

(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



(10) 国际公布号

WO 2020/233308 A1

(43) 国际公布日

2020 年 11 月 26 日 (26.11.2020)

WIPO | PCT

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
- (21) 国际申请号: PCT/CN2020/085577
- (22) 国际申请日: 2020 年 4 月 20 日 (20.04.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910430075.6 2019年5月22日 (22.05.2019) CN
- (71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。
- (72) 发明人: 陈步青 (CHEN, Buqing); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。
- (74) 代理人: 深圳众鼎专利商标代理事务所 (普通合伙) (SHENZHEN ZHONGDING INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区笋岗东路3012号中民时代广场B座7楼701室, Guangdong 518000 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) Title: SELF-CHECKING METHOD, APPARATUS AND DEVICE BASED ON LOCAL CERTIFICATE, AND STORAGE MEDIUM

(54) 发明名称: 基于本地证书的自校验方法、装置、设备及存储介质

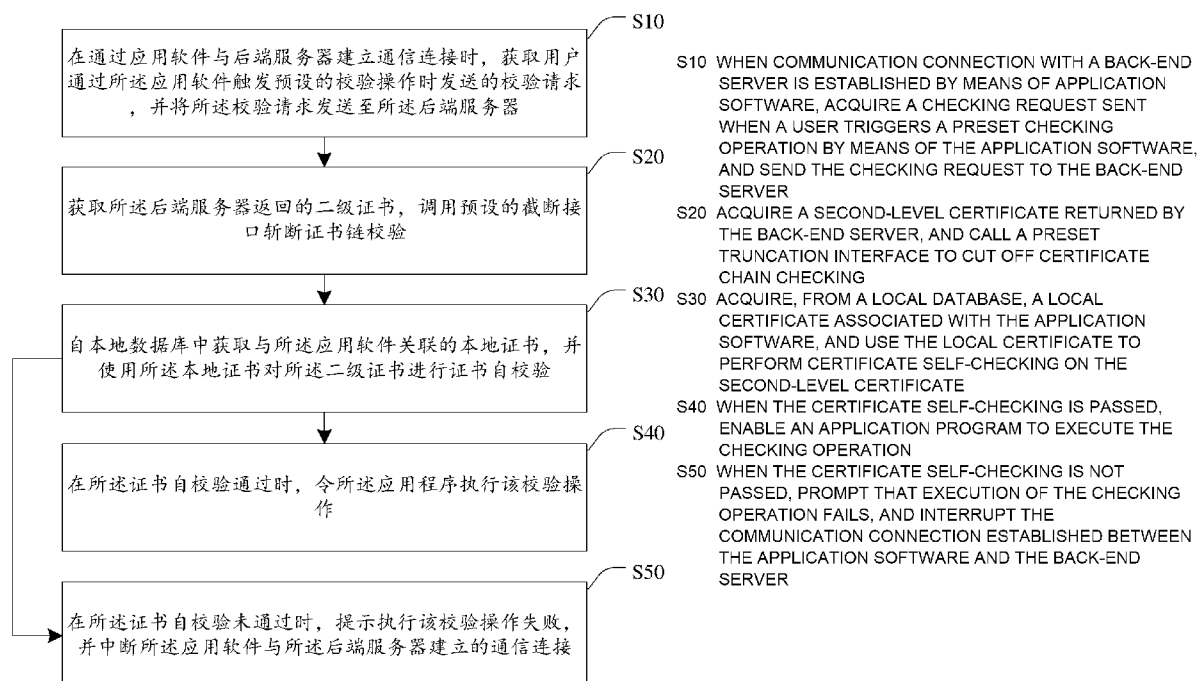


图 2

(57) Abstract: Provided are a self-checking method, apparatus and device based on a local certificate, and a storage medium. The method comprises: when communication connection with a back-end server is established by means of application software, acquiring a checking request sent when a user triggers a preset checking operation by means of the application software, and sending the checking request to the back-end server; acquiring a second-level certificate returned by the back-end server, and calling a preset truncation interface to cut off certificate chain checking; acquiring, from a local database, a local certificate associated with the application software,

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,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, 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, 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))。

and using the local certificate to perform certificate self-checking on the second-level certificate; when the certificate self-checking is passed, enabling an application program to execute the checking operation; and when the certificate self-checking is not passed, prompting that execution of the checking operation fails, and interrupting the communication connection established between the application software and the back-end server. According to the present application, communication security assurance of a higher level is provided for communication between application software and a back-end server.

(57) 摘要: 本申请公开了一种基于本地证书的自校验方法、装置、设备及存储介质。所述方法包括: 在通过应用软件与后端服务器建立通信连接时, 获取用户通过应用软件触发预设的校验操作时发送的校验请求, 并将所述校验请求发送至后端服务器; 获取后端服务器返回的二级证书, 调用预设的截断接口斩断证书链校验; 自本地数据库中获取与应用软件关联的本地证书, 并使用本地证书对二级证书进行证书自校验; 在证书自校验通过时, 令应用程序执行该校验操作; 在证书自校验未通过时, 提示执行该校验操作失败, 并中断应用软件与后端服务器建立的通信连接。本申请为应用软件与后端服务器之间的通信提供了更高级别的通信安全保障。

基于本地证书的自校验方法、装置、设备及存储介质

[0001] 本申请要求于2019年5月22日提交中国专利局、申请号为201910430075.6，发明名称为“基于本地证书的自校验方法、装置、设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及安全防护领域，具体涉及一种基于本地证书的自校验方法、装置、设备及存储介质。

[0003]

[0004] 背景技术

[0005] 目前，市面上的移动终端应用程序的HTTPS证书（Hyper Transfer Protocol Over Secure Socket Layer，以安全为目标的超文本传输协议）校验均使用标准的证书链校验方式，也即使用移动终端的操作系统预置的根证书进行验证。发明人意识到，目前的证书链校验方式在移动终端设备已存在安全隐患，原因在于目前很多钓鱼网站会引导用户在移动终端安装非法根证书，甚至有黑名单应用在移动客户端偷偷安装非法根证书，从而该移动终端的操作系统的HTTPS通信将如同虚设，该HTTPS通信可直接被钓鱼网站或者黑名单应用抓包并破解。

[0006] 基于此，有必要提供一种HTTPS证书校验方法，以保证高级别安全的HTTPS通信。

[0007]

[0008] 发明内容

[0009] 本申请实施例提供一种基于本地证书的自校验方法、装置、设备及存储介质，为应用程序与后端服务器之间的通信提供了更高级别的通信安全保障。

[0010] 一种基于本地证书的自校验方法，包括：

[0011] 在通过应用程序与后端服务器建立通信连接时，获取用户通过所述应用程序触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；

