(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
2016 年 7 月 7 日 (07.07.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/107319 A1

(51) 国际专利分类号:
G06F 21/62 (2013.01) *H04L 29/06* (2006.01)
G06F 21/64 (2013.01)

(21) 国际申请号: PCT/CN2015/094847

(22) 国际申请日: 2015 年 11 月 17 日 (17.11.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410851890.7 2014 年 12 月 30 日 (30.12.2014) 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: **杭程 (HANG, Cheng)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **石彦伟 (SHI, Yanwei)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **贾正强 (JIA, Zhengqiang)**; 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: **北京润泽恒知识产权代理有限公司 (BEIJING RISEHIGH INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区中关村南大街 31 号神舟大厦 702, Beijing 100081 (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, 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, ST, 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 LOADING SECURE KEY STORAGE HARDWARE, AND BROWSER CLIENT DEVICE

(54) **发明名称** : 加载安全密钥存储硬件的方法和浏览器客户端装置

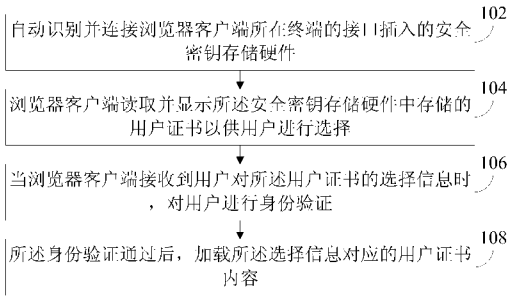


图 1 / FIG. 1

102 Secure key storage hardware inserted into interface of terminal in which browser client is located is automatically identified and connected
104 Browser client reads and displays user certificate stored in secure key storage hardware, for user to make selection
106 When browser client receives selection information of user with regard to user certificate, identity verification is performed on user
108 After identity verification has been passed, user certificate content corresponding to selection information is loaded

(57) **Abstract**: A method for loading secure key storage hardware, and a browser client device, the method comprising: secure key storage hardware inserted into an interface of a terminal in which a browser client is located is automatically identified and connected; the browser client reads and displays a user certificate stored in the secure key storage hardware, for a user to make a selection; when the browser client receives selection information of the user with regard to the user certificate, identity verification is performed on the user; after the identity verification has been passed, user certificate content corresponding to the selection information is loaded. The user certificate content stored in the secure key storage hardware is loaded when the identity of the user can be confirmed, preventing the user certificate stored in the secure key storage hardware from being leaked, and increasing the security of loading the secure key storage hardware.

(57) **摘要**:

[见续页]

WO 2016/107319 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))。

一种加载安全密钥存储硬件的方法和浏览器客户端装置，所述的方法包括：自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证；所述身份验证通过后，加载所述选择信息对应的用户证书内容。能够确认用户身份的情况下，加载安全密钥存储硬件中存储的用户证书的内容，可以防止安全密钥存储硬件中存储的用户证书被泄露，提高加载安全密钥存储硬件的安全性。

说 明 书

加载安全密钥存储硬件的方法和浏览器客户端装置

技术领域

本发明涉及通信技术领域，特别是涉及一种加载安全密钥存储硬件的方法和一种浏览器客户端装置。

背景技术

随着网络技术的不断发展，越来越多的用户通过浏览器访问网页获取信息，并进行各种操作，其中，浏览器是指可以显示网页服务器或者文件系统的 HTML（Hyper Text Mark-up Language，标准通用标记语言）文件内容，并让用户与这些文件交互的一种软件。

如在购物网站中购物，在视频网站中观看视频，在银行网站中进行金融业务，在游戏网站中玩游戏等。对于不同网站的网页请求，浏览器会执行不同的访问操作，从而访问该网页。在访问一些网站，如银行网站、支付宝网站等涉及金融业务的网站时，需要加载安全密钥存储硬件，但是加载安全密钥存储硬件中存在安全密钥存储硬件中存储的信息泄露、无法保证加载安全密钥存储硬件的安全性的等问题，给访问涉及金融业务的网站造成阻碍。

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加载安全密钥存储硬件方法和相应的浏览器客户端装置。

依据本发明的一个方面，提供了一种加载安全密钥存储硬件的方法，包括：自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证；所述身份验证通过后，加载所述选择信息对应的用户证书内容。

根据本发明的另一方面，提供了一种浏览器客户端装置，包括： 连接模块，用于自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；读取模块，用于读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；身份验证模块，用于当接收到用户对所述用户证书的选择信息时，对用户进行身份验证；加载模块，用于所述身份验证通过后，加载所述选择信息对应的用户证书内容。

根据本发明的另一方面，提供了一种程序，包括可读代码，当所述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本发明实施例所述的加载安全密钥存储硬件

的方法。

根据本发明的另一方面，提供了一种可读介质，其中存储了如本发明实施例所述的程序。

根据本发明的加载安全密钥存储硬件的方法可以在加载安全密钥存储硬件中存储的用户证书时，先对用户进行了身份验证，在身份验证通过，能够确认用户身份的情况下，加载安全密钥存储硬件中存储的用户证书的内容，由此解决了加载安全密钥存储硬件过程中存在的信息泄露、加载安全密钥存储硬件存在安全隐患等问题，取得了防止安全密钥存储硬件中存储的用户证书被泄露，从而提高加载安全密钥存储硬件的安全性的有益效果。

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一种加载安全密钥存储硬件的方法的流程图；

图 2 示出了根据本发明一个实施例的一种加载安全密钥存储硬件的方法的流程图；

图 3 示出了根据本发明一个实施例的加密子进程的一种代理机制示意图；

图 4 示出了根据本发明一个实施例的加密子进程和网络服务器的握手过程示意图；

图 5 示出了根据本发明一个实施例的在浏览器客户端中提示用户插入 USBKey 的示意图；

图 6 示出了根据本发明一个实施例的在浏览器客户端中弹窗证书选择对话框的示意图；

图 7 示出了根据本发明一个实施例的在浏览器客户端中提示用户输入保护口令的示意图；

图 8A 示出了根据本发明一个实施例的在浏览器客户端中加载用户证书中常规信息的示意图；

图 8B 示出了根据本发明一个实施例的在浏览器客户端中加载用户证书中详细信息的示意图；

图 9 示出了根据本发明一个实施例的一种浏览器客户端装置的结构框图；

图 10 示出了根据本发明一个实施例的一种浏览器客户端装置的结构框图；

图 11 示出了根据本发明一个实施例的读取模块的结构框图;

图 12 示出了根据本发明一个实施例的读取模块的结构框图;

图 13 示出了根据本发明一个实施例的加密子进程的结构框图;

图 14 示出了根据本发明一个实施例的主业务进程的结构框图;

图 15 示出了用于执行根据本发明的加载安全密钥存储硬件的方法的计算设备的框图;

图 16 示出了用于保持或者携带实现根据本发明的加载安全密钥存储硬件的方法的程序代码的存储单元。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

实施例一:

参照图 1,示出了根据本发明一个实施例的一种加载安全密钥存储硬件的方法实施例的步骤流程图，具体可以包括如下步骤:

步骤 102，自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件。

用户使用浏览器客户端登陆网上银行或支付宝等网上支付平台时，为了保证数据传输的安全性，需要用户插入安全密钥存储硬件。即用户在浏览器客户端的地址栏中输入上述网站的地址以请求对该网站地址对应网页进行访问时，浏览器客户端会提示用户插入安全密钥存储硬件。浏览器客户端的地址栏所接收的网站地址可能是用户直接输入的，也可以能是用户通过搜索点击搜索结果后输入的，本实施例对此不作限定。

安全密钥存储硬件，即 USBKey，安全密钥存储硬件中存储有用户证书，用户可以选择所述用户证书。需要说明的是，一个安全密钥存储硬件中通常存储有一个用户证书，各大银行有自己对应的安全密钥存储硬件。例如，北京银行的网上银行的安全密钥存储硬件中存储有北京银行下发用户证书；建设银行的网上银行的安全密钥存储硬件中存储有建设银行下发的用户证书。

需要说明的是，安全密钥存储硬件通常设置为与 USB（Universal Serial Bus，通用串行总线）接口匹配的形式，可以通过 USB 接口插入到电脑等终端上。当所述安全密钥存储硬件通过 USB 接口插入终端后，本实施例中浏览器客户端可以自动识别浏览器客户端所在终端的接口插入的安全密钥存储硬件，可以将所述安全密钥存储硬件与其他 USB 连接硬件区分开来。当识别出是有安全密钥存储硬件插入终端后，自动与所述安全密钥

存储硬件建立连接，这里所述建立连接，是下载驱动与所述安全密钥存储硬件建立通信连接，可以读取所述安全密钥存储硬件中存储的用户证书，而不限于物理上的连接。

步骤 104，浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择。

浏览器客户端与所述安全密钥存储硬件建立通信连接之后，可以读取所述安全密钥存储硬件中存储的用户证书，并将所述用户证书显示出来供用户进行选择。具体实现时，浏览器客户端可以通过弹窗的形式显示所述用户证书，也可以通过其他方式显示所述用户证书，本实施例对具体的显示方式不做限制，能够将用户证书显示数来，让用户直观看到用户证书以方便用户选择所述用户证书即可。

步骤 106，当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证。

浏览器客户端之所以需要自动识别安全密钥存储硬件，是因为访问网上银行等支付平台时，需要进行安全验证。本实施例中具体需要对用户的身份进行验证，在用户选择用户证书之后，对用户进行身份验证。需要说明的是，身份验证虽然在浏览器客户端进行，其实是银行的网络服务器要求对用户进行身份验证，以确认用户的身份。

需要说明的是，本实施例中对用户进行身份验证可以采取多种方式来实现。对于登录网上银行的情景，可以采用让用户输入银行卡的密码，或网上银行的单独密码的方式，对用户进行身份验证。因为银行的网络服务器中存储有用户设置的银行的密码或是网上银行的单独密码，浏览器客户端可以将用户输入的银行卡密码等身份信息发送到网络服务器，与网络服务器中存储的用户身份信息进行匹配，如果能够成功匹配，则用户的身份验证通过；如果匹配不成功，则身份验证失败。需要说明的是，对用户进行身份验证时，用户输入的身份信息可以是上述银行卡密码，也可以是保护口令，还可以是用户的身份证号等能够代表用户身份的信息，本实施例对身份信息的具体内容不做限制，对进行身份验证的具体过程也不做限制，只要能够确认用户身份即可。

