(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113328980 B
(45)授权公告日 2022.05.17

(21)申请号 202010132641.8
(22)申请日 2020.02.29
(65)同一申请的已公布的文献号
申请公布号 CN 113328980 A
(43)申请公布日 2021.08.31
(73)专利权人 杭州迪普科技股份有限公司
地址 310051 浙江省杭州市滨江区通和路68号中财大厦6楼
(72)发明人 李绍辉
(74)专利代理机构 北京金讯知识产权代理事务所(特殊普通合伙) 11554
专利代理师 黄剑飞
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/02(2022.01)
H04L 67/14(2022.01)
H04L 69/163(2022.01)
(56)对比文件
CN 110519304 A,2019.11.29
CN 104954315 A,2015.09.30
CN 106533689 A,2017.03.22
CN 102763395 A,2012.10.31
CN 109088889 A,2018.12.25
US 2019306166 A1,2019.10.03
US 2017223054 A1,2017.08.03
US 2020021659 A1,2020.01.16
CN 104580172 A,2015.04.29
审查员 肖云鹏

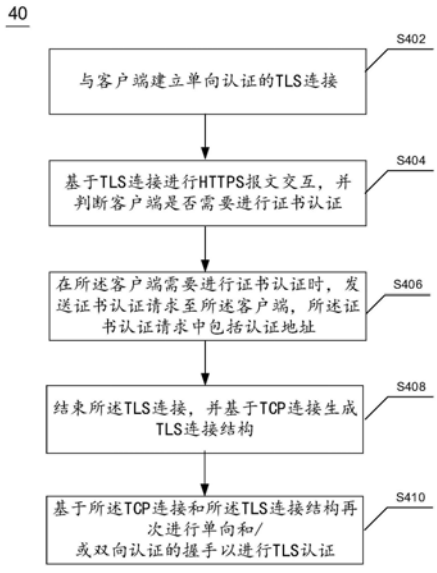
权利要求书2页 说明书12页 附图11页

(54)发明名称

TLS认证方法、装置、系统、电子设备及可读介质

(57)摘要

本公开提供一种TLS认证方法、装置、系统、电子设备及计算机可读介质。该方法包括:与客户端建立单向认证的TLS连接;基于所述TLS连接进行HTTPS报文交互,并判断所述客户端是否需要进行证书认证;在所述客户端需要进行证书认证时,发送证书认证请求至所述客户端,所述证书认证请求中包括认证地址;结束所述TLS连接,并基于TCP连接生成TLS连接结构;基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。本公开涉及的TLS认证方法、装置、系统、电子设备及计算机可读介质,能够在不改变开发者的程序框架流程、不增加额外认证服务器的基础上,实现更新版本的TLS协议认证。



CN 113328980 B

1.一种TLS认证方法,可用于服务端,其特征在于,包括:

与客户端建立单向认证的TLS连接;

基于所述TLS连接进行HTTPS报文交互,并判断所述客户端是否需要进行证书认证;

在所述客户端需要进行证书认证时,发送证书认证请求至所述客户端,所述证书认证请求中包括认证地址;

结束所述TLS连接,并基于TCP连接生成TLS连接结构;

基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

2.如权利要求1所述的方法,其特征在于,基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证,包括:

基于所述TCP连接和所述TLS连接结构生成客户端认证信息;

通过所述客户端认证信息与所述客户端再次进行单向和/或双向认证的握手以进行TLS认证。

3.如权利要求2所述的方法,其特征在于,通过所述客户端认证信息与所述客户端再次进行单向和/或双向认证的握手以进行TLS认证,包括:

通过所述客户端认证信息与所述客户端在握手中完成双向TLS认证;或

通过所述客户端认证信息与所述客户端在握手后完成双向TLS认证。

4.如权利要求3所述的方法,其特征在于,通过所述客户端认证信息与所述客户端在握手中完成双向TLS认证,包括:

通过所述客户端认证信息对所述客户端进行证书合法性认证;

在所述证书合法性认证通过后,与所述客户端再次建立TLS连接;

基于所述TLS连接和所述认证地址获取所述客户端的证书信息;

在所述证书信息满足匹配认证策略时,完成双向TLS认证。

5.如权利要求3所述的方法,其特征在于,通过所述客户端认证信息与所述客户端在握手后完成双向TLS认证,包括:

与所述客户端进行单向认证的握手;

在单向认证的握手通过后重新建立TLS连接;

基于所述TLS连接和所述认证地址获取所述客户端的证书和证书信息;

通过所述客户端认证信息对所述证书和所述证书信息进行校验,在校验通过时,完成双向TLS认证。

6.如权利要求5所述的方法,其特征在于,通过所述客户端认证信息对所述证书和所述证书信息进行校验,在校验通过时,完成双向TLS认证,包括:

通过所述客户端认证信息对所述客户端进行证书合法性认证;

在所述证书合法性认证通过后,对所述证书信息进行匹配策略认证;

在所述证书信息满足匹配认证策略时,完成双向TLS认证。

7.如权利要求1所述的方法,其特征在于,还包括:

基于已认证的TLS连接与客户端进行HTTPS报文交互。

8.一种TLS认证装置,可用于服务端,其特征在于,包括:

服务认证模块,用于与客户端建立单向认证的TLS连接;

报文交互模块，用于基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；

认证请求模块，用于在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；

连接结构模块，用于结束所述TLS连接，并基于TCP连接生成TLS连接结构；

握手认证模块，用于基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

9.一种TLS认证装置，可用于客户端，其特征在于，包括：

客户认证模块，用于与服务端建立单向认证的TLS连接；

交互报文模块，用于基于所述TLS连接进行HTTPS报文交互；

证书请求模块，用于在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；

安全连接模块，用于基于所述证书认证请求与所述服务端建立TCP连接；

再次认证模块，用于基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。

10.一种TLS认证系统，其特征在于，包括：

服务端，用于与客户端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；结束所述TLS连接，并基于TCP连接生成TLS连接结构；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证；

客户端，用于与服务端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互；在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；基于所述证书认证请求与所述服务端建立TCP连接；基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。

11.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-7中任一所述的方法。

12.一种计算机可读介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求1-7中任一所述的方法。

TLS认证方法、装置、系统、电子设备及可读介质

技术领域

[0001] 本公开涉及计算机信息处理领域，具体而言，涉及一种TLS认证方法、装置、系统、电子设备及计算机可读介质。

背景技术

[0002] 随着互联网的快速发展，人们对于网络传输安全性的要求也越来越高，HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer，基于安全套接层的超文本传输协议)协议因此出现，HTTPS协议可以认为是HTTP(Hyper TextTransfer Protocol，超文本传输协议)协议和SSL/TLS(Secure SocketsLayer/Transport Layer Security，安全套接层/传输层安全)协议的组合。其中，SSL/TLS协议作用在HTTP协议之下，用于对传输的数据进行加密处理，以保证数据在网络上传输的过程中不会被截取或窃听。

[0003] 2018年8月份，IETF正式宣布TLS 1.3规范落地，TLS 1.3协议的特性中认证部分，包括两点：1.禁止重协商；2.在客户端允许前提下，服务端在握手完成后任意时间认证客户端。目前很多HTTP服务器都能支持标准SSL协议，SSL协议支持在握手过程中对客户端进行认证，也支持在完成握手后对客户端进行认证；但是，TLS协议升级到TLSv1.3版本后禁止了重新协商功能。

[0004] 因此，需要一种新的TLS认证方法、装置、系统、电子设备及计算机可读介质。

[0005] 在所述背景技术部分公开的上述信息仅用于加强对本公开的背景的理解，因此它可以包括不构成对本领域普通技术人员已知的现有技术的信息。

发明内容

[0006] 有鉴于此，本公开提供一种TLS认证方法、装置、系统、电子设备及计算机可读介质，能够在不改变开发者的程序框架流程、不增加额外认证服务器的基础上，实现更新版本的TLS协议认证。

[0007] 本公开的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本公开的实践而习得。

[0008] 根据本公开的一方面，提出一种TLS认证方法，可应用于服务端，该方法包括：与客户端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；结束所述TLS连接，并基于TCP连接生成TLS连接结构；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

[0009] 在本公开的一种示例性实施例中，基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证，包括：基于所述TCP连接和所述TLS连接结构生成客户端认证信息；通过所述客户端认证信息与所述客户端再次进行单向和/或双向认证的握手以进行TLS认证。

[0010] 在本公开的一种示例性实施例中，通过所述客户端认证信息与所述客户端再次进行单向和/或双向认证的握手以进行TLS认证，包括：通过所述客户端认证信息与所述客户端在握手中完成双向TLS认证；或通过所述客户端认证信息与所述客户端在握手后完成双向TLS认证。

[0011] 在本公开的一种示例性实施例中，通过所述客户端认证信息与所述客户端在握手中完成双向TLS认证，包括：通过所述客户端认证信息对所述客户端进行证书合法性认证；在所述证书合法性认证通过后，与所述客户端再次建立TLS连接；基于所述TLS连接和所述认证地址获取所述客户端的证书信息；在所述证书信息满足匹配认证策略时，完成双向TLS认证。

[0012] 在本公开的一种示例性实施例中，通过所述客户端认证信息与所述客户端在握手后完成双向TLS认证，包括：与所述客户端进行单向认证的握手；在单向认证的握手通过后重新建立TLS连接；基于所述TLS连接和所述认证地址获取所述客户端的证书和证书信息；通过所述客户端认证信息对所述证书和所述证书信息进行校验，在校验通过时，完成双向TLS认证。

