(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 101790879 B
(45)授权公告日 2013.04.24

(21)申请号 200880102115.4
(22)申请日 2008.05.27
(30)优先权数据
07011126.5 2007.06.06 EP
(85)PCT申请进入国家阶段日
2010.02.05
(86)PCT申请的申请数据
PCT/EP2008/056466 2008.05.27
(87)PCT申请的公布数据
WO2008/148664 EN 2008.12.11
(73)专利权人 格马尔托股份有限公司
地址 法国默东
(72)发明人 O·约弗雷 P·斯马达
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 李娜 李家麟
(51)Int.Cl.
H04L 29/08(2006.01)
(56)对比文件
JP 2007079988 A,2007.03.29, 说明书第29,33-36,44-45,63-64段.
WO 2005064889 A1,2005.07.14, 说明书第5页第20行至第12页第30行、附图2-11.
审查员 杨威明

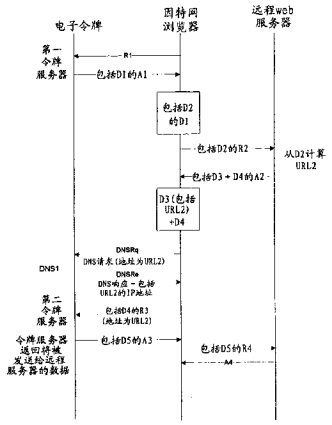
权利要求书2页 说明书5页 附图3页

(54)发明名称

管理电子令牌与远程web服务器之间的通信的方法

(57)摘要

本发明是一种管理电子令牌与远程web服务器之间的通信的方法。所述令牌和服务器连接到相同的主机。所述电子令牌包括第一和第二令牌服务器和包含HTML数据的存储器。该主机具有因特网web浏览器。所述方法包括步骤:将第一请求从因特网web浏览器发送给第一令牌服务器;将第一应答返回给该因特网浏览器,所述第一应答包括HTML数据,所述HTML数据包括与脚本相关联的连接信息;在因特网web浏览器上,执行与所述连接信息相关联的脚本。对所述脚本的执行建立到所述远程服务器的连接,所述连接通过充当网关的所述因特网浏览器允许在第二令牌服务器与所述远程服务器之间进行双向通信。



CN 101790879 B

1. 一种管理电子令牌 (ET) 与远程 web 服务器 (RS) 之间的通信的方法，所述电子令牌 (ET) 连接到主机 (HM) 并且包括微处理器 (MP)、通信接口 (INF)、以及存储器 (MEM)，所述存储器 (MEM) 包括操作系统 (OS) 和至少第一 HTML 数据 (D1)，所述电子令牌 (ET) 包括至少第一和第二令牌服务器 (CS1，CS2)，所述远程 web 服务器 (RS) 连接到所述主机 (HM)，所述主机 (HM) 具有因特网 web 浏览器 (WB)，所述方法如下步骤：

- 将第一请求 (R1) 从所述因特网 web 浏览器 (WB) 发送 (S2) 给第一令牌服务器 (CS1)，

- 从第一令牌服务器 (CS1) 将第一应答 (A1) 返回 (S3) 给所述因特网 web 浏览器 (WB)，所述第一应答 (A1) 包括第一 HTML 数据 (D1)，所述第一 HTML 数据 (D1) 包括与脚本 (SC1) 相关联的连接信息 (CI)，

- 在所述因特网 web 浏览器 (WB) 上，执行 (S5) 与所述连接信息 (CI) 相关联的脚本 (SC1)，

其特征在于，对所述脚本 (SC1) 的执行建立到所述远程 web 服务器 (RS) 的连接，所述连接通过充当网关的因特网 web 浏览器 (WB) 允许在第二令牌服务器 (CS2) 与所述远程 web 服务器 (RS) 之间进行双向通信，

其中第一 HTML 数据 (D1) 包括第二数据 (D2)，并且其中所述方法包括进一步的步骤：

- 从所述因特网 web 浏览器 (WB) 将第二请求 (R2) 发送 (S6) 给所述远程 web 服务器 (RS)，其中所述第二请求 (R2) 包括第二数据 (D2)，

