



## (12)发明专利

(10)授权公告号 CN 105262748 B

(45)授权公告日 2018.08.31

(21)申请号 201510680364.3

H04L 29/08(2006.01)

(22)申请日 2015.10.19

## (56)对比文件

(65)同一申请的已公布的文献号  
申请公布号 CN 105262748 A

CN 101594233 A, 2009.12.02,  
US 2014090021 A1, 2014.03.27,  
CN 101383842 A, 2009.03.11,  
CN 104506534 A, 2015.04.08,  
CN 103024740 A, 2013.04.03,  
CN 104143144 A, 2014.11.12,  
CN 101651541 A, 2010.02.17,  
CN 101729252 A, 2010.06.09,  
CN 101795272 A, 2010.08.04,  
CN 102857484 A, 2013.01.02,

(43)申请公布日 2016.01.20

审查员 周萍

(73)专利权人 北京东方棱镜科技有限公司  
地址 100084 北京市朝阳区大屯路科学园  
南里-风林绿洲I乙号楼2204号(72)发明人 何华 卢朋 何中天 何中旭  
张云禄(74)专利代理机构 北京市商泰律师事务所  
11255

代理人 毛燕生

(51)Int.Cl.

H04L 29/06(2006.01)

权利要求书3页 说明书8页 附图8页

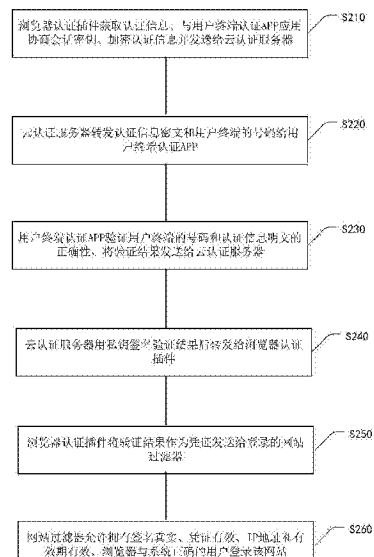
## (54)发明名称

广域网中对用户终端进行身份认证的方法  
和系统

## (57)摘要

本发明实施例提供了一种广域网中对用户终端进行身份认证的方法和系统。该方法主要包括：浏览器认证插件获取用户终端的认证信息并发送给云认证服务器，云认证服务器通过与用户终端进行数据通信交互，对认证信息进行验证，验证通过后，将验证结果发送给浏览器认证插件，浏览器认证插件将认证信息发送给网站的网站过滤器，网站过滤器验证认证信息中的IP地址、浏览器信息和操作系统信息正确后，允许用户终端登录网站。本发明实施例采用基于实名用户终端的云身份认证技术，可以将登录网站的用户与实名的用户终端捆绑在一起，间接使用户终端实名化，克服了Web SSO方法中存在的缺点，能够快速、简单、有效地验证Web用户终端身份的真实性。

CN 105262748 B



1. 一种广域网中对用户终端进行身份认证的方法,其特征在于,包括:

用户终端通过浏览器登录网站,浏览器认证插件获取所述用户终端的认证信息,将所述认证信息发送给云认证服务器,所述认证信息包括所述用户终端的号码、密码、IP地址、浏览器信息和操作系统信息;

所述云认证服务器通过与所述用户终端进行数据通信交互,对所述认证信息进行验证,验证通过后,将验证结果发送给所述浏览器认证插件;

所述浏览器认证插件将所述认证信息发送给所述网站的网站过滤器,所述网站过滤器验证所述认证信息中的IP地址、浏览器信息和操作系统信息正确后,允许所述用户终端登录所述网站;

所述的云认证服务器通过与所述用户终端进行数据通信交互,对所述认证信息进行验证,包括:

云认证服务器与用户终端认证APP之间通过使用椭圆曲线算法验证私钥签名,定期进行相互身份认证,相互身份认证成功后,云认证服务器接收用户终端认证APP定期发送的用户终端基本信息,将接收到的基本信息关联存储在映射表中,该映射表中存储的信息包括:用户终端的号码、用户终端的IP地址、公钥证书格式;

所述云认证服务器接收浏览器认证插件发送的用户终端的号码和认证信息密文后,根据用户终端的号码查询所述映射表,获取所述用户终端的号码对应的用户终端IP地址,根据获取的用户终端IP地址将认证信息密文和用户终端的号码发送给用户终端认证APP;

