的、不满足的、或不可接受的。

[0051] 验证上下文是一个或多个标准或限制的集合，其中在该集合中创建验证证书或或意图验证证书用于该集合。验证上下文可以指示怎样验证、使用何者来验证、和 / 或意图使用证书的范围。例如，可能已经由具体的验证实体生成了用户的验证证书，其中在该验证证书中指示了该验证实体的标识；换句话说，验证证书可以指示验证用户所使用或利用的实体。作为另一例子，已经通过具体类型、种类或类别的验证操作（例如，用户名 / 密码、硬

件记号、生物信息或者和其他的这种验证方法）来生成了用户的验证证书，在验证证书内指示了该具体类型、等级或类别的验证操作的标识；换句话说，验证证书可以指示如何验证用户。作为另一例子，用户的验证证书可以指示：证书意图有效的时间段；证书意图有效的业务上下文，比如仅用于银行业务或仅用于购买业务等；证书在各团体之间是否是可委托(delegatable)；或者其他意图的限制。

[0052] 因此，在图 4 的例子中，用户的当前证书可以指示在很多种特性上的无效或不足。例如，受保护资源的操作者可能无法识别用户的当前证书的发证机关 (issuing authority)。然而，可能存在由受保护资源的操作者识别的另一发证机关；此另一发证机关可以识别用户的当前证书内的所指示的发证机关，并且此另一发证机关可能将要基于那些证书的确认而重新发布用户的证书。作为另一例子，用户的当前证书可以指示它们是响应于验证操作、基于用户成功断言用户名 / 密码对的确认而生成的。然而，受保护资源的操作者可能需要响应于验证操作、基于用户的生物断言的确认而生成的验证证书。

[0053] 此时，不转发对于受保护资源的请求，反而会话管理服务器 404 将消息 418 发送到验证代理服务器 412；该消息包含用于请求与用户先前获得的不同的验证上下文的、用户的更新后的证书的信息。验证代理服务器 412 将到来的请求转发到后端验证服务器 420 中的适当一个，其基于在消息 418 中所包括的、用户的当前证书信息来生成更新后的证书。

[0054] 验证服务器 420 可以表示验证服务器、servlet、或其他类型的计算组件，其每个提供了对于完成或执行不同类型的验证操作和 / 或在不同验证上下文中的验证操作的支持，从而生成对于特定验证上下文来说有效的验证证书。依据所实现的操作，验证服务器可能需要与用户 / 客户端的交互 422 来收集用于建立更新后的证书的信息。

[0055] 如上述，验证上下文可以包括一个或多个标准或限制的集合，其每个可能是简单的或迟钝的 (obtuse)。因此，由验证服务器 420 之一实现的验证操作可能相应地简单或复杂。例如，如果用户的更新后的验证证书需要由新的发证机关来发布，则验证操作可能涉及具有另外的实体或操作者的冗长的下游处理。在此例子中，在如操作者或受保护资源需要、已经由特定发证机关来发布了用户的更新后的验证证书之后，认为对于由受保护资源所需要的验证上下文、已经生成了用户的更新后的验证证书。

[0056] 在另一例子中，如果用户的当前验证证书最近已经在先前的小时内过期，并且验证服务器具有将用户证书的生命期延长一个小时的授权，则验证操作可以仅包括更新后的验证证书的有效期的修改，尽管这可能还需要在证书中的数字校验和或其他数据项的修改。在此例子中，在如由受保护资源的操作者需要、已经由验证服务器生成了在当前时间段上有效的用户的更新后的验证证书之后，认为已经对于由受保护资源所需要的验证上下文生成了用户的 更新后的验证证书。

[0057] 然后，验证代理服务器 412 通过将到来的消息 424 发送到客户端 402 来返回更新后的证书，然后客户端 402 适当地将其转发到会话管理服务器 404。如果，会话管理服务 404 缓存、存储、或者更新、关联、或者修改关于更新后的证书的用户的当前会话状态信息。

[0058] 然后，会话管理服务器 404 将用户的原始请求发送到受保护资源。请求可以附有用户的更新后的证书，该更新后的证书指示如受保护资源所要求的适当的验证上下文、或者用户的更新后的证书仍然可用于在需要时由下游实体执行的检索。在任何情况下，用户都已经获得了在由用户试图访问的受保护资源所要求的验证上下文中有效的证书。尽管，

应当注意，用户对于在由受保护资源所要求的验证上下文中有效的证书的拥有并不一定保证用户对于访问受保护资源的请求将被准许或将成功；例如，可能发生各种错误，或者可能基于各种其他限制而否定或拒绝用户的请求，比如由被认为未被包括在受保护资源所要求的验证上下文中的限制策略的下游实体的断言。

[0059] 现在参考图 5，方框图绘出了根据本发明的实施例的、由支持扩展的验证操作的会话管理服务器所管理的一些信息。会话管理服务器 500 与图 4 所示的会话管理服务器 404 类似。会话管理服务器 500 在会话数据结构 502 中存储用于管理用户会话的信息，该会话数据结构 502 是包含了诸如会话项 504 的多个会话项的表格或某个其它类型的数据结构。会话项 504 包含会话标识符 506，会话标识符 506 是该会话的唯一标识符。会话项 504 还可以存储用户标识符 508，用户标识符 508 是用于与发起在包含会话管理服务器 500 的企业域内的会话的客户端相关联的、用户的唯一标识符。另外的会话状态变量 510 可以被本地存储在每个会话项中。