- 在所述远程 web 服务器 (WB) 上，基于第二数据 (D2) 计算 (S7) 特定的 URL(URL2)，所述特定的 URL(URL2) 允许连接到第二令牌服务器 (CS2)，

- 从所述远程 web 服务器 (RS) 将第二应答 (A2) 返回 (S8) 给所述因特网 web 浏览器 (WB)，所述第二应答 (A2) 包括第三数据 (D3)，所述第三数据 (D3) 包括所述特定的 URL(URL2)，

- 在所述因特网 web 浏览器 (WB) 上，利用第三请求 (R3) 将从所述远程 web 服务器 (RS) 所接收的所述第二应答 (A2) 路由 (S11) 到第二令牌服务器 (CS2)。

2. 根据权利要求 1 所述的方法，其中返回 (S8) 第二应答 (A2) 的步骤由 HTTP 重定向功能或者由 HTML 自动提交功能来执行。

3. 根据权利要求 1 所述的方法，其中所述电子令牌 (ET) 包括包含本地域名服务器 (DNS1) 的虚拟局域网，并且其中所述方法包括进一步的步骤：

- 从所述因特网 web 浏览器 (WB) 将 DNS 请求 (DNSRq) 发送 (S9) 给本地域名系统 DNS 服务器 (DNS1)，所述 DNS 请求 (DNSRq) 包括所述特定的 URL(URL2)，

- 接收 (S10) 包括 IP 地址的 DNS 应答 (DNSRe)，其中所述 IP 地址对应于由所述本地域名系统 DNS 服务器 (DNS1) 发送给所述因特网 web 浏览器 (WB) 的所述特定 URL(URL2)。

4. 根据权利要求 1 所述的方法，其中所述第二应答 (A2) 包括第四数据 (D4)，并且其中所述第三请求 (R3) 包括第四数据 (D4)。

5. 根据权利要求 1 所述的方法，其中所述方法包括进一步的步骤：

- 响应于第三请求 (R3)，将第三应答 (A3) 从第二令牌服务器 (CS2) 发送 (S12) 给所述因特网 web 浏览器 (WB)，所述第三应答 (A3) 包括第五数据 (D5)，

- 将所述第五数据 (D5) 从所述因特网 web 浏览器 (WB) 路由 (S13) 到所述远程 web 服务器 (RS)。

6. 根据权利要求 1 所述的方法，其中第二数据 (D2) 包括可变部分，所述可变部分被随机设置或者根据预先定义的序列而被计算出。

7. 根据权利要求 1-6 任一所述的方法，其中所述第一和第二令牌服务器 (CS1，CS2) 中的每个是 HTTP 服务器或者 HTTPS 服务器。

8. 根据权利要求 1-6 任一所述的方法，其中所述第一和第二令牌服务器 (CS1，CS2) 被并入唯一的令牌服务器中。

9. 根据权利要求 1-6 任一所述的方法，其中所述连接信息 (CI) 包括所述脚本 (SC1) 或者能够从其下载所述脚本 (SC1) 的脚本 URL(URL3)。

10. 根据权利要求 1-6 任一所述的方法，其中所述脚本 (SC1) 是 java 脚本。

管理电子令牌与远程 web 服务器之间的通信的方法

技术领域

[0001] 本发明涉及管理电子令牌与远程服务器之间的通信的方法。本发明尤其涉及管理包括服务器的电子令牌与远程 web 服务器之间的通信的方法。

背景技术

[0002] 电子令牌是便携式电子物体、比如智能卡、便携式音频设备、手机、个人数字助理、或者 USB 令牌。用语“因特网”是指“互连的网络”。电子令牌可以嵌入包括超文本传输协议 HTTP 服务器、本地域名系统 DNS 服务器、或者动态主机配置协议 DHCP 服务器的局域网。可替换地，该局域网可以是这些服务器的组合。该局域网可以包括唯一的或者几个将 HTTP 和 / 或 DNS 和 / 或 DHCP 的功能和 / 或根据万维网联盟 (W3C) 规则的任意服务或服务器的功能相组合的本地服务器，所述服务器具有唯一的 IP 地址。