[0013] 在本公开的一种示例性实施例中，通过所述客户端认证信息对所述证书和所述证书信息进行校验，在校验通过时，完成双向TLS认证，包括：通过所述客户端认证信息对所述客户端进行证书合法性认证；在所述证书合法性认证通过后，对所述证书信息进行匹配策略认证；在所述证书信息满足匹配认证策略时，完成双向TLS认证。

[0014] 在本公开的一种示例性实施例中，还包括：基于已认证的TLS连接与客户端进行HTTPS报文交互。

[0015] 根据本公开的一方面，提出一种TLS认证方法，可应用于客户端，该方法包括：与服务端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互；在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；基于所述证书认证请求与所述服务端建立TCP连接；基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。

[0016] 在本公开的一种示例性实施例中，基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证，包括：基于所述TCP和所述认证地址和所述服务端在握手中完成双向TLS认证；或基于所述TCP和所述认证地址和所述服务端在握手后完成双向TLS认证。

[0017] 在本公开的一种示例性实施例中，基于所述TCP和所述认证地址和所述服务端在握手中完成双向TLS认证，包括：基于所述TCP和所述认证地址发送证书至所述服务端以进行正式合法性认证；在所述证书合法性认证通过后，与所述客户端再次建立TLS连接，并发送认证请求，所述认证请求中包含证书信息；在所述证书信息满足所述服务端的匹配认证策略时，完成双向TLS认证。

[0018] 在本公开的一种示例性实施例中，基于所述TCP和所述认证地址和所述服务端在握手后完成双向TLS认证，包括：重新生成TLS结构，所述TLS结构支持post_handshake_auth协议；基于post_handshake_auth协议与所述服务端再次建立TLS连接；基于所述TLS连接发送认证请求，所述认证请求中包含证书和证书信息；在所述证书和证书信息认证通过时，完成双向TLS认证。

[0019] 在本公开的一种示例性实施例中，还包括：基于已认证的TLS连接与服务端进行HTTPS报文交互。

[0020] 根据本公开的一方面，提出一种TLS认证装置，该装置可应用在服务端，包括：服务认证模块，用于与客户端建立单向认证的TLS连接；报文交互模块，用于基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；认证请求模块，用于在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；连接结构模块，用于结束所述TLS连接，并基于TCP连接生成TLS连接结构；握手认证模块，用于基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

[0021] 根据本公开的一方面，提出一种TLS认证装置，该装置可应用在客户端，包括：客户认证模块，用于与服务端建立单向认证的TLS连接；交互报文模块，用于基于所述TLS连接进行HTTPS报文交互；证书请求模块，用于在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；安全连接模块，用于基于所述证书认证请求与所述服务端建立TCP连接；再次认证模块，用于基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。

[0022] 根据本公开的一方面，提出一种TLS认证系统，该系统包括：服务端，用于与客户端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；结束所述TLS连接，并基于TCP连接生成TLS连接结构；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证；客户端，用于与服务端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互；在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；基于所述证书认证请求与所述服务端建立TCP连接；基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。

[0023] 根据本公开的一方面，提出一种电子设备，该电子设备包括：一个或多个处理器；存储装置，用于存储一个或多个程序；当一个或多个程序被一个或多个处理器执行，使得一个或多个处理器实现如上文的方法。

[0024] 根据本公开的一方面，提出一种计算机可读介质，其上存储有计算机程序，该程序被处理器执行时实现如上文中的方法。

[0025] 根据本公开的TLS认证方法、装置、系统、电子设备及计算机可读介质，服务器与客户端建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；在所述客户端需要进行证书认证时，服务器发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证的方式，能够在不改变开发者的程序框架流程、不增加额外认证服务器的基础上，实现更新版本的TLS协议认证。

[0026] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性的，并不能限制本公开。

附图说明

[0027] 通过结合附图对于本公开的示例性实施例进行描述，可以更好地理解本公开，在附图中：

[0028] 图1是现有技术中TLS认证方法中单向认证和双向认证的示意图。

[0029] 图2是现有技术中TLS认证方法中增加SSL协议负载后的部署示意图。

[0030] 图3是根据一示例性实施例示出的一种TLS认证方法的交互过程示意图。

[0031] 图4是根据一示例性实施例示出的一种用于服务端的TLS认证方法的流程图。

[0032] 图5是根据一示例性实施例示出的一种用于客户端的TLS认证方法的流程图。

[0033] 图6是根据一示例性实施例示出的一种TLS认证系统的框图。

[0034] 图7是根据一示例性实施例示出的一种TLS认证方法的流程图。

[0035] 图8是根据一示例性实施例示出的一种TLS认证方法的示意图。

[0036] 图9是根据一示例性实施例示出的一种TLS认证方法的流程图。

[0037] 图10是根据一示例性实施例示出的一种TLS认证方法的示意图。

[0038] 图11是根据一示例性实施例示出的一种TLS认证装置的框图。

[0039] 图12是根据另一示例性实施例示出的一种TLS认证装置的框图。

[0040] 图13是根据一示例性实施例示出的一种电子设备的框图。

[0041] 图14是根据一示例性实施例示出的一种计算机可读介质的框图。

具体实施方式

[0042] 现在将参考附图更全面地描述示例实施例。然而，示例实施例能够以多种形式实施，且不应被理解为限于在此阐述的实施例；相反，提供这些实施例使得本公开将全面和完整，并将示例实施例的构思全面地传达给本领域的技术人员。在图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。

[0043] 此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。在下面的描述中，提供许多具体细节从而给出对本公开的实施例的充分理解。然而，本领域技术人员将意识到，可以实践本公开的技术方案而没有特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知方法、装置、实现或者操作以避免模糊本公开的各方面。

[0044] 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0045] 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

[0046] SSL(Secure Sockets Layer，安全套接层)是为网络通信提供安全及数据完整性的一种安全协议。SSL协议介于TCP(Transmission Control Protocol传输控制协议)层与应用层之间，是Web浏览器与Web服务器之间安全交换信息的协议，提供两个基本的安全服务：鉴别与保密。SSL协议可分为两层：SSL记录协议(SSL Record Protocol)：它建立在可靠的传输协议(如TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL握

手协议(SSL Handshake Protocol):它建立在SSL记录协议之上,用于在实际的数据传输开始前,通讯双方进行身份认证、协商加密算法、交换加密密钥等。

[0047] 根据认证方式的不同,SSL协议分为单向认证和双向认证两种。单向认证为服务器需要向客户端提供数字证书,客户端对服务器进行身份验证。双向认证为客户端和服务器双方均需要向对方提供数字证书,并对对方的数字证书进行验证。目前的技术方案中,一个服务器(唯一的IP地址和端口)对外提供SSL服务,多是使用单一认证方式,要么使用单向认证,要么使用双向认证,不同认证方式需单独搭建认证系统,资源的利用效率较低。

[0048] 本公开的发明人发现,目前很多HTTP服务器都能支持标准SSL协议,SSL协议支持在握手过程中对客户端进行认证,也支持在完成握手后对客户端进行认证;但是,TLS协议升级到TLSv1.3版本后禁止了重新协商功能。

[0049] 如图1所示,单向认证和双向认证在两个服务中支持,多数情况下只有单向认证,只有匹配上策略需要进行客户端认证后才将流量重定向到双向认证服务中进行认证。此方案中,需要部署两个服务,至少需要开放两个端口,浪费服务端口资源及增加遭受攻击的风险,同时还对共享信息在两个服务间同步增加了开销。

[0050] 如图2所示,单向认证和双向认证在同一个服务中支持,多数情况下只有单向认证,只有匹配上策略需要进行客户端认证后才将SSL连接打上认证客户端的标记,然后发起重协商。此方案中,明显需要在同一个连接中发起重协商,存在重协商遭受攻击的风险及TLS 1.3版本已经禁止重协商功能,该方案在TLS 1.3版本协议中失效。

[0051] 本公开提出的TLS认证方法,能够实现的基于TLS 1.3协议版本的证书认证方法,主要解决以下几个方面:

[0052] 1、TLS 1.3版本中实现证书认证。

[0053] 2、HTTPS服务器支持TLS 1.3版本后,不改变开发者的程序框架流程。

[0054] 3、不需要增加额外的认证服务。

[0055] 下面将结合具体的实施例对本公开的内容进行详细描述。

[0056] 图3是根据一示例性实施例示出的一种TLS认证方法的交互过程示意图。TLS1.3协议能够完整非常有效的让客户和服务器之间完成相互之间的身份认证,认证相关部分的过程如下:

[0057] ①服务器向客户端发送证书请求报文(CertificateRequest),请求对客户端进行认证;

[0058] ②服务器向客户端发送自己的证书(Certificate);

[0059] ③服务器向客户端发送自己的证书私钥对整个握手报文的签名值(CertificateVerify);

[0060] ④服务器向客户端发送对整个握手报文的MAC值(Finished);

[0061] ⑤客户端收到服务端的证书信息及认证消息后,对证书进行验证,包括:证书是否过期,发行服务器证书的CA是否可靠,发行者证书的公钥能否正确解开服务器证书的“发行者的数字签名”,服务器证书上的域名是否和服务器的实际域名相匹配。如果合法性验证没有通过,通讯将断开;