[0060] 会话项 504 还包含用户证书 512，当需要时使用该用户证书 512 来授权拥有该证书的用户访问受保护资源。用户证书 512 指示其中生成该证书的验证上下文或上下文 514。会话项 504 还可以包含缓存的请求消息 516，其是来自发起进行验证操作以获得更新后的证书的需要的客户端 / 用户的原始请求消息的所存储的副本。

[0061] 会话管理服务器 500 还存储指示需要特定验证上下文的受保护资源的表格 518 或类似的数据结构。每个资源可以由其 URI 来标识，并且可以与 URI 关联地存储其所要求的验证上下文，从而对于每个所呈现的受保护资源形成 具有 URI 520 和验证上下文指示符 522 的密钥值对。依据验证上下文的实施方式，验证上下文指示符 522 可以是一个或多个数据项的集合。

[0062] 会话管理服务器 500 还存储指示验证代理服务器的位置的可配置的验证代理服务器 URI 524。在会话管理服务器 500 的初始化阶段期间，可配置 URI524 和可配置的表格 518 在从配置文件中检索之后，可以被缓存在存储器中。

[0063] 现在参考图 6，方框图绘出了根据本发明的实施例的、由支持验证操作的验证代理服务器所管理的一些信息。验证代理服务器 600 与图 4 所示的验证代理服务器 412 类似。验证代理服务器 600 存储用于从所请求的验证上下文映射到能够生成对于相关验证上下文有效的用户证书的验证操作的信息。例如，可以是表格或类似数据结构的数据结构 602 包含密钥值对；验证上下文 604 的每个指示符与验证操作 606 成对。依据验证上下文的实施方式，验证上下文指示符 604 可以是一个或多个数据项的集合。

[0064] 另外，验证代理服务器 600 还存储可配置的会话管理服务器 URI 608，其指示从其处接收验证请求和 / 或应该将验证响应返回到其处的会话管理服务器的位置。在验证代理服务器 600 的初始化阶段期间，可配置 URI 608 和可配置的表格 602 在从配置文件中检索之后，可以被缓存在存储器中。

[0065] 现在参考图 7，方框图绘出了根据本发明的实施例的、在会话管理服务器到验证代理服务器之间的验证请求消息中可能包含的一些信息。验证请求消息 702 包含用户当前证书 704 的副本；如由后端验证方法 / 服务器要求、使用用户当前证书来生成更新后的用户证书。被请求的验证上下文 706 指示更新后的用户证书所要求的验证上下文，如由已经发起验证操作的会话管理服务器所确定的。在某些情况下，后端验证方法 / 服务器可能需要与

用户交互以完成验证操作；对于那些情况，定制信息 708 被包括在验证请求 702 中。应当注意，验证请求消息 702 表示被关联地存储和 / 或传送的信息项，并且可以以各种数据格式来实现这些信息项，包括作为嵌入其他消息中的它们的包含物。

[0066] 当请求与用户交互以完成验证操作时，定制信息 708 可以用于定制与用户的客户端交换的信息。通过提供用户名或其他前后关系的信息，可以更加用户友好地进行验证操作，或者关于对验证操作的需要更多信息量地进行验证操作，例如指示用户所请求的业务需要另外的安全进程，因为该业务必须与用户已知的另一网站交互。

[0067] 现在参考图 8，方框图绘出了根据本发明的实施例的、在从验证代理服务器到会话管理服务器的验证响应消息中可能包含的一些信息。验证响应消息 802 包含用户的更新后的证书的副本 804。当由初始地请求更新后的证书的会话管理服务器通过验证操作接收更新后的证书时，更新后的证书将被缓存。例如，更新后的证书可能被缓存在适当的用户的会话项信息中，用于随后在访问受保护资源中使用。应当注意，验证响应消息 802 表示被关联地存储和 / 或传送的信息项，并且可以以各种数据格式实现这些信息项，包括作为嵌入其他消息中的它们的包含物。

[0068] 现在参考图 9，流程图绘出了根据本发明的实施例的处理，通过该处理，会话管理服务器发起验证操作。当诸如图 4 所示的会话管理服务器 404 的会话管理服务器接收了要访问受保护资源的请求时，处理开始（步骤 902）；该请求可以被缓存在用户的会话信息中用于随后检索。会话管理服务器从到来的请求消息中提取所请求的受保护资源的 URI（步骤 904），并使用所提取的 URI 执行查找操作，以获得受保护资源所要求的验证上下文（步骤 906）；使用诸如图 5 所示的表格的可配置表格或其他数据存储来执行查找操作。在此例子中，会话管理服务器确定，用户的证书缺乏所要求的验证上下文（步骤 908）。换句话说，用户的当前证书无效、不合适、不足够、不满足或与由用户正试图访问的受保护资源所要求的类型或特性不同的类型或特性。因此，会话管理服务器确定，需要验证操作来更新用户的证书。如果用户的证书满足受保护资源对于特定验证上下文的要求，则如需要、可以转发用户的请求以尝试获得对于受保护资源的访问，而不需进一步处理，这在图中未示出。