步骤 108，所述身份验证通过后，加载所述选择信息对应的用户证书内容。

在身份验证通过后，浏览器客户端可以确认该用户是安全的，不是黑客等恶意攻击的用户，此时加载所述选择信息对应的用户证书的具体内容。步骤 104 中显示出来的用户证书仅仅为了供用户进行选择，因此步骤 104 中显示出来的可以不是用户证书的具体内容，而是用户证书的名称。在身份验证通过后，浏览器客户端确认用户安全的情况下，加载所述选择信息对应的用户证书的具体内容。

综上所述，本实施例浏览器客户端在加载安全密钥存储硬件时，首先自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；然后浏览器客户端读取并显

示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；接着当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证；最后所述身份验证通过后，加载所述选择信息对应的用户证书内容。本实施例在加载安全密钥存储硬件中存储的用户证书时，先对用户进行了身份验证，在身份验证通过，能够确认用户身份的情况下，加载安全密钥存储硬件中存储的用户证书的内容，可以防止安全密钥存储硬件中存储的用户证书被泄露，提高加载安全密钥存储硬件的安全性。

实施例二:

在上述实施例的基础上，本实施例继续加载安全密钥存储硬件的方法。

参照图 2,示出了根据本发明一个实施例的一种加载安全密钥存储硬件的方法实施例的步骤流程图，具体可以包括如下步骤:

步骤 202，在浏览器客户端中启动与主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发。

对于一些网站，如银行网站、支付宝网站等涉及金融业务的网站需要通过以安全为目标的 HTTP（Hyper Text Transfer Protocol，超文本传送协议）通道进行加密数据的传输，但是有时浏览器主业务进程与网络服务器采用不同的加密协议或算法，导致两者无法直接通信，无法对该网络服务器的网页进行访问。

本实施例中，提供了一种安全浏览器客户端，其在浏览器中还设置了与浏览器主业务进程进行通信的加密子进程。为了使得安全浏览器能够实现，需要首先在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程。所述加密子进程的主要功能是作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发。即采用加密子进程作为主业务进程的代理，其既能与浏览器主业务进程进行加密的安全通行，也能够与网络服务器进行加密的安全通信，如对于浏览器主业务进程的业务数据通过第一加密通道发送给加密子进程，该加密子进程将业务数据通过第二加密通道传输给网络服务器，实现数据转发以及两个加密通道的连通。

需要说明的是，通常情况下，浏览器的主业务进程与网络服务器直接进行通信，但是，在以安全为目标的 HTTP 通道进行通信时，若主业务进程无法对网络服务器反馈的数据信息进行解析，启动所述加密子进程作为代理连接，即所述加密子进程作为所述主业务进程与所述网络服务器之间的代理。本实施例中上述第一加密通道为所述浏览器主业务进程和所述加密子进程的安全通信通道；所述第二加密通道为所述加密子进程和网络服务器的安全通信通道。因此所述加密子进程通过将加密子进程与所述主业务进程的第一加密通道，转换为加密子进程与网络服务器的第二加密通道，来实现所述主业务进程与所述网络服务器之间的连接代理。当然对于主业务进程通过所述第一加密通道发送

给加密子进程的业务数据，加密子进程可以将所述业务数据通过第二加密通道发送给网络服务器。具体地，可以将在第二加密通道中进行通信的数据采用对称加密算法 SM4 对业务数据进行加密。

本实施例中，浏览器主业务进程与加密子进程采用代理及 IPC（Inter-Process Communication，进程间通信）两种通信方式，从而加密子进程可以作为连接代理，负责和浏览器主业务进程第一加密通道，到和网络服务器的第二加密通道的通道转换及数据转发，而 IPC 通信方式负责进程间数据传递。本实施例中，加密子进程代理实现机制如图 3 所示，具体可以包括如下结构：

主线程：读取各类配置，创建监听线程、主业务线程，以及浏览器主进程 IPC 通。

侦听线程：用于监听服务端口，当有主业务进程存在连接请求并接收（accept）成功执行相应的代理操作。

业务处理线程：与主业务进程和网络服务器两端分别建立相应加密通道连接并维持，从而作为桥梁进行两端的数据交换。

需要说明的是，业务处理线程的具体流程如下：（1）接收代理数据，具体接收代理连接的 http request 数据。（2）与网络服务器进行 SSL（Secure Sockets Layer，安全套接层）连接，具体包括 SSL 连接的建立，SSL 协议协商，算法协商，客户端证书验证（CRL 检查或 OCSP 认证）（3）与 web 服务器交互。具体将代理连接 http request 数据经由国密 SSL 通道发给 Web 服务器，获取 Web 服务器的 http response。（4）发送网络服务器返回数据给代理连接。具体将网络服务器的 http response 转给代理连接。（5）关闭连接。业务处理流程中如果发生错误，则关闭连接，同时给代理连接返回错误页面。需要说明的是，所述第二对称算法具体可以是国密算法。

需要说明的是，采用 SSL 的安全技术解决网络应用身份认证以及数据保密性得到广泛的认可，主流的浏览器和网络服务器中也内置了 SSL 模块，专业的 SSL 硬件产品也广泛使用。但当前 SSL 产品还都存在一定局限性：

（1）当前 SSL 产品普遍采用单证书机制。而双证书机制是当前 PKI（Public Key Infrastructure，公钥基础设施）体系建设的主流模式。本实施例使用签名证书进行身份认证，使用加密证书进行密钥的交换和保护，发挥了 PKI 技术非对称密钥的优势。

（2）当前的 SSL 产品中普遍采用国外公开的对称算法，不符合保密要求，具有一定风险性。本实施例中密码产品对称算法采用 SM1 算法或 SM4 算法。

（3）当前的证书非对称算法采用 RSA 算法，而本实施例采用的椭圆曲线密码（ECC）是一种比 RSA 具有更高安全性、更高效率的公钥密码，具有加密/解密、数字签名和密钥协商等重要的密码功能，可以安全且方便地满足各种信息网络中的用户身份识别、电子

信息的真伪鉴别和保密传输等重要的信息安全需求，是信息安全领域的核心技术，并已逐渐被诸多国际和国家标准组织采纳为公钥密码标准（IEEE P1363、ANSI X9、ISO/IEC 和 IETF 等），将会成为信息安全产业界使用的主流密码技术之一。将该 ECC（ECDSA+ECDH）算法命名为 SM2。

本实施例提供的加载安全密钥存储硬件的方法，符合该 PKI 机制和密码产品管理政策的要求，对国内安全产品的管理的规范性和网络应用的快速增长都起到积极的推动作用。

步骤 204，所述加密子进程通过握手过程与所述网络服务器进行数字证书双向认证。

本实施例中，双向认证是对所访问网站的网络服务器和浏览器客户端彼此均要进行认证，确认访问的网络服务器的数字证书以及浏览器客户端所加载的数字证书是安全有效的，因此双向认证时需要认证的证书包括访问的网站的站点证书以及浏览器客户端所加载的用户证书。本实施例中所述加密子进程通过握手过程与所述网络服务器进行数字证书的双向认证的步骤，具体可以通过以下方式来实现：所述加密子进程通过握手过程与所述网络服务器依次执行以下安全认证操作：加密数据协商、证书认证、密钥交换和签名认证。

需要说明的是，上述双向认证的过程同样是在浏览器客户端和网站所属网络服务器的握手过程中完成的，该握手过程至少可以通过以下方式来实现：

首先，浏览器客户端向所述网络服务器发送客户端问候消息 ClientHello，所述网络服务器向所述浏览器客户端反馈服务端问候消息 SeverHello，协商加密数据。

然后，网络服务器向所述浏览器客户端发送服务端证书消息 SeverCertificate，由于要进行双向认证，网络服务器向浏览器客户端依次发送服务端密钥交换消息 SeverKeyExchange、证书认证请求消息 SeverRequest 和服务端问候完结消息 SeverHelloDone。其中。所述证书认证请求消息用于指示进行客户端的证书认证。

然后，浏览器客户端采用非对称算法 SM2 对所述网络服务器的站点证书进行认证，在认证通过后，浏览器客户端向所述网络服务器发送客户端证书消息 ClientCertificate，该客户端证书消息包括浏览器客户端加载的用户证书，从而网络服务器基于非对称算法 SM2 对所述浏览器客户端加载的用户证书进行认证。

后续的握手过程中，浏览器客户端还可以向网络服务器发送客户密钥交换消息 ClientKeyExchange 和客户端问候完结消息 ClientHelloDone，以及密钥交换和签名认证所需的其他握手消息，本实施例不一一论述。

需要说明的是，上述客户端问候消息（ClientHello 消息）作为浏览器客户端和网络服务器握手协议的第一条消息，所述加密子进程向所述网络服务器发送客户端问候消息之

后，等待网络服务器返回服务器问候消息。客户端问题消息结构定义:

1、Clien_vision 表示客户端在这个会话中使用的协议版本。如协议版本号是 1.1。

2、Radom 是客户端产生的随机信息，其内容包括始终和随机数。

3、session_id 是客户端在连接中使用的会话标识。session_id 是一个可变长字段，其值由服务器决定。如果没有可重用的会话标识或希望协商安全参数，该字段为空，否则表示客户端希望重用该会话。这个会话标识可能是之前的连接标识，当前连接标识，或其他处于连接状态的连接标识。会话标识生成后应一致保持到被超时删除或与这个会话相关的连接遇到致命错误被关闭。一个会话失效或被关闭时则与其相关的连接都应被强制关闭。

4、cipher_suites 是客户端所支持的密码套件列表，客户端应按照密码套件使用的优先级顺序排列，优先级最高的密码套件应排在首位。如果会话标识字段不为空，本字段应至少包含将重用的会话所使用的密码套件。每个密码套件包括一个密钥交换算法，一个加密算法和一个校验算法。服务器将在密码套件列表中选择一个与之匹配的密码套件，如果没有可匹配的密码套件，应返回握手失败报警消息并且关闭连接。

5、compression_methods 是客户端所支持的压缩算法列表，客户端应该按照压缩算法使用的优先级顺序排列，优先级最高的压缩算法排在首位。服务器将在压缩算法列表中选择一个与之匹配的压缩算法，列表中必须包含空压缩算法，这样客户端和服务器总能协商出一致的压缩算法。

需要说明的是，服务器如果能从客户端问候消息中找到匹配的密码套件，服务器发送所述服务端问候消息（Server Hello 消息）作为对客户端问候消息的回复。如果找不到匹配的密码套件，服务器将回应报警消息。

本实施例中，数字证书的认证过程中采用非对称算法进行认证，即发送者采用接收者的公钥对数据进行加密，对应接收者采用自己的私钥对数据进行解密。其中，证书的非对称算法采用 SM2 算法，使用签名证书基于 ECDSA 签名实现身份认证，使用加密证书基于 ECDH 实现密钥协商。

在本发明实施例的一种可选示例中，所述加密子进程和所述网络服务器进行双向证书认证，具体可以通过以下方式来实现:

1）所述加密子进程接收所述网络服务器发送的服务端证书消息，所述服务端证书消息包括所述网络服务器的站点签名证书;

2）所述加密子进程接收所述网络服务器发送的证书认证请求消息，所述证书认证请求消息用于指示进行客户端的证书认证;

3）所述加密子进程接收所述网络服务器发送的服务端密钥交换消息，包括密钥交换

参数;

4）所述加密子进程接收所述网络服务器发送的服务端问候完结消息;

5）所述加密子进程对所述站点签名证书进行认证;

6）当所述站点签名证书认证通过后，所述加密子进程向所述网络服务器发送客户端证书消息，所述客户端证书消息包括所述浏览器客户端的签名证书，以使所述网络服务器对所述签名证书进行认证。

本实施例中，上述加密数据协商、证书认证、密钥交换以及签名认证都是在安全浏览器客户端的加密子进程和网络服务器的握手过程中执行的。本实施例中，双向认证采用了双证书机制，证书的非对称算法采用 SM2 算法，使用签名证书基于 ECDSA 签名实现身份认证,使用加密证书基于 ECDH 实现密钥协商。使用的 SM4 算法对数据进行加密，使用 SM3 算法对数据进行摘要。

其中，SM2 算法（SM2 algorithm）是一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。SM3 算法（SM3 algorithm）是一种密码杂凑算法，其密钥长度为 128 比特，SM4 算法（SM4 algorithm）是一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

如图 4 所示，加密子进程和网络服务器的握手过程包括:

4.02、加密子进程发送客户端问候消息 ClientHello 给网络服务器。

4.04、网络服务器发送服务端问候消息 SeverHello 给所述安全浏览器客户端的加密子进程。

其中，网络服务器从 ClientHello 消息中找到匹配的密码套件，发送 SeverHello 作为回复，若找不到匹配的密码套件，则发送报警消息。该 SeverHello 中，Sever_vision，表示服务器支持的版本号，如 1.1; Radom 服务器端产生的随机数; session_id 服务端使用的会话标识; cipher_suites 服务端从 ClientHello 消息中选取的密码套件; compression_methods 服务端从 ClientHello 消息中选取的压缩算法。

4.06、网络服务器发送服务端证书消息 Certificate 给加密子进程。

即 SeverCertificate 本消息内容为签名证书和加密证书。如服务端的站点签名证书（X.509 序列）

4.08、网络服务器发送证书认证请求消息 SeverRequest 给加密子进程。

通过 SeverRequest 消息要求客户端提供证书。同时指明了认证类型（ECDSA）

4.10、网络服务器发送服务端密钥交换消息 SeverKeyExchange 给加密子进程。

SeverKeyExchange 用于客户端计算产生 48 字节的预主密钥。公钥可以直接从服务器端的加密证书中获取。如客户端随机产生预主密钥 pre_master_seceret 密钥，并使用服务

器证书的公钥进行 ECDH 运算

4.12、网络服务器发送问候完结消息 SeverHelloDone 给加密子进程。

SeverHelloDone 表征握手过程的 hello 消息阶段完成，然后等待客户端的响应消息。

4.14、加密子进程发送客户密钥交换消息 Certificate 给网络服务器。

即 ClientCertificate 消息是 hello 消息阶段完成后的第一条消息，如包括客户的签名证书（X.509 序列）。

4.16、加密子进程发送客户密钥交换消息 ClientKeyExchange 给网络服务器。

ClientKeyExchange 消息中网络服务器的公钥加密预主密钥。

4.18、加密子进程发送证书校验消息 CertificateVerify 给网络服务器。

CertificateVerify 消息用于鉴别客户端是够为证书的合法持有者。本实施例中，提示用户插入 USBKey 后可以提示用户输入保护口令，该保护口令即携带在该消息中验证用户是否合法。

如，客户端使用签名证书的 ECC 私钥对握手信息的摘要进行 ESDSA 签名

4.20、加密子进程发送客户端密码规格变更消息 ChangeCipherSpec 给网络服务器。

即 ClientChangeCipherSpec 消息向服务端表明算法及密钥协商完成。

4.22、加密子进程发送客户端握手结束消息 Finished 给网络服务器。

本实施例中，加密子进程根据客户端的随机数、服务端的随机数、pre_master_seceret 使用密钥算法计算 master_seceret，然后再使用随机数和 master_seceret 计算真正的数据加密密钥，然后将所有握手消息摘要后加密形成 ClientFinished 消息向服务端发送。

4.24、网络服务器发送服务端密码规格变更消息 ChangeCipherSpec 给加密子进程。

4.26、网络服务器发送服务端握手结束消息 Finished 给加密子进程。

服务端验证客户端证书，使用客户端的签名证书验证客户端的签名。服务使用自身的加密私钥和进行 ECDH 运算，获得 pre_master_seceret，采用客户端同样的算法计算 master_seceret 和数据加密密钥，验证 SeverFinished 消息的正确性，向客户端发送 SeverChangeCipherSpec 消息，表示认可算法及密钥协商。

通过上述握手过程完成了浏览器客户端和网络服务器双方的认证、密钥协商等过程，从而加密子进程和网络服务端可以分别使用协商计算出的密钥加密应用数据。

步骤 206，自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件。

本实施例以所访问的网站需要进行双向认证为例进行说明，当浏览器客户端的地址栏接收到用户输入的需要双向认证的网站地址时，浏览器客户端弹出对话框提示用户插入安全密钥存储硬件，即提示用户插入 USBKey，如图 5 所示。双向认证是对所访问网站的网络服务器和浏览器客户端彼此均要进行认证，确认访问的网络服务器的数字证书

以及浏览器客户端所加载的数字证书是安全有效的，因此双向认证时需要认证的证书包括访问的网站的站点证书以及浏览器客户端所加载的用户证书。因此，本实施例中所述自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件，具体可以包括以下两个子步骤：

子步骤一，在进行数字证书的双向认证时，所述加密子进程通过所述安全密钥存储硬件的供应方标识和产品编号关联到对应的驱动位置和驱动接口。需要说明的是，进行双向认证时所述数字证书具体包括访问的网站的站点证书以及浏览器客户端所加载的存储在安全密钥存储硬件中的用户证书。浏览器的加密子进程可以通过所述安全密钥存储硬件的供应方标识和产品编号关联到对应的驱动位置和驱动接口。

子步骤二，通过所述驱动位置和驱动接口与所述安全密钥存储硬件建立连接通道。获知所述安全密钥存储硬件的驱动位置和驱动接口之后，可以根据所述驱动位置和驱动接口与所述安全密钥存储硬件建立通信通道。

需要说明的是，在本发明实施例的一种可选示例中，所述步骤 206 自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件之前，还包括：所述加密子进程在握手过程中确定是否接收所述网络服务器发送的证书认证请求消息；当接收到所述网络服务器发送的证书认证请求消息时，监测浏览器客户端所在终端的接口是否有安全密钥存储硬件插入；当监测到有安全密钥存储硬件插入时，执行所述步骤 206 自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件。

步骤 208，浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择。

本实施例中所述浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择，具体可以通过以下子步骤：

子步骤一，所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书。所述加密子进程根据所述驱动位置和驱动接口与所述安全密钥存储硬件建立了连接通道，可以通过所述连接通道读取安全密钥存储硬件中存储用户证书。需要说明的是，此时加密子进程读取到的只是用户证书的名称等不包含用户证书具体内容的信息。在本发明实施例的一种可选示例中，所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书，具体可以包括：所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的应用，显示所述应用以供用户进行选择，其中每个应用包括容器和容器中存储的用户证书；打开用户选择的应用，加载所述用户选择的应用下的容器和容器中存储的用户证书。

子步骤二，弹出证书选择对话框，在所述证书选择对话框中加载所述用户证书以提

示用户选择所述用户证书。需要说明的是，如图 6 所示，本实施例在浏览器客户端中弹窗证书选择对话框，证书选择对话框中具体可以包括以下任意一种或几种：当前设备、应用名称、容器名称、证书 CN、颁发者、生效日期、失效时间、用户证书的名称等信息，能够提示用户选择所述用户证书即可，本实施例并非对证书选择对话框具体形式或具体内容的限制。

本实施例中，为了保证访问网站和用户的安全，CA（Certificate Authority，认证中心）机构为不同的网站颁布不同的站点证书，同时为不同网站的不同用户颁布不同的用户证书。其中，数字证书中包括站点或用户的公钥，站点或用户的信息，以及数字签名等内容。

因此，在进行数字证书认证之前，优选的，在双向认证过程中，可以在浏览器客户端中弹出证书选择框，在该证书选择框中加载浏览器所在终端当前所具有的用户证书，用户在对用户证书进行选择后，提示用户输入保护口令，如图 7 所示，输入个人识别码（Personal Identification Number，PIN），从而在保护口令通过验证后说明该用户对该用户证书具有权项。并且，上述用户证书和保护口令可以作为用户证书认证过程中的认证数据发送给网络服务器。

在本发明实施例的一种可选示例中，所述子步骤一中加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书之后，还包括：所述加密子进程对所述安全密钥存储硬件中存储的用户证书进行证书站点识别，以证书站点为单位对所述用户证书进行分类；相应地，所述子步骤二中弹出证书选择对话框，在所述证书选择对话框中加载所述用户证书以提示用户选择所述用户证书，具体可以包括：弹出证书选择对话框，在所述证书选择对话框中以证书站点为索引显示所述用户证书。需要说明的是，证书站点即该证书对应的银行站点，证书站点具体可以是：建行、工行、农行等。换句话说，在本实施例中，具体可以在证书选择对话框中显示用户证书具体是哪个银行的，直观地显示所述安全密钥存储硬件是哪个银行的，方便用户根据银行判断是否是需要的用户证书，即根据所述证书站点判断是否是需要的用户证书。

步骤 210，当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证。

本实施例中所述当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证，具体可以通过以下方式来实现：当接收到用户对所述用户证书的选择信息时，所述加密子进程弹出口令输入框，并通过所述口令输入框接收用户输入的保护口令。依据所述用户输入的保护口令对用户进行身份验证。需要说明的是，本实施例中选用保护口令作为用户的身份信息进行身份验证，具体实现时，也可以采用其他方式进行

