

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2014 年 10 月 2 日 (02.10.2014)



(10) 国际公布号
WO 2014/154095 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号:
PCT/CN2014/073478
- (22) 国际申请日:
2014 年 3 月 14 日 (14.03.2014)
- (25) 申请语言:
中文
- (26) 公布语言:
中文
- (30) 优先权:
201310097545.4 2013 年 3 月 25 日 (25.03.2013) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。
- (72) 发明人: 朱玫 (ZHU, Mei); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。李宝生 (LI, Baosheng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。纪尚越 (JI, Shangyue); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼,

Beijing 100015 (CN)。王小龙 (WANG, Xiaolong); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。任寰 (REN, Huan); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区成府路 28 号优盛大厦 D-1111 室, Beijing 100083 (CN)。

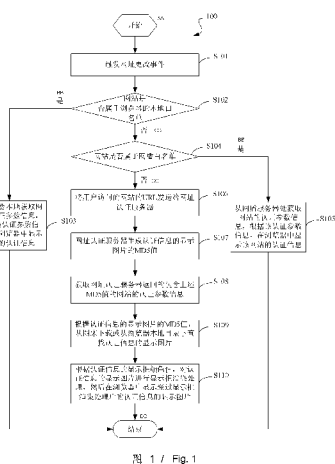
(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,

[见续页]

(54) Title: METHOD FOR DISPLAYING WEBSITE AUTHENTICATION INFORMATION AND BROWSER

(54) 发明名称: 网站认证信息的显示方法及浏览器



S101 Trigger a network address change event
S102 Whether the website belongs in the local white list of browser
S103 Acquire authentication parameter information of the website locally via the browser, and display the authentication information of the website in the browser according to the authentication parameter information
S104 Whether the website belongs in the white list of network shield
S105 Acquire the authentication parameter information of the website from a network shield server, and display the authentication information of the website in the browser according to the authentication parameter information
S106 Send to a network address authentication server the URL of the website visited by users
S107 The network address authentication server generates a MD5 value for the display picture of the authentication information
S108 Acquire the authentication parameter information of the website comprising the MD5 value and returned by the network address authentication server
S109 Download the display picture of the authentication information from a gallery or search for the display picture of the authentication information in the local directories of the browser according to the MD5 value for the display picture of the authentication information
S110 Carry out display frame rendering on the display picture of the authentication information according to the display frame color value of the authentication information, and then display in the browser the display picture of the authentication information which undergoes display frame rendering
AA Begin CC No
BB Yes DD End

(57) Abstract: Disclosed in the present invention are a method for displaying website authentication information and a browser, the method comprising: acquiring, by cloud query, authentication parameter information of a website provided by a network address authentication server after a network address change event is triggered, wherein the authentication parameter information at least comprises display picture information of the authentication information, and the display picture information of the authentication information is generated by the network address authentication server according to the source of the authentication information and website type information; and displaying the authentication information of the website in the browser according to the authentication parameter information. According to the technical solution provided by the present invention, the information authenticated by authority can be displayed in real time when users visit the website, enabling the users to have a proper understanding of the security of the currently-visited website.

(57) 摘要:

[见续页]



WO 2014/154095 A1



IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,
RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD,
TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种网站认证信息的显示方法及浏览器。其中，方法包括：在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，所述认证参数信息至少包括认证信息的显示图片信息，所述认证信息的显示图片信息是所述网址认证服务器根据所述认证信息的来源和网站类型信息而生成的；根据所述认证参数信息，在浏览器中显示所述网站的认证信息。根据本发明提供的方案，在用户访问网站时可以实时的展现经过权威认证的信息，让用户对于当前访问的网站有了就其安全性的公证的认识。

网站认证信息的显示方法及浏览器

技术领域

5 本发明涉及计算机网络技术领域，具体涉及一种网站认证信息的显示方法及浏览器。

背景技术

网页浏览器是个显示网页服务器或档案系统内的文件，并让用户与这些文件互动的一种软件。网页浏览器所显示的内容包括万维网或局部局域网络等网络内的文字、影像及其他信息。这些文字或影像可以是连接其他网址的超链接，通过这些超链接用户可迅速及轻易地浏览各种资讯。网页一般是 HTML（Hypertext Markup Language，超文本标记语言）的格式。有些网页是需使用特定的浏览器才能正确显示。网址通常指因特网上网页的地址。如果要从一台计算机访问网上另一台计算机，就必须知道对方的网址。这里所说的网址实际上指两个内涵，即 IP（Internet Protocol，因特网协议）地址和域名地址。

网页浏览器中的地址栏经常用于进行网址的输入和网页访问时网址的显示。网页浏览器对于网址没有甄别功能，对于一些不法网站，通过将网址的名称设为非常接近正规网站的方式，骗取用户信任，损害用户利益。

20 发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的网站认证信息的显示方法和相应的浏览器。

根据本发明的一个方面，提供了一种网站认证信息的显示方法，包括：在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，认证参数信息至少包括认证信息的显示图片信息，认证信息的显示图片信息是网址认证服务器根据认证信息的来源和网站类型信息而生成的；根据认证参数信息，在浏览器中显示网站的认证信息。

根据本发明的另一方面，提供了一种浏览器，包括：云端查询模块，适于在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，认证参数信息至少包括认证信息的显示图片信息，认证信息的显示图片信息是网址认证服务器根据认证信息的来源和网站类型信息而生成的；认证信息显示模块，适于根据认证参数信息，在浏览器中显示网站的认证信息。

根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行上述的网站认证信息的显示方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了上述计算机程序。

本发明的有益效果为：

根据本发明提供的网站认证信息的显示方法及浏览器，在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，根据认证参数信息，可以在浏览器中显示网站的认证信息。这样在用户访问网站时可以实时的展现经过权威认证的信息，让用户对于当前访问的网站有了就其安全性的公证的认识。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的网站认证信息的显示方法的流程图；

图 2 示出了认证信息的显示图片的一个例子的示意图；

图 3 示出了认证信息的显示图片的另一个例子的示意图；

图 4 示出了在浏览器中显示认证信息的显示图片的示意图；

图 5 示出了根据本发明一个实施例的网站名片的显示方法的流程图；

图 6 示出了网站名片弹窗页面的一个例子的实物图片；

图 7 示出了网站名片弹窗页面的另一个例子的实物图片；

图 8 示出了安全防护设置页面的实物图片；

图 9 示出了根据本发明一个实施例的浏览器的结构框图；

图 10 示意性地示出了用于执行根据本发明的网站认证信息的显示方法的计算设备的框图；以及

图 11 示意性地示出了用于保持或者携带实现根据本发明的网站认证信息的显示方法的程序代码的存储单元。

具体实施方式

下面结合附图和具体的实施方式对本发明作进一步的描述。

图 1 示出了根据本发明一个实施例的网站认证信息的显示方法 100 的流程图。如图 1 所示，方法 100 始于步骤 S101，其中在用户访问网站时，浏览器首先触发网址更改事件。在用户访问某网站时，会在浏览器的地址栏输入该网站的网址或者通过其他网站链接到该网站，此时浏览器的地址栏的网站的网址（例如 URL）会发生改变，浏览器一旦检测到这种改变，便会触发网址更改事件（url change）。

随后，方法 100 进入步骤 S102，其中浏览器查询本地白名单，判断该网站是否属于浏览器的本地白名单，若是，执行步骤 S103；否则，执行步骤 S104。浏览器本

地白名单是可信白名单，其中存储有可信的网站的 URL 及其认证参数信息。浏览器根据用户访问的网站的 URL 查询该本地白名单，如果该网站属于本地白名单，则执行步骤 S103；如果该网站不属于本地白名单，则执行步骤 S104。

在步骤 S103 中，在浏览器本地获取网站的认证参数信息，根据该认证参数信息，
5 在浏览器中显示网站的认证信息，方法 100 结束。如果用户访问的网站属于本地白名单，那么可在本地白名单中查找到该网站的认证参数信息，该认证参数信息至少包括认证信息的显示图片信息，可选地，认证信息的显示图片信息为认证信息的显示图片的 MD5（Message Digest Algorithm 5，消息摘要算法第五版）值。浏览器根据认证信息的显示图片的 MD5 值，可在浏览器本地目录下查找或从图床下载认证信息的显示图片，查找或下载认证信息的显示图片的具体方法将在后面详细描述。在获得认证信息的显示图片之后，在浏览器地址栏的旁边显示该认证信息的显示图片。
10 通过这种方式，浏览器可以将用户访问的网站的权威的认证信息利用认证信息的显示图片展现给用户，让用户对于当前访问的网站有就其安全性的公证的认识。

需要说明的是，上述步骤 S102 和步骤 S103 为可选的步骤，即在步骤 S101 之后，方法 100 可直接进入后续步骤，无需进行查询浏览器本地白名单的步骤。
15

在步骤 S104 中，浏览器通过直接或间接的方式，查询网盾白名单，判断该网站是否属于网盾白名单，若是，执行步骤 S105；否则，执行步骤 S106。网盾白名单是保存在网盾服务器中的可信白名单，其中存储有可信的网站的 URL 及其认证参数信息。通过间接的方式，浏览器将用户访问的网站的 URL 上报给网盾服务器，由网盾服务器判断该网站是否属于网盾白名单；或者通过直接的方式，网盾服务器将网盾白名单返回给浏览器，由浏览器查询网盾白名单，判断该网站是否属于网盾白名单。
20 如果用户访问的网站属于网盾白名单，则执行步骤 S105；如果用户访问的网站不属于网盾白名单，则执行步骤 S106。