- [0012] 获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；
- [0013] 自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；
- [0014] 在所述证书自校验通过时，令所述应用程序执行该校验操作；
- [0015] 在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。
- [0016] 一种基于本地证书的自校验装置，包括：
- [0017] 发送模块，用于在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；
- [0018] 调用模块，用于获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；
- [0019] 自校验模块，用于自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；
- [0020] 执行模块，用于在所述证书自校验通过时，令所述应用程序执行该校验操作。
- [0021] 提示中断模块，用于在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。
- [0022] 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现上述基于本地证书的自校验方法。
- [0023] 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可读指令，所述计算机可读指令被处理器执行时实现上述基于本地证书的自校验方法。
- [0024] 本申请提供的基于本地证书的自校验方法、装置、设备及存储介质，在通过应用软件与后端服务器建立通信连接时，将针对用户在应用软件上触发校验操作生成的校验请求发送至所述后端服务器；而在获取所述后端服务器返回的二级证书之后，调用预设的截断接口斩断证书链校验，使得校验过程无需CA认证，也无需申请CA证书，省钱省事；进一步的，自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验，使

得第三方中间人无法攻击应用软件与后端服务器之间的通信过程，提供更高级别的通信安全保障。

[0025]

[0026] 附图说明

[0027] 图1是本申请一实施例中基于本地证书的自校验方法的应用环境示意图；

[0028] 图2是本申请一实施例中基于本地证书的自校验方法的流程图；

[0029] 图3是本申请一实施例中基于本地证书的自校验方法的流程图；

[0030] 图4是本申请一实施例中基于本地证书的自校验方法的步骤S30的流程图；

[0031] 图5是本申请一实施例中基于本地证书的自校验装置的原理框图；

[0032] 图6是本申请另一实施例中基于本地证书的自校验装置的原理框图；

[0033] 图7是本申请一实施例中基于本地证书的自校验装置的分配模块的原理框图；

[0034] 图8是本申请一实施例中计算机设备的示意图。

[0035]

[0036] 具体实施方式

[0037] 本申请提供的基于本地证书的自校验方法，可应用在如图1的应用环境中，其中，客户端通过网络与服务器进行通信。其中，客户端包括但不限于为各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备。服务器可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

[0038] 在一实施例中，如图2所示，提供一种基于本地证书的自校验方法，以该方法应用在图1中的服务器为例进行说明，包括以下步骤：

[0039] S10，在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器。

[0040] 其中，所述应用软件（也称APP）是指用户可以使用的各种程序设计语言，以及用各种程序语言编制的应用程序的集合，分为应用软件包和用户程序；所述应用软件包是指预先编制好的、能完成一定功能的、供出售或出租的成套软件系统，所述应用软件包可以小到只有一项功能（例如，打印邮签），也可以是具有复杂功能、运行在主机上的大系统；所述用户程序是指为满足用户不同领

域、不同问题的应用需求而提供的那部分软件，例如，游戏小程序。

[0041] 所述后端服务器可以通过安装在客户端上的浏览器（即某一客户端上的应用软件）访问的网页，且该后端服务器区别于本地服务器；可理解的，一个所述本地服务器对应于一个客户端。

[0042] 所述校验请求是指用户通过客户端的应用软件触发预设的校验操作生成的，而在与该客户端通信连接的本地服务器接收到该校验请求时，将该校验请求发送至后端服务器；每个所述校验操作对应一个功能按钮，例如，登录操作，转账操作。

[0043] 在本实施例中，在客户端的应用软件与后端服务器建立HTTPS（以安全为目标的超文本传输协议）通信连接时，在用户触发所述应用软件上的功能按钮时，将针对校验操作生成的校验请求发送至后端服务器，此时，本地服务器将等待后端服务器响应所述校验请求之后发送其二级证书。作为优选，所述二级证书为应用软件的发布方向CA机构（Certificate Authority，证书授权机构）申请的HTTPS证书。

[0044] 可理解的，应用软件的发布方向CA机构发送包含发布方信息的证书申请之后，接收CA机构根据所述发布方信息从CA根证书派生的二级证书，并将所述二级证书配置到后端服务器中，同时开发应用软件给用户使用。其中，所述发布方信息包含发布方组织、域名等信息；所述二级证书包含证书公钥、证书序列号、证书授权中心的数字签名和证书有效时间等。

[0045] S20，获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验。

[0046] 其中，所述截断接口是由编程语言提供的应用程序接口。

[0047] 所述证书链式校验是指使用客户端操作系统预置的CA根证书对二级证书进行校验。作为优选，所述CA根证书存放在可信证书列表中，若客户端在访问钓鱼网站或者安装黑名单应用软件时安装了第三方中间人的非法根证书，则所述可信证书列表中还包含第三方中间人的非法根证书。

[0048] 在本实施例中，在后端服务器接收到针对用户通过客户端的应用软件触发校验操作时发送的校验请求时，该后端服务器响应该校验请求，并将存储在后端服

务器上的二级证书返回至本地服务器；而本地服务器在获取到后端服务器返回的二级证书之后，获取客户端操作系统中预置的截断接口，令该截断接口斩断证书链式校验。作为优选，在等待所述后端服务器返回二级证书时，获取等待时长，并检测所述等待时长是否超过预设时长阈值；在所述等待时长超过（大于）预设时长阈值时，提示用户发送请求失败；而在所述等待时长未超过（等于或小于）预设时长阈值时，提示用户正在校验过程中。其中，所述等待时长是指发送所述校验请求的时间与当前时间的差值。

[0049] S30，自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验。

[0050] 作为优选，根据应用软件的唯一标识自本地数据库中获取与所述应用软件关联的本地证书，使用与所述应用软件关联的本地证书对所述步骤S20中后端服务器返回的二级证书进行自校验，以验证所述二级证书的合法性，避免通信的安全隐患问题。其中，所述本地证书是在用户在客户端安装所述发布方发布的应用软件时，将经过加固之后的所述二级证书作为本地证书存储在本地数据库中。

[0051] 可理解的，中间人窃取HTTPS通信过程中的加密信息需要达到三个条件：必须在客户端操作系统预先安装非法根证书；必须在HTTPS握手过程中下发中间人二级证书；客户端的应用软件走的是系统校验。而本实施例中，所述应用软件无需请求向客户端操作系统发送用于验证二级证书合法性的系统校验请求，而是直接采用应用软件内部的本地证书对返回的服务端证书进行校验，使得客户端操作系统安装了第三方中间人的非法根证书，并在第三方中间人攻击了HTTPS握手过程返回的二级证书，依然无法通过校验。

[0052] S40，在所述证书自校验通过时，令所述应用程序执行该校验操作。

[0053] 也即，在所述证书自校验通过时，可以将与该校验操作关联的操作页面显示在客户端，例如，移动终端。

[0054] S50，在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。

[0055] 在所述二级证书检验未通过时，提示当前的校验操作为异常操作，并强行断开与后端服务器的通信连接，而在所述应用软件与所述后端服务器重新建立通信

连接之后，所述用户针可以再次触发与所述校验操作对应的功能按钮，向后端服务器重新发送校验请求。

[0056] 综上所述，本申请提供的基于本地证书的自校验方法，在获取所述后端服务器返回的二级证书之后，调用预设的截断接口斩断证书链校验，自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验。若所述证书自校验通过，则执行该校验操作；若所述证书自校验未通过，则中断所述应用软件与所述后端服务器之间的通信连接，使得自校验过程无需CA认证，也无需申请CA证书，省钱省事；同时使得第三方中间人无法攻击应用软件与后端服务器之间的通信过程，提供更高级别的通信安全保障。