[0069] 会话管理服务器生成验证请求（步骤 910），其包括当前用户证书和由受保护资源所要求的验证上下文的指示。然后，会话管理服务器将所生成的消息内的验证请求发送到验证代理服务器（步骤 912），并且处理终止。验证代理服务器的 URI 可以是由会话管理服务器从适当的数据存储中检索的可配置的值，例如图 5 所示。

[0070] 现在参考图 10，流程图绘出了根据本发明的实施例的处理，通过该处理，验证代理服务器管理如所请求的验证操作。当验证代理服务器接收到验证请求时，处理开始（步骤 1002）。所接收的请求以某种方式指示，关于如所接收的请求内所指示的具体类型的验证上下文，正请求更新当前证书。验证代理服务器从到来的请求中提取所指示的验证上下文（步骤 1004），并使用所 指示的验证上下文来执行查找操作以获得已经与验证上下文相关联的验证操作（步骤 1006）；使用诸如图 6 所示的表格的可配置表格或其他数据存储来执行查找操作。

[0071] 如从查找操作所确定的，仍然包含用户的当前证书的验证请求被转发或被发送到适当的后端验证服务器（步骤 1008）。如果需要，验证服务器与用户交互，以获得附加信息或完成关于用户的所请求的验证操作（步骤 1010）。验证服务器生成更新后的用户证书（步

骤1012)，其以某种方式被提供给或发送到验证代理服务器。验证代理服务器向发出请求的会话管理服务器发送更新后的用户证书作为消息内的验证响应（步骤1014)，从而终止处理。发出请求的会话管理服务器的URI可以是由验证代理服务器从适当的数据存储中检索的可配置的值，例如图6所示。

[0072] 现在参考图11，流程图绘出了根据本发明的实施例的处理，通过该处理，会话管理服务器完成验证操作。当已经发起验证操作的会话管理服务器接收到对于其请求的响应时，处理开始（步骤1102)，并且从该响应中提取更新后的用户证书（步骤1104)，并将更新后的用户证书缓存用于随后使用（步骤1106)。然后例如从用户的会话信息中检索访问受保护资源的用户原始请求，并以适当的方式将其发送到受保护资源（步骤1108)，从而终止处理。该请求可以附有用户的更新后的证书，其指示如由受保护资源所要求的适当的验证上下文，或者用户的更新后的证书仍然可用于当需要时由下游实体检索。

[0073] 考虑到以上提供的本发明的详细描述，本发明的优点显而易见。受保护资源可以要求用户已经获得如由与受保护资源的URI相关联的可配置的验证上下文指示符所指示的特定验证上下文内的验证证书。当接收到访问受保护资源的请求时，将所请求的受保护资源所需的验证上下文与例如用户证书内所指示的、其中或对于其生成用户证书的验证上下文相比较。如果用户在该验证上下文内还没有被验证，即，如果用户的证书没有指示适当的验证上下文，则本发明使用适合于受保护资源所要求的验证上下文的验证操作来触发用户的再验证。

[0074] 本发明允许系统管理员通过在单一的验证代理服务器后面布置验证操作或服务器，来有效地扩展可用于数据处理系统内使用的验证操作。因此，通过指定单一的验证代理服务器的单一URI，可以容易地执行会话管理服务器 的配置。然后，由会话管理服务器等同地对待需要验证的所有到来的请求。会话管理服务器保持预先存在的用户会话，更新后的证书变得与预先存在的用户会话关联，而不建立更新后的证书的新会话。

[0075] 重要的是，注意，尽管在具有充分功能的数据处理系统的上下文中描述了本发明，但是本领域普通技术人员将认识到，能够以计算机可读介质中的指令的形式和各种其他形式来分配本发明的处理，无论实际用于实行分配的承载介质的具体类型。计算机可读介质的例子包括诸如EPROM、ROM、磁带、纸张、软盘、硬盘驱动、RAM和CD-ROM的介质、以及诸如数字和模拟通信链接的传输型介质。

[0076] 一般将方法构思为通向所希望的结果的前后一致的步骤的序列。这些步骤要求对物理量的物理操纵。一般而言，尽管不是必须的，这些量采取能够被存储、传送、组合、比较或操纵的电或磁信号的形式。有时，主要由于一般使用的原因，将这些信号称作位、值、参数、项、元件、对象、符号、字符、术语、数字等很方便。然而，应当注意，所有这些术语和类似的术语都与适当的物理量有关，并且仅是方便应用于这些量的标签。

[0077] 出于说明的目的已经给出了本发明的描述，但是不意要详尽或限制本发明于所公开的实施例。对于本领域普通技术人员而言，很多修改和变更将是显然的。选择实施例以说明本发明的原理及其实际应用，以及以使本领域普通技术人员能够理解本发明以便用可能适合于其他预期使用的各种修改来实现各种实施例。