在步骤 S105 中，浏览器从网盾服务器处获取网站的认证参数信息，根据该认证参数信息，在浏览器中显示该网站的认证信息，方法 100 结束。如果网盾服务器判断出用户访问的网站属于网盾白名单，那么浏览器从网盾服务器处获取网站的认证参数信息；或者，如果浏览器判断出用户访问的网站属于网盾白名单，那么浏览器从网盾服务器之前返回的网盾白名单中获取网站的认证参数信息。该认证参数信息至少包括认证信息的显示图片信息，可选地，认证信息的显示图片信息为认证信息的显示图片的 MD5 值。浏览器根据认证信息的显示图片的 MD5 值，可在浏览器本地目录下查找或从图床下载认证信息的显示图片，查找或下载认证信息的显示图片的具体方法将在后面详细描述。在获得认证信息的显示图片之后，在浏览器地址栏的旁边显示该认证信息的显示图片。通过这种方式，浏览器可以将用户访问的网站的权威的认证信息利用认证信息的显示图片展现给用户，让用户对于当前访问的网站有就其安全性的公证的认识。
25
30
35

需要说明的是，上述步骤 S104 和步骤 S105 为可选的步骤，即在步骤 S101 或步骤 S102 之后，方法 100 可直接进入后续步骤，无需进行查询网盾白名单的步骤。

也就是说，本方法 100 可同时包括查询浏览器本地白名单和查询网盾白名单的

步骤，也可仅包括查询浏览器本地白名单或查询网盾白名单的步骤，还可既不包括查询浏览器本地白名单的步骤，也不包括查询网盾白名单的步骤。

在步骤 S106 中，浏览器将用户访问的网站的 URL 发送给网址认证服务器。网址认证服务器是专用于向浏览器提供经过权威认证的认证信息的服务器，该网址认证服务器所包括的信息主要来自于浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息。其中浏览器提供方和认证授权机构所提供的信息主要包括以下类型的网站的认证信息：企业、品牌官网、学校、商城、团购网、银行、医院、游戏官网、政府、事业单位等等。认证授权机构一般基于第三方的 CA(Certificate Authority, 认证中心) 认证的流程提供相应的信息。网站备案许可信息是指在权威备案机构经过备案的信息，如在工信部 ICP(中华人民共和国电信与信息服务业务经营许可证) 备案中心所备案的信息，经备案的网站类型主要包括：企业、政府、军队、社会团体、事业单位、个人。本发明中网址认证服务器可以是一个开放的平台，多个不同的认证授权机构和/或权威备案机构都可以通过配置的接口接入该平台，从而向网址认证服务器提供信息。

在步骤 S106 之后，方法 100 进入步骤 S107，其中，网址认证服务器基于浏览器提供的网站的 URL，从网址认证服务器所包括信息中查询该 URL 对应的认证信息的来源和网站类型信息，根据该 URL 对应的认证信息的来源和网站类型信息，对原始显示图片进行处理，得到认证信息的显示图片，然后生成认证信息的显示图片信息，可选地，该认证信息的显示图片信息具体为认证信息的显示图片的 MD5 值。

具体来说，网址认证服务器从上述浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息中查询浏览器提供的网站的 URL 对应的认证信息的来源和网站类型信息，其中认证信息的来源是关于该认证信息来源于浏览器提供方、认证授权机构或权威备案机构的标识信息。本方法中采用标识“0”表示认证信息来源于浏览器提供方，采用标识“1”表示认证信息来源于认证授权机构或权威备案机构。但本发明不仅限于此，为了提供更加精细的信息，可用三个不同的标识来标识这三种来源。网站类型信息是关于网站的 URL 对应的网站类型的标识信息，本方法中，“企业”的标识为“1”，“商城”的标识为“2”、“政府”的标识为“3”、“支付”的标识为“4”、“银行”的标识为“5”、“事业单位”的标识为“6”、“团购网”的标识为“7”、“学校”的标识为“8”、“医院”的标识为“9”、“游戏官网”的标识为“10”、“品牌官网”的标识为“11”。为了提供更加精细的信息，网站类型信息还可以包括在上述网站类型基础上进一步细分的网站子类型的标识信息，本发明对此不做限制。

本方法中，原始显示图片是由浏览器提供方和/或认证授权机构提供的，不同的认证授权机构所提供的原始显示图片的样式可以各有不同。网址认证服务器可以根据用户访问的网站的 URL 对应的认证信息的来源和网站类型信息，对原始显示图片进行再加工处理，得到认证信息的显示图片。作为一种可选的实施方式，认证信息的来源决定了认证信息的显示图片上所显示的认证图标、以及认证信息的显示图片的背景颜色和/或文字颜色。网站类型信息决定了认证信息的显示图片上所显示的文

字内容。下面通过一个具体的例子进行说明。

图 2 示出了认证信息的显示图片的一个例子的示意图。对于图 2 所示的例子，用户访问的网站的 URL 对应的认证信息的来源为标识“1”，表明该网站的认证信息来源于认证授权机构或权威备案机构，对于此来源，认证信息的显示图片上所显示的认证图标为“证”，认证信息的显示图片的背景颜色为绿色，文字颜色也为绿色（由于图 2 为示意图，其中并未显示出相应的颜色）。用户访问的网站的 URL 对应的网站类型信息为标识“9”，表明该网站为医院类网站，则认证信息的显示图片上显示出“医院”。图 3 示出了认证信息的显示图片的另一个例子的示意图。对于图 3 所示的例子，用户访问的网站的 URL 对应的认证信息的来源为标识“0”，表明该网站的认证信息来源于浏览器提供方，对于此来源，认证信息的显示图片上所显示的认证图片为“V”，认证信息的显示图片的背景颜色为绿色，文字颜色也为绿色（由于图 3 为示意图，其中并未显示出相应的颜色）。用户访问的网站的 URL 对应的网站类型信息为标识“5”，表明该网站为银行类网站，则认证信息的显示图片上显示出“银行”。

在得到图 2 或图 3 示出的显示图片之后，生成该显示图片的 MD5 值，该 MD5 值即为认证信息的显示图片信息。

在步骤 S107 之后，方法 100 进入步骤 S108，其中浏览器获取网址认证服务器返回的网站的认证参数信息。网址认证服务器返回的认证参数信息至少包括认证信息的显示图片的 MD5 值（以下用参数 m 来表示），除此之外，还可包括网站的域名信息（以下用参数 d 来表示）和认证信息的显示框颜色值（以下用参数 c 来表示）。可选地，认证参数信息还可以包括认证信息的来源和网站类型信息（以下用参数 s 来表示认证信息的来源和网站类型信息）。

作为一个具体的例子，网址认证服务器返回给浏览器的数据格式如下：

*trust.info:{d: 域名}{c: 显示框颜色值}{m: 显示图片的 MD5 值}*以及

kx.info:{d: 域名}{s: 来源: 类型: 子类型 1: 子类型 2: 子类型 3……}

表 1 和表 2 示出了对上述数据格式的说明。

表 1. 数据格式说明表一

项目	说明	容错处理	举例
{d: 域名}	网站的域名信息	d 为空或异常数据时，在浏览器中不显示网站的认证信息	{d:360.cn}
{c: 显示框颜色值}	显示框的颜色：1 为蓝色；2 为绿色	c 不是指定数值 1 或 2，在浏览器中不显示网站的认证信息	{c:1}
{m: 显示图片的 MD5 值}	显示图片取其 MD5 值	无法获取此值或者显示图片未正确下载时，在浏览器中不显示网站的认证信息	{m:e79389bda6a764850c81dd1faa8c0776}

表 2. 数据格式说明表二

项目	说明		举例
{d: 域名}	网站的域名信息		{d:360.cn}
{s: 来源:类型:子类型 1:子类型 2:子类型 3……}	来源	0 为浏览器提供方; 1 为认证授权机构或权威备案机构	{s:0:4}
	类型	1-企业 2-商城 3-政府 4-支付 5-银行 6-事业单位 7-团购网 8-学校 9-医院 10- 游戏官网 11- 品牌官网	
	子类型 1: 子类型 2:子类型 3……	目前未使用	

在步骤 S108 之后，方法 100 进入步骤 S109，其中根据认证信息的显示图片的 MD5 值，从图床下载或从浏览器本地目录下查找认证信息的显示图片。浏览器本地目录下保存有一部分认证信息的显示图片，如果网址认证服务器返回的认证信息的显示图片的 MD5 值对应的显示图片没有保存在浏览器本地目录下，可以从图床下载。

具体来说，在浏览器接收到网址认证服务器返回的认证参数信息之后，首先判断浏览器本地目录下是否存在与认证信息的显示图片的 MD5 值一致的显示图片；若是，则获取对应的显示图片作为认证信息的显示图片；若否，从图床下载显示图片作为认证信息的显示图片，从图床下载的显示图片的 MD5 值与认证信息的显示图片的 MD5 值一致。举例来说，设图床的 URL 为：http://p0.qhimg.com/d/webidnameplate/ 文件名，若网址认证服务器返回的数据包括 {trust.info:{d:360.cn}{c:1}{m:e79389bda6a764850c81dd1faa8c0776}{v:1.0}{p:*}}，则