[0003] 电子令牌可以连接到主机。主机可以通过因特网连接到远程服务器。远程服务器是被放置在可通过因特网到达的机器上的远距离服务器。当远程服务器和电子令牌二者都连接到同一主机时，所述远程服务器和电子令牌可以通过该主机进行通信。连接到因特网的现有主机具有因特网 web 浏览器、比如 Microsoft Internet **Explorer ®** 或者 Mozilla **Firefox ®**。

[0004] 目前为了建立电子令牌与远程服务器之间的通信，必需使用共享机制的因特网连接或者通过安装保证相同功能的专用软件来定制主机。然而，管理权可能对主机的定制进行限制或者禁止。

发明内容

[0005] 本发明的目的在于允许通过主机在没有对所述主机进行定制的情况下在电子令牌与远程服务器之间的通信。本发明的目的在于允许电子令牌与远程服务器之间的在两个方向上的通信连接和自动数据路由。

[0006] 本发明的目的是一种管理电子令牌与远程 web 服务器之间的通信的方法。该电子令牌连接到主机并且包括微处理器、通信接口、以及存储器。所述存储器包括操作系统和至少第一 HTML 数据。所述电子令牌包括至少第一和第二令牌服务器。该远程 web 服务器连接到所述相同的主机。该主机具有因特网 web 浏览器。所述方法包括步骤：

[0007] - 将第一请求从因特网 web 浏览器发送给第一令牌服务器，

[0008] - 从第一令牌服务器将第一应答返回给该因特网 web 浏览器，所述第一应答包括第一 HTML 数据，所述第一 HTML 数据包括与脚本相关联的连接信息，

[0009] - 在该因特网 web 浏览器上，执行与所述连接信息相关联的脚本，

[0010] 其特征在于，对所述脚本的执行建立到所述远程 web 服务器的连接，所述连接通过充当网关的所述因特网 web 浏览器允许在第二令牌服务器与所述远程 web 服务器之间进行双向通信。

[0011] 第一 HTML 数据可以包括第二数据，并且所述方法可以包括进一步的步骤：

[0012] -从所述因特网web浏览器将第二请求发送给所述远程web服务器，其中所述第二请求包括第二数据，

[0013] -在所述远程web服务器上，基于第二数据计算特定的URL，所述特定的URL允许连接到第二令牌服务器，

[0014] -从所述远程web服务器将第二应答返回给所述因特网web浏览器，所述第二应答包括第三数据，所述第三数据包括所述特定的URL，

[0015] -在所述因特网web浏览器上，利用第三请求将从所述远程web服务器所接收的所述第二应答路由到第二令牌服务器。

[0016] 返回第二应答的步骤可以由HTTP重定向功能或者由HTML自动提交功能来执行。

[0017] 该电子令牌可以包括包含本地域名服务器的虚拟局域网。该方法可以包括进一步的步骤：

[0018] -从所述因特网web浏览器将DNS请求发送给本地域名系统DNS服务器，所述DNS请求包括所述特定的URL，

[0019] -接收包括IP地址的DNS应答，其中所述IP地址对应于由所述本地域名系统DNS服务器发送给所述因特网web浏览器的所述特定URL。

[0020] 第二应答可以包括第四数据，并且第三请求可以包括第四数据。

[0021] 该方法可以包括进一步的步骤：

[0022] -响应于第三请求，将第三应答从第二令牌服务器发送给所述因特网web浏览器，所述第三应答包括第五数据，

[0023] -将所述第五数据从所述因特网web浏览器路由到所述远程web服务器。

[0024] 第二数据可以包括可变部分，所述可变部分可以被随机设置或者根据预先定义的序列而被计算出。

[0025] 所述第一和第二令牌服务器中的每个都可以是HTTP服务器或者HTTPS服务器。

[0026] 所述第一和第二令牌服务器可以被并入唯一的令牌服务器中。

[0027] 所述连接信息可以包括所述脚本或者从其可以下载所述脚本的脚本URL。

[0028] 所述脚本可以是java脚本。

[0029] 本发明的另一目的是一种旨在连接到主机的电子令牌。所述令牌含有微处理器、通信接口、以及存储器。所述存储器包括操作系统和至少第一HTML数据。所述令牌包括至少第一和第二令牌服务器。该主机具有因特网web浏览器并且连接到远程web服务器。所述令牌的特征在于，第一HTML数据包括与脚本相关联的连接信息，所述连接信息旨在被第一令牌服务器发送。由所述主机的因特网web浏览器对所述脚本的执行建立到所述远程web服务器的连接，所述连接通过充当网关的所述因特网web浏览器允许在第二令牌服务器与所述远程web服务器之间进行双向通信。