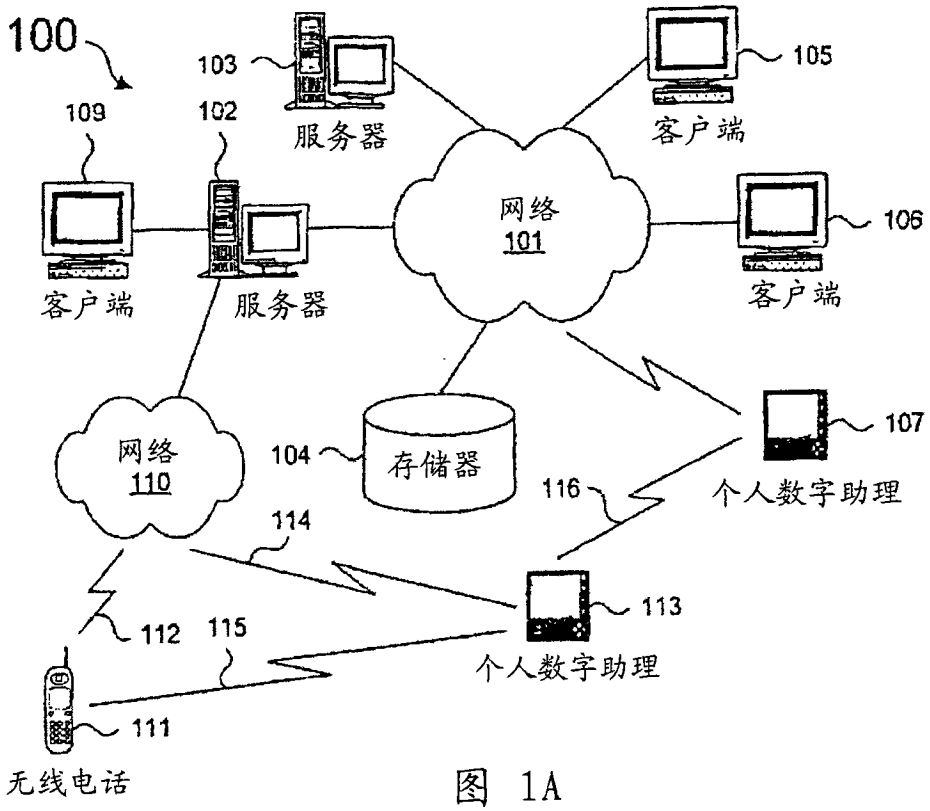


图 1A
(现有技术)