[0062] ⑥客户端收到服务端发送的证书请求后,将客户端自己的证书发送给服务端认证;

[0063] ⑦客户端服向务器发送自己的证书(Certificate)；

[0064] ⑧客户端服向务器发送自己的证书私钥对整个握手报文的签名值(CertificateVerify)；

[0065] ⑨客户端服向务器发送对整个握手报文的MAC值(Finished)；

[0066] ⑩服务端收到客户端的证书信息及认证消息后，对客户端证书进行验证，包括：证书是否过期，发行客户端证书的CA是否可靠，发行者证书的公钥能否正确解开客户端证书的“发行者的数字签名”，客户端证书上的名字是否和用户的账号名相匹配。如果合法性验证没有通过，通讯将断开；

[0067] 以上这种方法是在握手中实现的双向认证过程；还有另一种方法是在握手完成后对客户端进行认证：

[0068] ①客户端在ClientHello报文中发送了“post_handshake_auth”扩展信息，表示客户端支持在完成握手后的任意时间对客户端进行认证；

[0069] ②在握手协商过程中，客户端完成了对服务器的单向认证；

[0070] ③服务端在握手完成后的任意时间对客户端发起证书请求报文，请求认证客户端

[0071] ④客户端收到服务端发送的证书请求后，将客户端自己的证书发送给服务端认证；

[0072] ⑤客户端服向务器发送自己的证书(Certificate)；

[0073] ⑥客户端服向务器发送自己的证书私钥对整个握手报文的签名值(CertificateVerify)；

[0074] ⑦客户端服向务器发送对整个握手报文的MAC值(Finished)；

[0075] ⑧服务端收到客户端的证书信息及认证消息后，对客户端证书进行验证，包括：证书是否过期，发行客户端证书的CA是否可靠，发行者证书的公钥能否正确解开客户端证书的“发行者的数字签名”，客户端证书上的名字是否和用户的账号名相匹配。如果合法性验证没有通过，通讯将断开；

[0076] 图4是根据另一示例性实施例示出的一种TLS认证方法的流程图。图4所示的流程是对图3所示的流程中服务端流程的详细描述。

[0077] 如图4所示，在S402中，与客户端建立单向认证的TLS连接。

[0078] 在S404中，基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证。

[0079] 在S406中，在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址。

[0080] 在S408中，结束所述TLS连接，并基于TCP连接生成TLS连接结构。

[0081] 在S410中，基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。还包括：基于已认证的TLS连接与客户端进行HTTPS报文交互。

[0082] 具体步骤可包括：基于所述TCP连接和所述TLS连接结构生成客户端认证信息；通过所述客户端认证信息与所述客户端再次进行单向和/或双向认证的握手以进行TLS认证。

[0083] 在一个实施例中，通过所述客户端认证信息与所述客户端再次进行单向和/或双向认证的握手以进行TLS认证，包括：通过所述客户端认证信息与所述客户端在握手中完成双向TLS认证；或通过所述客户端认证信息与所述客户端在握手后完成双向TLS认证。

[0084] 在一个实施例中，通过所述客户端认证信息与所述客户端在握手中完成双向TLS认证，包括：通过所述客户端认证信息对所述客户端进行证书合法性认证；在所述证书合法性认证通过后，与所述客户端再次建立TLS连接；基于所述TLS连接和所述认证地址获取所述客户端的证书信息；在所述证书信息满足匹配认证策略时，完成双向TLS认证。

[0085] 在一个实施例中，通过所述客户端认证信息与所述客户端在握手后完成双向TLS认证，包括：与所述客户端进行单向认证的握手；在单向认证的握手通过后重新建立TLS连接；基于所述TLS连接和所述认证地址获取所述客户端的证书和证书信息；通过所述客户端认证信息对所述客户端进行证书合法性认证；在所述证书合法性认证通过后，对所述证书信息进行匹配策略认证；在所述证书信息满足匹配认证策略时，完成双向TLS认证。

[0086] 图5是根据另一示例性实施例示出的一种TLS认证方法的流程图。图5所示的流程是对图3所示的流程中客户端流程的详细描述。

[0087] 如图5所示，在S502中，与服务端建立单向认证的TLS连接。

[0088] 在S504中，基于所述TLS连接进行HTTPS报文交互。

[0089] 在S506中，在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址。

[0090] 在S508中，基于所述证书认证请求与所述服务端建立TCP连接。

[0091] 在S510中，基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。还包括：基于已认证的TLS连接与服务端进行HTTPS报文交互。

[0092] 具体可包括：基于所述TCP和所述认证地址和所述服务端在握手中完成双向TLS认证；或基于所述TCP和所述认证地址和所述服务端在握手后完成双向TLS认证。

[0093] 在一个实施例中，基于所述TCP和所述认证地址和所述服务端在握手中完成双向TLS认证，包括：基于所述TCP和所述认证地址发送证书至所述服务端以进行正式合法性认证；在所述证书合法性认证通过后，与所述客户端再次建立TLS连接，并发送认证请求，所述认证请求中包含证书信息；在所述证书信息满足所述服务端的匹配认证策略时，完成双向TLS认证。

[0094] 在一个实施例中，基于所述TCP和所述认证地址和所述服务端在握手后完成双向TLS认证，包括：重新生成TLS结构，所述TLS结构支持post_handshake_auth协议；基于post_handshake_auth协议与所述服务端再次建立TLS连接；基于所述TLS连接发送认证请求，所述认证请求中包含证书和证书信息；在所述证书和证书信息认证通过时，完成双向TLS认证。

[0095] 根据本公开的TLS认证方法，能够在TLS 1.3协议版本中进行了数据交互后匹配策略实现证书认证。能够使得HTTPS服务器支持TLS 1.3版本后，不改变开发者的程序框架流程。在实现TLS 1.3协议认证的时候不需要增加额外的认证服务端口。

[0096] 图6是根据一示例性实施例示出的一种TLS认证系统的框图。

[0097] 如图6所示，系统架构60可以包括客户端设备601、602、603，网络604和服务端设备605。网络604用以在客户端设备601、602、603和服务端设备605之间提供通信链路的介质。网络604可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0098] 用户可以使用客户端设备601、602、603通过网络604与服务端设备605交互，以接收或发送消息等。客户端设备601、602、603上可以安装有各种通讯客户端应用，例如购物类

应用、网页浏览器应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等。

[0099] 客户端设备601、602、603可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于服务器、平板电脑、膝上型便携计算机和台式计算机等等。

[0100] 服务端设备605可以是提供各种服务的服务器，例如对用户利用客户端设备601、602、603所浏览的网站提供支持的后台管理服务器。服务端设备605首先对可以客户端设备601、602、603进行TLS的认证，在认证通过后，服务端设备605与客户端设备601、602、603建立安全的TLS协议连接，并基于此连接进行数据传输。

[0101] 服务端设备605可例如与客户端设备601(或602或603)建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互，并判断客户端设备601是否需要进行证书认证；在客户端设备601需要进行证书认证时，发送证书认证请求至客户端设备601，所述证书认证请求中包括认证地址；结束所述TLS连接，并基于TCP连接生成TLS连接结构；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

[0102] 客户端设备601(或602或603)可例如与服务端设备605建立单向认证的TLS连接；基于所述TLS连接进行HTTPS报文交互；在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；基于所述证书认证请求与服务端设备605建立TCP连接；基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证

[0103] 其中，客户端设备601、602、603或服务端设备605均可以是一个实体的服务器，还可例如为多个服务器组成，需要说明的是，本公开实施例所提供的TLS认证方法可以由服务端设备605和客户端设备601、602、603执行，相应地，TLS认证装置可以设置于服务端设备605和客户端设备601、602、603中。

[0104] 图7和图8是对“在握手中完成双向TLS认证”的详细说明。如图所示，在握手中完成双向TLS认证的具体步骤如下：

[0105] ①客户端与服务端进行单向认证的TLS握手，建立TLS连接；

[0106] ②在HTTPS数据交互中用户匹配上需要进行证书认证的认证策略时，服务端使用HTTPS报文通知客户端当前TLS连接需要进行对客户端认证，需要结束当前TLS连接并在当前TCP连接上重新建立TLS连接，重新建立TLS连接后HTTPS连接重定向到/UKey_auth_login的认证URL；

[0107] ③服务端结束当前TLS连接，在当前TCP连接重新生成TLS连接结构，设置认证客户端的选项后等待客户端在该TCP连接上进行TLS双向认证的握手；

[0108] ④如果认证过程中证书合法性验证没有通过，则通讯将断开，认证失败；

[0109] ⑤服务端重新建立TLS连接后，收到客户端的/UKey_auth_login请求，服务端提取客户端证书信息进一步匹配认证策略，如果使用者与策略不匹配，则通讯将断开，认证失败；

[0110] ⑥成功建立TLS连接，正常进行HTTPS报文交互，不影响其他连接。

[0111] 图9和图10是对“在握手后完成双向TLS认证”的详细说明。如图所示，在握手后完成双向TLS认证的具体步骤如下：

[0112] ①客户端与服务端进行单向认证的TLS握手，建立TLS连接；

[0113] ②在HTTPS数据交互中用户匹配上需要进行证书认证的认证策略时，服务端使用HTTPS报文通知客户端当前TLS连接需要进行对客户端认证，需要结束当前TLS连接并在当