通过访问 <http://p0.qhimg.com/d/webidnameplate/e79389bda6a764850c81dd1faa8c0776> 下载显示图片。

根据容错处理机制，若从图床下载显示图片失败，在浏览器中不显示网站的认证信息。另外，如果网址认证服务器返回的认证参数信息中网站的域名信息为空或异常信息，则在浏览器中不显示网站的认证信息。如果网址认证服务器返回的认证参数信息中显示框颜色值不是指定数值（如 1 或 2），则在浏览器中不显示网站的认证信息。

在步骤 S109 之后，方法 100 进入步骤 S110，其中根据认证信息的显示框颜色值，对认证信息的显示图片进行显示框渲染处理，然后在浏览器中显示经过显示框渲染处理后的认证信息的显示图片。如果认证信息的显示框颜色值为 1，则将认证信息的显示图片的显示框渲染成蓝色，如果认证信息的显示框颜色值为 2，则将认证信息的显示图片的显示框渲染成绿色。图 4 示出了在浏览器中显示认证信息的显示图片的示意图。如图 4 所示，在浏览器地址栏 41 的左侧显示认证信息的显示图片 42，该认证信息的显示图片的显示框 43 的颜色是由认证信息的显示框颜色值决定的（由于图 4 为示意图，其中并未显示出相应的颜色）。

进一步的，本方法中网址认证服务器除了返回用户访问的网站的认证参数信息之外，还可以返回由该网站的二级以上子域名对应的网站的认证参数信息形成的认证参数信息列表，浏览器将该认证参数信息列表存储在浏览器本地。在触发该网站的二级以上子域名对应的网站的网址更改事件之后，直接在浏览器本地查询该网站的认证参数信息，根据该认证参数信息，在浏览器中显示网站的认证信息。例如，设用户访问的网站为 qq.com，网址认证服务器除了返回 qq.com 的认证参数信息之外，还返回 mail.qq.com 等二级子域名对应的网站的认证参数信息。后续当用户访问 mail.qq.com 时，浏览器直接在本地查找 mail.qq.com 的认证参数信息，根据该认证参数信息在浏览器中显示网站的认证信息，使得浏览器实时响应并展现认证信息。可选地，上述认证参数信息列表可以存储在前面所描述的浏览器本地白名单中。需要说明的是，浏览器本地白名单中的信息除了来源于网址认证服务器之外，来源于其它渠道，本发明对此不做限制。

为了向用户提供更为详细全面的认证信息，本发明除了显示上述认证信息的显示图片之外，还可以根据用户触发的命令进一步显示网站名片。图 5 示出了根据本发明一个实施例的网站名片的显示方法 200 的流程图。图 5 所示的步骤是在上述步骤 S110 之后执行的。

如图 5 所示，方法 200 始于步骤 S201，其中浏览器接收用户触发的网站名片显示命令。如图 2、3 和 4 所示，在认证信息的显示图片上所显示的认证图标的旁边显示有下拉箭头，用户点击该下拉箭头就可以触发网站名片显示命令。

随后，方法 200 进入步骤 S202，其中浏览器根据用户触发的网站名片显示命令，向指定服务器发起第一次请求，请求获取网站名片弹窗页面的大小信息。所谓指定服务器是设定网站名片弹窗页面大小的服务器，它可以是浏览器提供方的服务器，也可以是网址认证服务器。第一次请求中携带有网站的域名信息（如 host）。举例来

说，设指定服务器的接口地址为：

`http://webid.360.cn/nameplate_v2_conf.php`，第一次请求可以携带如下参数：

`host=当前域名` 可不带端口号

`key=md5(host+密钥)` 密钥为预设值

5 `v=浏览器版本号`

在步骤 S202 之后，方法 200 进入步骤 S203，其中浏览器判断是否接收到指定服务器响应第一次请求而返回的网站名片弹窗页面的大小信息，若是，方法 200 进入步骤 S204；否则，方法 200 进入步骤 S205。如果浏览器接收到网站名片弹窗页面的大小信息，表明第一次请求成功；如果浏览器没有接收到网站名片弹窗页面的大小信息，表明第一次请求失败。

在步骤 S204 中，根据网站名片弹窗页面的大小信息，格式化一个白板。网站名片弹窗页面的大小信息通常为网站名片弹窗页面的长度和宽度（返回值为：长度*宽度，如 400*200），根据网站名片弹窗页面的长度和宽度，格式化相应大小的白板。

在步骤 S205 中，根据认证信息的显示框颜色值，显示相应颜色和默认大小的网站名片弹窗页面，并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及查询失败信息，方法 200 结束。在第一次请求失败的情况下，浏览器根据认证信息的显示框颜色值，显示相应颜色和默认大小的网站名片弹窗页面，其中默认大小为浏览器预设值。然后在网站名片弹窗页面展现认证信息的来源和网站类型信息，例如“经认证授权机构认证的医院网站”的内容，并在其下展现“详细信息查询失败，请稍候再试”的查询失败信息。可选地，网站名片弹窗页面与认证信息的显示图片中线对齐。

在步骤 S204 之后，方法 200 进入步骤 S206，其中浏览器向网址认证服务器发起第二次请求，请求获取网站名片的显示内容信息。第二次请求中携带有网站的域名信息以及认证信息的显示图片信息和/或认证信息的显示框颜色值。举例来说，设网址认证服务器的接口地址为：`http://webid.360.cn/nameplate_v2.php`，第二次请求可以携带如下参数：

`host=当前域名` 可不带端口号

`key=md5(host+密钥)` 密钥为预设值

`v=浏览器版本号`

30 `m=云端查询结果的 m 值；无查询结果时，为默认“网站名片”对应图片的 md5 值`

`c=云端查询结果的 c 值；无查询结果时，为默认“网站名片”对应的值，如 1`

在步骤 S206 之后，方法 200 进入步骤 S207，其中浏览器判断是否接收到网址认证服务器响应第二次请求而返回的网站名片的显示内容信息，若是，方法 200 进入步骤 S208；否则，方法 200 进入步骤 S209。如果浏览器接收到网站名片的显示内容信息，表明第二次请求成功；如果浏览器没有接收到网站名片的显示内容信息，表明第二次请求失败。

在步骤 S208 中，根据网站名片弹窗页面的大小信息，显示网站名片弹窗页面，

并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及网站名片的显示内容信息，方法 200 结束。可选地，浏览器显示的网站名片弹窗页面与认证信息的显示图片的中线对齐，网站名片弹窗页面的大小与网站名片弹窗页面的大小信息一致，网站名片弹窗页面的颜色与认证信息的显示框颜色值对应。当浏览器处于屏幕边缘时，网站名片弹窗页面不做处理，舍弃屏幕外的部分。图 6 示出了网站名片弹窗页面的一个例子的实物图片。如图 6 所示，在网站名片弹窗页面的区域 61 中展现了认证信息的来源（UTN）和网站类型信息（医院），即“UTN 认证的医院网站”。在网站名片弹窗页面的区域 62 中展现了网站名片的显示内容信息，这些信息是通过第二次请求获得的。由于图 6 为灰度图片，其中并未显示出应有的颜色。

在步骤 S209 中，根据认证信息的显示框颜色值和网站名片弹窗页面的大小信息，显示相应颜色和相应大小的网站名片弹窗页面，并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及查询失败信息，方法 200 结束。在第二次请求失败的情况下，浏览器根据认证信息的显示框颜色值和网站名片弹窗页面的大小信息，显示相应颜色和相应大小的网站名片弹窗页面；然后在网站名片弹窗页面展现认证信息的来源和网站类型信息，例如“经认证授权机构认证的医院网站”的内容，并在其下展现“详细信息查询失败，请稍候再试”的查询失败信息。可选地，网站名片弹窗页面与认证信息的显示图片中线对齐。

作为另一种实施方式，在第二次请求失败的情况下，浏览器根据认证信息的显示框颜色值和网站名片弹窗页面的大小信息显示相应颜色和相应大小的网站名片弹窗页面之后，可以在网站名片弹窗页面展现认证信息的来源和网站类型信息，并在其下面展现“正在查询信息”的信息。继续等待预设时间（如 5s），若在预设时间内接收到网址认证服务器响应第二次请求而返回的网站名片的显示内容信息，则在网站名片弹窗页面显示“正在查询信息”的位置展现该网站名片的显示内容信息；若在预设时间内未接收到网址认证服务器响应第二次请求而返回的网站名片的显示内容信息，则网站名片弹窗页面显示“正在查询信息”的位置展现“详细信息查询失败，请稍候再试”的查询失败信息。

图 7 示出了网站名片弹窗页面的另一个例子的实物图片。如图 7 所示，该网站名片弹窗页面展现出一些扩展的信息和选项，如“同类网站”、“投诉此网站”、“评论”等。如果用户点击选项 A，则触发关闭网站名片弹窗页面的命令，浏览器接收到此命令后，执行关闭网站名片弹窗页面的操作。如果用户点击选项 B，则触发投诉网站的命令，浏览器接收到此命令后，执行关闭网站名片弹窗页面，接着打开投诉页面的操作，供用户输入投诉信息。如果用户点击选项 C，则触发评论网站的命令，浏览器接收到此命令后，执行关闭网站名片弹窗页面，接着打开评论页面的操作，供用户输入评论信息。进一步的，网站名片弹窗页面也可展现出打开安全防护的选项，如果用户点击该选项，则触发打开安全防护的命令，浏览器接收到此命令后，在网站名片弹窗页面展现安全防护的设置项，参见图 8。