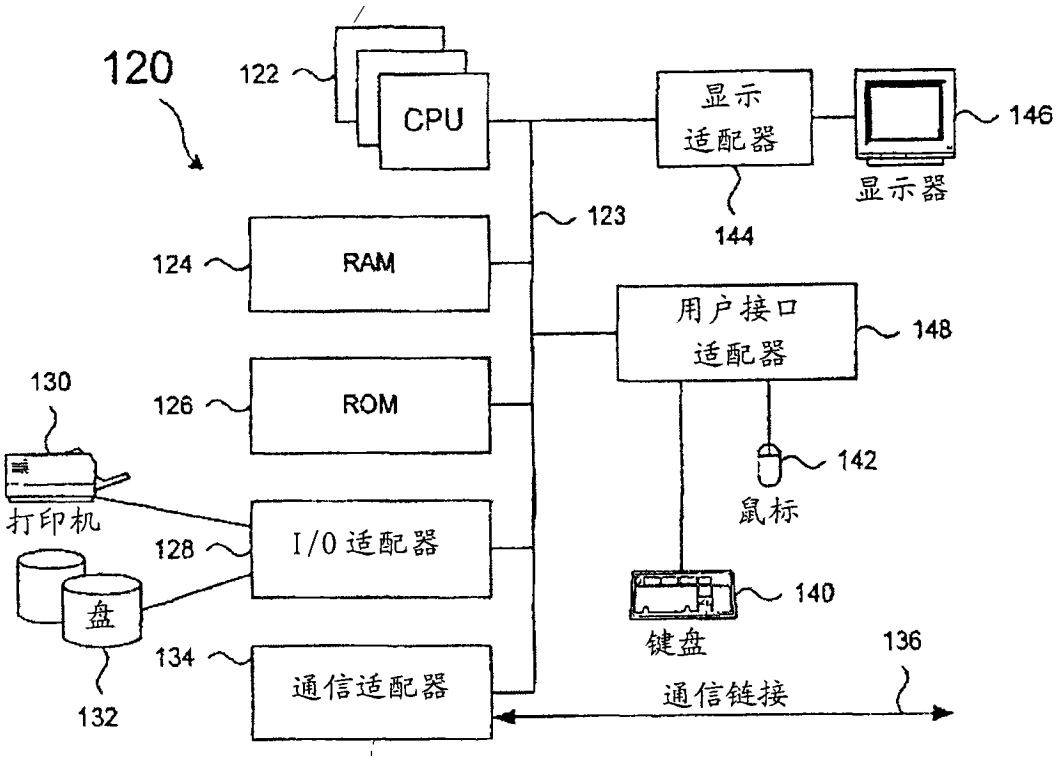


图 1B （现有技术）

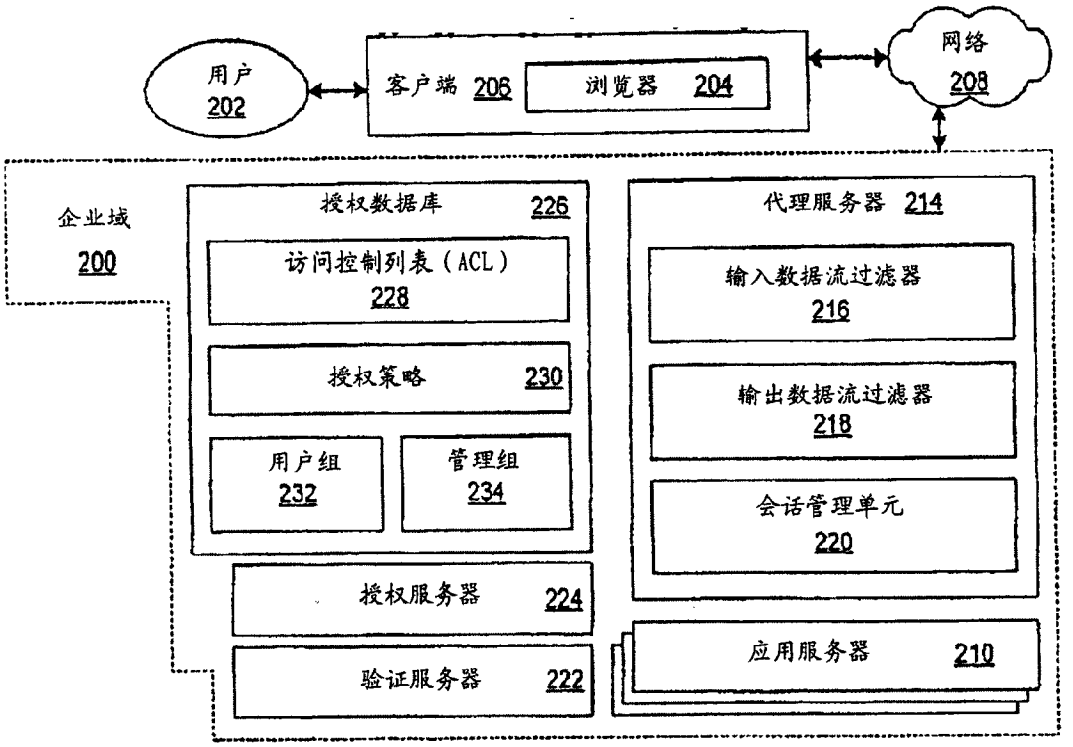


图 2
（现有技术）

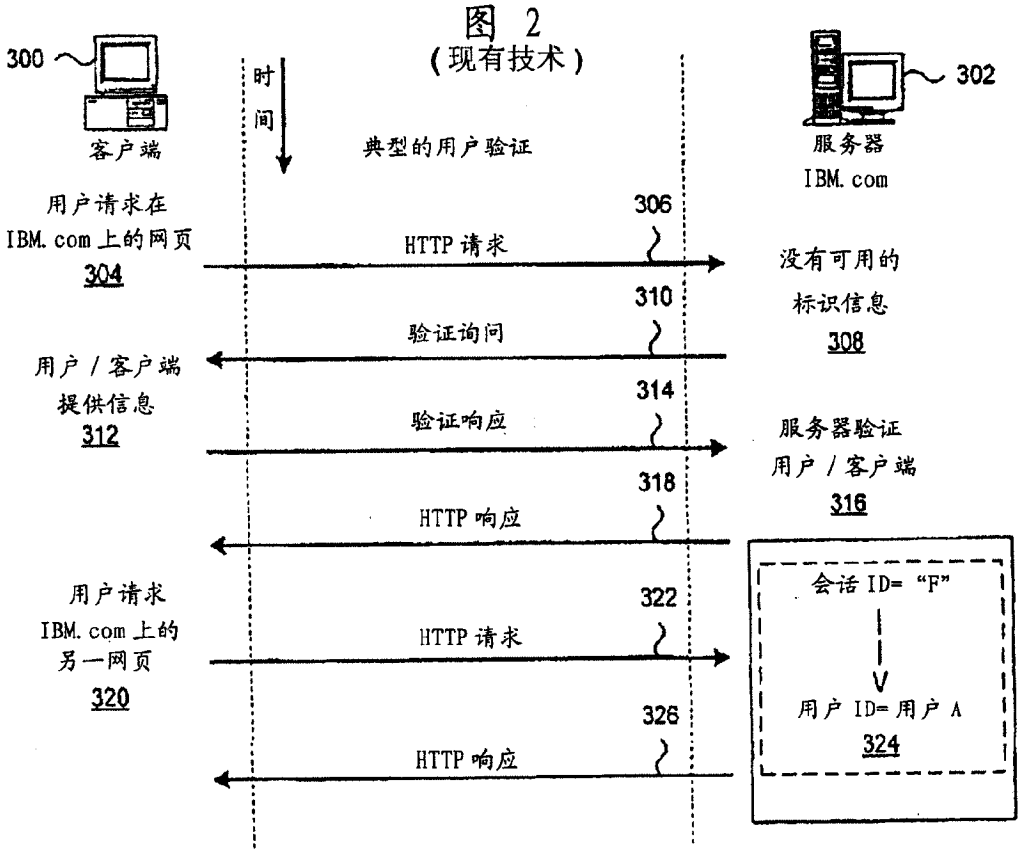


图 3
（现有技术）

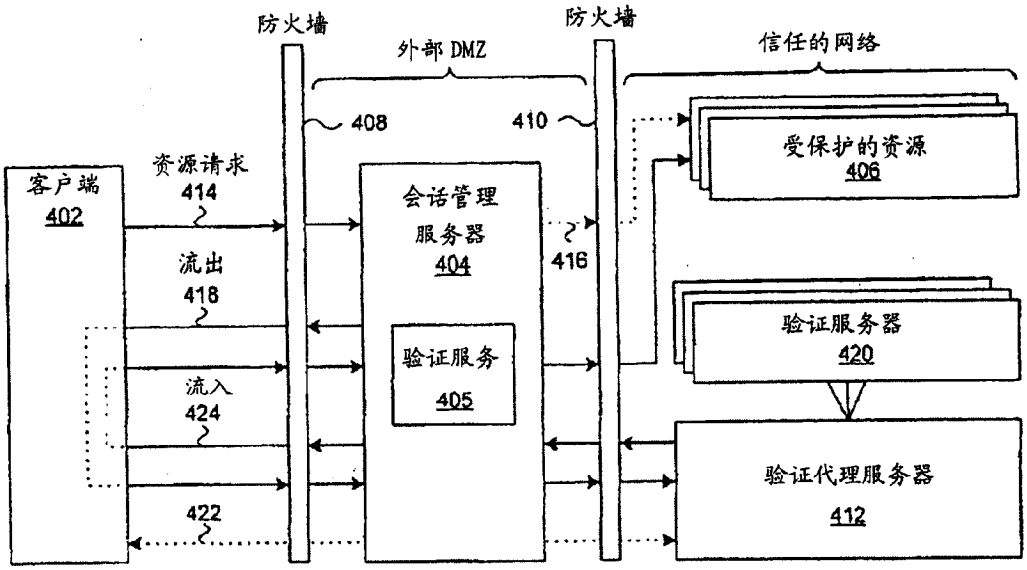

防火墙
外部 DMZ
防火墙
信任的网络
408
410
客户端
402
资源请求
414
会话管理
服务器
404
416