前TCP连接上重新建立TLS连接，重新建立TLS连接后HTTPS连接重定向到/UKey_auth_login的认证URL；

[0114] ③客户端重新生成TLS结构，并支持“post_handshake_auth”；

[0115] ④服务端结束当前TLS连接，在当前TCP连接重新生成TLS连接结构，设置认证客户端的选项后等待客户端在该TCP连接上进行TLS双单向认证的握手；

[0116] ⑤服务端重新建立TLS连接后，收到客户端的/UKey_auth_login请求，服务端发起对客户端的认证请求；

[0117] ⑥客户端发送证书及认证消息给服务端，服务端提取客户端证书信息进一步匹配认证策略，如果证书合法性验证没有通过，或者使用者与策略不匹配，则通讯将断开，认证失败；

[0118] ⑦成功建立TLS连接，正常进行HTTPS报文交互，不影响其他连接。

[0119] 以上步骤中，值得一提的是：单向认证服务器建立TLS 1.3连接后进行HTTPS数据交互匹配认证策略后才进行证书认证；服务端在HTTPS报文中指明客户端进行重启TLS连接的操作；服务端和客户端在同一条TCP连接中实现认证。

[0120] 根据本公开的TLS认证方法，在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；结束所述TLS连接，并基于TCP连接生成TLS连接结构；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证的方式，能够在不改变开发者的程序框架流程、不增加额外认证服务器的基础上，实现更新版本的TLS协议认证。

[0121] 应清楚地理解，本公开描述了如何形成和使用特定示例，但本公开的原理不限于这些示例的任何细节。相反，基于本公开公开的内容的教导，这些原理能够应用于许多其它实施例。

[0122] 此外，需要注意的是，上述附图仅是根据本公开示例性实施例的方法所包括的处理的示意性说明，而不是限制目的。易于理解，上述附图所示的处理并不表明或限制这些处理的时间顺序。另外，也易于理解，这些处理可以是例如在多个模块中同步或异步执行的。

[0123] 下述为本公开装置实施例，可以用于执行本公开方法实施例。对于本公开装置实施例中未披露的细节，请参照本公开方法实施例。

[0124] 图11是根据一示例性实施例示出的一种TLS认证装置的框图。如图11所示，TLS认证装置110可用于服务端，包括：服务认证模块1102，报文交互模块1104，认证请求模块1106，连接结构模块1108，握手认证模块1110。

[0125] 服务认证模块1102用于与客户端建立单向认证的TLS连接；

[0126] 报文交互模块1104用于基于所述TLS连接进行HTTPS报文交互，并判断所述客户端是否需要进行证书认证；

[0127] 认证请求模块1106用于在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；

[0128] 连接结构模块1108用于结束所述TLS连接，并基于TCP连接生成TLS连接结构；

[0129] 握手认证模块1110用于基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

[0130] 图12是根据另一示例性实施例示出的一种TLS认证装置的框图。如图12所示，TLS

认证装置120可用于客户端，包括：客户认证模块1202，交互报文模块1204，证书请求模块1206，安全连接模块1208，再次认证模块1210。

[0131] 客户认证模块1202用于与服务端建立单向认证的TLS连接；

[0132] 交互报文模块1204用于基于所述TLS连接进行HTTPS报文交互；

[0133] 证书请求模块1206用于在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址；

[0134] 安全连接模块1208用于基于所述证书认证请求与所述服务端建立TCP连接；

[0135] 再次认证模块1210用于基于所述TCP和所述认证地址再次进行单向和/或双向认证的握手以进行TLS认证。

[0136] 根据本公开的TLS认证装置，服务端在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址；基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证的方式，能够在不改变开发者的程序框架流程、不增加额外认证服务器的基础上，实现更新版本的TLS协议认证。

[0137] 图13是根据一示例性实施例示出的一种电子设备的框图。

[0138] 下面参照图13来描述根据本公开的这种实施方式的电子设备1300。图13显示的电子设备1300仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

[0139] 如图13所示，电子设备1300以通用计算设备的形式表现。电子设备1300的组件可以包括但不限于：至少一个处理单元1310、至少一个存储单元1320、连接不同系统组件(包括存储单元1320和处理单元1310)的总线1330、显示单元1340等。

[0140] 其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元1310执行，使得所述处理单元1310执行本说明书上述电子处方流转处理方法部分中描述的根据本公开各种示例性实施方式的步骤。例如，所述处理单元1310可以执行如图4，图5中所示的步骤。

[0141] 所述存储单元1320可以包括易失性存储单元形式的可读介质，例如随机存取存储单元(RAM)13201和/或高速缓存存储单元13202，还可以进一步包括只读存储单元(ROM)13203。

[0142] 所述存储单元1320还可以包括具有一组(至少一个)程序模块13205的程序/实用工具13204，这样的程序模块13205包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0143] 总线1330可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

[0144] 电子设备1300也可以与一个或多个外部设备1300’(例如键盘、指向设备、蓝牙设备等)通信，还可与一个或者多个使得用户能与该电子设备1300交互的设备通信，和/或与使得该电子设备1300能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口1350进行。并且，电子设备1300还可以通过网络适配器1360与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。网络适配器1360可以通过总线1330与电子设备1300的其它模块通信。应当明白，尽管图中未示出，可以结合电子设备1300使用其它硬件和/或软件模

块,包括但不限于:微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0145] 通过以上的实施方式的描述,本领域的技术人员易于理解,这里描述的示例实施方式可以通过软件实现,也可以通过软件结合必要的硬件的方式来实现。因此,如图14所示,根据本公开实施方式的技术方案可以以软件产品的形式体现出来,该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM,U盘,移动硬盘等)中或网络上,包括若干指令以使得一台计算设备(可以是个人计算机、服务器、或者网络设备等)执行根据本公开实施方式的上述方法。

[0146] 所述软件产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0147] 所述计算机可读存储介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了可读程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。可读存储介质还可以是可读存储介质以外的任何可读介质,该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。可读存储介质上包含的程序代码可以用任何适当的介质传输,包括但不限于无线、有线、光缆、RF等等,或者上述的任意合适的组合。

[0148] 可以以一种或多种程序设计语言的任意组合来编写用于执行本公开操作的程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中,远程计算设备可以通过任意种类的网络,包括局域网(LAN)或广域网(WAN),连接到用户计算设备,或者,可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0149] 上述计算机可读介质承载有一个或者多个程序,当上述一个或者多个程序被一个该设备执行时,使得该计算机可读介质实现如下功能:与客户端建立单向认证的TLS连接;基于所述TLS连接进行HTTPS报文交互,并判断所述客户端是否需要进行证书认证;在所述客户端需要进行证书认证时,发送证书认证请求至所述客户端,所述证书认证请求中包括认证地址;结束所述TLS连接,并基于TCP连接生成TLS连接结构;基于所述TCP连接和所述TLS连接结构再次进行单向和/或双向认证的握手以进行TLS认证。

[0150] 本领域技术人员可以理解上述各模块可以按照实施例的描述分布于装置中,也可以进行相应变化唯一不同于本实施例的一个或多个装置中。上述实施例的模块可以合并为一个模块,也可以进一步拆分成多个子模块。

[0151] 以上具体地示出和描述了本公开的示例性实施例。应可理解的是,本公开不限于这里描述的详细结构、设置方式或实现方法;相反,本公开意图涵盖包含在所附权利要求的

精神和范围内的各种修改和等效设置。

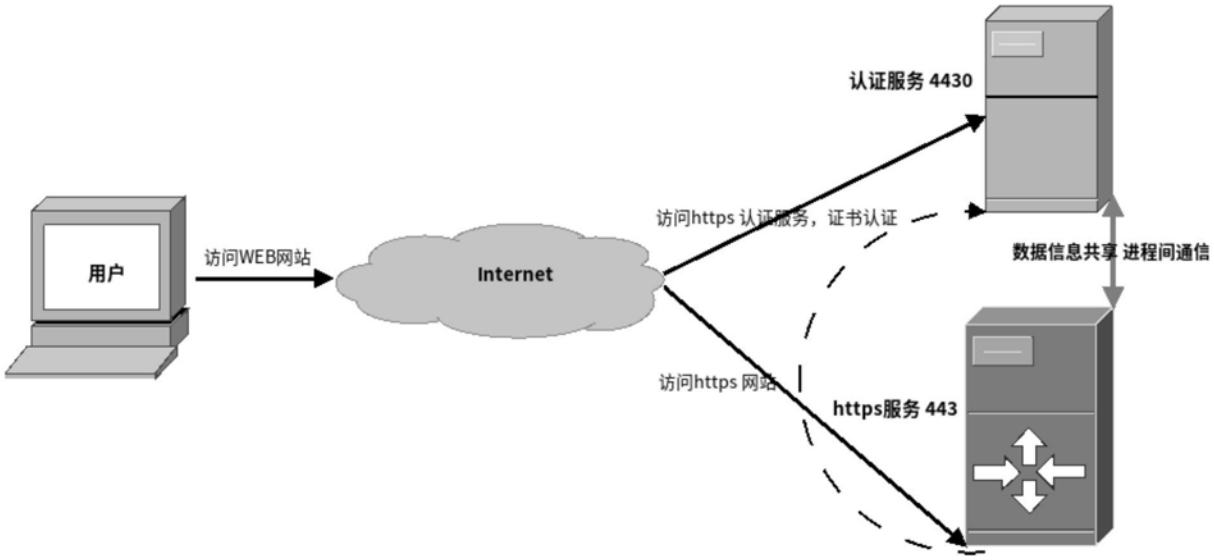

认证服务 4430
用户
访问WEB网站
Internet
访问https 认证服务，证书认证
数据信息共享 进程间通信
访问https 网站
https服务 443