根据本发明提供的网站认证信息的显示方法，在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，根据认证参数信息，

可以在浏览器中显示网站的认证信息。这样在用户访问网站时可以实时的展现经过权威认证的信息，让用户对于当前访问的网站有了就其安全性的公证的认识。网址认证服务器可以提供允许多个权威备案机构和认证授权机构接入其平台的接口，使其所包括的信息来自于浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息，信息的来源绝对权威和公证。而且，本方法除了可以显示认证信息的显示图片，还可以进一步显示网站名片，该网站名片中所展现的认证信息更加丰富和全面，让用户对于当前访问的网站有了更为全面的了解。本方法中，网站名片弹窗页面的大小是通过指定服务器预设的，如果指定服务器为浏览器提供方的服务器，那么浏览器方就可自定义网站名片弹窗页面的大小。另外，网站名片中还

5 包括附加的功能选项，如投诉、评论、打开安全防护等，通过这些附加功能，可以得到用户的反馈信息，能更好的服务于网站认证信息的显示。

图 9 示出了根据本发明一个实施例的浏览器的结构框图。如图 9 所示，该浏览器包括：云端查询模块 900 和认证信息显示模块 910；可选地，浏览器还包括认证信息的显示图片获取模块 920。

15 云端查询模块 900 适于在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，该认证参数信息至少包括认证信息的显示图片信息，认证信息的显示图片信息是网址认证服务器根据认证信息的来源和网站类型信息而生成的。可选地，认证信息的显示图片信息具体为认证信息的显示图片的 MD5 值；认证参数信息还包括以下信息：网站的域名信息和认证信息的显示框颜色值。

网址认证服务器是专用于向浏览器提供经过权威认证的认证信息的服务器，该网址认证服务器所包括的信息主要来自于浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息。其中浏览器提供方和认证授权机构所提供的信息主要包括以下类型的网站的认证信息：企业、品牌官网、学校、商城、团购网、

25 银行、医院、游戏官网、政府、事业单位等等。认证授权机构一般基于第三方的 CA（Certificate Authority，认证中心）认证的流程提供相应的信息。网站备案许可信息是指在权威备案机构经过备案的信息，如在工信部 ICP（中华人民共和国电信与信息服务业务经营许可证）备案中心所备案的信息，经备案的网站类型主要包括：企业、政府、军队、社会团体、事业单位、个人。本发明中网址认证服务器可以是一个开放的平台，多个不同的认证授权机构和/或权威备案机构都可以通过配置的接口接入该平台，从而向网址认证服务器提供信息。

浏览器向网址认证服务器提供网站的 URL，网址认证服务器在其所包括信息中查询该 URL 对应的认证信息的来源和网站类型信息，根据 URL 对应的认证信息的来源和网站类型信息，对原始显示图片进行处理，得到认证信息的显示图片，然后

35 生成认证信息的显示图片的 MD5 值。认证信息的来源决定了认证信息的显示图片上所显示的认证图标、以及认证信息的显示图片的背景颜色和/或文字颜色，网站类型信息决定了认证信息的显示图片上所显示的文字内容。关于认证信息的来源和网站类型信息的具体内容、以及网址认证服务器得到认证信息的显示图片的过程可以参

见上述方法实施例的描述，在此不再赘述。

云端查询模块 900 所获取的认证参数信息的数据格式可以参见上述方法实施例的描述。

认证信息的显示图片获取模块 920 适于根据认证信息的显示图片的 MD5 值，
5 从图床下载或从浏览器本地目录下查找认证信息的显示图片。进一步的，认证信息的显示图片获取模块 920 包括：判断模块 921、本地查找模块 922、下载模块 923。其中，判断模块 921 适于判断浏览器本地目录下是否存在与认证信息的显示图片的 MD5 值一致的显示图片。本地查找模块 922 适于在判断模块 921 判断出浏览器本地目录下存在与认证信息的显示图片的 MD5 值一致的显示图片的情况下，获取对应的
10 显示图片作为认证信息的显示图片。下载模块 923 适于在判断模块 921 判断出浏览器本地目录下不存在与认证信息的显示图片的 MD5 值一致的显示图片的情况下，从图床下载显示图片作为认证信息的显示图片，从图床下载的显示图片的 MD5 值与认证信息的显示图片的 MD5 值一致。

认证信息显示模块 910 适于根据认证参数信息，在浏览器中显示网站的认证信
15 息。进一步的，认证信息显示模块 910 适于根据认证信息的显示框颜色值，对认证信息的显示图片进行显示框渲染处理，然后在浏览器中显示经过显示框渲染处理后的认证信息的显示图片。如果认证信息的显示框颜色值为 1，则将认证信息的显示图片的显示框渲染成蓝色，如果认证信息的显示框颜色值为 2，则将认证信息的显示图片的显示框渲染成绿色。

20 根据容错处理机制，认证信息显示模块 910 进一步适于在下载模块 923 从图床下载显示图片失败的情况下，在浏览器中不显示网站的认证信息；或者，在网站的域名信息为空或异常信息的情况下，在浏览器中不显示网站的认证信息；或者，在认证信息的显示框颜色值不是指定数值的情况下，在浏览器中不显示网站的认证信息。

25 进一步的，云端查询模块 900 除了获取网站的认证参数信息之外，还可以获取网站的二级以上子域名对应的网站的认证参数信息形成认证参数信息列表。具体地，浏览器还包括：存储模块 930 和本地查询模块 931。存储模块 930 适于在浏览器本地存储认证参数信息列表；本地查询模块 931 适于在触发网站的二级以上子域名对应的网站的网址更改事件之后，直接在存储模块 930 中查询该网站的认证参数信息。

30 可选地，浏览器还包括本地白名单查询模块 940 和/或网盾查询模块 950。

本地白名单查询模块 940 适于查询浏览器本地白名单，如果网站属于浏览器本地白名单，则在浏览器本地获取网站的认证参数信息；如果网站不属于浏览器本地白名单，本地白名单查询模块 940 触发云端查询模块 900 或网盾查询模块 950 工作。在云端查询模块 900 工作之前，本地白名单查询模块 940 首先查询本地白名单，判
35 断该网站是否属于浏览器的本地白名单，浏览器本地白名单是可信白名单，其中存储有可信的网站的 URL 及其认证参数信息。如果该网站属于本地白名单，则本地白名单查询模块 940 直接在本地获取网站的认证参数信息。如果该网站不属于本地白名单，在浏览器包括网盾查询模块 950 的情况下，本地白名单查询模块 940 触发网

盾查询模块 950 工作；在浏览器不包括网盾查询模块 950 的情况下，本地白名单查询模块 940 触发云端查询模块 900 工作。

网盾查询模块 950 适于查询网盾白名单，如果网站属于网盾白名单，则从网盾服务器处获取网站的认证参数信息；如果网站不属于网盾白名单，网盾查询模块 950 5 触发云端查询模块 900 工作。在云端查询模块 900 工作之前，网盾查询模块 950 可以查询保存在网盾服务器中的网盾白名单，判断网站是否属于网盾白名单。如果该网站属于网盾白名单，则网盾查询模块 950 从网盾服务器处获取网站的认证参数信息。如果该网站不属于网盾白名单，网盾查询模块 950 触发云端查询模块 900 工作。

10 为了向用户提供更为详细全面的认证信息，本发明所提供的浏览器除了显示上述认证信息的显示图片之外，还可以根据用户触发的命令进一步显示网站名片。

具体来说，浏览器还包括：第一请求模块 960、第二请求模块 970 和网站名片显示模块 980。

第一请求模块 960 适于根据用户触发的网站名片显示命令，向指定服务器发起第一次请求，接收指定服务器响应第一次请求而返回的网站名片弹窗页面的大小信息。15 所谓指定服务器是设定网站名片弹窗页面大小的服务器，它可以是浏览器提供方的服务器，也可以是网址认证服务器。第一次请求中携带有网站的域名信息（如 host）。举例来说，设指定服务器的接口地址为：
http://webid.360.cn/nameplate_v2_conf.php，第一次请求可以携带如下参数：

host=当前域名 可不带端口号
20 key=md5(host+密钥) 密钥为预设值
v=浏览器版本号

第二请求模块 970 适于向网址认证服务器发起第二次请求，接收网址认证服务器响应第二次请求而返回的网站名片的显示内容信息。第二次请求中携带有网站的域名信息以及认证信息的显示图片信息和/或认证信息的显示框颜色值。举例来说，25 设网址认证服务器的接口地址为：http://webid.360.cn/nameplate_v2.php，第二次请求可以携带如下参数：

host=当前域名 可不带端口号
key=md5(host+密钥) 密钥为预设值
v=浏览器版本号
30 m=云端查询结果的 m 值；无查询结果时，为默认“网站名片”对应图片的 md5
值

c=云端查询结果的 c 值；无查询结果时，为默认“网站名片”对应的值，如 1

网站名片显示模块 980 适于根据网站名片弹窗页面的大小信息，显示网站名片弹窗页面，并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及网站名片35 片的显示内容信息。可选地，浏览器显示的网站名片弹窗页面与认证信息的显示图片的中线对齐，网站名片弹窗页面的大小与网站名片弹窗页面的大小信息一致，网站名片弹窗页面的颜色与认证信息的显示框颜色值对应。当浏览器处于屏幕边缘时，网站名片弹窗页面不做处理，舍弃屏幕外的部分。参见图 6，在网站名片弹窗页面的