受保护的资源
406
流出
418
验证服务
405
验证服务器
420
流入
424
验证代理服务器
412
422

图 4

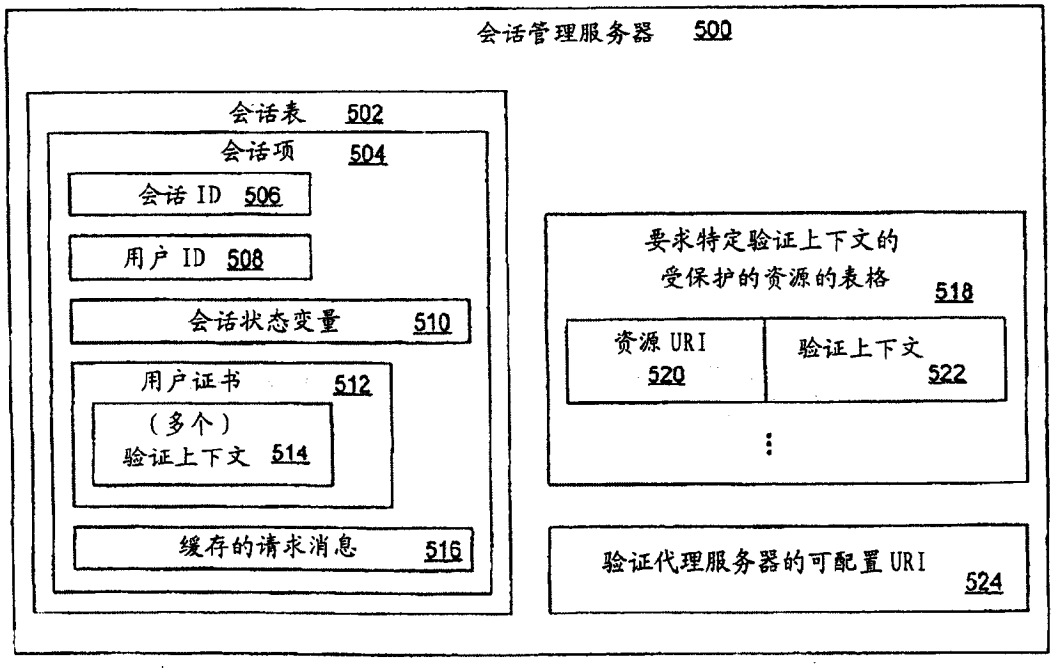

会话管理服务器 500
会话表 502
会话项 504
会话 ID 506
用户 ID 508
会话状态变量 510
用户证书 512
(多个)
验证上下文 514
缓存的请求消息 516
要求特定验证上下文的
受保护的资源的表格 518
资源 URI
520
验证上下文
522
验证代理服务器的可配置 URI
524