[0030] 所述令牌可以是智能卡、便携式音频设备、手机、个人数字助理、或者USB令牌。

附图说明

[0031] 参考相应附图，阅读下面对本发明多个优选实施例的描述，本发明的其它特征和优点将更清楚地显现，其中：

[0032] 图1示意性地示出了根据本发明的智能卡类型的电子令牌的体系结构；

[0033] 图 2 示意性地示出了根据本发明的在电子令牌、主机和远程 web 服务器之间的交互；

[0034] 图 3 是根据本发明的用于管理电子令牌与远程 web 服务器之间的通信的一系列步骤的例子；

[0035] 图 4 是根据本发明的在电子令牌、主机和远程 web 服务器之间的数据交换的例子。

具体实施方式

[0036] 本发明可以适用于连接到主机的任意类型的电子令牌。在本说明书中，所述电子令牌是智能卡，但是其可以是任意其它种类的嵌入了服务器的电子令牌或者便携式设备。

[0037] 本发明的优点是：借助于由所连接的主机的因特网 web 浏览器所管理的网关，允许自动处理在电子令牌与远程 web 服务器之间所交换的数据。

[0038] 图 1 示出了智能卡的体系结构作为根据本发明优选实施例的电子令牌的例子。该智能卡 ET 含有微处理器 MP、通信接口 INT、以及存储器 MEM。存储器 MEM 含有操作系统 OS 和第一 HTML 数据 D1。第一 HTML 数据 D1 可以对应于 HTML 页面内容。第一 HTML 数据 D1 含有连接信息 CI 和第二数据 D2。存储器 MEM 可以包括唯一的电路或者可以具有不同类型的几个电路。

[0039] 如图 2 所示，智能卡 ET 含有第一服务器 CS1、第二服务器 CS2、以及本地域名系统 DNS 服务器 DNS1。主机 HM 含有因特网 web 浏览器 WB。因特网 web 浏览器 WB 具有脚本引擎 EN。脚本引擎能够执行脚本。在该文献的下面的部分中，当脚本被因特网 web 浏览器 WB 执行时，该脚本是由该因特网 web 浏览器 WB 的脚本引擎执行的。

[0040] 智能卡 ET 通过读卡器或者专用接口连接到主机 HM、比如个人计算机。该电子令牌可以通过接触链路或者无线链路连接到该主机。

[0041] 远程 web 服务器 RS 仅通过因特网或者通过几个通信渠道（比如因特网和空中下载 (OTA) 电信通信）的组合连接到主机 HM。在因特网上可以使用第二域名系统 DNS 服务器 DNS2。DNS2 可以返回与服务器相关的名称（比如“***.MyCompany.com”）的 IP 地址。

[0042] 图 3 示出了用于管理电子令牌与远程 web 服务器之间的连接和数据交换的步骤序列的例子。首先，用户启动主机 HM 上的因特网 web 浏览器 WB。在步骤 S1，该用户通过在因特网 web 浏览器 WB 中键入相应的地址来选择第一令牌服务器 CS1。例如，要到达的地址可以是 http://john.smith.secure 或者 https://john.smith.secure。第一请求 R1 然后在步骤 S2 被发送给所连接的电子令牌 ET 的服务器 CS1。然后在步骤 S3，第一应答 A1 被返回给主机 HM 的因特网 web 浏览器 WB。所述第一应答 A1 含有对应于第一 HTML 页面的第一 HTML 数据 D1。所述第一 HTML 数据 D1 含有连接信息 CI 和第二数据 D2。第二数据 D2 与第二令牌服务器 CS2 相关。第一 HTML 页面由因特网 web 浏览器 WB 来显示。所述第一 HTML 页面提供连接远程服务器 RS。然后，该用户选择连接远程服务器 RS。所述连接可以通过 HTTP 重定向或者 HTML 自动提交功能而是自动的。在步骤 S4 期间，因特网 web 浏览器 WB 从前面所接收的连接信息 CI 中提取脚本 SC1。然后，因特网 web 浏览器 WB 执行脚本 SC1。在步骤 S6，所述脚本执行将第二请求 R2 发送给远程服务器 RS。所述第二请求 R2 含有前面所接收的第二数据 D2。所述第二数据 D2 包括标识出电子令牌 ET 中的将要到达的服务器的信息。在步骤 S7，远程服务器 RS 借助于第二数据 D2 计算特定的 URL URL2。例如，第二数