区域 61 中展现了认证信息的来源 (UTN) 和网站类型信息 (医院), 即 “UTN 认证的医院网站”。在网站名片弹窗页面的区域 62 中展现了网站名片的显示内容信息, 这些信息是通过第二次请求获得的。

网站名片显示模块 980 进一步适于在第一次请求失败的情况下, 根据认证信息的显示框颜色值, 显示相应颜色和默认大小的网站名片弹窗页面, 并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及查询失败信息; 在第二次请求失败的情况下, 根据认证信息的显示框颜色值和网站名片弹窗页面的大小信息, 显示相应颜色和相应大小的网站名片弹窗页面, 并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及查询失败信息。

作为另一种实施方式, 网站名片显示模块 980 进一步适于在第二次请求失败的情况下, 根据认证信息的显示框颜色值和网站名片弹窗页面的大小信息, 显示相应颜色和相应大小的网站名片弹窗页面, 并在网站名片弹窗页面展现认证信息的来源和网站类型信息以及正在查询的信息; 等待预设时间, 若在预设时间内接收到网址认证服务器响应第二次请求而返回的网站名片的显示内容信息, 则在网站名片弹窗页面展现网站名片的显示内容信息; 若在预设时间内未接收到网址认证服务器响应第二次请求而返回的网站名片的显示内容信息, 则网站名片弹窗页面展现查询失败信息。

可选地, 浏览器的网站名片弹窗页面还可以提供一些附加的功能, 这样浏览器还包括: 命令处理模块 990, 适于根据用户触发的关闭网站名片弹窗页面的命令, 关闭网站名片弹窗页面; 或, 根据用户触发的投诉网站的命令, 关闭网站名片弹窗页面, 打开投诉页面; 或, 根据用户触发的评论网站的命令, 关闭网站名片弹窗页面, 打开评论页面; 或, 根据用户触发的打开安全防护的命令, 在网站名片弹窗页面展现安全防护的设置项。

根据本发明提供的浏览器, 在触发网址更改事件之后, 通过云端查询获取由网址认证服务器所提供的网站的认证参数信息, 根据认证参数信息, 可以在浏览器中显示网站的认证信息。这样在用户访问网站时可以实时的展现经过权威认证的信息, 让用户对于当前访问的网站有了就其安全性的公证的认识。本发明中, 网址认证服务器可以提供允许多个权威备案机构和认证授权机构接入其平台的接口, 使其所包括的信息来自于浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息, 信息的来源绝对权威和公证。而且, 本发明提供的浏览器除了可以显示认证信息的显示图片, 还可以进一步显示网站名片, 该网站名片中所展现的认证信息更加丰富和全面, 让用户对于当前访问的网站有了更为全面的了解。本发明中, 网站名片弹窗页面的大小是通过指定服务器预设的, 如果指定服务器为浏览器提供方的服务器, 那么浏览器方就可自定义网站名片弹窗页面的大小。另外, 网站名片中还包括附加的功能选项, 如投诉、评论、打开安全防护等, 通过这些附加功能, 可以得到用户的反馈信息, 能更好的服务于网站认证信息的显示。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述, 构造这类系统

所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的
5 实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下
10 意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性
15 地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非
20 另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中
所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求
25 保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行
的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的网站认证信息的显示设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现
30 为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 10 示出了可以实现根据本发明的网站认证信息的显示方法的计算设
35 备。该计算设备传统上包括处理器 1010 和以存储器 1020 形式的计算机程序产品或者计算机可读介质。存储器 1020 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 1020 具有用于执行上述方法中的任何方法步骤的程序代码 1031 的存储空间 1030。例如，用于程序代码

的存储空间 1030 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 1031。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 11 所述的便携式或者固定存储单元。该存储单元可以具有与图 10 的计算设备中的存储器 1020 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 1031'，即可以由例如诸如 1010 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种网站认证信息的显示方法，包括：

5 在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，所述认证参数信息至少包括认证信息的显示图片信息，所述认证信息的显示图片信息是所述网址认证服务器根据所述认证信息的来源和网站类型信息而生成的；

根据所述认证参数信息，在浏览器中显示所述网站的认证信息。

10 2、根据权利要求 1 所述的方法，所述认证信息的显示图片信息具体为认证信息的显示图片的 MD5 值；所述认证参数信息还包括以下信息：所述网站的域名信息和所述认证信息的显示框颜色值。

3、根据权利要求 2 所述的方法，所述网址认证服务器所包括信息来自于浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息；

15 所述网址认证服务器是基于浏览器提供的网站的网址，从所述网址认证服务器所包括信息中查询所述网址对应的认证信息的来源和网站类型信息，根据所述网址对应的认证信息的来源和网站类型信息，对原始显示图片进行处理，得到认证信息的显示图片，然后生成认证信息的显示图片的 MD5 值。

4、根据权利要求 2 所述的方法，还包括：根据所述认证信息的显示图片的 MD5 值，从图床下载或从浏览器本地目录下查找所述认证信息的显示图片。

20 5、根据权利要求 4 所述的方法，所述从图床下载或从浏览器本地目录下查找所述认证信息的显示图片进一步包括：

判断浏览器本地目录下是否存在与所述认证信息的显示图片的 MD5 值一致的显示图片；

若是，则获取对应的显示图片作为所述认证信息的显示图片；

25 若否，从图床下载显示图片作为所述认证信息的显示图片，从图床下载的显示图片的 MD5 值与所述认证信息的显示图片的 MD5 值一致。

6、根据权利要求 5 所述的方法，还包括：若从图床下载显示图片失败，则在浏览器中不显示所述网站的认证信息。

30 7、根据权利要求 4 所述的方法，所述根据认证参数信息，在浏览器中显示所述网站的认证信息的步骤进一步包括：

根据所述认证信息的显示框颜色值，对所述认证信息的显示图片进行显示框渲染处理，然后在浏览器中显示经过显示框渲染处理后的认证信息的显示图片。

35 8、根据权利要求 1 所述的方法，所述认证信息的来源决定了所述认证信息的显示图片上所显示的认证图标、以及所述认证信息的显示图片的背景颜色和/或文字颜色。

9、根据权利要求 1 所述的方法，所述网站类型信息决定了所述认证信息的显示图片上所显示的文字内容。

10、根据权利要求 2 所述的方法，若所述网站的域名信息为空或异常信息，则在浏览器中不显示所述网站的认证信息。

11、根据权利要求 2 所述的方法，若所述认证信息的显示框颜色值不是指定数值，则在浏览器中不显示所述网站的认证信息。

5 12、根据权利要求 3 所述的方法，所述原始显示图片是由浏览器提供方和/或认证授权机构提供的；不同的认证授权机构所提供的原始显示图片的样式不同。

13、根据权利要求 1 所述的方法，通过云端查询除了获取所述网站的认证参数信息之外，还获取所述网站的二级以上子域名对应的网站的认证参数信息形成认证参数信息列表，存储在浏览器本地；在触发所述网站的二级以上子域名对应的网站的网址更改事件之后，直接在浏览器本地查询该网站的认证参数信息，根据该认证参数信息，在浏览器中显示网站的认证信息。

14、根据权利要求 1 所述的方法，在所述通过云端查询获取由网址认证服务器所提供的网站的认证参数信息之前进一步包括：

15 查询浏览器本地白名单，如果所述网站属于浏览器本地白名单，则在浏览器本地获取所述网站的认证参数信息，根据所述认证参数信息，在浏览器中显示所述网站的认证信息；

如果所述网站不属于浏览器本地白名单，则执行所述通过云端查询获取由网址认证服务器所提供的网站的认证参数信息的步骤。

20 15、根据权利要求 1 或 14 所述的方法，在所述通过云端查询获取由网址认证服务器所提供的网站的认证参数信息之前进一步包括：

查询网盾白名单，如果所述网站属于网盾白名单，则从网盾服务器处获取所述网站的认证参数信息，根据所述认证参数信息，在浏览器中显示所述网站的认证信息；

25 如果所述网站不属于网盾白名单，则执行所述通过云端查询获取由网址认证服务器所提供的网站的认证参数信息的步骤。

16、根据权利要求 1 至 15 任一项所述的方法，所述认证参数信息还包括所述认证信息的来源和网站类型信息；

在所述在浏览器中显示所述网站的认证信息的步骤之后进一步包括：

30 根据用户触发的网站名片显示命令，向指定服务器发起第一次请求，接收所述指定服务器响应所述第一次请求而返回的网站名片弹窗页面的大小信息；

向所述网址认证服务器发起第二次请求，接收所述网址认证服务器响应所述第二次请求而返回的网站名片的显示内容信息；

35 根据网站名片弹窗页面的大小信息，显示网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及网站名片的显示内容信息。

17、根据权利要求 16 所述的方法，所述第一次请求中携带有所述网站的域名信息；所述第二次请求中携带有所述网站的域名信息，以及所述认证信息的显示图片信息和/或所述认证信息的显示框颜色值。

18、根据权利要求 16 所述的方法，若所述第一次请求失败，则根据所述认证信息的显示框颜色值，显示相应颜色和默认大小的网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及查询失败信息；