图1

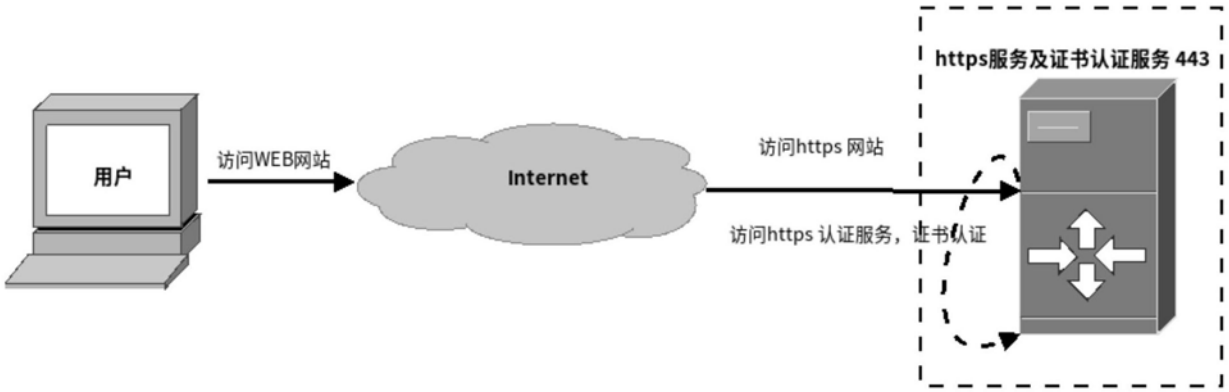

https服务及证书认证服务 443
用户
访问WEB网站
Internet
访问https 网站
访问https 认证服务，证书认证

图2

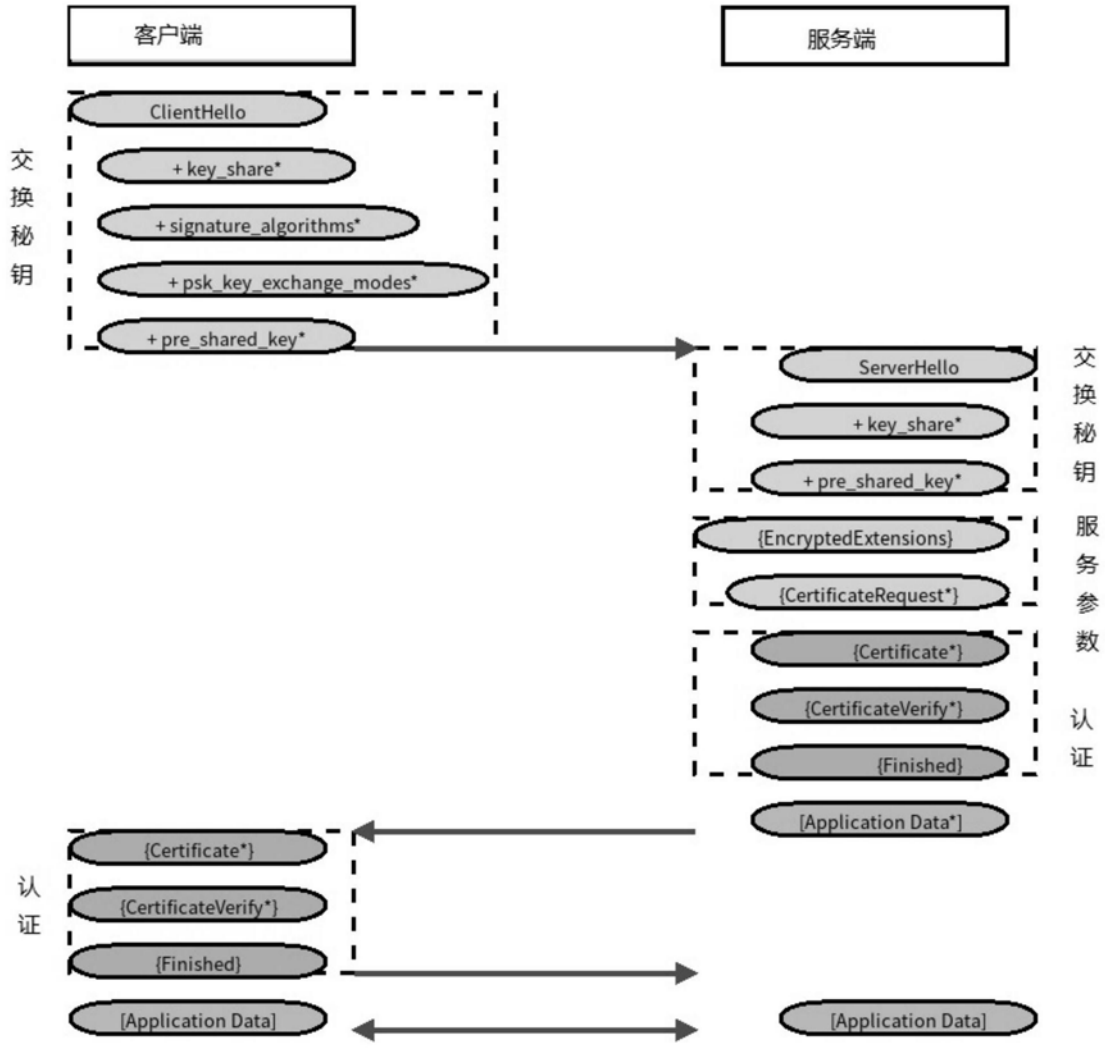

客户端
服务端
交换秘钥
ClientHello
+ key_share*
+ signature_algorithms*
+ psk_key_exchange_modes*
+ pre_shared_key*
ServerHello
+ key_share*
+ pre_shared_key*
交换秘钥
{EncryptedExtensions}
{CertificateRequest*}
服务参数
{Certificate*}
{CertificateVerify*}
{Finished}
认证
[Application Data*]
认证
{Certificate*}
{CertificateVerify*}
{Finished}
[Application Data]
[Application Data]

图3

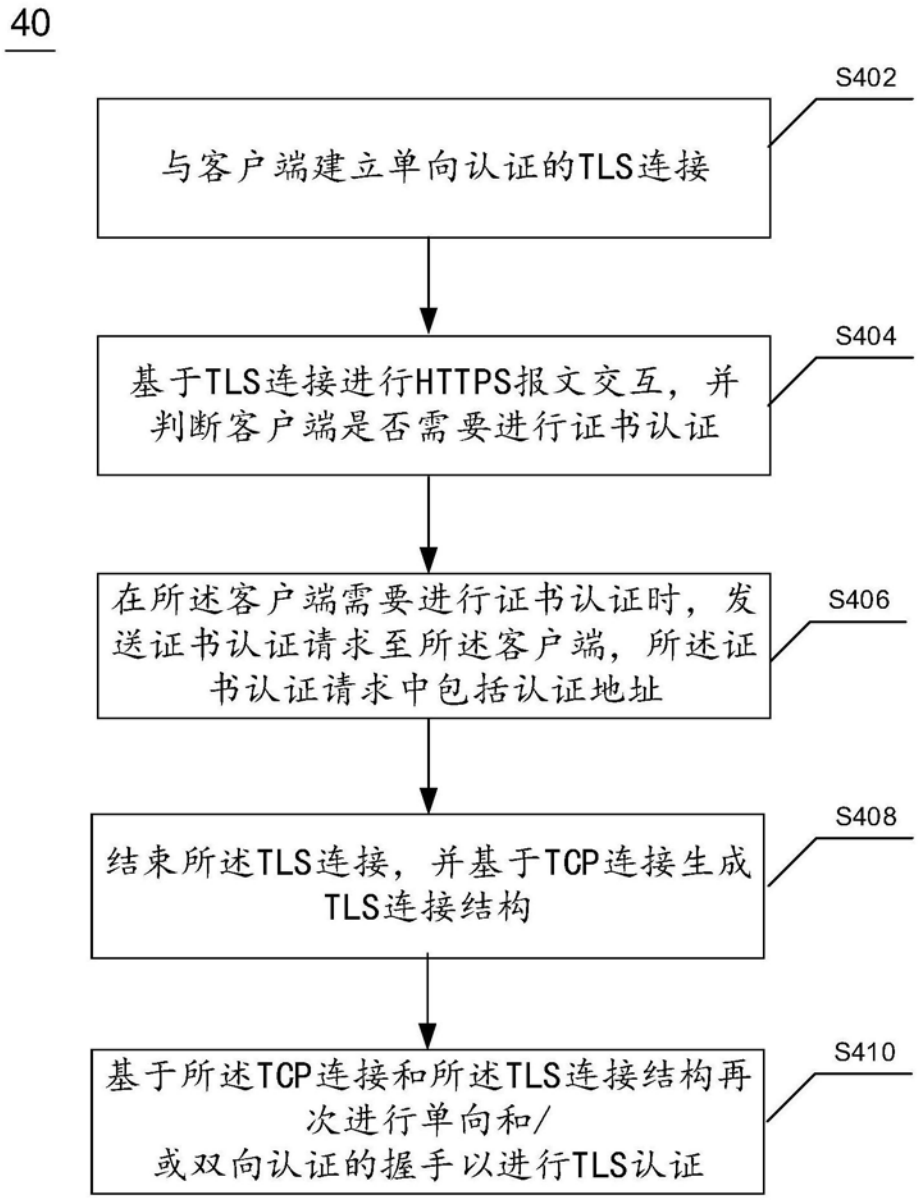

40
S402
与客户端建立单向认证的TLS连接
S404
基于TLS连接进行HTTPS报文交互，并判断客户端是否需要进行证书认证
S406
在所述客户端需要进行证书认证时，发送证书认证请求至所述客户端，所述证书认证请求中包括认证地址
S408
结束所述TLS连接，并基于TCP连接生成TLS连接结构
S410
基于所述TCP连接和所述TLS连接结构再次进行单向和/
或双向认证的握手以进行TLS认证