身份验证，本实施例并非对身份验证具体方式的限定。

在本发明实施例的一种可选示例中，所述当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证，具体还包括：若所述身份验证未通过，则在所述口令输入框中显示口令错误并提示用户重新输入保护口令，依据所述重新输入的保护口令进行身份验证。由于用户在输入保护口令时键盘误操作等原因，用户存储输错保护口令的情况时有发生，因此本可选示例在身份验证未通过时，不是直接断开与安全密钥存储硬件的连接，而是允许用户重新输入保护口令，通常不允许用户无限次的输入保护口令，因此可以对输入保护口令的次数进行限制。即在本发明实施例的一种可选示例中，所述当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证，还包括：所述加密子进程设置所述口令输入框的最大输入次数，当所述口令输入框中用户输入的保护口令的次数达到所述最大输入次数时，关闭所述个人密码输入框，并断开与所述安全密钥存储硬件的连接。这样既可以避免用户一次输错保护口令就断开与所述安全密钥存储硬件的连接，所造成的用户需要重新插入所述安全密钥存储硬件进行用户验证的操作繁琐且加载安全密钥存储硬件效率不高的问题，也避免了无限次输入密保口令造成的资源占用或死循环问题，提高了加载安全密钥存储硬件的效率。

步骤 212，所述身份验证通过后，加载所述选择信息对应的用户证书内容。

本实施例中所述身份验证通过后，加载所述选择信息对应的用户证书内容，具体可以包括以下子步骤：

子步骤一，所述身份验证通过后，所述加密子进程获取所述用户证书中的认证信息，并将所述认证信息加载到证书查看器中。

子步骤二，所述加密子进程依据触发指示启动所述证书查看器，在所述证书查看器中显示所述用户证书的认证信息。需要说明的是，在所述证书查看器中显示所述用户证书的认证信息，具体可以通过以下方式来实现：在所述证书查看器中分别设置常规选项卡和详细选项卡；在所述常规选项卡中显示所述选择信息对应的用户证书的常规信息；在所述详细选项卡中显示所述选择信息对应的用户证书的详细信息。即根据触发指示启动所述证书查看器，该证书查看器中分别设置由常规选项卡和详细选项卡，在常规选项卡中加载所述用户证书的常规信息，如图 8A 所示，在所述详细选项卡中加载所述用户证书的详细信息，如图 8B 所示，通过对不同选项卡的选择可以查看用户证书的不同内容。

需要说明的是，在本发明实施例的一种可选示例中，所述加载所述选择信息对应的用户证书内容之后，还包括：所述加密子进程断开与所述安全密钥存储硬件的连接。

在本发明实施例的一种可选示例中，浏览器客户端加载用户证书时，首先可以弹出证书选择框提示用户插入安全密钥存储硬件，该安全密钥存储硬件即 USB Key，它是一

种 USB 接口的硬件设备，内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书，利用 USB Key 内置的公钥算法实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。

在用户插入安全密钥存储硬件后，调用所述安全密钥存储硬件的驱动程序在所述通过所述证书选择框中加载安全密钥存储硬件中的证书信息，然后接收用户选择的证书信息；在所述证书选择框中弹出保护口令输入窗口，再接收用户输入的保护口令。

其中，浏览器自动识别 USBKey 需要依赖 CSP（Cryptographic Service Provider，加密服务提供）注册表项中的两个关键信息：SKFImagePath：指定 SKF 动态库的路径。TokenVidPid：字符串格式。KEY 设备的 VendorID 和 ProductID，采用的格式类似 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB 中的格式，也即 VID_XXXX&PID_XXXX。

浏览器会通过 USBKey 设备的供应方标识 vendorid、产品编号 productid 关联到相应驱动，完成相关操作。浏览器不会存储用户输入的 pin 密码，也不会存储 USBKey 中的私钥信息。对 USBKey 的操作流程如下：连接到 USBKey 设备；打开相应的应用 Application，Application 由用户选择决定；打开相应的容器 Container，Container 由用户选择决定，然后输入校验 PIN 码，验证错误后会提示重新输入，然后获取签名证书信息，获取加密证书信息，进行数字证书的认证，后续在与网络服务器进行数据交互的过程中，对数据的加、解密过程也是在 USBKey 中完成的，从而在对该网站访问完成后关闭设备并断开连接。

本发明一个可选实施例中，接收所述网络服务器返回的允许连接消息，建立所述浏览器和所述网站对应网络服务器之间进行加密数据传输的安全连接通道，所述允许连接消息是由所述网络服务器对所述用户证书的安全认证通过后发送的。

上述证书认证通过后，网络服务器返回允许连接消息，此时建立所述浏览器和所述网站对应网络服务器之间进行加密数据传输的安全连接通道。在该安全连接通道中传输数据，本实施例中，采用对称算法 SM4 算法对数据进行加、解密，其中 SM4 算法即 SM4 algorithm，是一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明实施例并不受所描述的动作顺序的限制，因为依据本发明实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本发明实施例所必须的。

实施例三：

在上述实施例的基础上，本实施例还公开了一种浏览器客户端装置。

参照图 9，示出了根据本发明一个实施例的一种浏览器客户端装置实施例的结构框图，具体可以包括：连接模块 902、读取模块 904、身份验证模块 906 和加载模块 908，其中，

连接模块 902，用于自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；

读取模块 904，用于读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；

身份验证模块 906，用于当接收到用户对所述用户证书的选择信息时，对用户进行身份验证；

加载模块 908，用于所述身份验证通过后，加载所述选择信息对应的用户证书内容。

综上所述，本实施例提供的浏览器客户端在加载安全密钥存储硬件时，首先通过连接模块 902 自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；然后读取模块 904 读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；接着身份验证模块 906 当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证；最后加载模块 908 在所述身份验证通过后，加载所述选择信息对应的用户证书内容。本实施例提供的浏览器客户端在加载安全密钥存储硬件中存储的用户证书时，先通过身份验证模块 906 对用户进行了身份验证，加载模块 908 在身份验证通过，能够确认用户身份的情况下，加载安全密钥存储硬件中存储的用户证书的内容，可以防止安全密钥存储硬件中存储的用户证书被泄露，提高了浏览器客户端加载安全密钥存储硬件时的安全性。

在本发明实施例的如图 10 所示的一种可选示例中，所说浏览器客户端装置还包括：主业务进程模块 910 和加密子进程模块 912，其中，主业务进程模块 910，用于在浏览器客户端中启动与主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；加密子进程模块 912，用于通过握手过程与所述网络服务器进行数字证书双向认证。

在本发明实施例的一种可选示例中，所述加密子进程模块，用于通过握手过程与所述网络服务器依次执行以下安全认证操作：加密数据协商、证书认证、密钥交换和签名认证。

在本发明实施例的一种可选示例中，所述连接模块，用于在进行数字证书的双向认证时，所述加密子进程通过所述安全密钥存储硬件的供应方标识和产品编号关联到对应的驱动位置和驱动接口；通过所述驱动位置和驱动接口与所述安全密钥存储硬件建立连

接通道。

在本发明实施例的如图 11 所示的一种可选示例中，所述读取模块 904 包括：读取子模块 9042，用于通过所述连接通道读取所述安全密钥存储硬件中存储用户证书；加载子模块 9044，用于弹出证书选择对话框，在所述证书选择对话框中加载所述用户证书以提示用户选择所述用户证书。

在本发明实施例的如图 12 所示的一种可选示例中，所述读取模块 904 还包括：识别子模块 9046，用于通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书之后，对所述安全密钥存储硬件中存储的用户证书进行证书站点识别，以证书站点为单位对所述用户证书进行分类；所述加载子模块 9044，具体用于弹出证书选择对话框，在所述证书选择对话框中以证书站点为索引显示所述用户证书。

在本发明实施例的一种可选示例中，所述读取子模块，具体用于通过所述连接通道读取所述安全密钥存储硬件中存储的应用，显示所述应用以供用户进行选择，其中每个应用包括容器和容器中存储的用户证书；打开用户选择的应用，加载所述用户选择的应用下的容器和容器中存储的用户证书。

在本发明实施例的一种可选示例中，所述身份验证模块，具体用于当接收到用户对所述用户证书的选择信息时，弹出口令输入框，并通过所述口令输入框接收用户输入的保护口令；依据所述用户输入的保护口令对用户进行身份验证。

在本发明实施例的一种可选示例中，所述身份验证模块，还用于在所述身份验证未通过时，在所述口令输入框中显示口令错误并提示用户重新输入保护口令，依据所述重新输入的保护口令进行身份验证。

在本发明实施例的一种可选示例中，所述身份验证模块，还用于对所述口令输入框设置最大输入次数，当所述口令输入框中用户输入的保护口令的次数达到所述最大输入次数时，关闭所述个人密码输入框，并断开与所述安全密钥存储硬件的连接。

在本发明实施例的一种可选示例中，所述加载模块，具体用于所述身份验证通过后，获取所述用户证书中的认证信息，并将所述认证信息加载到证书查看器中；所述加密子进程模块，用于依据触发指示启动所述证书查看器，在所述证书查看器中显示所述用户证书的认证信息。

在本发明实施例的一种可选示例中，所述加密子进程模块，用于在所述证书查看器中分别设置常规选项卡和详细选项卡；在所述常规选项卡中显示所述选择信息对应的用户证书的常规信息；在所述详细选项卡中显示所述选择信息对应的用户证书的详细信息。

在本发明实施例的一种可选示例中，所述加密子进程模块，还用于在握手过程中确定是否接收所述网络服务器发送的证书认证请求消息；所述连接模块，还用于当所述加

密子进程接收到所述网络服务器发送的证书认证请求消息时，监测浏览器客户端所在终端的接口是否有安全密钥存储硬件插入；当监测到有安全密钥存储硬件插入时，自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件。

在本发明实施例的一种可选示例中，所述加密子进程模块，还用于所述加载模块加载所述选择信息对应的用户证书内容之后，断开与所述安全密钥存储硬件的连接。

需要说明的是，可以参照图 13 所示的加密子进程的结构框图对加密子进程进行理解，如图 13 所示，加密子进程包括：配置模块 1302、代理模块 1304、CTL 管理模块 1306、CRL 管理模块 1308、Session 管理模块 1310、证书验证模块 1312、SSL 连接模块 1314、USBKey 操作模块 1316。其中，代理模块接受浏览器主业务进程连接，根据浏览器主业务进程连接的类型进行相应处理，形成浏览器主业务进程的连接代理。CTL 模块用于管理信任根证书列表。CRL 管理模块用于获取 CRL 列表，管理本地 CRL 列表。Session 管理模块管理代理进程与 web 服务器的 session 连接。SSL 连接模块负责建立与 web 服务器的安全连接。USBKey 管理模块负责操作 USBKey 设备。配置模块负责读取、存储客户端的相关配置。

其中，对于 CTL 管理模块 1306，其工作原理如下：CTL 描述的是浏览器信任根证书列表，用于验证服务器端证书。360 安全浏览器中，支持的信任根证书为 PEM 编码方式，同时支持两种证书添加方式：1）程序内部添加信任根证书；2）配置文件添加信任根证书，配置文件采用 des 加密保存。其中，CTL 可以配置为不支持导入导出功能。