[0057] 在另一实施例中，如图3所示，为了提升用户体验，便于用户操作客户端的应用软件，可以在不中断该应用软件与后端服务器建立的通信连接情况下，根据用户触发的选择按钮令应用软件执行与该选择按钮关联的操作。此时，所述步骤S30之后包括以下步骤：

[0058] S50，在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，并根据预设显示模式将包含安全警告信息的预设窗口显示在客户端。

[0059] 其中，所述显示模式包括弹窗模式或重新加载转入模式等。

[0060] 所述预设窗口包含多个选择按钮；所述选择按钮是指除与所述校验操作对应的功能按钮之外的非校验按钮；例如，取消按钮，继续按钮，返回按钮等。

[0061] 可理解的，在所述证书自校验未通过时，不中断所述应用软件与所述后端服务器的通信连接。示例性的，用户在移动终端的银行系统执行转账操作，若所述证书自校验失败，弹窗显示一条“转账异常”的信息以供用户重新执行该转账操作，避免转账请求被劫持，转账账号被篡改为攻击者的账号。

[0062] S60，根据所述用户在所述预设窗口触发的选择按钮令所述应用程序执行与所述选择按钮关联的操作。

[0063] 示例性的，在所述用户触发预设窗口上的返回按钮时，继续所述应用软件与所述后端服务器之间的通信连接；

- [0064] 在所述用户触发预设窗口上的取消按钮时，结束所述客户端应用与所述服务端应用之间的通信连接。
- [0065] 在一实施例中，在所述证书自校验未通过时，若所述应用软件与所述后端服务器仍在通信连接，为了减小安全隐患，令所述后端服务器不响应用户针对所述校验操作重新发送的所述校验请求；此时，所述步骤S30之后包括以下步骤：
- [0066] 在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，若针对用户通过所述应用软件触发所述校验操作重新向所述后端服务器发送所述校验请求，则令所述应用软件拒绝执行所述校验操作。
- [0067] 作为优选，将校验未通过的记录信息暂存至本地数据库中的缓存区域，在所述应用软件与所述后端服务器未重新建立通信连接之前，不删除所述缓存区域中的记录信息，此时，在针对用户通过所述应用软件触发所述校验操作重新向后端服务器发送所述校验请求时，根据所述缓存区域中的记录信息直接驳回所述校验请求，且可以提示用户中断通信连接之后再返回该应用软件。
- [0068] 在一实施例中，为了避免中间人攻击，提高所述应用软件与后端服务器之间的通信安全，可以对所述应用软件的本地证书进行加固；此时，所述步骤S10之前，具体包括以下步骤：
- [0069] 接收所述应用软件的安装指令，获取并安装从软件发布方下载在所述本地数据库中的所述应用软件；其中，所述应用软件中包含所述本地证书；所述本地证书在所述软件发布方发布时已被预置在所述应用软件的二进制代码中，并已通过预设的加固工具进行加固。
- [0070] 可理解的，客户端上的应用软件为了防止第三方中间人攻击（即中间人窃取HTTPS通信过程中的加密信息），可以将本地证书打包进应用软件中，后续在收到后端服务器的二级证书时，能够有效地验证后端服务器是否可信，加密信息是否被第三方中间人窃取。
- [0071] 具体的，接收用户自客户端发送的包含应用软件名称的安装指令，从本地数据库中获取与所述应用软件名称匹配的应用软件、安装该应用软件所需的本地证书以及加固工具的调用接口，自动安装由发布方发布的该应用软件，并在安装该应用软件过程中时，将该本地证书预置在安装好的所述应用软件的二进制代

码，并通过加固工具的调用接口调用加固工具对所述本地证书进行加固，进一步保障通信连接的安全性。

[0072] 综上所述，本申请提供的基于本地证书的自校验方法，在发布方发布的应用软件时，已将证书预置到应用软件的二进制代码中并进行加固，使得应用软件与后端服务器建立通信连接时，达到了更高的安全级别，加密信息破解难度高。

[0073] 在一实施例中，如图4所示，所述步骤S30，即所述自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验，包括以下步骤：

[0074] S301，在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥。

[0075] 可理解的，所述证书链式校验是在客户端操作系统安装现有CA机构颁发的CA根证书，并对所述根证书无条件信息，后续应用软件的发布方向所述CA机构申请HTTPS证书，并接收所述CA机构会根据本身的根证书以及发布方信息生成二级证书，该二级证书由后端服务器返回；若本地服务器获取到由后端服务器返回该二级证书，则请求客户端操作系统校验该二级证书的合法性，此时，客户端操作系统会使用现有的CA根证书对二级证书进行校验，并将校验结果返回给本地服务器。

[0076] 而在本实施例中，本地服务器在获取到后端服务器返回的二级证书之后，获取客户端操作系统中预置的截断接口，令该截断接口斩断证书链式校验，在本地服务器检测到向客户端操作系统发送系统校验请求失败时，确定斩断了证书链式校验，并发出系统校验失败的提示，此时，自动运行自校验，也即获取内置在本地数据库中与所述应用程序关联的本地证书的本地公钥，并在所述步骤S202获取所述二级证书的待校验公钥之后，根据所述本地证书的本地公钥和所述二级证书的待校验公钥在应用软件内部进行自校验。

[0077] S302，对获取到的所述二级证书进行解析之后，获取所述二级证书的待校验公钥，并检测所述本地公钥与所述待校验公钥是否一致。

[0078] S303，在所述本地公钥与所述待校验公钥一致时，确定所述证书自校验通过。

[0079] S304，在所述本地公钥与所述待校验公钥不一致时，确定所述证书自校验未通

过。

[0080] 在本实施例中，所述二级证书中包含后端服务器的地址标识（域名或者统一资源定位符）、证书序列号、证书颁发者名称、证书公钥（即待校验公钥）等。

[0081] 具体的，对二级证书进行解析之后，获取该二级证书的待校验公钥，使用数据库中与所述应用软件关联的本地证书的本地公钥对该二级证书的待校验公钥进行公钥验证（自校验方式之一），以验证所述待校验公钥与所述本地公钥是否一致。在所述本地公钥与所述待校验公钥一致时，确定该二级证书为合法证书且校验通过；而在所述本地公钥与所述待校验公钥不一致时，确定该二级证书为非法证书且校验未通过。

[0082] 在另一实施例中，所述步骤S301之后还包括以下步骤：

[0083] 对获取到的所述二级证书进行解析之后，获取所述二级证书的地址标识和待校验公钥，调用预设的地址检测接口对所述二级证书的所述地址标识进行地址校验，且使用所述本地公钥对所述二级证书的所述待校验公钥进行公钥校验。