据 D2 可以含有 URL2 的第一部分，并且远程服务器 RS 可以通过添加特定于该令牌 ET 的补充数据来完成所计算的特定 URL。因此，如果第二数据 D2 提供“smartcard192_168_1_1”并且远程服务器 RS 添加“MyCompany.c om”，则所计算的 URL2 是指“smartcard192_168_1_1.MyCompany.com”。然后，所计算的 URL2 可以被 DNS1 解析成该令牌 ET 中的服务器 CS2 的真实 IP 地址。例如，服务器 CS2 的真实 IP 地址可以等于 192.168.1.1。

[0043] 可替换地，所计算的 URL2 可以由远程 DNS2 来解析。

[0044] 然后在步骤 S8，远程 web 服务器 RS 将第二应答 A2 发送给所连接的主机 HM 的因特网 web 浏览器 WB。第二应答 A2 含有第三数据 D3，所述第三数据 D3 包括所计算的特定 URL URL2。

[0045] 可以利用 HTTP 重定向功能或者利用 HTML 自动提交功能来执行对第二应答 A2 的发送。

[0046] 可替换地，只要因特网 web 浏览器的使用允许自动连接功能，所述因特网 web 浏览器的其它功能就可以被挪用 (embezzle)。

[0047] 远程 URL URL1 被用于第二请求 R2。在优选的实施例中，远程 URLURL1 属于与所计算的特定 URL URL2 相同的域。

[0048] 在接收第二应答 A2 以后，因特网 web 浏览器 WB 可以在步骤 S9 将请求 DNSRq 发送给电子令牌 ET 的域名系统 DNS 服务器 DNS1。所述请求 DNSRq 允许获取对应于所接收的 URL2 的 IP 地址。然后在步骤 S10，DNS1 服务器发回对应于 URL2 的 IP 地址。所述 IP 地址对应于第二令牌服务器 CS2。

[0049] 然后在步骤 S11，因特网 web 浏览器 WB 通过将第三请求 R3 发送给令牌 ET 来将第二应答 A2 路由到第二令牌服务器 CS2。

[0050] 附加地，如图 4 所示，第二应答 A2 可以含有第四数据 D4，所述数据 D4 旨在供第二令牌服务器 CS2 使用。在这种情况下，第三请求 R3 含有第四数据 D4。例如，第四数据 D4 可以与对用户来说可用的新服务相关。在接收到第三请求 R3 以后，第一 HTML 数据 D1 可以被更新以便根据第四数据 D4 的内容来声明 (declare) 新服务。

[0051] 可替换地，含有第五数据 D5 的第三应答 A3 可以在步骤 S12 期间由第二令牌服务器 CS2 发送给因特网 web 浏览器 WB。所述第三应答 A3 可以由主机 HM 的因特网 web 浏览器 WB 路由到远程 web 服务器 RS。

[0052] 因此，两个连接被建立在因特网 web 浏览器 WB 上 :一个到远程服务器 RS，并且另一个使用 URL2 而到第二令牌服务器 CS2。

[0053] 有利地，第一令牌服务器 CS1 可以是 HTTP 服务器或者 HTTPS 服务器。第二令牌服务器 CS2 可以是 HTTP 服务器或者 HTTPS 服务器。

[0054] 有利地，第一和第二令牌服务器 CS1 和 CS2 可以被并入唯一的令牌服务器中。

[0055] 在上述的例子中，令牌 ET 包括虚拟局域网，所述虚拟局域网包括本地域名系统 DNS 服务器 DNS1。本发明还适用于未嵌入了虚拟局域网的电子令牌 ET。

[0056] 可替换地，因特网 web 浏览器 WB 可以在步骤 S4 期间从所接收的连接信息 CI 中提取脚本 URL URL3。URL3 对应于所述脚本 SC1 可以被找到的地址。脚本 SC1 然后从 URL3 中被下载并且被因特网 web 浏览器 WB 执行。