对于 CRL 管理模块 1308，其工作原理如下：CRL 描述的是证书颁发机构 CA 的证书撤销列表，其本质是证书序列号，证书序列号以 ASN.1 编码的 Integer 表示。X509v3 证书中的一个扩展项（OID 为 2.5.29.31）用于指定该证书的 CRL 发布点。本实施例的安全浏览器中装置对 CRL 进行了本地缓存，同时 CRL 查找根据 CA 进行一级索引。对 CRL 的验证操作的步骤如下：（1）获取证书中的 Issuer 项，定位对应的 CA 节点，如果 Issuer 项不存在或者找不到对应的 CA 项，则认为是非法证书。（2）使用二分法搜索该 CA 下所有的 CRL 项。

对于 Session 管理模块 1310，SSL 连接需要在 TCP 3 次握手的基础上增加 4 次握手，连接建立过程是比较耗时的，因此保存 Session、复用之前的连接可以有效优化连接性能。本实施例的安全浏览器装置中在一次 SSL 连接建立完成之后，会建立 host+port 到 session 的内存索引，后续操作会复用之前的 session，如 session 有效期为 1 小时。浏览器关闭、USBKey 设备拔出时会清空之前的 session。

对于证书验证模块 1312，SSL 连接建立过程中如果需要双向认证，所述加密子进程会提示用户插入安全密钥存储硬件，即 USBKey 设备。在用户插入安全密钥存储硬件后

能够自动识别并弹出证书选择对话框，提示用户选择证书。所述加密子进程自动识别安全密钥存储硬件需要依赖 CSP 注册表项中的两个关键信息：SKFImagePath：指定 SKF 动态库的路径和 TokenVidPid：字符串格式。KEY 设备的 VendorID 和 ProductID，采用的格式类似 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB 中的格式，也即 VID_XXXX&PID_XXXX。浏览器会通过 USBKey 设备的 vendorid、productid 关联到相应驱动，完成相关操作。浏览器不会存储用户输入的 pin 密码，也不会存储 USBKey 中的私钥信息。具体流程如下：首先连接到 USBKey 设备；然后打开相应应用（Application），Application 由用户选择决定；然后打开相应容器（Container），Container 由用户选择决定；接着校验 PIN 码（个人身份识别码），验证错误后会提示重新输入；然后获取签名证书信息；接着获取加密证书信息；最后关闭设备、断开连接。

本实施例中，针对上述方法实施例的证书验证过程，对服务器端的证书验证发生在握手协议过程中，浏览器收到 ServerHelloDone 消息之后，发送 Certificate 消息之前。证书验证主要确保服务器的合理性，验证过程依赖于 CTL，CRL 模块，具体过程在子进程证书验证线程池中进行。检查步骤如下：初始化受信任根证书列表；检查是否是自签名证书；检查证书扩展信息；检查证书信任关系；检查 CRL 列表；检查证书签名；检查证书时间有效性；检查证书是否在黑名单中。

需要说明的是，可以参照图 14 所示的主业务进程的结构框图对主业务进程进行理解，如图 14 所示，主业务进程包括：证书显示模块 1402、白名单管理模块 1404、网络服务器证书存储模块 1406、代理设置模块 14014。其中证书显示模块 1402 负责显示数字证书。白名单管理模块 1404 负责管理支持本实施例的加密算法的 web 服务器列表。网络服务器证书存储模块 1406 用于存储负责管理网络服务器的证书。代理设置模块 14014 代理设置负责设置与加密子进程的代理。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

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，以及此外可以把它们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加载安全密钥存储硬件的方法和浏览器客户端装置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15示出了可以实现根据本发明的加载安全密钥存储硬件的方法的计算设备。该计算设备传统上包括处理器1510和以存储器1520形式的程序产品或者可读介质。存储器1520可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM或者ROM之类的电子存储器。存储器1520具有用于执行上述方法中的任何方法步骤的程序代码1531的存储空间1530。例如，用于程序代码的存储空间1530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 1531。这些程序代码可以从一个或者多个程序产品中读出或者写入到这一个或者多个程序产品中。这些程序产品包括诸如存储卡之类的程序代码载体。这样的程序产品通常为如参考图 16 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 15 的计算设备中的存储器 1520 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，存储单元包括可读代码 1531'，即可以由例如诸如 1510 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。

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。

权 利 要 求 书

1、一种加载安全密钥存储硬件的方法，包括:

自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件;

浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择;

当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证;

所述身份验证通过后，加载所述选择信息对应的用户证书内容。

2、根据权利要求 1 所述的方法，其特征在于，还包括:

在浏览器客户端中启动与主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发;

所述加密子进程通过握手过程与所述网络服务器进行数字证书双向认证。

3、根据权利要求 2 所述的方法，其特征在于，所述加密子进程通过握手过程与所述网络服务器进行数字证书的双向认证的步骤，包括:

所述加密子进程通过握手过程与所述网络服务器依次执行以下安全认证操作：加密数据协商、证书认证、密钥交换和签名认证。

4、根据权利要求 3 所述的方法，其特征在于，所述自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件，包括:

在进行数字证书的双向认证时，所述加密子进程通过所述安全密钥存储硬件的供应方标识和产品编号关联到对应的驱动位置和驱动接口;

通过所述驱动位置和驱动接口与所述安全密钥存储硬件建立连接通道。

5、根据权利要求 4 所述的方法，其特征在于，所述浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择，包括:

所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储用户证书;

弹出证书选择对话框，在所述证书选择对话框中加载所述用户证书以提示用户选择所述用户证书。

6、根据权利要求 5 所述的方法，其特征在于，所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书之后，还包括:

所述加密子进程对所述安全密钥存储硬件中存储的用户证书进行证书站点识别，以证书站点为单位对所述用户证书进行分类;

所述弹出证书选择对话框，在所述证书选择对话框中加载所述用户证书以提示用户选择所述用户证书，包括:

弹出证书选择对话框，在所述证书选择对话框中以证书站点为索引显示所述用户证书。

7、根据权利要求 5 所述的方法，其特征在于，所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书，包括:

所述加密子进程通过所述连接通道读取所述安全密钥存储硬件中存储的应用，显示所述应用以供用户进行选择，其中每个应用包括容器和容器中存储的用户证书;

打开用户选择的应用，加载所述用户选择的应用下的容器和容器中存储的用户证书。

8、根据权利要求 5 所述的方法，其特征在于，所述当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证，包括:

当接收到用户对所述用户证书的选择信息时，所述加密子进程弹出口令输入框，并通过所述口令输入框接收用户输入的保护口令;

依据所述用户输入的保护口令对用户进行身份验证。

9、根据权利要求 8 所述的方法，其特征在于，所述当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证，还包括:

若所述身份验证未通过，则在所述口令输入框中显示口令错误并提示用户重新输入保护口令，依据所述重新输入的保护口令进行身份验证。

10、根据权利要求 9 所述的方法，其特征在于，所述当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证，还包括:

所述加密子进程设置所述口令输入框的最大输入次数，当所述口令输入框中用户输入的保护口令的次数达到所述最大输入次数时，关闭所述个人密码输入框，并断开与所述安全密钥存储硬件的连接。

11、根据权利要求 2 所述的方法，其特征在于，所述身份验证通过后，加载所述选择信息对应的用户证书内容，包括:

所述身份验证通过后，所述加密子进程获取所述用户证书中的认证信息，并将所述认证信息加载到证书查看器中;

所述加密子进程依据触发指示启动所述证书查看器，在所述证书查看器中显示所述用户证书的认证信息。

12、根据权利要求 11 所述的方法，其特征在于，在所述证书查看器中显示所述用户证书的认证信息，包括:

在所述证书查看器中分别设置常规选项卡和详细选项卡;

在所述常规选项卡中显示所述选择信息对应的用户证书的常规信息;

在所述详细选项卡中显示所述选择信息对应的用户证书的详细信息。

13、根据权利要求 3 所述的方法，其特征在于，所述自动识别并连接浏览器客户端

所在终端的接口插入的安全密钥存储硬件之前，还包括：

所述加密子进程在握手过程中确定是否接收所述网络服务器发送的证书认证请求消息；

当接收到所述网络服务器发送的证书认证请求消息时，监测浏览器客户端所在终端的接口是否有安全密钥存储硬件插入；

当监测到有安全密钥存储硬件插入时，执行所述自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件的步骤。

14、根据权利要求 2 所述的方法，其特征在于，所述加载所述选择信息对应的用户证书内容之后，还包括：

所述加密子进程断开与所述安全密钥存储硬件的连接。

15、一种浏览器客户端装置，包括：

连接模块，用于自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件；

读取模块，用于读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择；

身份验证模块，用于当接收到用户对所述用户证书的选择信息时，对用户进行身份验证；

加载模块，用于所述身份验证通过后，加载所述选择信息对应的用户证书内容。

16、根据权利要求 15 所述的装置，其特征在于，还包括：

主业务进程模块，用于在浏览器客户端中启动与主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发；

加密子进程模块，用于通过握手过程与所述网络服务器进行数字证书双向认证。

17、根据权利要求 16 所述的装置，其特征在于：

所述加密子进程模块，用于通过握手过程与所述网络服务器依次执行以下安全认证操作：加密数据协商、证书认证、密钥交换和签名认证。

18、根据权利要求 17 所述的装置，其特征在于：

所述连接模块，用于在进行数字证书的双向认证时，所述加密子进程通过所述安全密钥存储硬件的供应方标识和产品编号关联到对应的驱动位置和驱动接口；通过所述驱动位置和驱动接口与所述安全密钥存储硬件建立连接通道。

19、根据权利要求 18 所述的装置，其特征在于，所述读取模块，包括：

读取子模块，用于通过所述连接通道读取所述安全密钥存储硬件中存储用户证书；

加载子模块，用于弹出证书选择对话框，在所述证书选择对话框中加载所述用户证书以提示用户选择所述用户证书。

20、根据权利要求 19 所述的装置，其特征在于，所述读取模块还包括:

识别子模块，用于通过所述连接通道读取所述安全密钥存储硬件中存储的用户证书之后，对所述安全密钥存储硬件中存储的用户证书进行证书站点识别，以证书站点为单位对所述用户证书进行分类;

所述加载子模块，具体用于弹出证书选择对话框，在所述证书选择对话框中以证书站点为索引显示所述用户证书。

21、根据权利要求 19 所述的装置，其特征在于:

所述读取子模块，具体用于通过所述连接通道读取所述安全密钥存储硬件中存储的应用，显示所述应用以供用户进行选择，其中每个应用包括容器和容器中存储的用户证书；打开用户选择的应用，加载所述用户选择的应用下的容器和容器中存储的用户证书。