图 5

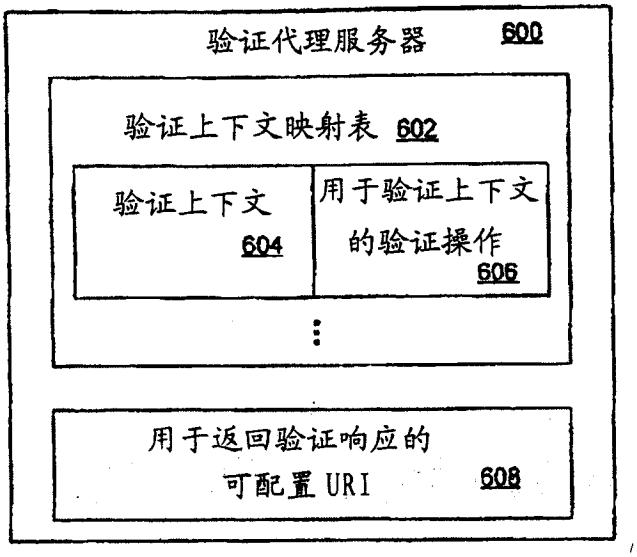

验证代理服务器 600
验证上下文映射表 602
验证上下文 604
用于验证上下文的验证操作 606
用于返回验证响应的可配置 URI 608

图 6

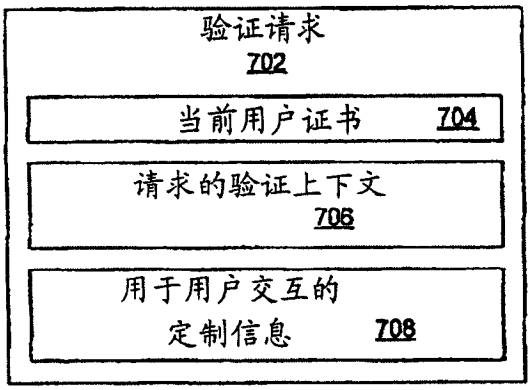

验证请求 702
当前用户证书 704
请求的验证上下文 706
用于用户交互的定制信息 708

图 7

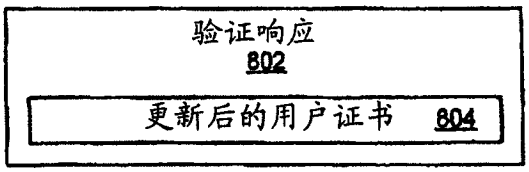

验证响应 802
更新后的用户证书 804

图 8

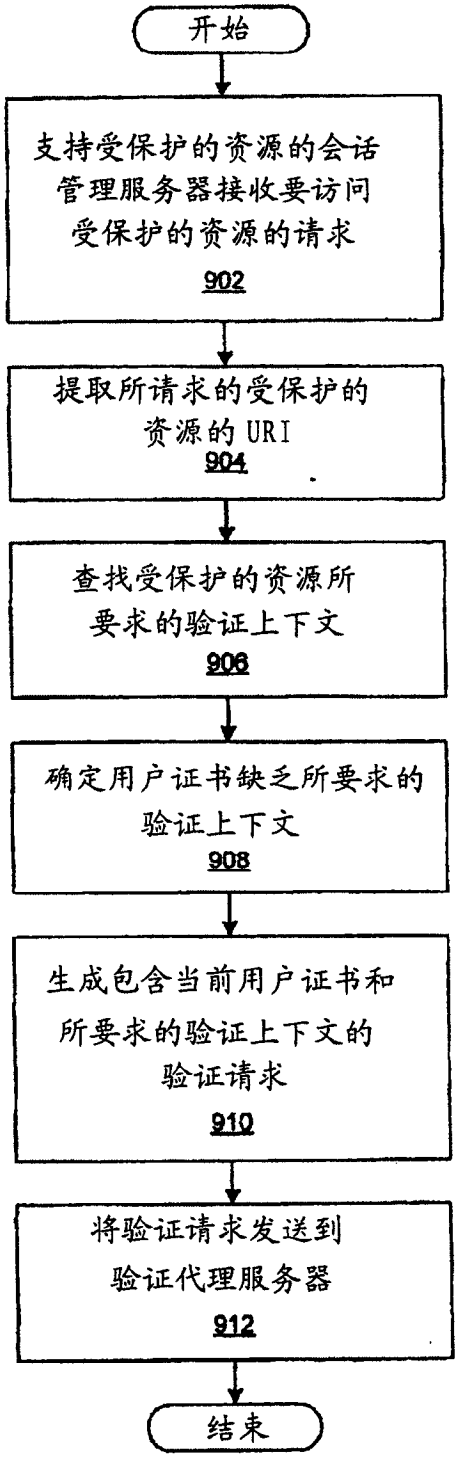

开始
支持受保护的资源的会话管理服务器接收要访问受保护的资源的请求
902
提取所请求的受保护的资源的 URI
904
查找受保护的资源所要求的验证上下文
906
确定用户证书缺乏所要求的验证上下文
908
生成包含当前用户证书和所要求的验证上下文的验证请求
910
将验证请求发送到验证代理服务器
912
结束