所述用户终端认证APP用协商得到的会话密钥解密所述认证信息密文,得到认证信息明文,验证用户终端的号码与认证信息明文的正确性,生成验证结果,将验证结果用私钥签名后发送给云认证服务器,所述验证结果包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号。

2. 根据权利要求1所述的广域网中对用户终端进行身份认证的方法,其特征在于,所述的用户终端通过浏览器登录网站,浏览器认证插件获取所述用户终端的认证信息,将所述认证信息发送给云认证服务器,所述认证信息包括所述用户终端的号码、密码、IP地址、浏览器信息和操作系统信息,包括:

用户终端通过自带的浏览器登录网站,在网站页面上输入用户终端的基本信息,该基本信息包括用户终端的号码、密码、IP地址与云认证服务器域名;

浏览器认证插件接收所述用户终端的基本信息,获取所述用户终端的认证信息,该认证信息包括:用户终端的号码、密码、IP地址、云认证服务器域名、浏览器的名称与版本号、操作系统名称与版本号;

所述浏览器认证插件使用密钥交换算法通过云认证服务器与用户终端认证APP协商会话密钥,使用协商得到的会话密钥加密除用户终端的号码外的其它认证信息,得到认证信息密文,将所述认证信息密文和用户终端的号码发送给云认证服务器。

3. 根据权利要求1所述的广域网中对用户终端进行身份认证的方法,其特征在于,所述的验证通过后,将验证结果发送给所述浏览器认证插件,包括:

云认证服务器接收用户终端认证APP发送的验证结果,验证所述验证结果上的用户终端认证APP私钥签名有效后,在所述验证结果上添加自己的域名,用自己的私钥签名所述验证结果,将签名后的验证结果发送给浏览器认证插件。

4. 根据权利要求3所述的广域网中对用户终端进行身份认证的方法,其特征在于,所述的浏览器认证插件将所述认证信息发送给所述网站的网站过滤器,所述网站过滤器验证所述认证信息中的IP地址、浏览器信息和操作系统信息正确后,允许所述用户终端登录所述网站,包括:

浏览器认证插件接收到云认证服务器私钥签名后的验证结果后,将验证结果存储到Cookie域,并将云认证服务器私钥签名后的验证结果作为凭证发送给所述网站的网站过滤器;

所述网站过滤器从证书权威处获取云认证服务器的公钥证书,用该云认证服务器的公钥证书验证所述验证结果上的云认证服务器私钥签名的真实性,验证成功后,确定所述凭证有效;

所述网站过滤器验证所述验证结果中的登录主机的IP地址、有效期的有效性通过,并且验证所述验证结果中的浏览器名称与版本号、操作系统名称与版本号的正确性通过后,允许所述用户终端登录所述网站。

5. 一种广域网中对用户终端进行身份认证的系统,其特征在于,包括:浏览器认证插件、云认证服务器和网站过滤器;

所述的浏览器认证插件,用于在用户终端通过浏览器登录网站后,获取所述用户终端的认证信息,将所述认证信息发送给云认证服务器,所述认证信息包括所述用户终端的号码、密码、IP地址、浏览器信息和操作系统信息;在接收到所述云认证服务器返回的验证结果后,将所述认证信息发送给所述网站的网站过滤器;

所述云认证服务器,用于通过与所述用户终端进行数据通信交互,对所述认证信息进行验证,验证通过后,将验证结果发送给所述浏览器认证插件;

所述的网站过滤器验证,用于对所述认证信息中的IP地址、浏览器信息和操作系统信息正确后,允许所述用户终端登录所述网站;

所述的云认证服务器,具体用于与用户终端认证APP之间通过使用椭圆曲线算法验证私钥签名,定期相互进行认证身份,相互认证身份成功后,接收用户终端认证APP定期发送的用户终端基本信息,将接收到的基本信息关联存储在映射表中,该映射表中存储的信息包括:用户终端的号码、用户终端

IP、公钥证书格式符合X.509证书标准;

接收浏览器认证插件发送的用户终端的号码和认证信息密文后,根据用户终端的号码查询所述映射表,获取所述用户终端的号码对应的用户终端IP地址,根据获取的用户终端IP地址将认证信息密文和用户终端的号码转发给用户终端认证APP;