[0057] 在优选的实施例中，脚本 SC1 是 java 脚本。脚本 SC1 可以使用

XMLHttpRequestAPI。

[0058] 有利地，第二数据 D2 可以包括可变部分。所述可变部分可以被随机地设置或者根据预先定义的序列被计算出。所述可变部分可供 DNS1 使用。

[0059] 本发明的附加的优点是使用于到达第二令牌服务器 CS2 的特定 URLURL2 安全。URL2 可以在每当进行 (engage) 到远程 web 服务器 RS 的连接时改变。在所有情况下，远程 web 服务器 RS 和 DNS1 二者都动态地从相同信息中计算出 URL2。

[0060] 可替换地，可以从主机 HM 到达第二域名系统 DNS 服务器 DNS2。当利用 HTTP 重定向功能执行对第二应答 A2 的发送时，如果该电子令牌不具有 DNS1 则可以使用 DNS2。此外，如果该电子令牌不是 IP 令牌并且通过位于所连接的主机 HM 上的软件代理而被访问，则可以使用 DNS2。在这样的情况下，第一请求 R1 可以被寻址到主机地址（比如 http://127.0.0.1:4116）而不是 http://john.smith.secure，并且 URL2 指的是名称、比如被远程 DNS2 解析为“127.0.0.1”的“smartcard.MyCompagny.com”。