5 若所述第二次请求失败，则根据所述认证信息的显示框颜色值和网站名片弹窗页面的大小信息，显示相应颜色和相应大小的网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及查询失败信息。

19、根据权利要求 16 所述的方法，若所述第二次请求失败，则根据所述认证信息的显示框颜色值和网站名片弹窗页面的大小信息，显示相应颜色和相应大小的网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型
10 信息以及正在查询的信息；

等待预设时间，若在所述预设时间内接收到所述网址认证服务器响应所述第二次请求而返回的网站名片的显示内容信息，则在所述网站名片弹窗页面展现所述网站名片的显示内容信息；若在所述预设时间内未接收到所述网址认证服务器响应所述第二次请求而返回的网站名片的显示内容信息，则所述网站名片弹窗页面展现查
15 询失败信息。

20、根据权利要求 16 所述的方法，还包括：

根据用户触发的关闭网站名片弹窗页面的命令，关闭所述网站名片弹窗页面；

或，根据用户触发的投诉网站的命令，关闭所述网站名片弹窗页面，打开投诉
页面；

20 或，根据用户触发的评论网站的命令，关闭所述网站名片弹窗页面，打开评论
页面；

或，根据用户触发的打开安全防护的命令，在所述网站名片弹窗页面展现安全防护的设置项。

21、一种浏览器，包括：

25 云端查询模块，适于在触发网址更改事件之后，通过云端查询获取由网址认证服务器所提供的网站的认证参数信息，所述认证参数信息至少包括认证信息的显示图片信息，所述认证信息的显示图片信息是所述网址认证服务器根据所述认证信息的来源和网站类型信息而生成的；

认证信息显示模块，适于根据所述认证参数信息，在浏览器中显示所述网站的
30 认证信息。

22、根据权利要求 21 所述的浏览器，所述认证信息的显示图片信息具体为认证信息的显示图片的 MD5 值；所述认证参数信息还包括以下信息：所述网站的域名信息和所述认证信息的显示框颜色值。

23、根据权利要求 22 所述的浏览器，所述网址认证服务器所包括信息来自于浏览器提供方的信息、和/或网站备案许可信息、和/或认证授权机构提供的信息；
35

所述浏览器向所述网址认证服务器提供网站的网址，所述网址认证服务器在其所包括信息中查询所述网址对应的认证信息的来源和网站类型信息，根据所述网址对应的认证信息的来源和网站类型信息，对原始显示图片进行处理，得到认证信息

的显示图片，然后生成认证信息的显示图片的 MD5 值。

24、根据权利要求 22 所述的浏览器，还包括：认证信息的显示图片获取模块，适于根据所述认证信息的显示图片的 MD5 值，从图床下载或从浏览器本地目录下查找所述认证信息的显示图片。

5 25、根据权利要求 24 所述的浏览器，所述认证信息的显示图片获取模块进一步包括：

判断模块，适于判断浏览器本地目录下是否存在与所述认证信息的显示图片的 MD5 值一致的显示图片；

10 本地查找模块，适于在所述判断模块判断出浏览器本地目录下存在与所述认证信息的显示图片的 MD5 值一致的显示图片的情况下，获取对应的显示图片作为所述认证信息的显示图片；

下载模块，适于在所述判断模块判断出浏览器本地目录下不存在与所述认证信息的显示图片的 MD5 值一致的显示图片的情况下，从图床下载显示图片作为所述认证信息的显示图片，从图床下载的显示图片的 MD5 值与所述认证信息的显示图片的 MD5 值一致。

26、根据权利要求 25 所述的浏览器，所述认证信息显示模块进一步适于在所述下载模块从图床下载显示图片失败的情况下，在浏览器中不显示所述网站的认证信息。

20 27、根据权利要求 24 所述的浏览器，所述认证信息显示模块进一步适于根据所述认证信息的显示框颜色值，对所述认证信息的显示图片进行显示框渲染处理，然后在浏览器中显示经过显示框渲染处理后的认证信息的显示图片。

28、根据权利要求 21 所述的浏览器，所述认证信息的来源决定了所述认证信息的显示图片上所显示的认证图标、以及所述认证信息的显示图片的背景颜色和/或文字颜色。

25 29、根据权利要求 21 所述的浏览器，所述网站类型信息决定了所述认证信息的显示图片上所显示的文字内容。

30、根据权利要求 22 所述的浏览器，所述认证信息显示模块进一步适于在所述网站的域名信息为空或异常信息的情况下，在浏览器中不显示所述网站的认证信息。

30 31、根据权利要求 22 所述的浏览器，所述认证信息显示模块进一步适于在所述认证信息的显示框颜色值不是指定数值的情况下，在浏览器中不显示所述网站的认证信息。

32、根据权利要求 21 所述的浏览器，所述云端查询模块除了获取所述网站的认证参数信息之外，还获取所述网站的二级以上子域名对应的网站的认证参数信息形成认证参数信息列表；

35 所述浏览器还包括：

存储模块，用于在浏览器本地存储所述认证参数信息列表；

本地查询模块，适于在触发所述网站的二级以上子域名对应的网站的网址更改事件之后，直接在所述存储模块中查询该网站的认证参数信息。

33、根据权利要求 21 所述的浏览器，还包括：本地白名单查询模块，适于查询浏览器本地白名单，如果所述网站属于浏览器本地白名单，则在浏览器本地获取所述网站的认证参数信息；

5 如果所述网站不属于浏览器本地白名单，所述本地白名单查询模块触发所述云端查询模块工作。

34、根据权利要求 21 所述的浏览器，还包括：网盾查询模块，适于查询网盾白名单，如果所述网站属于网盾白名单，则从网盾服务器处获取所述网站的认证参数信息；

10 如果所述网站不属于网盾白名单，所述网盾查询模块触发所述云端查询模块工作。

35、根据权利要求 21 至 34 任一项所述的浏览器，还包括：

第一请求模块，适于根据用户触发的网站名片显示命令，向指定服务器发起第一次请求，接收所述指定服务器响应所述第一次请求而返回的网站名片弹窗页面的大小信息；

15 第二请求模块，适于向所述网址认证服务器发起第二次请求，接收所述网址认证服务器响应所述第二次请求而返回的网站名片的显示内容信息；

网站名片显示模块，适于根据网站名片弹窗页面的大小信息，显示网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及网站名片的显示内容信息。

20 36、根据权利要求 35 所述的浏览器，所述第一请求模块发起的第一次请求中携带有所述网站的域名信息；所述第二请求模块发起的第二次请求中携带有所述网站的域名信息，以及所述认证信息的显示图片名的相关信息和/或所述认证信息的显示框颜色值。

25 37、根据权利要求 35 所述的浏览器，所述网站名片显示模块进一步适于在所述第一次请求失败的情况下，根据所述认证信息的显示框颜色值，显示相应颜色和默认大小的网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及查询失败信息；在所述第二次请求失败的情况下，根据所述认证信息的显示框颜色值和网站名片弹窗页面的大小信息，显示相应颜色和相应大小的网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及查询失败信息。

30 38、根据权利要求 35 所述的浏览器，所述网站名片显示模块进一步适于在所述第二次请求失败的情况下，根据所述认证信息的显示框颜色值和网站名片弹窗页面的大小信息，显示相应颜色和相应大小的网站名片弹窗页面，并在所述网站名片弹窗页面展现所述认证信息的来源和网站类型信息以及正在查询的信息；等待预设时间，若在上述预设时间内接收到所述网址认证服务器响应所述第二次请求而返回的网站名片的显示内容信息，则在所述网站名片弹窗页面展现所述网站名片的显示内容信息；若在上述预设时间内未接收到所述网址认证服务器响应所述第二次请求而返回的网站名片的显示内容信息，则所述网站名片弹窗页面展现查询失败信息。

39、根据权利要求 35 所述的浏览器，还包括：命令处理模块，适于根据用户触发的关闭网站名片弹窗页面的命令，关闭所述网站名片弹窗页面；或，根据用户触发的投诉网站的命令，关闭所述网站名片弹窗页面，打开投诉页面；或，根据用户触发的评论网站的命令，关闭所述网站名片弹窗页面，打开评论页面；或，根据用户触发的打开安全防护的命令，在所述网站名片弹窗页面展现安全防护的设置项。