图4

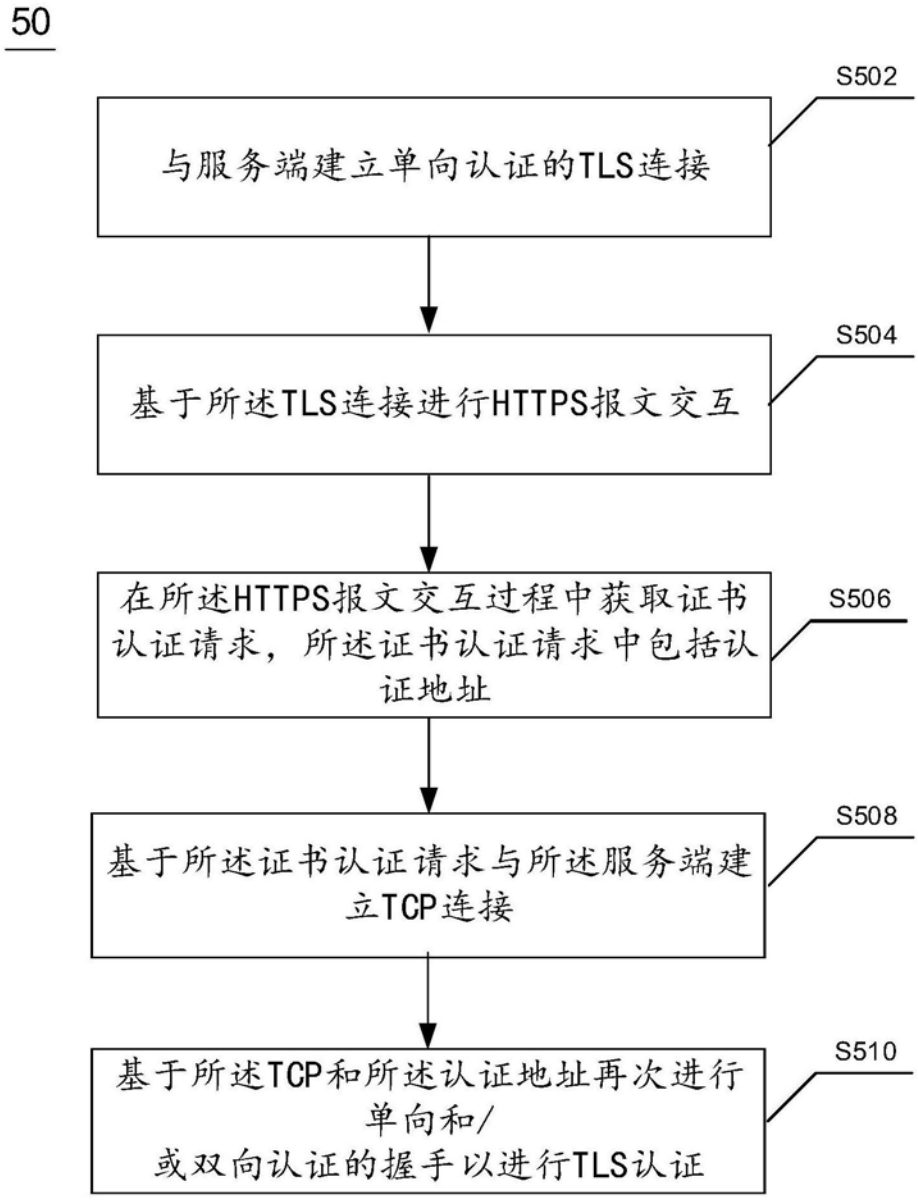

50
S502
与服务端建立单向认证的TLS连接
S504
基于所述TLS连接进行HTTPS报文交互
S506
在所述HTTPS报文交互过程中获取证书认证请求，所述证书认证请求中包括认证地址
S508
基于所述证书认证请求与所述服务端建立TCP连接
S510
基于所述TCP和所述认证地址再次进行单向和/
或双向认证的握手以进行TLS认证