所述的用户终端认证APP,具体用于用协商得到的会话密钥解密所述认证信息密文,得到认证信息明文,验证用户终端的号码与认证信息明文的正确性,生成验证结果,将验证结果用私钥签名后发送给云认证服务器,所述验证结果包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号。

6. 根据权利要求5所述的广域网中对用户终端进行身份认证的系统,其特征在于,所述的系统还包括用户终端认证APP;

所述的用户终端认证APP,用于在用户终端通过自带的浏览器登录网站后,在网站页面上输入用户终端的基本信息,该基本信息包括用户终端的号码、密码、IP地址与云认证服务

器域名；通过云认证服务器与浏览器认证插件协商会话密钥；

所述的浏览器认证插件，用于接收所述用户终端的基本信息，获取所述用户终端的认证信息，该认证信息包括：用户终端的号码、密码、IP地址、云认证服务器域名、浏览器的名称与版本号、操作系统名称与版本号；

使用密钥交换算法通过云认证服务器与用户终端认证APP协商会话密钥，使用协商得到的会话密钥加密除用户终端的号码外的其它认证信息，得到认证信息密文，将所述认证信息密文和用户终端的号码发送给云认证服务器。

7. 根据权利要求5所述的广域网中对用户终端进行身份认证的系统，其特征在于：

所述的云认证服务器，具体用于接收用户终端认证APP发送的验证结果，验证所述验证结果上的用户终端认证APP私钥签名有效后，在所述验证结果上添加自己的域名，用自己的私钥签名所述验证结果，将签名后的验证结果发送给浏览器认证插件。

8. 根据权利要求7所述的广域网中对用户终端进行身份认证的系统，其特征在于：

所述的浏览器认证插件，具体用于接收到云认证服务器私钥签名后的验证结果后，将验证结果存储到Cookie域，并将云认证服务器私钥签名后的验证结果作为凭证发送给所述网站的网站过滤器；

所述的网站过滤器，具体用于从证书权威处获取云认证服务器的公钥证书，用该云认证服务器的公钥证书验证所述验证结果上的云认证服务器私钥签名的真实性，验证成功后，确定所述凭证有效；

验证所述验证结果中的登录主机的IP地址、有效期的有效性通过，并且验证所述验证结果中的浏览器名称与版本号、操作系统名称与版本号的正确性通过后，允许所述用户终端登录所述网站。

## 广域网中对用户终端进行身份认证的方法和系统

### 技术领域

[0001] 本发明涉及网络安全技术领域，尤其涉及一种广域网中对用户终端进行身份认证的方法和系统。

### 背景技术

[0002] 在互联网与云计算飞速发展、Web应用几乎统治绝大部分软件应用系统的今天，我们的网民数量正在以每分钟百人的速度激增，就在这互联网遍及千家万户的时候，广域网中的Web攻击频繁发生，例如2014年9月，大约有500万谷歌的gmail账户和密码被泄露给一家俄罗斯互联网网络安全论坛；2014年12月25日，乌云漏洞报告平台报告称，大量12306网站的13多万条用户数据在互联网疯传，内容包括用户帐号、明文密码、身份证号码、用户终端的号码和电子邮箱等。这些窃密背后都是黑客在操纵，因此对登录网站的用户进行身份认证可以有效阻止SQL注入、XSS攻击等Web攻击。

[0003] 目前，广域网中云身份认证的技术主要是Web SSO技术，该技术比较成熟、实现简单。缺陷是实施过程中用户帐户统一管理复杂、认证方式统一实施复杂、跨域认证实施复杂，并且多数Web SSO技术使用了Cookie技术，从而使得用户个人信息与上网行为很容易被窃取。

### 发明内容

[0004] 本发明的实施例提供了一种广域网中对用户终端进行身份认证的方法和系统，以实现有效地验证Web用户终端身份的真实性。

[0005] 为了实现上述目的，本发明采取了如下技术方案。

[0006] 一种广域网中对用户终端进行身份认证的方法，包括：

[0007] 用户终端通过浏览器登录网站，浏览器认证插件获取所述用户终端的认证信息，将所述认证信息发送给云认证服务器，所述认证信息包括所述用户终端的号码、密码、IP地址、浏览器信息和操作系统信息；

[0008] 所述云认证服务器通过与所述用户终端进行数据通信交互，对所述认证信息进行验证，验证通过后，将验证结果发送给所述浏览器认证插件；

[0009] 所述浏览器认证插件将所述认证信息发送给所述网站的网站过滤器，所述网站过滤器验证所述认证信息中的IP地址、浏览器信息和操作系统信息正确后，允许所述用户终端登录所述网站。