22、根据权利要求 19 所述的装置，其特征在于:

所述身份验证模块，具体用于当接收到用户对所述用户证书的选择信息时，弹出口令输入框，并通过所述口令输入框接收用户输入的保护口令；依据所述用户输入的保护口令对用户进行身份验证。

23、根据权利要求 22 所述的装置，其特征在于:

所述身份验证模块，还用于在所述身份验证未通过时，在所述口令输入框中显示口令错误并提示用户重新输入保护口令，依据所述重新输入的保护口令进行身份验证。

24、根据权利要求 23 所述的装置，其特征在于:

所述身份验证模块，还用于对所述口令输入框设置最大输入次数，当所述口令输入框中用户输入的保护口令的次数达到所述最大输入次数时，关闭所述个人密码输入框，并断开与所述安全密钥存储硬件的连接。

25、根据权利要求 16 所述的装置，其特征在于:

所述加载模块，具体用于所述身份验证通过后，获取所述用户证书中的认证信息，并将所述认证信息加载到证书查看器中;

所述加密子进程模块，用于依据触发指示启动所述证书查看器，在所述证书查看器中显示所述用户证书的认证信息。

26、根据权利要求 25 所述的装置，其特征在于:

所述加密子进程模块，用于在所述证书查看器中分别设置常规选项卡和详细选项卡；在所述常规选项卡中显示所述选择信息对应的用户证书的常规信息；在所述详细选项卡中显示所述选择信息对应的用户证书的详细信息。

27、根据权利要求 17 所述的装置，其特征在于:

所述加密子进程模块，还用于在握手过程中确定是否接收所述网络服务器发送的证书认证请求消息;

所述连接模块，还用于当所述加密子进程接收到所述网络服务器发送的证书认证请求消息时，监测浏览器客户端所在终端的接口是否有安全密钥存储硬件插入；当监测到有安全密钥存储硬件插入时，自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件。

28、根据权利要求 16 所述的装置，其特征在于:

所述加密子进程模块，还用于所述加载模块加载所述选择信息对应的用户证书内容之后，断开与所述安全密钥存储硬件的连接。

29、一种程序，包括可读代码，当所述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 1-14 中的任一个所述的加载安全密钥存储硬件的方法。

30、一种可读介质，其中存储了如权利要求 29 所述的程序。

说 明 书 附 图

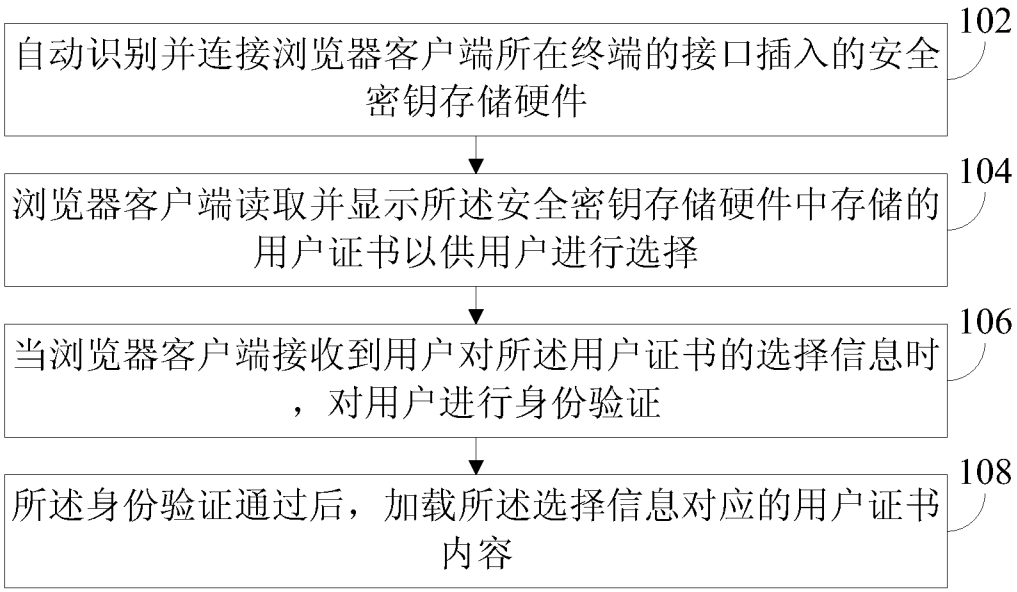

102
自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件
104
浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择
106
当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证
108
所述身份验证通过后，加载所述选择信息对应的用户证书内容

图 1

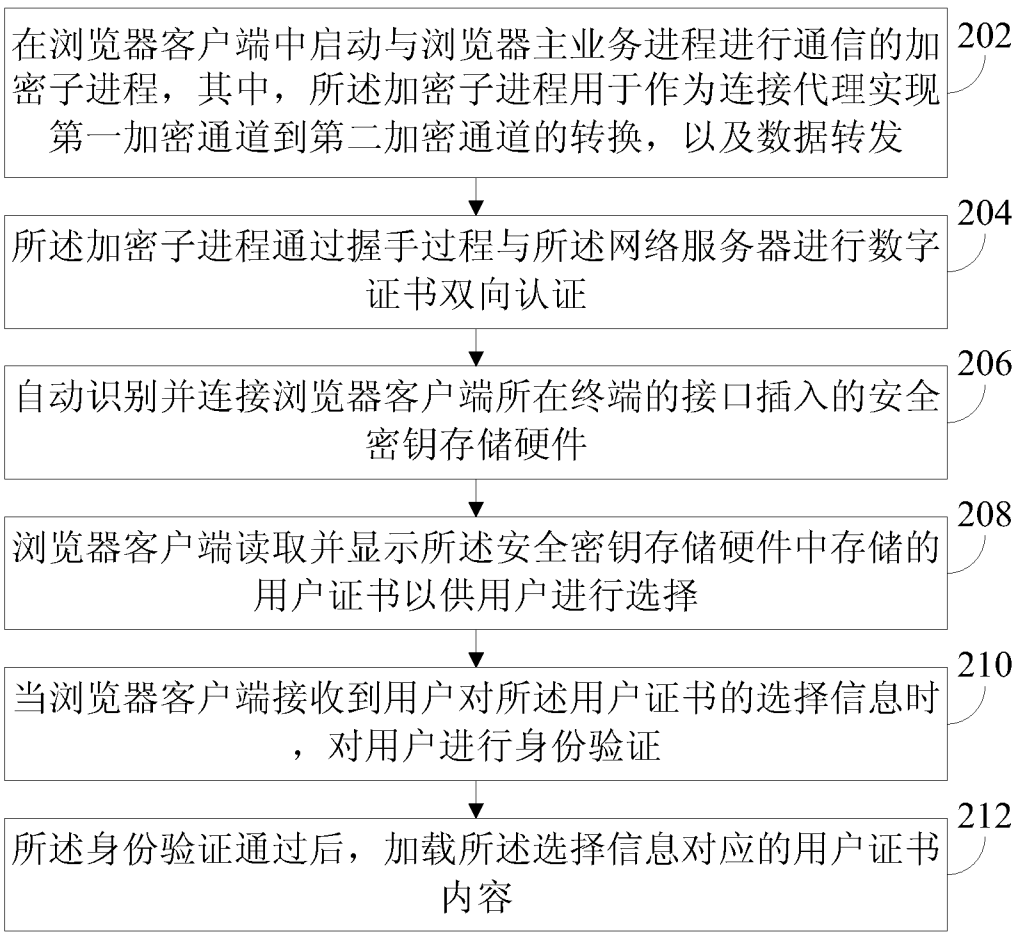

202
在浏览器客户端中启动与浏览器主业务进程进行通信的加密子进程，其中，所述加密子进程用于作为连接代理实现第一加密通道到第二加密通道的转换，以及数据转发
204
所述加密子进程通过握手过程与所述网络服务器进行数字证书双向认证
206
自动识别并连接浏览器客户端所在终端的接口插入的安全密钥存储硬件
208
浏览器客户端读取并显示所述安全密钥存储硬件中存储的用户证书以供用户进行选择
210
当浏览器客户端接收到用户对所述用户证书的选择信息时，对用户进行身份验证
212
所述身份验证通过后，加载所述选择信息对应的用户证书内容