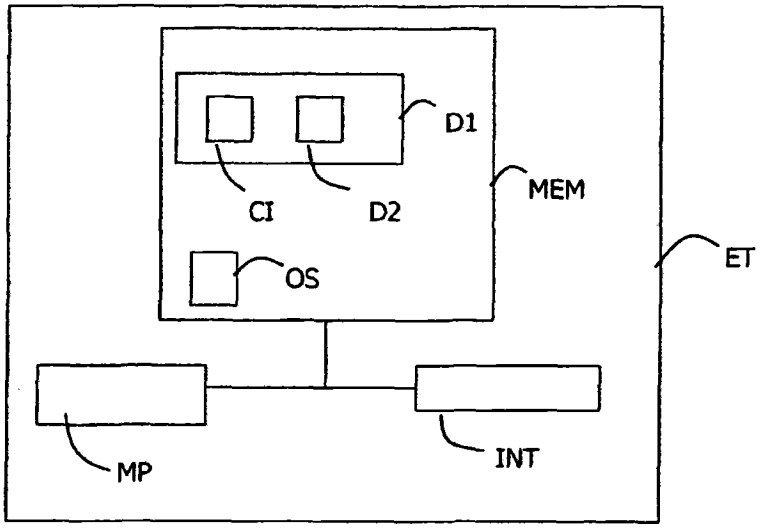


图 1

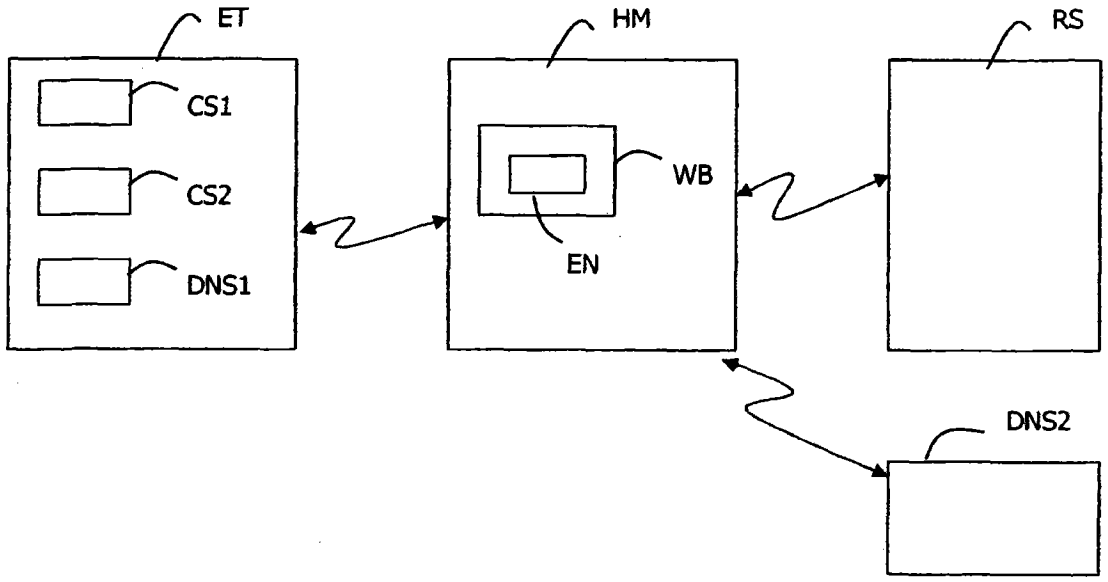


图 2

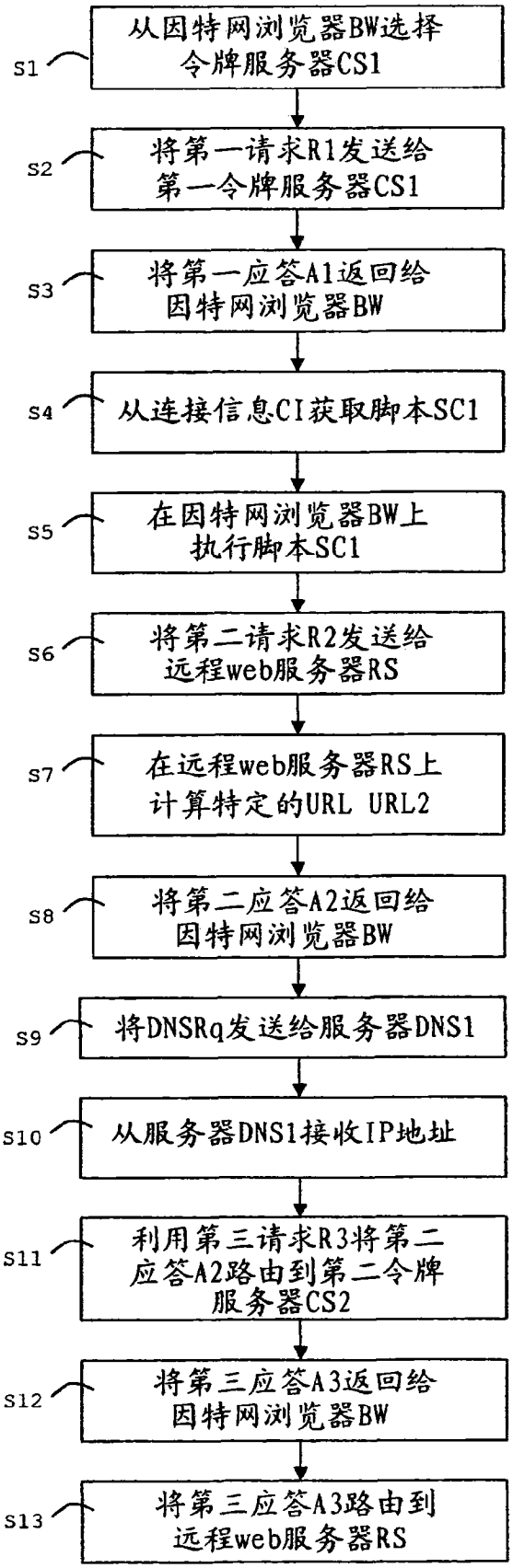

S1
从因特网浏览器BW选择令牌服务器CS1
S2
将第一请求R1发送给第一令牌服务器CS1
S3
将第一应答A1返回给因特网浏览器BW
S4
从连接信息CI获取脚本SC1
S5
在因特网浏览器BW上执行脚本SC1
S6
将第二请求R2发送给远程web服务器RS
S7
在远程web服务器RS上计算特定的URL URL2
S8
将第二应答A2返回给因特网浏览器BW
S9
将DNSRq发送给服务器DNS1
S10
从服务器DNS1接收IP地址
S11
利用第三请求R3将第二应答A2路由到第二令牌服务器CS2
S12
将第三应答A3返回给因特网浏览器BW
S13
将第三应答A3路由到远程web服务器RS