[0010] 优选地，所述的用户终端通过浏览器登录网站，浏览器认证插件获取所述用户终端的认证信息，将所述认证信息发送给云认证服务器，所述认证信息包括所述用户终端的号码、密码、IP地址、浏览器信息和操作系统信息，包括：

[0011] 用户终端通过自带的浏览器登录网站，在网站页面上输入用户终端的基本信息，该基本信息包括用户终端的号码、密码、IP地址与云认证服务器域名；

[0012] 浏览器认证插件接收所述用户终端的基本信息，获取所述用户终端的认证信息，

该认证信息包括：用户终端的号码、密码、IP地址、云认证服务器域名、浏览器的名称与版本号、操作系统名称与版本号；

[0013] 所述浏览器认证插件使用密钥交换算法通过云认证服务器与用户终端认证APP协商会话密钥，使用协商得到的会话密钥加密除用户终端的号码外的其它认证信息，得到认证信息密文，将所述认证信息密文和用户终端的号码发送给云认证服务器。

[0014] 优选地，所述的所述云认证服务器通过与所述用户终端进行数据通信交互，对所述认证信息进行验证，包括：

[0015] 云认证服务器与用户终端认证APP之间通过使用椭圆曲线算法验证私钥签名，定期进行相互身份认证，相互身份认证成功后，云认证服务器接收用户终端认证APP定期发送的用户终端基本信息，将接收到的基本信息关联存储在映射表中，该映射表中存储的信息包括：用户终端的号码、用户终端的IP地址、公钥证书格式；

[0016] 所述云认证服务器接收浏览器认证插件发送的用户终端的号码和认证信息密文后，根据用户终端的号码查询所述映射表，获取所述用户终端的号码对应的用户终端IP地址，根据获取的用户终端IP地址将认证信息密文和用户终端的号码发送给用户终端认证APP；

[0017] 所述用户终端认证APP用所述协商得到的会话密钥解密所述认证信息密文，得到认证信息明文，验证用户终端的号码与认证信息明文的正确性，生成验证结果，将验证结果用私钥签名后发送给云认证服务器，所述验证结果包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号。

[0018] 优选地，所述的验证通过后，将验证结果发送给所述浏览器认证插件，包括：

[0019] 云认证服务器接收用户终端认证APP发送的验证结果，验证所述验证结果上的用户终端认证APP私钥签名有效后，在所述验证结果上添加自己的域名，用自己的私钥签名所述验证结果，将签名后的验证结果发送给浏览器认证插件。

[0020] 优选地，所述的浏览器认证插件将所述认证信息发送给所述网站的网站过滤器，所述网站过滤器验证所述认证信息中的IP地址、浏览器信息和操作系统信息正确后，允许所述用户终端登录所述网站，包括：

[0021] 浏览器认证插件接收到云认证服务器私钥签名后的验证结果后，将验证结果存储到Cookie域，并将云认证服务器私钥签名后的验证结果作为凭证发送给所述网站的网站过滤器；

[0022] 所述网站过滤器从证书权威处获取云认证服务器的公钥证书，用该云认证服务器的公钥证书验证所述验证结果上的云认证服务器私钥签名的真实性，验证成功后，确定所述凭证有效；

[0023] 所述网站过滤器验证所述验证结果中的登录主机的IP地址、有效期的有效性通过，并且验证所述验证结果中的浏览器名称与版本号、操作系统名称与版本号的正确性通过后，允许所述用户终端登录所述网站。

[0024] 一种广域网中对用户终端进行身份认证的系统，包括：浏览器认证插件、云认证服务器和网站过滤器；

[0025] 所述的浏览器认证插件，用于在用户终端通过浏览器登录网站后，获取所述用户终端的认证信息，将所述认证信息发送给云认证服务器，所述认证信息包括所述用户终端