40、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-20 中的任一个所述的网站认证信息的显示方法。

41、一种计算机可读介质，其中存储了如权利要求 40 所述的计算机程序。

1/7

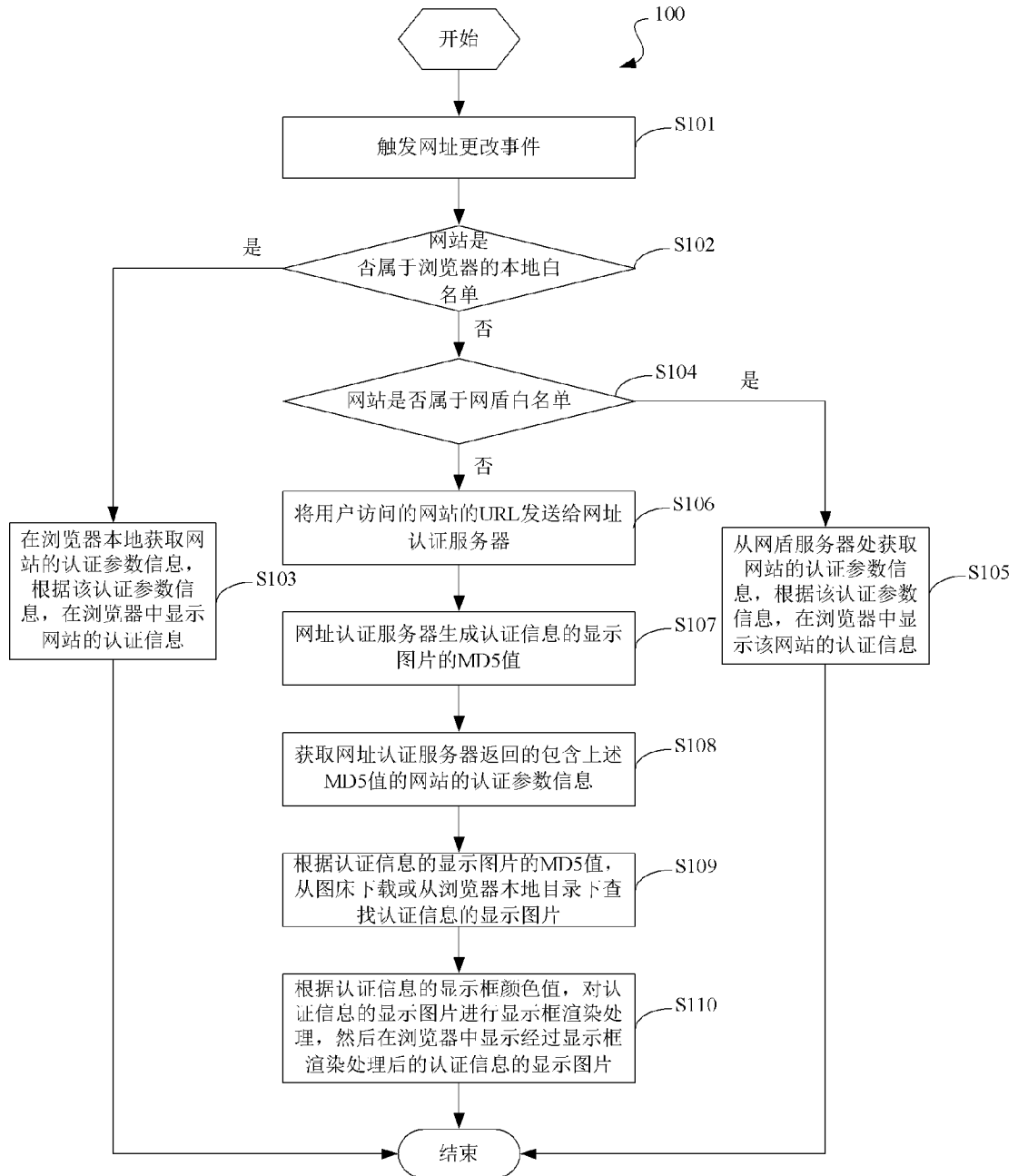


图 1

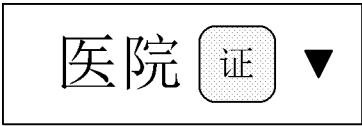


图 2

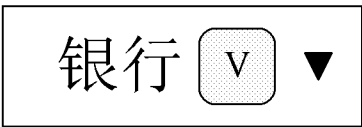


图 3

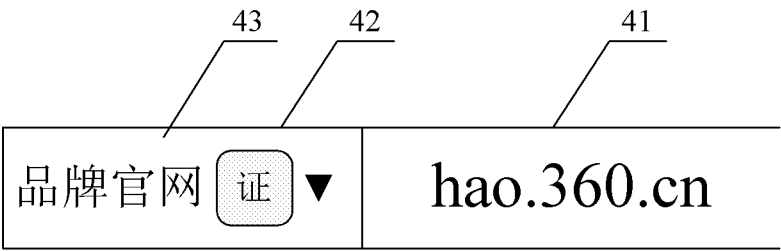


图 4

3/7

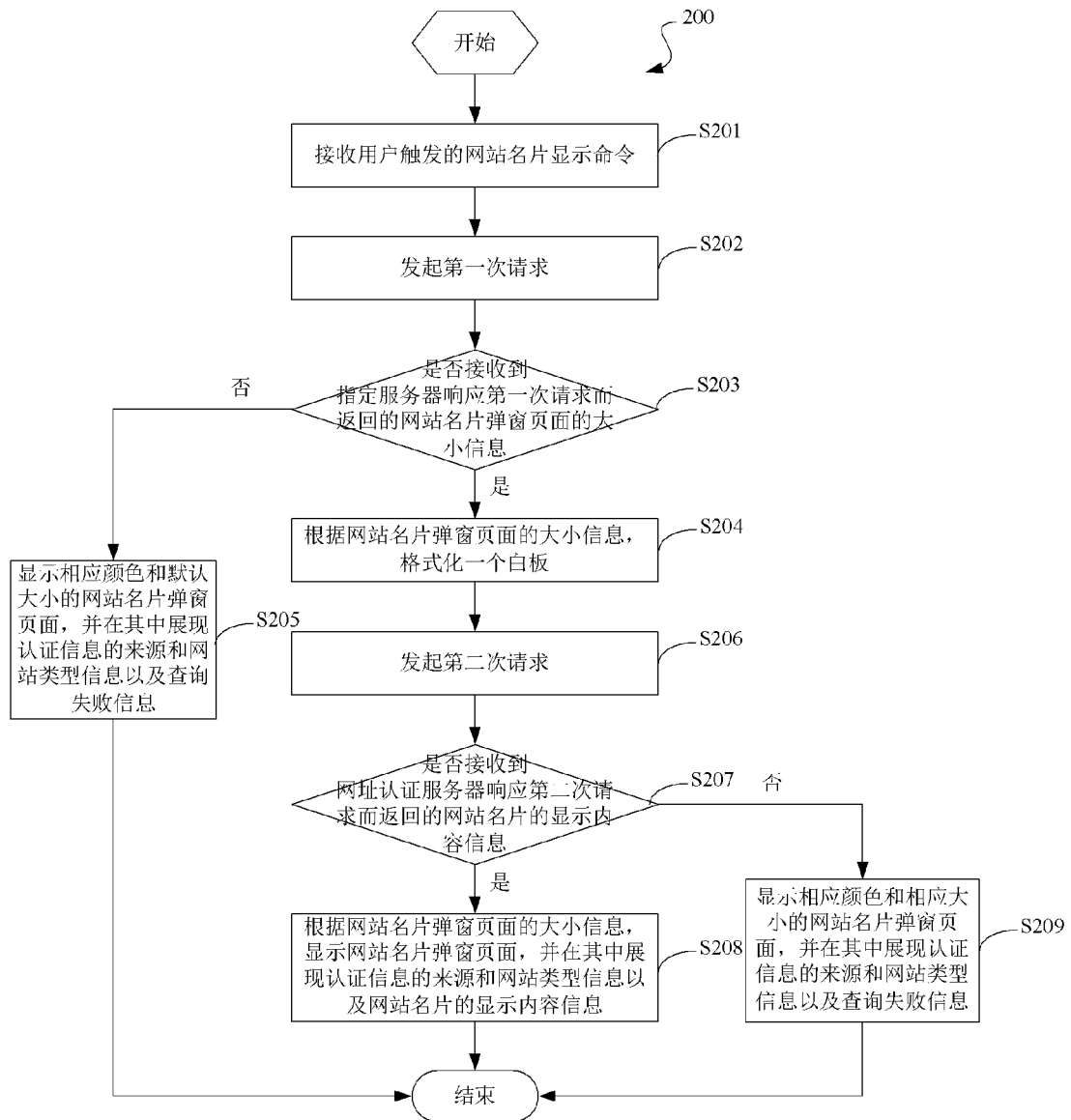


图 5

4/7



图 6



图 7



图 8

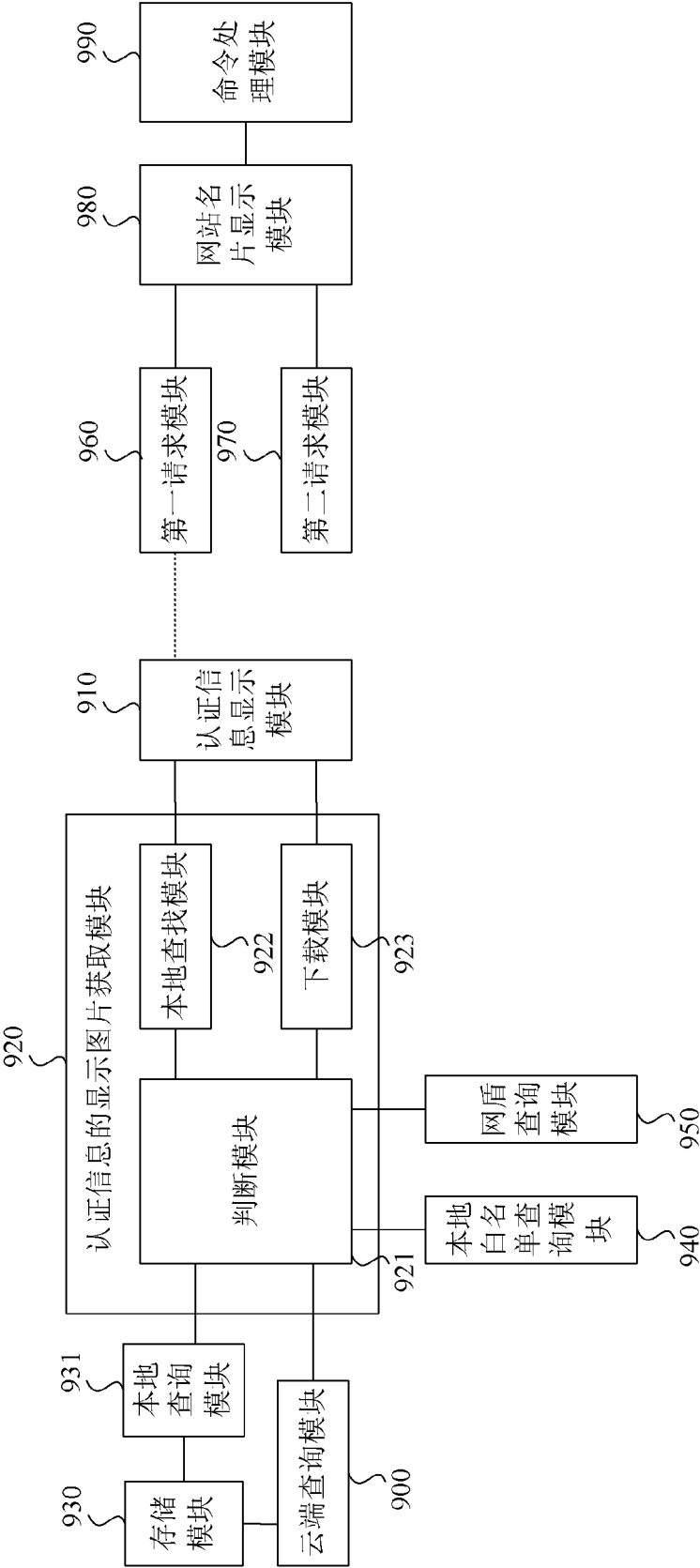


图9

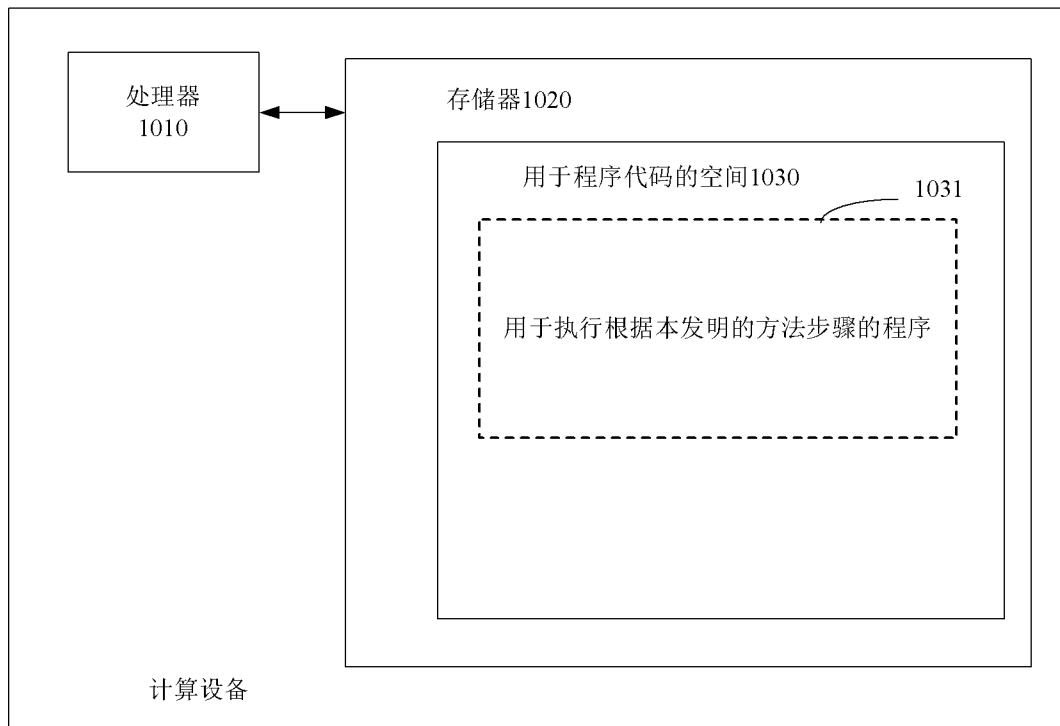


图 10

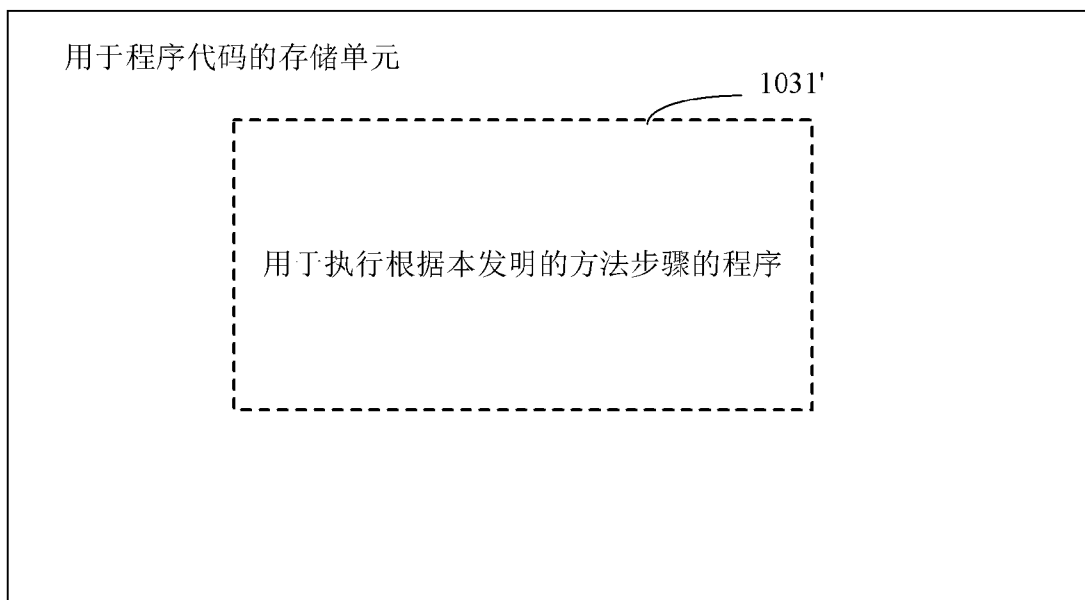


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/073478

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: web address, website, network, domain, name, authenticat+, malicious

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103179125 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 26 June 2013 (26.06.2013), claims 1-39, and description, paragraph [0103]	1-41
X	CN 102917049 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 06 February 2013 (06.02.2013), description, paragraphs [0054], [0077]-[0083], [0093], [0096] and [0106], and figures 3-6	1-41
A	CN 102882886 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 16 January 2013 (16.01.2013), the whole document	1-41
A	US 2009100505 A1 (TRUSTED PARTNERS, INC.), 16 April 2009 (16.04.2009), the whole document	1-41

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 06 May 2014 (06.05.2014)	Date of mailing of the international search report 30 May 2014 (30.05.2014)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LIU, Man Telephone No.: (86-10) 62414025