图 3

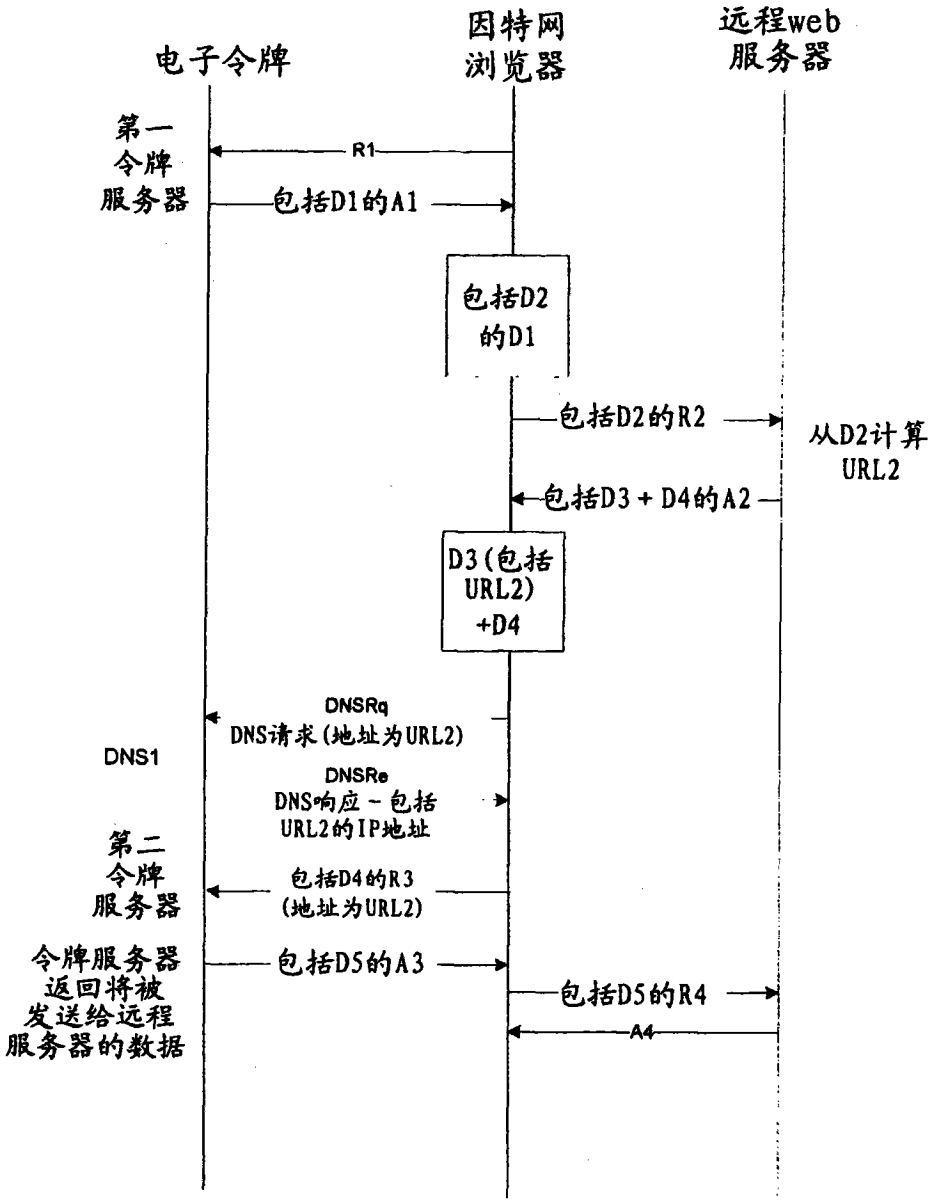

电子令牌
因特网浏览器
远程web服务器
第一令牌服务器
R1
包括D1的A1
包括D2的D1
包括D2的R2
从D2计算URL2
包括D3 + D4的A2
D3(包括URL2)+D4
DNSRq
DNS请求(地址为URL2)
DNS1
DNSRe
DNS响应 - 包括URL2的IP地址
第二令牌服务器
包括D4的R3
(地址为URL2)
令牌服务器返回将被发送给远程服务器的数据
包括D5的A3
包括D5的R4
A4

图 4