的号码、密码、IP地址、浏览器信息和操作系统信息；在接收到所述云认证服务器返回的验证结果后，将所述认证信息发送给所述网站的网站过滤器；

[0026] 所述云认证服务器，用于通过与所述用户终端进行数据通信交互，对所述认证信息进行验证，验证通过后，将验证结果发送给所述浏览器认证插件；

[0027] 所述的网站过滤器验证，用于对所述认证信息中的IP地址、浏览器信息和操作系统信息正确后，允许所述用户终端登录所述网站。

[0028] 优选地，所述的系统还包括用户终端认证APP；

[0029] 所述的用户终端认证APP，用于在用户终端通过自带的浏览器登录网站后，在网站页面上输入用户终端的基本信息，该基本信息包括用户终端的号码、密码、IP地址与云认证服务器域名；通过云认证服务器与浏览器认证插件协商会话密码；

[0030] 所述的浏览器认证插件，用于接收所述用户终端的基本信息，获取所述用户终端的认证信息，该认证信息包括：用户终端的号码、密码、IP地址、云认证服务器域名、浏览器的名称与版本号、操作系统名称与版本号；

[0031] 使用密钥交换算法通过云认证服务器与用户终端认证APP协商会话密码，使用协商得到的会话密钥加密除用户终端的号码外的其它认证信息，得到认证信息密文，将所述认证信息密文和用户终端的号码发送给云认证服务器。

[0032] 优选地，所述的云认证服务器，具体用于与用户终端认证APP之间通过使用椭圆曲线算法验证私钥签名，定期相互进行认证身份，相互认证身份成功后，接收用户终端认证APP定期发送的用户终端基本信息，将接收到的基本信息关联存储在映射表中，该映射表中存储的信息包括：用户终端的号码、用户终端IP、公钥证书格式符合X.509证书标准；

[0033] 接收浏览器认证插件发送的用户终端的号码和认证信息密文后，根据用户终端的号码查询所述映射表，获取所述用户终端的号码对应的用户终端IP地址，根据获取的用户终端IP地址将认证信息密文和用户终端的号码转发给用户终端认证APP；

[0034] 所述的用户终端认证APP，具体用于用所述协商得到的会话密钥解密所述认证信息密文，得到认证信息明文，验证用户终端的号码与认证信息明文的正确性，生成验证结果，将验证结果用私钥签名后发送给云认证服务器，所述验证结果包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号。

[0035] 优选地，所述的云认证服务器，具体用于接收用户终端认证APP发送的验证结果，验证所述验证结果上的用户终端认证APP私钥签名有效后，在所述验证结果上添加自己的域名，用自己的私钥签名所述验证结果，将签名后的验证结果发送给浏览器认证插件。

[0036] 优选地，所述的浏览器认证插件，具体用于接收到云认证服务器私钥签名后的验证结果后，将验证结果存储到Cookie域，并将云认证服务器私钥签名后的验证结果作为凭证发给所述网站的网站过滤器；

[0037] 所述的网站过滤器，具体用于从证书权威处获取云认证服务器的公钥证书，用该云认证服务器的公钥证书验证所述验证结果上的云认证服务器私钥签名的真实性，验证成功后，确定所述凭证有效；

[0038] 验证所述验证结果中的登录主机的IP地址、有效期的有效性通过，并且验证所述验证结果中的浏览器名称与版本号、操作系统名称与版本号的正确性通过后，允许所述用户终端登录所述网站。

[0039] 由上述本发明的实施例提供的技术方案可以看出，本发明实施例提供了一种广域网中对用户终端进行身份认证的方法，通过浏览器认证插件获取用户终端的认证信息，将认证信息发送给云认证服务器和浏览器认证插件，采用基于实名用户终端的云身份认证技术，可以将登录网站的用户与实名的用户终端捆绑在一起，间接使用户终端实名化，克服了Web SSO方法中存在的缺点，能够快速、简单、有效地验证Web用户终端身份的真实性，以保证网络Web应用的安全性与可用性，给网络用户一个安全、可用的网络应用环境。

[0040] 本发明附加的方面和优点将在下面的描述中部分给出，这些将从下面的描述中变得明显，或通过本发明的实践了解到。

## 附图说明

[0041] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0042] 图1是本发明实施例一提供的一种广域网中用户终端云身份认证的方法的应用场景示意图；