图 2

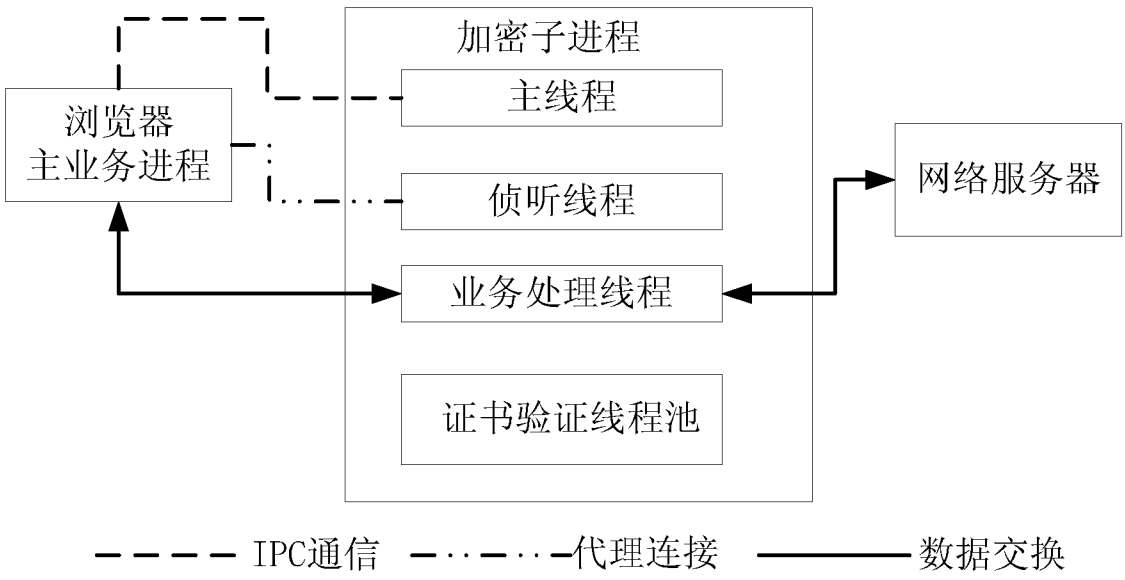

加密子进程
主线程
浏览器
主业务进程
侦听线程
网络服务器
业务处理线程
证书验证线程池
IPC通信
代理连接
数据交换

图 3

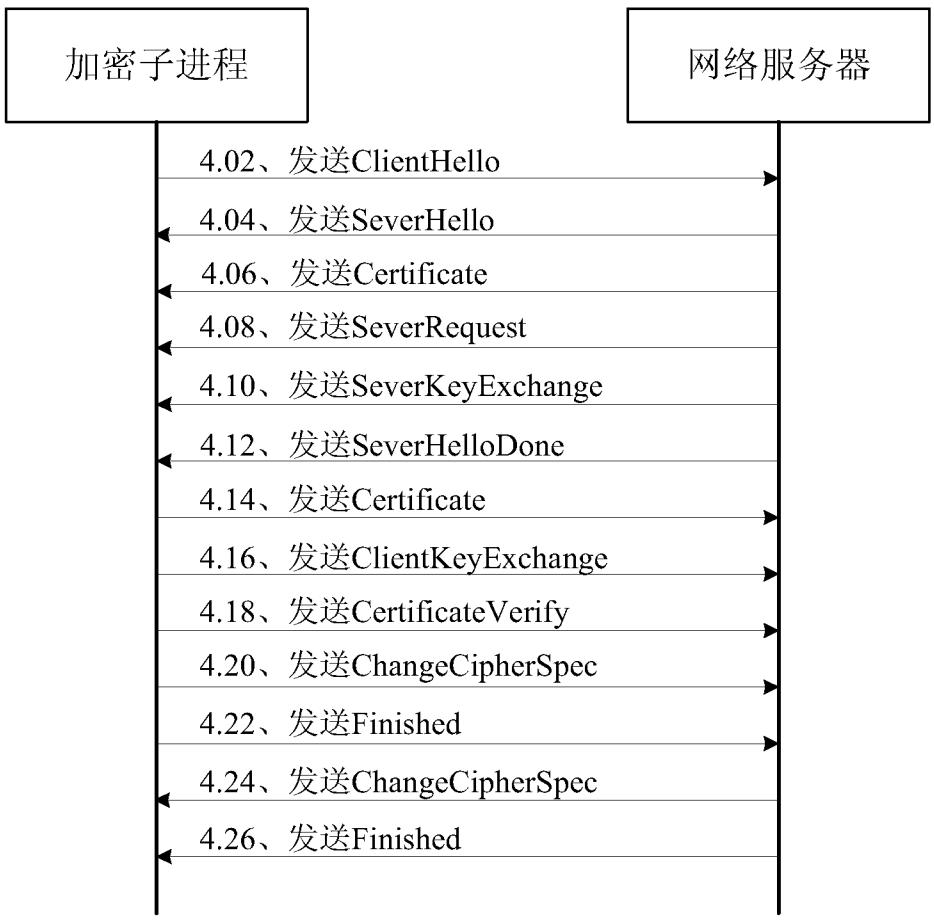

加密子进程
网络服务器
4.02、发送ClientHello
4.04、发送SeverHello
4.06、发送Certificate
4.08、发送SeverRequest
4.10、发送SeverKeyExchange
4.12、发送SeverHelloDone
4.14、发送Certificate
4.16、发送ClientKeyExchange
4.18、发送CertificateVerify
4.20、发送ChangeCipherSpec
4.22、发送Finished
4.24、发送ChangeCipherSpec
4.26、发送Finished

图 4

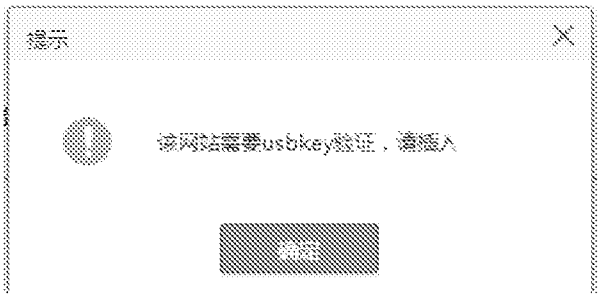

提示
确定

图 5

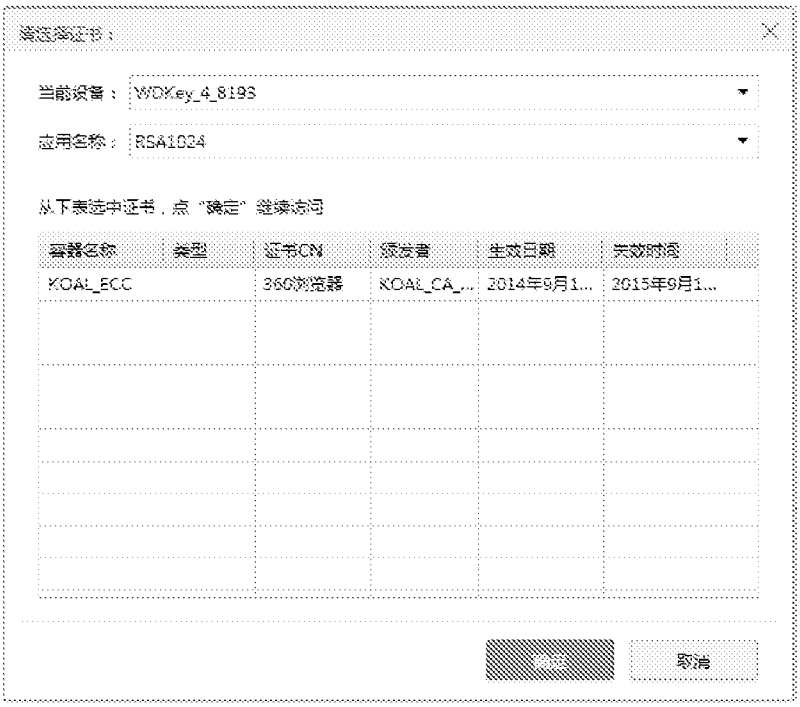

当前设备：
WDKey_4_8193
应用名称：
RSA1024
从下表选中证书，点“确定”继续访问
容器名称
类型
证书CN
颁发者
生效日期
KOAL_ECC
360浏览器
KOAL_CA_...
2014年9月1...
2015年9月1...
确定
取消

图 6


请输入pin码
pin:
确定
取消

图 7


证书查看器
常规
详细信息
此证书已经过认证，可用于下列用途：
SSL服务器验证书
颁发给
通用名(CN) ecc-site-sig
组织 Koal Software
组织单元 SSL Group
序列号 00:AD:F9:D0:F6:F8:53:3F:4F
颁发者
通用名(CN) ecc-ca
组织 Koal Software
组织单元 SSL Group
有效期
生效时间 2014年07月25日 18:07:07
过期时间 2017年04月19日 18:07:07
指纹
SHA1指纹 46:C9:C2:94:25:84:09:21:06:F2:04:1C:44:9C:4F:F5:FE:A8:CB:00
关闭

图 8A


证书查看器
常规
详细信息
证书结构
ecc-ca
ecc-site-sig
证书字段
ecc-site-sig
证书
版本
序列号
证书签名算法
颁发者
有效期限
使用者
字段值
关闭