图5

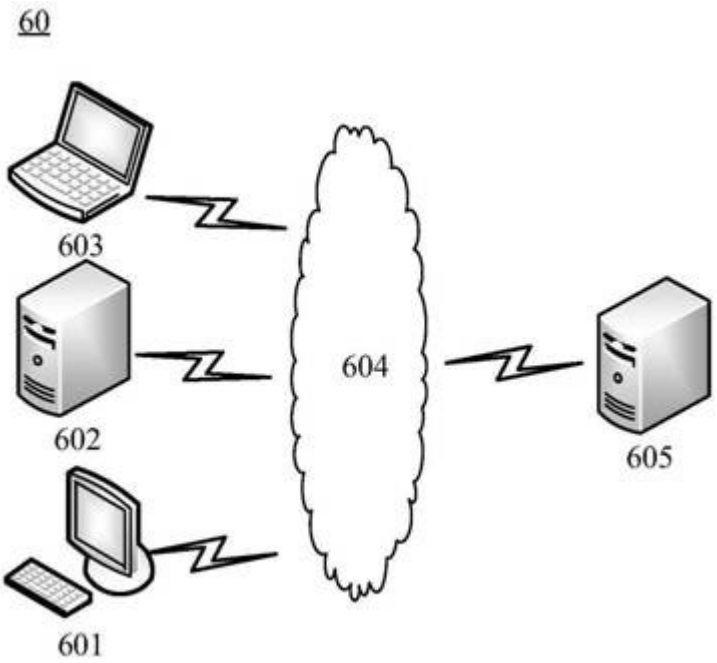

60
603
602
601
604
605

图6

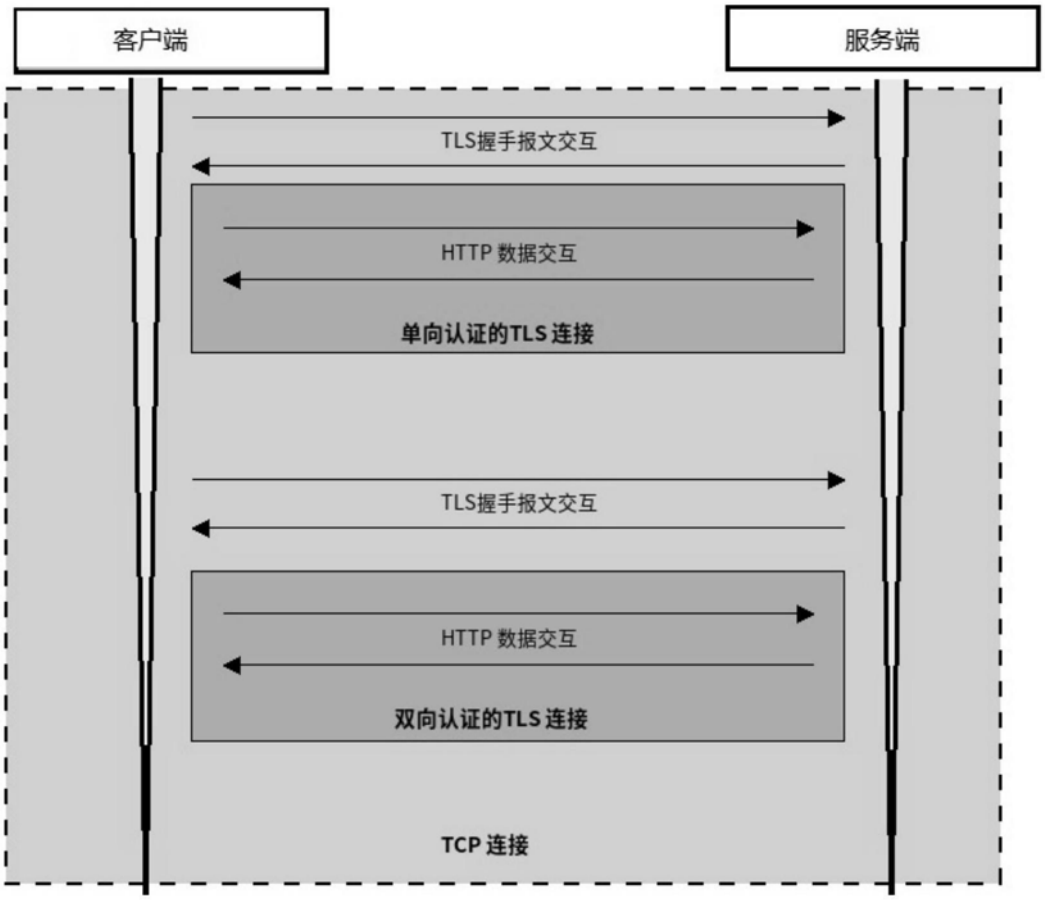

客户端
服务端
TLS握手报文交互
HTTP 数据交互
单向认证的TLS 连接
TLS握手报文交互
HTTP 数据交互
双向认证的TLS 连接
TCP 连接

图7

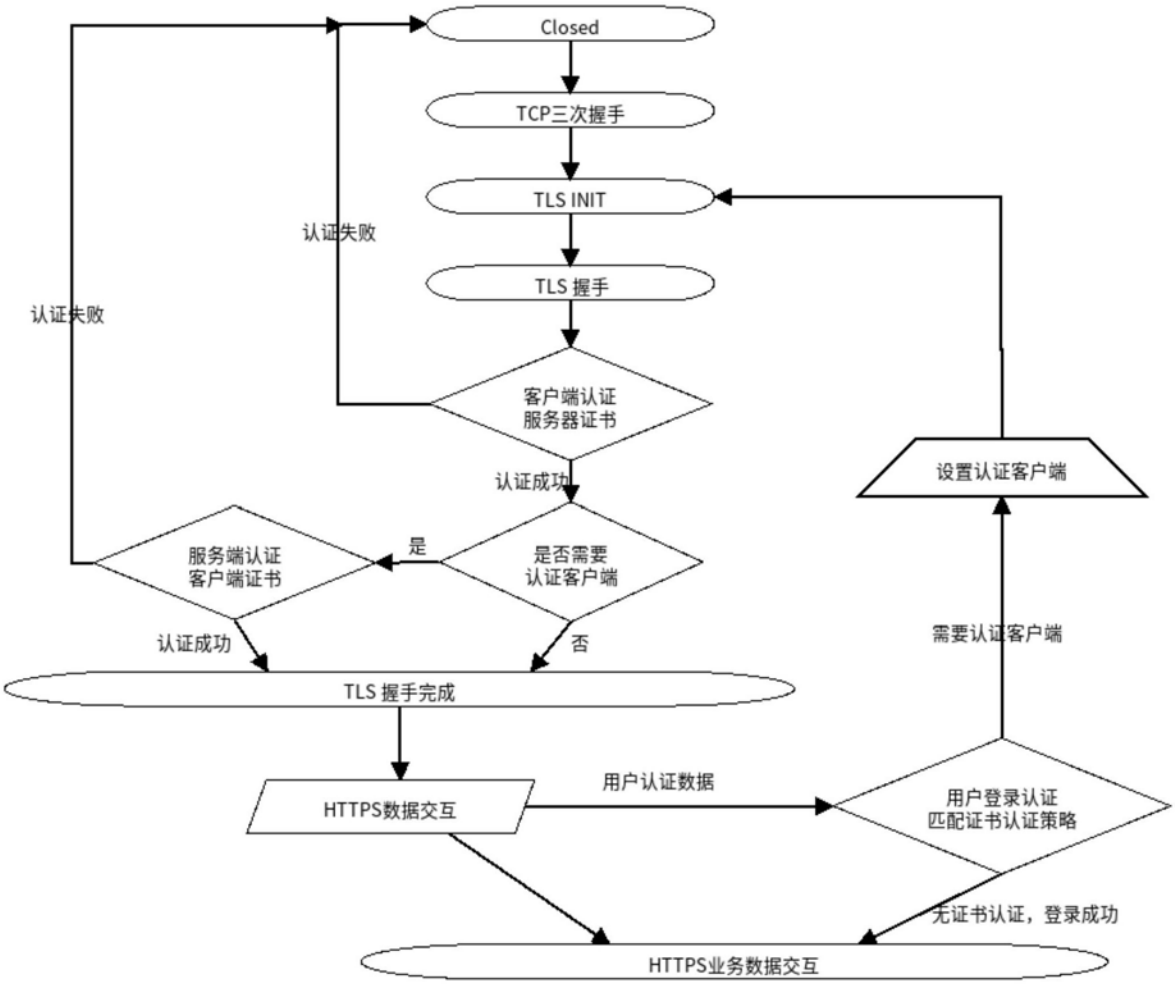

Closed
TCP三次握手
TLS INIT
TLS 握手
客户端认证
服务器证书
认证失败
认证失败
认证成功
是否需要
认证客户端
是
服务端认证
客户端证书
认证成功
否
TLS 握手完成
HTTPS数据交互
用户认证数据
用户登录认证
匹配证书认证策略
设置认证客户端
需要认证客户端
无证书认证，登录成功
HTTPS业务数据交互

图8

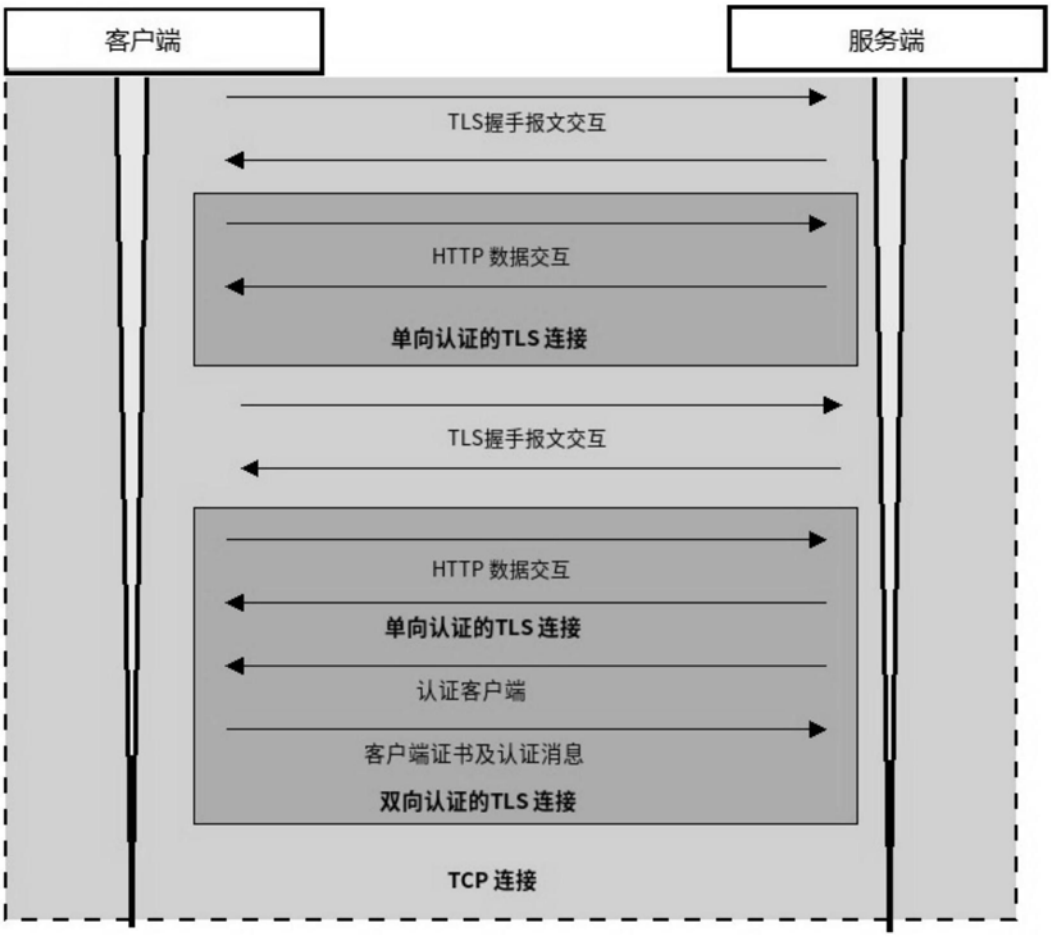

客户端
服务端
TLS握手报文交互
HTTP 数据交互
单向认证的TLS 连接
TLS握手报文交互
HTTP 数据交互
单向认证的TLS 连接
认证客户端
客户端证书及认证消息
双向认证的TLS 连接
TCP 连接