[0084] 其中，所述地址检测接口是由编程语言提供的应用程序接口。

[0085] 在本实施例中，对二级证书进行解析之后，获取所述二级证书的地址标识（域名或者统一资源定位符）和待校验公钥，调用客户端操作系统中预置的地址检测接口对所述地址标识进行地址校验，以验证该地址标识的有效性以及合法性；同时使用所述本地公钥对所述待校验公钥进行公钥验证，以验证所述待校验公钥与所述本地公钥是否一致。在所述地址标识为有效合法地址，且所述本地公钥与所述待校验公钥一致时，确定该二级证书为合法证书且校验通过；而在所述地址标识为无效非法地址，或所述本地公钥与所述待校验公钥不一致时，确定该二级证书为非法证书且校验未通过。

[0086] 示例性的，用户使用客户端上的浏览器访问域名1的网站A，由于网站域名被第三方中间人劫持，会将用户带到域名2的伪造网站B；若伪造网站B的证书是非CA机构颁发的伪造二级证书，则浏览器会提示当前网站的证书不可信；而若伪造网站B的证书是CA机构颁发的二级证书，在不做地址校验的情况下，客户端上的浏览器可能不会有任何的警告。

[0087] 在一实施例中，如图5所示，提供一种基于本地证书的自校验装置，该基于本

地证书的自校验装置与上述实施例中基于本地证书的自校验方法一一对应。该基于本地证书的自校验装置包括发送模块110、调用模块120、自校验模块130、执行模块140和提示中断模块150。各功能模块详细说明如下：

[0088] 发送模块110，用于在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器。

[0089] 调用模块120，用于获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验。

[0090] 自校验模块130，用于自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验。

[0091] 执行模块140，用于在所述证书自校验通过时，令所述应用程序执行该校验操作。

[0092] 提示中断模块150，用于在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。

[0093] 在另一实施例中，如图6所示，基于本地证书的自校验装置还包括显示模块60和选择模块70，各功能模块详细说明如下：

[0094] 显示模块60，用于在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，并根据预设显示模式将包含安全警告信息的预设窗口显示在客户端。

[0095] 选择模块70，用于根据所述用户在所述预设窗口触发的选择按钮令所述应用程序执行与所述选择按钮关联的操作。

[0096] 在另一实施例中，基于本地证书的自校验装置还包括安装模块，该功能模块详细说明如下：

[0097] 安装模块，用于接收所述应用软件的安装指令，获取并安装从软件发布方下载在所述本地数据库中的所述应用软件；其中，所述应用软件中包含所述本地证书；所述本地证书在所述软件发布方发布时已被预置在所述应用软件的二进制代码中，并已通过预设的加固工具进行加固。

[0098] 在一实施例中，如图7所示，所述自校验模块130包括以下子模块，各功能子模

块详细说明如下：

- [0099] 获取子模块131，用于在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥。
- [0100] 检测子模块132，用于对获取到的所述二级证书进行解析之后，获取所述二级证书的待校验公钥，并检测所述本地公钥与所述待校验公钥是否一致。
- [0101] 第一结果子模块133，用于在所述本地公钥与所述待校验公钥一致时，确定所述证书自校验通过。
- [0102] 第二结果子模块134，用于在所述本地公钥与所述待校验公钥不一致时，确定所述证书自校验未通过。
- [0103] 在另一实施例中，所述自校验模块130还包括以下子模块，各功能子模块详细说明如下：
- [0104] 双重校验模块，用于对获取到的所述二级证书进行解析之后，获取所述二级证书的地址标识和待校验公钥，调用预设的地址检测接口对所述二级证书的所述地址标识进行地址校验，且使用所述本地公钥对所述二级证书的所述待校验公钥进行公钥校验。
- [0105] 关于基于本地证书的自校验装置的具体限定可以参见上文中对于基于本地证书的自校验方法的限定，在此不再赘述。上述基于本地证书的自校验装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。
- [0106] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图8所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机可读指令和数据库。该内存储器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机可读指令被处理器执行时以实现一种基于本地证书的自校验方法。
- [0107] 在一个实施例中，提供了一种计算机设备，包括存储器、处理器及存储在存储器

器上并可在处理器上运行的计算机可读指令，处理器执行计算机可读指令时实现以下步骤：

- [0108] 在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；
- [0109] 获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；
- [0110] 自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；
- [0111] 在所述证书自校验通过时，令所述应用程序执行该校验操作；
- [0112] 在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。
- [0113] 在一个实施例中，提供了一种计算机可读存储介质，计算机可读存储介质可以是非易失性，也可以是易失性，其上存储有计算机可读指令，计算机可读指令被处理器执行时实现以下步骤：
 - [0114] 在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；
 - [0115] 获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；
 - [0116] 自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；
 - [0117] 在所述证书自校验通过时，令所述应用程序执行该校验操作；
 - [0118] 在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。
- [0119] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失

性存储器。非易失性存储器可包括只读存储器（ROM）、可编程ROM（PROM）、电可编程ROM（EPROM）、电可擦除可编程ROM（EEPROM）或闪存。易失性存储器可包括随机存取存储器（RAM）或者外部高速缓冲存储器。作为说明而非局限，RAM以多种形式可得，诸如静态RAM（SRAM）、动态RAM（DRAM）、同步DRAM（SDRAM）、双数据率SDRAM（DDRSDRAM）、增强型SDRAM（ESDRAM）、同步链路DRAM（SLDRAM）、存储器总线直接RAM（RDRAM）、直接存储器总线动态RAM（DRDRAM）、以及存储器总线动态RAM（RDRAM）等。

[0120] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元或模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元或模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。

[0121] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。。

发明概述

技术问题

问题的解决方案

发明的有益效果

权利要求书

- [权利要求 1] 一种基于本地证书的自校验方法，其中，包括：
- 在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；
- 获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；
- 自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；
- 在所述证书自校验通过时，令所述应用程序执行该校验操作；
- 在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。
- [权利要求 2] 如权利要求1所述的基于本地证书的自校验方法，所述自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行比对校验，包括：
- 在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥；
- 对获取到的所述二级证书进行解析之后，获取所述二级证书的待校验公钥，并检测所述本地公钥与所述待校验公钥是否一致；
- 在所述本地公钥与所述待校验公钥一致时，确定所述证书自校验通过；
- 在所述本地公钥与所述待校验公钥不一致时，确定所述证书自校验未通过。
- [权利要求 3] 如权利要求2所述的基于本地证书的自校验方法，所述在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥之后，包括：
- 对获取到的所述二级证书进行解析之后，获取所述二级证书的地址标识和待校验公钥，调用预设的地址检测接口对所述二级证书的所述地

址标识进行地址校验，且使用所述本地公钥对所述二级证书的所述待校验公钥进行公钥校验。

[权利要求 4]

如权利要求1所述的基于本地证书的自校验方法，所述自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验之后，包括：

在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，并根据预设显示模式将包含安全警告信息的预设窗口显示在客户端；