图 8B

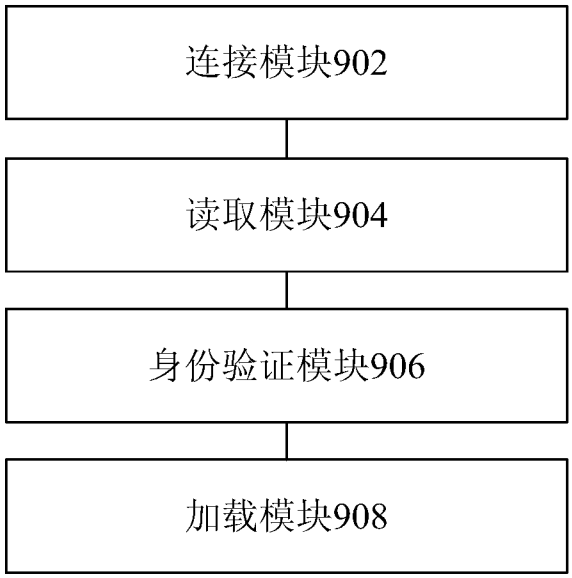

连接模块902
读取模块904
身份验证模块906
加载模块908

图 9


主业务进程模块910
加密子进程模块912
连接模块902
读取模块904
身份验证模块906
加载模块908

图 10

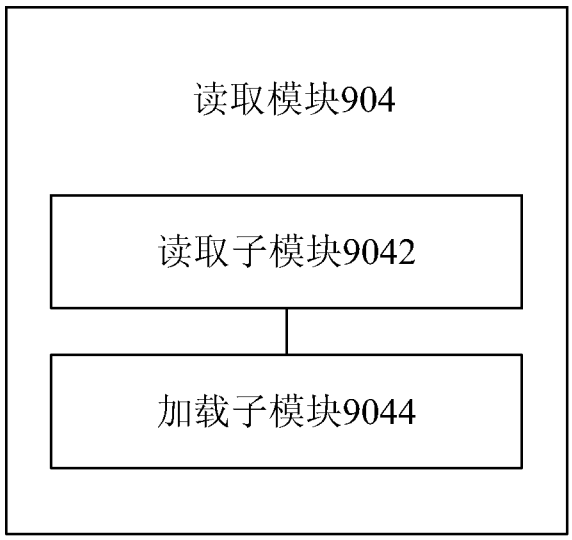

读取模块904
读取子模块9042
加载子模块9044

图 11

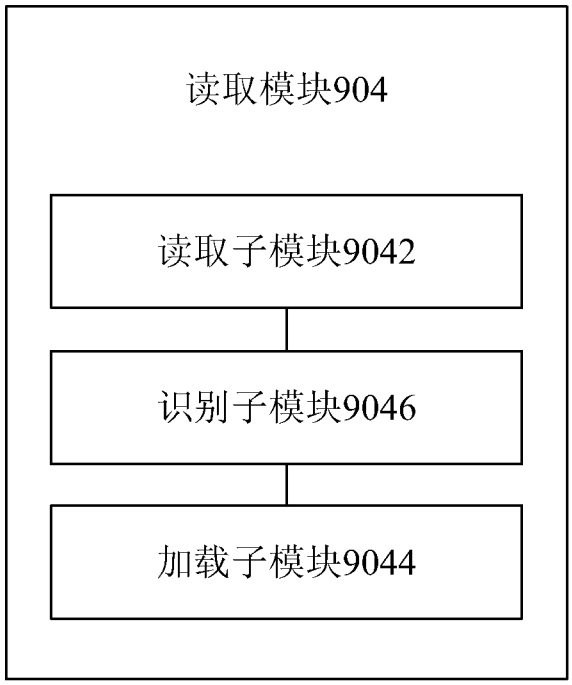

读取模块904
读取子模块9042
识别子模块9046
加载子模块9044

图 12

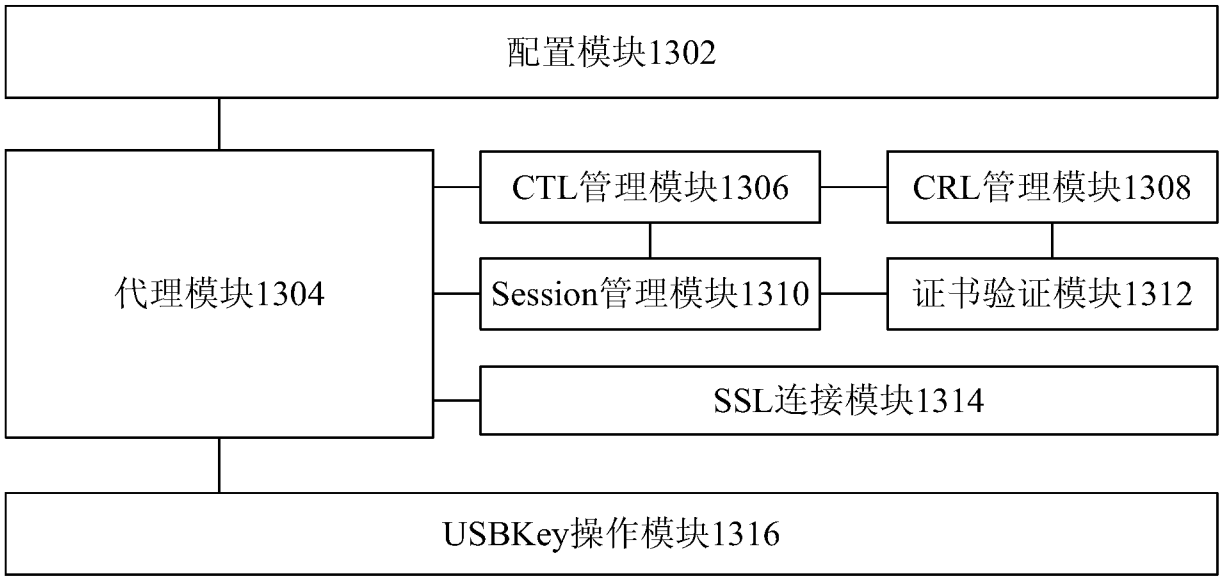

配置模块1302
代理模块1304
CTL管理模块1306
CRL管理模块1308
Session管理模块1310
证书验证模块1312
SSL连接模块1314
USBKey操作模块1316

图 13

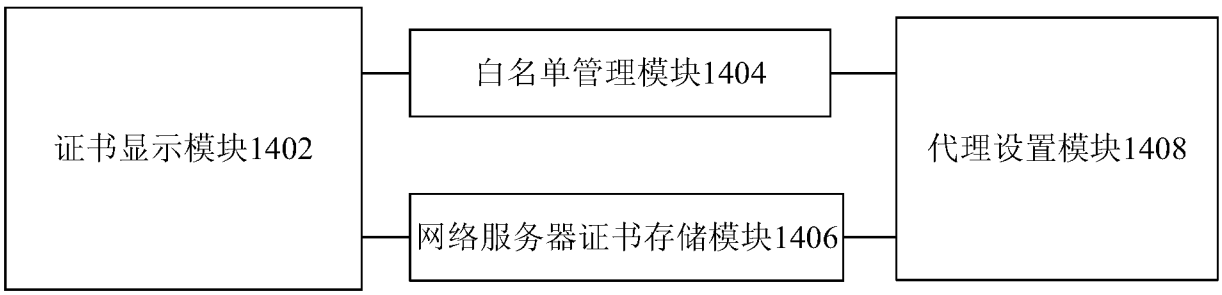

证书显示模块1402
白名单管理模块1404
网络服务器证书存储模块1406
代理设置模块1408

图 14

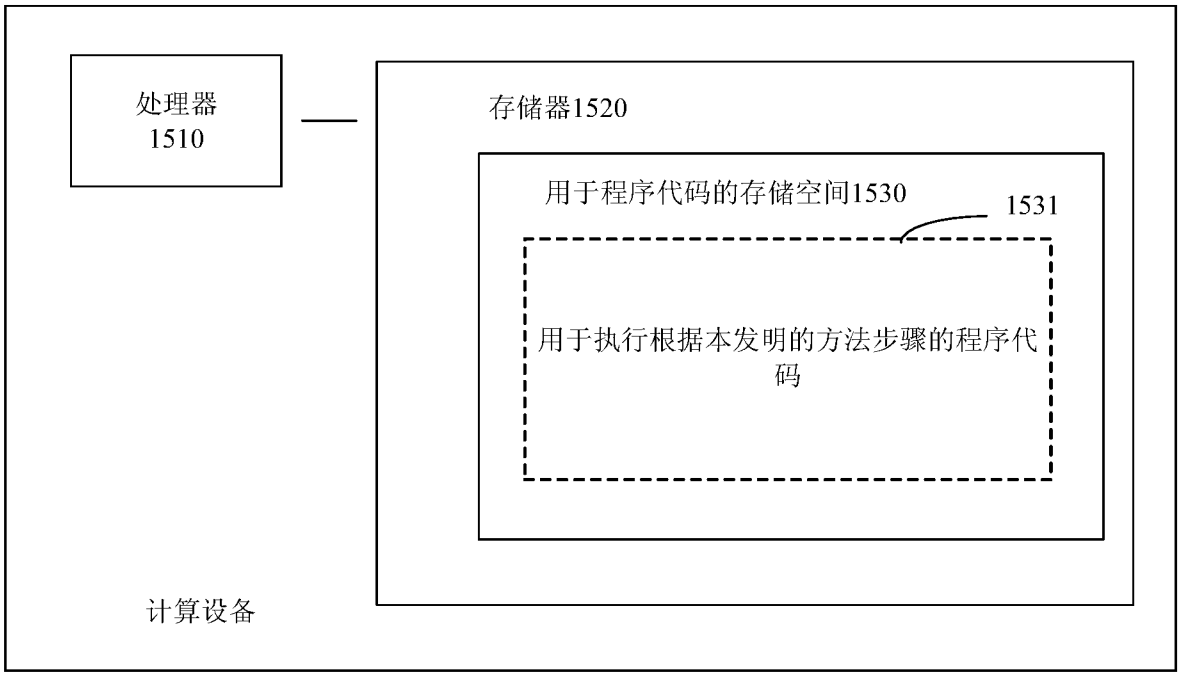

处理器
1510
存储器1520
用于程序代码的存储空间1530
1531
用于执行根据本发明的方法步骤的程序代码
计算设备

图 15

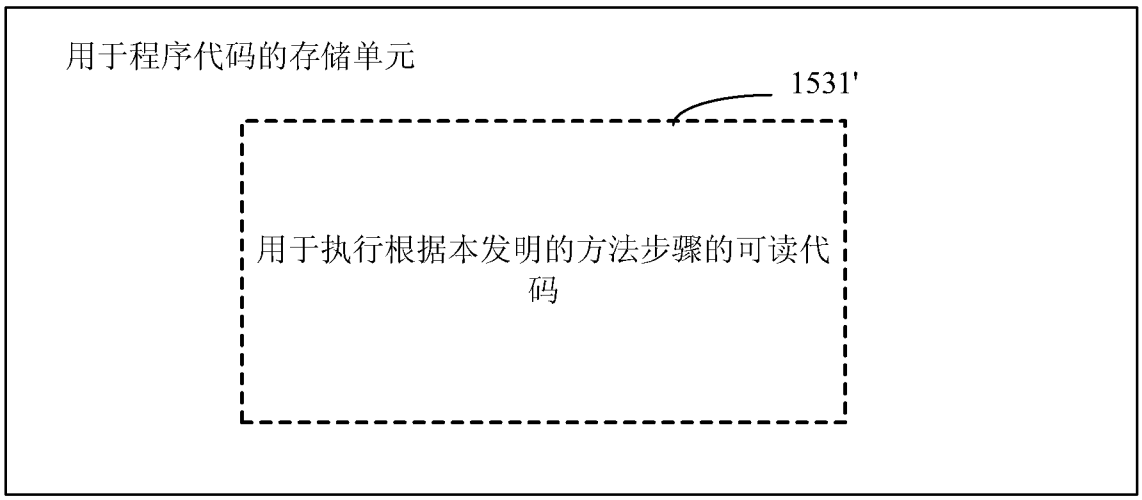

用于程序代码的存储单元
1531'
用于执行根据本发明的方法步骤的可读代码

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/094847

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/62 (2013.01) i; G06F 21/64 (2013.01) i; 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)

G06F H04L

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)

CNABS, SIPOABS, DWPI, CNKI: security, key, storage, memory, certificate, validate, identity, encrypt, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104573554 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 29 April 2015 (29.04.2015), the whole document	1-30
X	CN 102368773 A (TENDYRON CORPORATION), 07 March 2012 (07.03.2012), description, paragraphs 71-96	1, 15, 29, 30
A	CN 101848090 A (WUHAN LUOJIA NEW CENTURY INFORMATION CO., LTD.), 29 September 2010 (29.09.2010), the whole document	1-30

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2016 (14.02.2016)	**29 February 2016 (29.02.2016)**
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 **ZAHNG, Yan** Telephone No.: (86-10) **62089421**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/094847

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104573554 A	29 April 2015	None	
CN 102368773 A	07 March 2012	CN 102368773 B	09 April 2014
CN 101848090 A	29 September 2010	CN 101848090 B	25 July 2012

国际检索报告

国际申请号
PCT/CN2015/094847

A. 主题的分类

G06F 21/62(2013.01)i；G06F 21/64(2013.01)i；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)

G06F H04L

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））

CNABS，SIPOABS，DWPI，CNKI：安全，密钥，存储，证书，验证，身份，加密，认证，security， key， storage, memory, certificate, validate, identity, encrypt, authentication

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 104573554 A (北京奇虎科技有限公司等) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-30
X	CN 102368773 A (天地融科技股份有限公司) 2012年 3月 7日 (2012 - 03 - 07) 说明书第71-96段	1，15，29，30
A	CN 101848090 A (武汉珞珈新世纪信息有限公司) 2010年 9月 29日 (2010 - 09 - 29) 全文	1-30

☐ 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	国际检索报告邮寄日期
2016年 2月 14日	2016年 2月 29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) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张妍 电话号码 (86-10)62089421

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/094847

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	104573554	A	2015年 4月 29日	无			
CN	102368773	A	2012年 3月 7日	CN	102368773	B	2014年 4月 9日
CN	101848090	A	2010年 9月 29日	CN	101848090	B	2012年 7月 25日