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/073478

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103179125 A	26.06.2013	None	
CN 102917049 A	06.02.2013	WO 2014059895 A1	24.04.2014
CN 102882886 A	16.01.2013	None	
US 2009100505 A1	16.04.2009	WO 2009050704 A2	23.04.2009
		US 2010251144 A1	30.09.2010
		US 2012030732 A1	02.02.2012

国际检索报告

国际申请号

PCT/CN2014/073478

A. 主题的分类

H04L 29/06(2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L, H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPODOC: 网址, 网站, 认证, 授权, network, domain, name, authenticat+, malicious

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 103179125A (北京奇虎科技有限公司等) 2013年 6月 26日 (2013 - 06 - 26) 权利要求1-39、说明书第[0103]段	1-41
X	CN 102917049A (北京奇虎科技有限公司等) 2013年 2月 06日 (2013 - 02 - 06) 说明书第[0054], [0077]-[0083], [0093], [0096], [0106]段、说明书附图3-6	1-41
A	CN 102882886A (北京奇虎科技有限公司等) 2013年 1月 16日 (2013 - 01 - 16) 全文	1-41
A	US 2009100505A1 (TRUSTED PARTNERS, INC.) 2009年 4月 16日 (2009 - 04 - 16) 全文	1-41

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2014年 5月 06日

国际检索报告邮寄日期

2014年 5月 30日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

授权官员

刘曼

传真号 (86-10)62019451

电话号码 (86-10)62414025

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/073478

检索报告引用的专利文件		公布日 (年/月/日)	同族专利		公布日 (年/月/日)
CN	103179125A	2013年 6月 26日	无		
CN	102917049A	2013年 2月 06日	WO	2014059895A1	2014年 4月 24日
CN	102882886A	2013年 1月 16日	无		
US	2009100505A1	2009年 4月 16日	WO	2009050704A2	2009年 4月 23日
			US	2010251144A1	2010年 9月 30日
			US	2012030732A1	2012年 2月 02日

表 PCT/ISA/210 (同族专利附件) (2009年7月)