根据所述用户在所述预设窗口触发的选择按钮令所述应用程序执行与所述选择按钮关联的操作。

[权利要求 5]

如权利要求1所述的基于本地证书的自校验方法，所述在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器之前，包括：

接收所述应用软件的安装指令，获取并安装从软件发布方下载在所述本地数据库中的所述应用软件；其中，所述应用软件中包含所述本地证书；所述本地证书在所述软件发布方发布时已被预置在所述应用软件的二进制代码中，并已通过预设的加固工具进行加固。

[权利要求 6]

一种基于本地证书的自校验装置，包括：

发送模块，用于在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；

调用模块，用于获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；

自校验模块，用于自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；

执行模块，用于在所述证书自校验通过时，令所述应用程序执行该校验操作；

提示中断模块，用于在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。

[权利要求 7]

如权利要求6所述的基于本地证书的自校验装置，所述自校验模块，包括：

获取子模块，用于在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥；

检测子模块，用于对获取到的所述二级证书进行解析之后，获取所述二级证书的待校验公钥，并检测所述本地公钥与所述待校验公钥是否一致；

第一结果子模块，用于在所述本地公钥与所述待校验公钥一致时，确定所述证书自校验通过；

第二结果子模块，用于在所述本地公钥与所述待校验公钥不一致时，确定所述证书自校验未通过。

[权利要求 8]

如权利要求6所述的基于本地证书的自校验装置，所述装置还包括：

显示模块，用于在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，并根据预设显示模式将包含安全警告信息的预设窗口显示在客户端；

选择模块，用于根据所述用户在所述预设窗口触发的选择按钮令所述应用程序执行与所述选择按钮关联的操作。

[权利要求 9]

如权利要求6所述的基于本地证书的自校验装置，还包括：

双重校验模块，用于对获取到的所述二级证书进行解析之后，获取所述二级证书的地址标识和待校验公钥，调用预设的地址检测接口对所述二级证书的所述地址标识进行地址校验，且使用所述本地公钥对所述二级证书的所述待校验公钥进行公钥校验。

[权利要求 10]

如权利要求6所述的基于本地证书的自校验装置，还包括：

安装模块，用于接收所述应用软件的安装指令，获取并安装从软件发布方下载在所述本地数据库中的所述应用软件；其中，所述应用软件中包含所述本地证书；所述本地证书在所述软件发布方发布时已被预

置在所述应用程序的二进制代码中，并已通过预设的加固工具进行加固。

[权利要求 11] 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现基于本地证书的自校验方法；
其中，所述基于本地证书的自校验方法包括：
在通过应用程序与后端服务器建立通信连接时，获取用户通过所述应用程序触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；
获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；
自本地数据库中获取与所述应用程序关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；
在所述证书自校验通过时，令所述应用程序执行该校验操作；
在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用程序与所述后端服务器建立的通信连接。

[权利要求 12] 如权利要求11所述的计算机设备，所述自本地数据库中获取与所述应用程序关联的本地证书，并使用所述本地证书对所述二级证书进行比对校验，包括：
在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥；
对获取到的所述二级证书进行解析之后，获取所述二级证书的待校验公钥，并检测所述本地公钥与所述待校验公钥是否一致；
在所述本地公钥与所述待校验公钥一致时，确定所述证书自校验通过；
在所述本地公钥与所述待校验公钥不一致时，确定所述证书自校验未通过。

[权利要求 13] 如权利要求11所述的计算机设备，所述在确认已经斩断所述证书链校

验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥之后，包括：

对获取到的所述二级证书进行解析之后，获取所述二级证书的地址标识和待校验公钥，调用预设的地址检测接口对所述二级证书的所述地址标识进行地址校验，且使用所述本地公钥对所述二级证书的所述待校验公钥进行公钥校验。

[权利要求 14] 如权利要求11所述的基于本地证书的计算机设备，所述自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验之后，包括：

在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，并根据预设显示模式将包含安全警告信息的预设窗口显示在客户端；

根据所述用户在所述预设窗口触发的选择按钮令所述应用程序执行与所述选择按钮关联的操作。

[权利要求 15] 如权利要求11所述的计算机设备，所述在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器之前，包括：

接收所述应用软件的安装指令，获取并安装从软件发布方下载在所述本地数据库中的所述应用软件；其中，所述应用软件中包含所述本地证书；所述本地证书在所述软件发布方发布时已被预置在所述应用软件的二进制代码中，并已通过预设的加固工具进行加固。

[权利要求 16] 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可读指令，所述计算机可读指令被处理器执行时实现基于本地证书的自校验方法，其中，所述基于本地证书的自校验方法包括如下步骤：
在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器；

获取所述后端服务器返回的二级证书，调用预设的截断接口斩断证书链校验；

自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验；

在所述证书自校验通过时，令所述应用程序执行该校验操作；

在所述证书自校验未通过时，提示执行该校验操作失败，并中断所述应用软件与所述后端服务器建立的通信连接。

[权利要求 17] 如权利要求16所述的计算机可读存储介质，所述自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行比对校验，包括：

在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥；

对获取到的所述二级证书进行解析之后，获取所述二级证书的待校验公钥，并检测所述本地公钥与所述待校验公钥是否一致；

在所述本地公钥与所述待校验公钥一致时，确定所述证书自校验通过；

在所述本地公钥与所述待校验公钥不一致时，确定所述证书自校验未通过。

[权利要求 18] 如权利要求17所述的计算机可读存储介质，所述在确认已经斩断所述证书链校验之后，获取内置在所述本地数据库中与所述应用程序关联的本地证书的本地公钥之后，包括：

对获取到的所述二级证书进行解析之后，获取所述二级证书的地址标识和待校验公钥，调用预设的地址检测接口对所述二级证书的所述地址标识进行地址校验，且使用所述本地公钥对所述二级证书的所述待校验公钥进行公钥校验。

[权利要求 19] 如权利要求16所述的计算机可读存储介质，所述自本地数据库中获取与所述应用软件关联的本地证书，并使用所述本地证书对所述二级证书进行证书自校验之后，包括：

在所述证书自校验未通过时，继续保持所述应用软件与所述后端服务器建立的通信连接，并根据预设显示模式将包含安全警告信息的预设窗口显示在客户端；

根据所述用户在所述预设窗口触发的选择按钮令所述应用程序执行与所述选择按钮关联的操作。

[权利要求 20] 如权利要求16所述的计算机可读存储介质，所述在通过应用软件与后端服务器建立通信连接时，获取用户通过所述应用软件触发预设的校验操作时发送的校验请求，并将所述校验请求发送至所述后端服务器之前，包括：

接收所述应用软件的安装指令，获取并安装从软件发布方下载在所述本地数据库中的所述应用软件；其中，所述应用软件中包含所述本地证书；所述本地证书在所述软件发布方发布时已被预置在所述应用软件的二进制代码中，并已通过预设的加固工具进行加固。