图 9

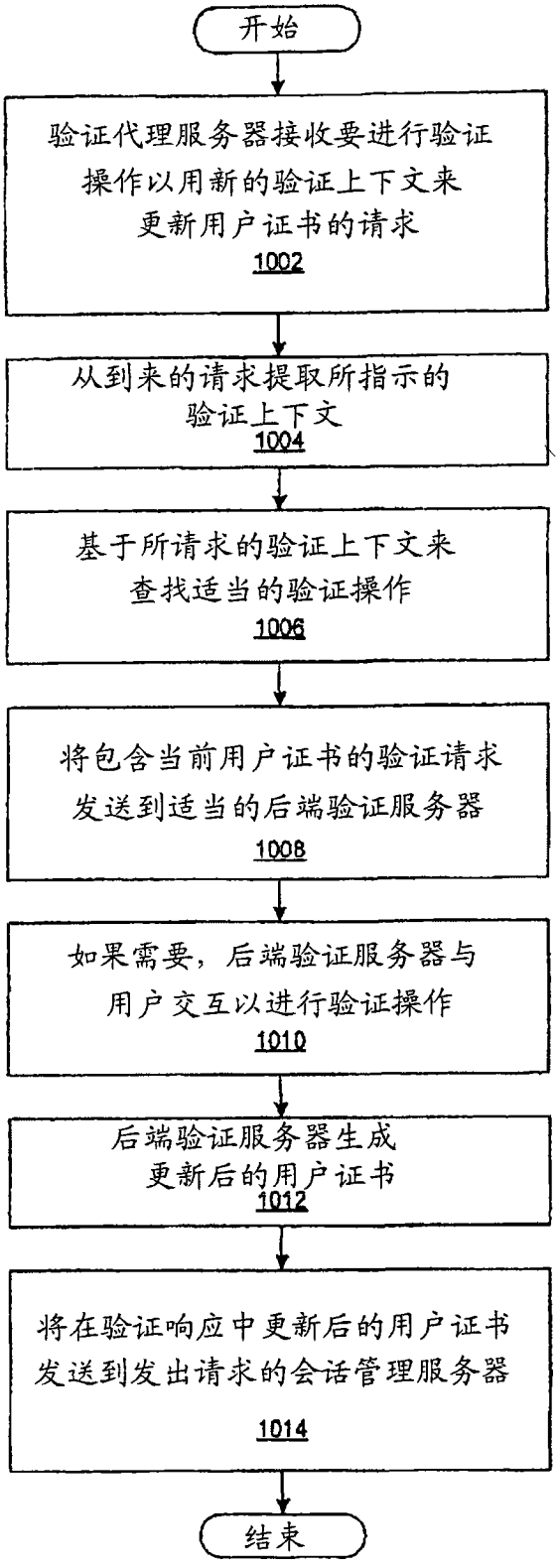

开始
验证代理服务器接收要进行验证操作以用新的验证上下文来更新用户证书的请求
1002
从到来的请求提取所指示的验证上下文
1004
基于所请求的验证上下文来查找适当的验证操作
1006
将包含当前用户证书的验证请求发送到适当的后端验证服务器
1008
如果需要，后端验证服务器与用户交互以进行验证操作
1010
后端验证服务器生成更新后的用户证书
1012
将在验证响应中更新后的用户证书发送到发出请求的会话管理服务器
1014
结束

图 10

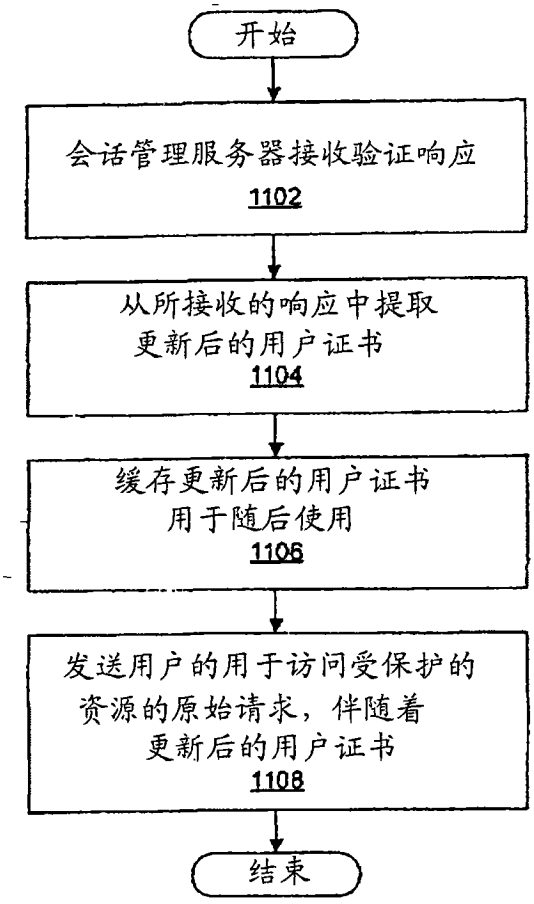

开始
会话管理服务器接收验证响应
1102
从所接收的响应中提取
更新后的用户证书
1104
缓存更新后的用户证书
用于随后使用
1106
发送用户的用于访问受保护的
资源的原始请求，伴随着
更新后的用户证书
1108
结束

图 11