图9

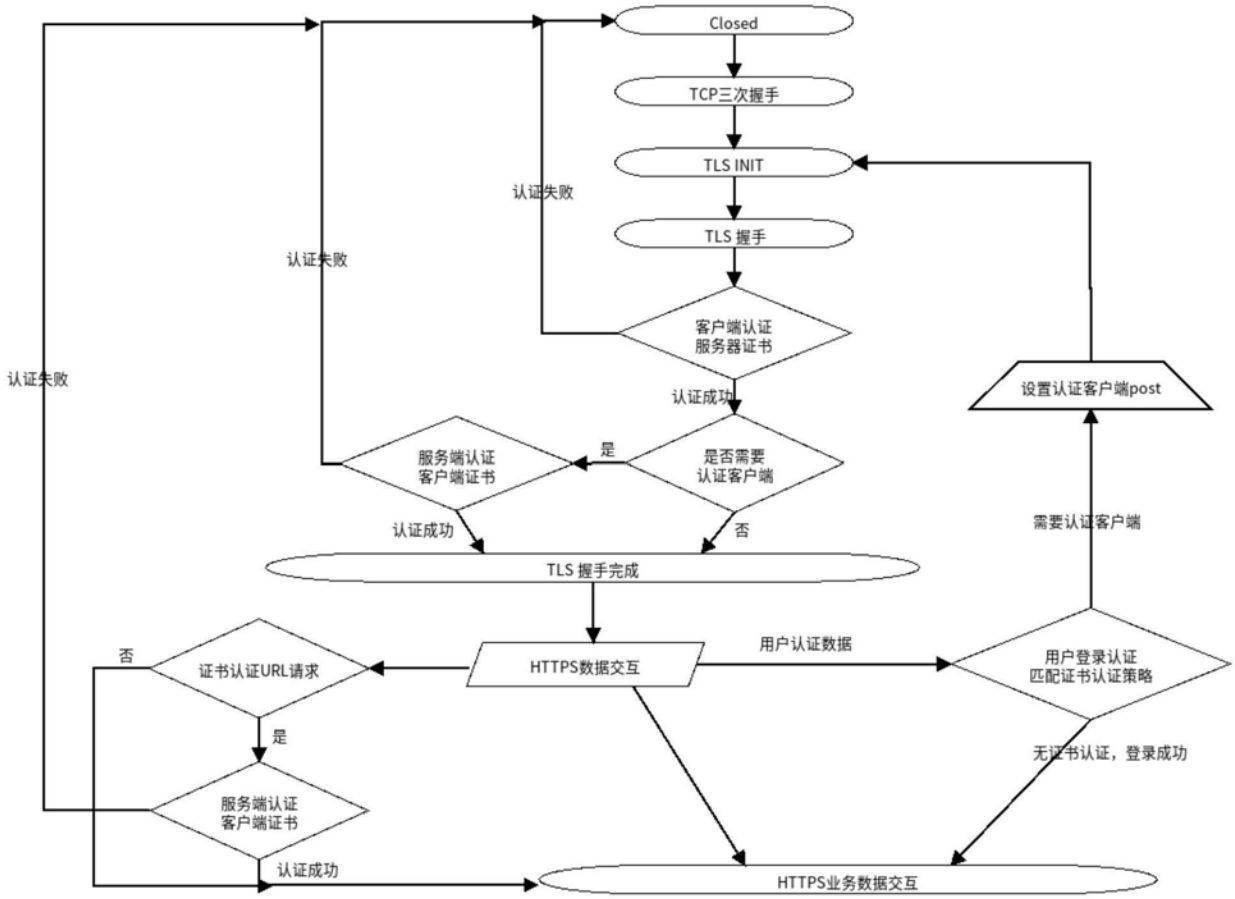

Closed
TCP三次握手
TLS INIT
TLS 握手
客户端认证
服务器证书
认证失败
认证失败
认证失败
认证成功
是否需要
认证客户端
是
服务端认证
客户端证书
认证成功
否
TLS 握手完成
设置认证客户端post
需要认证客户端
HTTPS数据交互
用户认证数据
用户登录认证
匹配证书认证策略
否
证书认证URL请求
是
服务端认证
客户端证书
无证书认证，登录成功
认证成功
HTTPS业务数据交互

图10

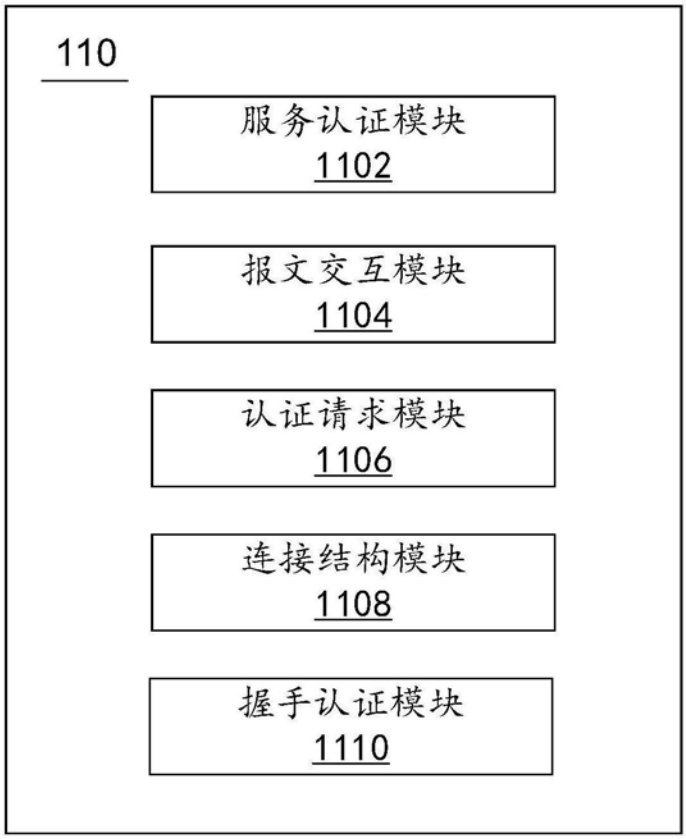

110
服务认证模块
1102
报文交互模块
1104
认证请求模块
1106
连接结构模块
1108
握手认证模块
1110

图11


120
客户认证模块
1202
交互报文模块
1204
证书请求模块
1206
安全连接模块
1208
再次认证模块
1210

图12

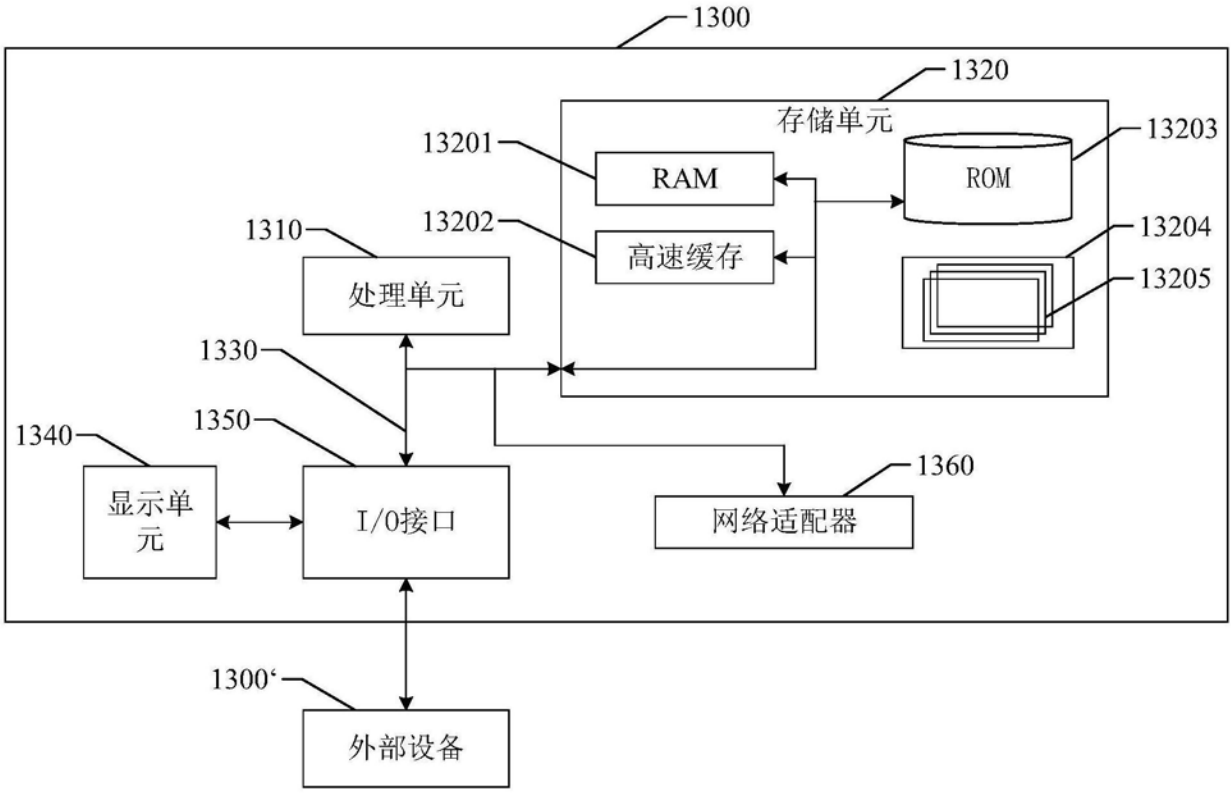

1300
1320
存储单元
13201
RAM
ROM
13203
1310
13202
高速缓存
13204
处理单元
13205
1330
1350
1340
1360
显示单元
I/O接口
网络适配器
1300‘
外部设备

图13

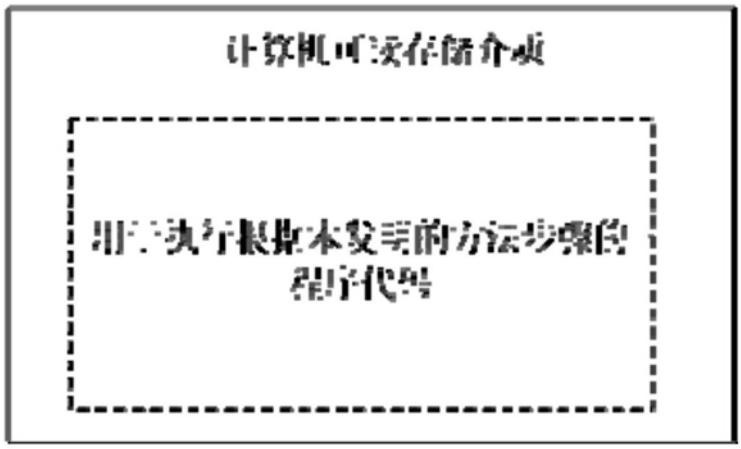

计算机可读存储介质
用于执行根据本发明的方法步骤的
程序代码

图14