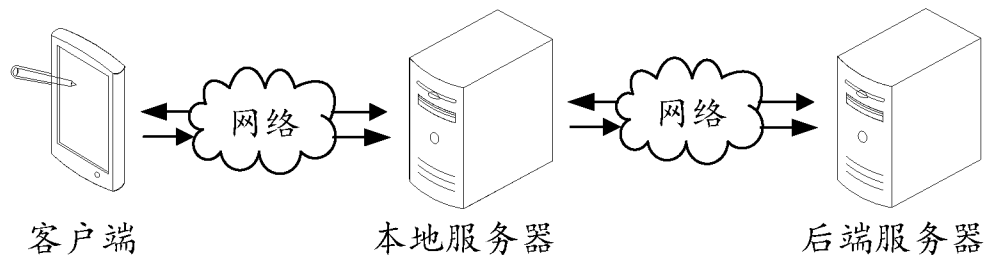


图 1

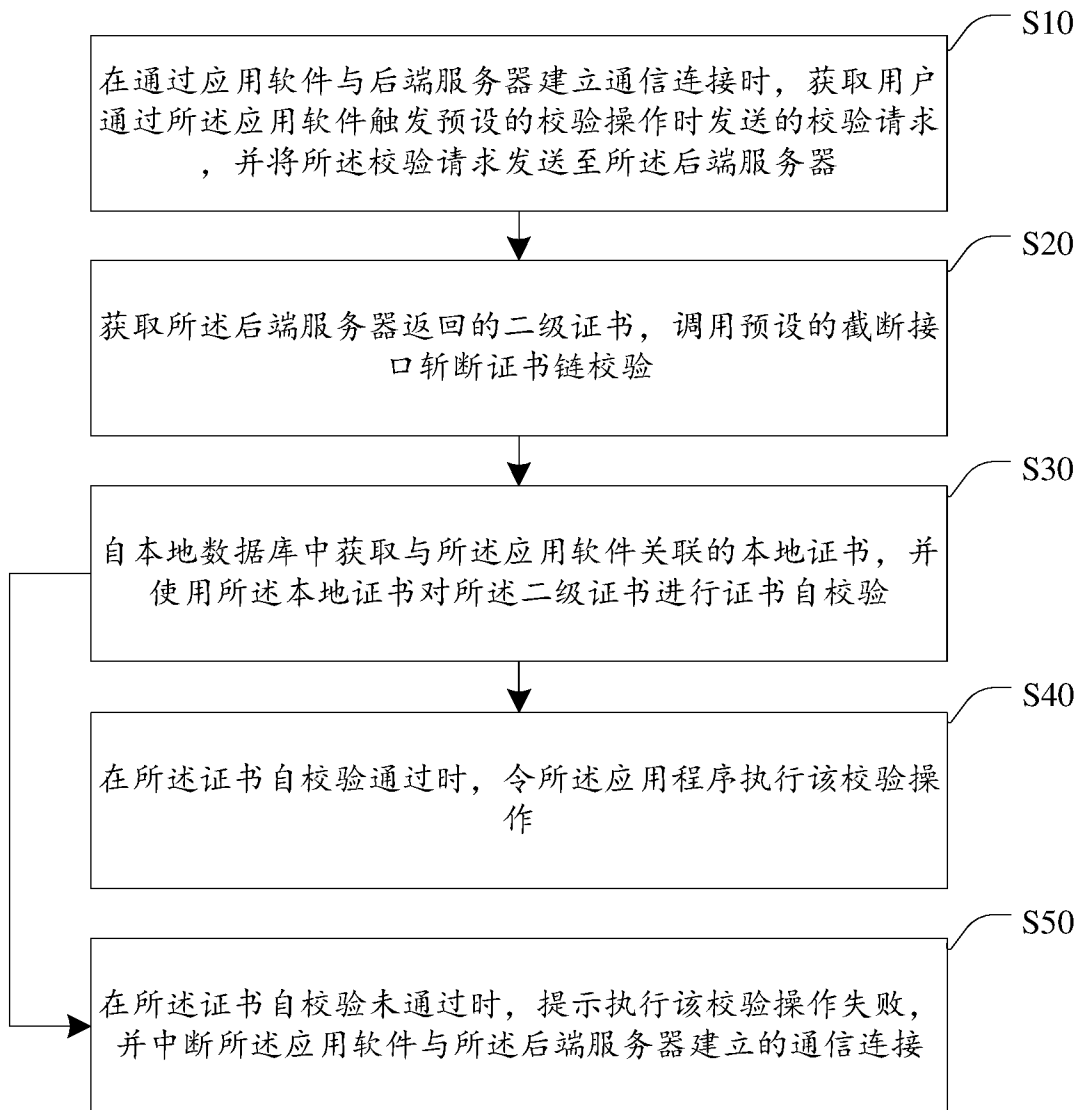


图 2

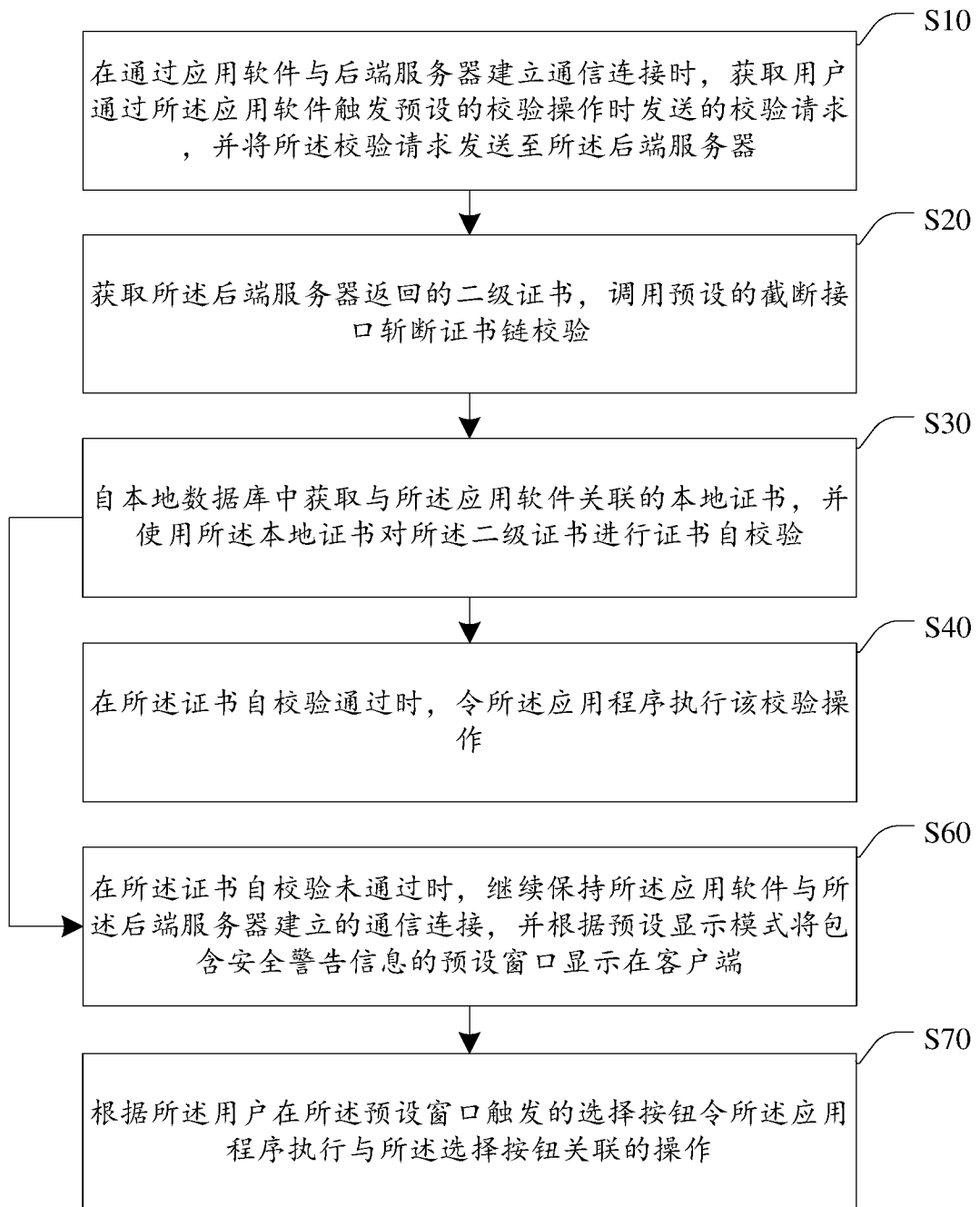


图 3

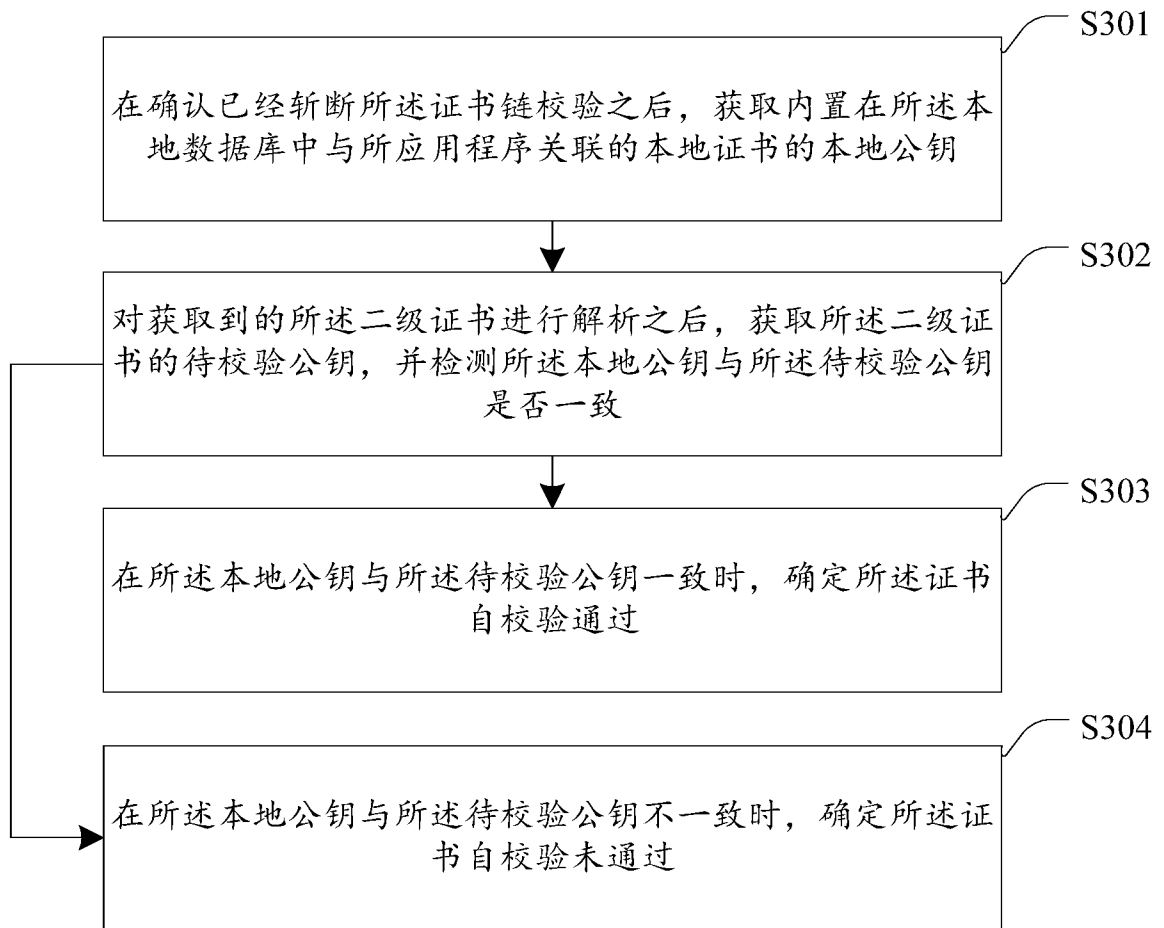


图 4

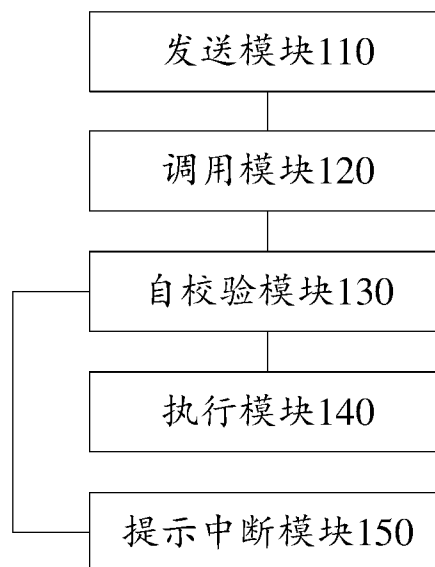


图 5

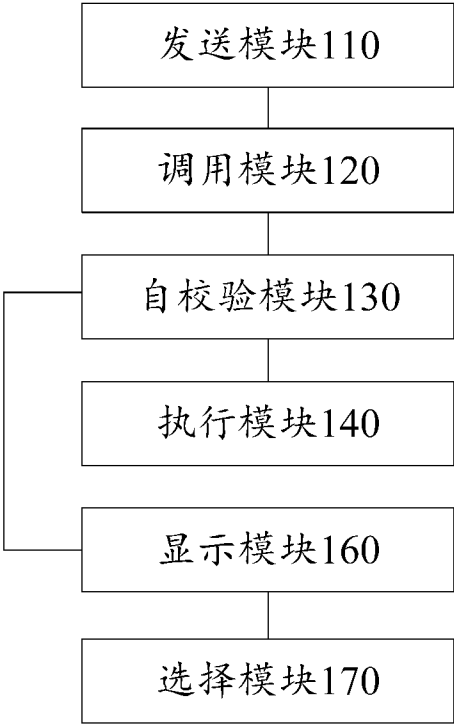


图 6

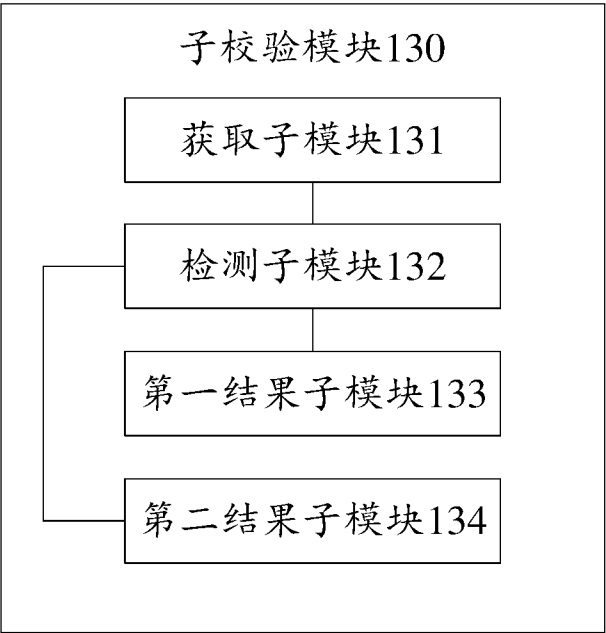


图 7

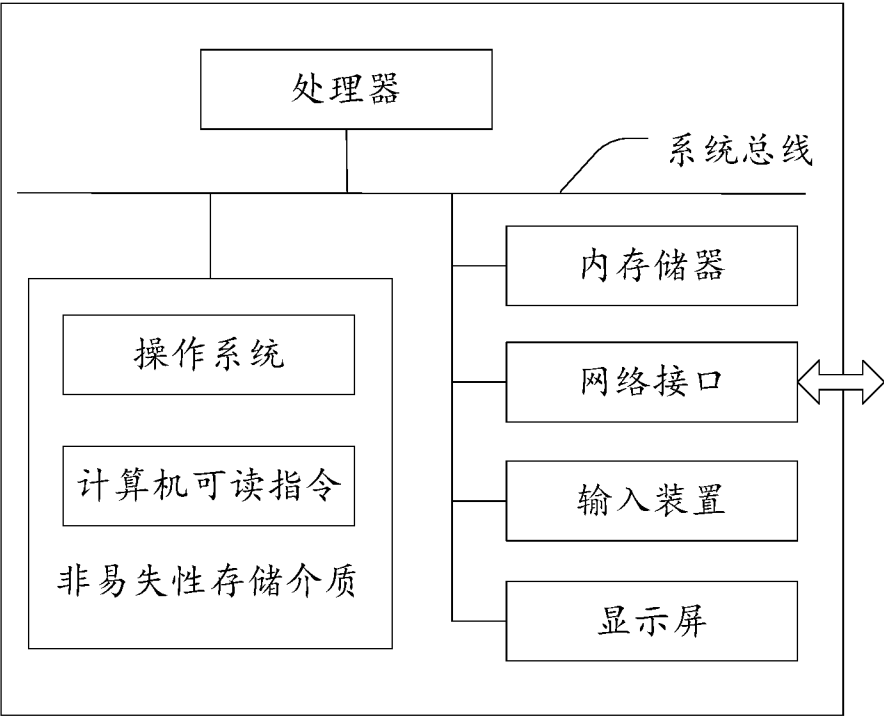


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/085577

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 29/08(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; G06Q; G06F

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; IEEE: HTTPS, 证书链, 根证书, 本地, 证书, 校验, 验证, 接口, 请求, 返回, 服务器, 应用, 斩断, 切断, 截断, certificate, verify, check, preset, root, local, link, chain, interface, request, server, app, cut off

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110300096 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 01 October 2019 (2019-10-01) claims 1-10	1-20
X	US 2018302787 A1 (SYNCHRONOSS TECHNOLOGIES INC.) 18 October 2018 (2018-10-18) description paragraphs [0023]-[0055], [0062]-[0073], figures 1-5	1-20
X	CN 109359977 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 19 February 2019 (2019-02-19) description, paragraphs [0041]-[0070]	1-20
A	CN 107819584 A (HANGZHOU DPTECH TECHNOLOGIES CO., LTD.) 20 March 2018 (2018-03-20) entire document	1-20
A	CN 108989039 A (ZTE CORPORATION) 11 December 2018 (2018-12-11) entire document	1-20
A	US 2019087639 A1 (CRANE, Darien) 21 March 2019 (2019-03-21) entire document	1-20

☐ 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

07 July 2020

Date of mailing of the international search report

21 July 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/085577

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	110300096	A	01 October 2019	None		
US	2018302787	A1	18 October 2018	None		
CN	109359977	A	19 February 2019	None		
CN	107819584	A	20 March 2018	None		
CN	108989039	A	11 December 2018	WO	2018219009	A1 06 December 2018
US	2019087639	A1	21 March 2019	None		

国际检索报告

国际申请号

PCT/CN2020/085577

A. 主题的分类

H04L 29/06 (2006.01) i; H04L 29/08 (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; G06Q; G06F

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; EPDOC; IEEE; HTTPS, 证书链, 根证书, 本地, 证书, 校验, 验证, 接口, 请求, 返回, 服务器, 应用, 斩断, 切断, 截断, certificate, verify, check, preset, root, local, link, chain, interface, request, server, app, cut off

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 110300096 A (深圳壹账通智能科技有限公司) 2019年 10月 1日 (2019 - 10 - 01) 权利要求1-10	1-20
X	US 2018302787 A1 (SYNCHRONOSS TECHNOLOGIES INC.) 2018年 10月 18日 (2018 - 10 - 18) 说明书第[0023]-[0055]、[0062]-[0073]段, 附图1-5	1-20
X	CN 109359977 A (平安科技深圳有限公司) 2019年 2月 19日 (2019 - 02 - 19) 说明书第[0041]-[0070]段	1-20
A	CN 107819584 A (杭州迪普科技股份有限公司) 2018年 3月 20日 (2018 - 03 - 20) 全文	1-20
A	CN 108989039 A (中兴通讯股份有限公司) 2018年 12月 11日 (2018 - 12 - 11) 全文	1-20
A	US 2019087639 A1 (CRANE, Darien) 2019年 3月 21日 (2019 - 03 - 21) 全文	1-20

☐ 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

2020年 7月 7日

国际检索报告邮寄日期

2020年 7月 21日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (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

向琳

电话号码 86-10-53961566

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/085577

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	110300096	A	2019年 10月 1日	无	
US	2018302787	A1	2018年 10月 18日	无	
CN	109359977	A	2019年 2月 19日	无	
CN	107819584	A	2018年 3月 20日	无	
CN	108989039	A	2018年 12月 11日	W0 2018219009 A1	2018年 12月 6日
US	2019087639	A1	2019年 3月 21日	无	