[0043] 图2是本发明实施例一提供的一种广域网中对用户终端进行身份认证的方法的处理流程图；

[0044] 图3是本发明实施例一提供的一种浏览器认证插件的处理流程图；

[0045] 图4是本发明实施例一提供的一种云认证服务器的处理流程图；

[0046] 图5是本发明实施例一提供的一种手机认证APP的处理流程图；

[0047] 图6是本发明实施例一提供的一种网站过滤器的处理流程图；

[0048] 图7是本发明实施例二提供的一种广域网中对用户终端进行身份认证的系统中的信息交互时序图；

[0049] 图8是本发明实施例二提供的一种广域网中对用户终端进行身份认证的系统的具体实现结构图。

## 具体实施方式

[0050] 下面详细描述本发明的实施方式，所述实施方式的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施方式是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0051] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解，当我们称元件被“连接”或“耦接”到另一元件时，它可以直接连接或耦接到其他元件，或者也可以存在中间元件。此外，这里使用的“连接”或“耦接”可以包括无线连接或耦接。这里使用的措辞“和/或”包括一个或更多个相关联的列出项的任一单元和全部组合。

[0052] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语（包括技术

语和科学术语)具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是,诸如通用字典中定义的那些术语应该被理解为具有与现有技术的上下文中的意义一致的意义,并且除非像这里一样定义,不会用理想化或过于正式的含义来解释。

[0053] 为便于对本发明实施例的理解,下面将结合附图以几个具体实施例为例做进一步的解释说明,且各个实施例并不构成对本发明实施例的限定。

[0054] 实施例一

[0055] 本发明实施例采用基于实名用户终端的云身份认证技术,克服了Web SSO方法中存在的缺点,能够快速、简单、有效地验证Web用户身份的真实性。

[0056] 本发明实施例提供的一种广域网中云身份认证的方法的应用场景示意图如图1所示,该实施例提供了一种广域网中云身份认证的方法的处理流程如图2所示,包括如下的处理步骤:

[0057] 步骤S210、浏览器认证插件获取认证信息、与用户终端认证APP (Application, 计算机应用程序) 应用协商会话密钥、加密认证信息并发送给云认证服务器。

[0058] 用户终端通过自带的浏览器登录网站,在网站页面上输入用户终端的基本信息,该基本信息包括用户终端的号码、密码、IP地址与云认证服务器域名。

[0059] 本发明实施例提供的一种浏览器认证插件的处理流程图如图3所示,浏览器认证插件获取认证信息,该认证信息包括:用户终端的号码、密码、IP地址、云认证服务器域名、浏览器的名称与版本号、操作系统名称与版本号。

[0060] 浏览器认证插件使用Diffie-Hellman (Diffie-Hellman key exchange, 迪菲—赫尔曼密钥交换) 算法通过云认证服务器与用户终端认证APP协商会话密钥,浏览器认证插件使用协商得到的会话密钥加密除用户终端的号码外的其它认证信息,得到认证信息密文。然后,浏览器认证插件将上述认证信息密文和用户终端的号码发送给云认证服务器。

[0061] 步骤S220、云认证服务器转发认证信息密文和用户终端的号码给用户终端认证APP。

[0062] 本发明实施例提供的一种云认证服务器的处理流程图如图4所示,云认证服务器与用户终端认证APP通过使用椭圆曲线算法验证私钥签名,定期进行相互身份认证,相互身份认证成功后,云认证服务器接收用户终端认证APP定期发送的用户终端的号码与用户终端IP地址等信息,将接收到的信息关联存储在映射表中,该映射表中存储的信息包括:用户终端的号码、用户终端IP;公钥证书格式(符合X.509证书标准)。

[0063] 云认证服务器接收浏览器认证插件发送的用户终端的号码和认证信息密文后,根据用户终端的号码查询上述映射表,获取该用户终端的号码对应的用户终端IP地址。然后,云认证服务器根据获取的用户终端IP地址将认证信息密文和用户终端的号码发送给用户终端认证APP。

[0064] 步骤S230、用户终端认证APP验证用户终端的号码和认证信息明文的正确性,将验证结果发送给云认证服务器。

[0065] 本发明实施例提供的一种手机认证APP的处理流程图如图5所示,用户终端认证APP接收云认证服务器转发的认证信息密文和用户终端的号码后,用上述协商得到的会话密钥解密认证信息密文,得到认证信息明文,验证用户终端的号码与认证信息明文的正确性,生成验证结果。

[0066] 然后,用户终端认证APP将验证结果用私钥签名后发送给云认证服务器,当上述用户终端的号码与认证信息明文的正确性验证通过后,则验证结果中包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号。当上述用户终端的号码与认证信息明文的正确性验证不通过后,则验证结果中包括验证不通过信息。

[0067] 步骤S240、云认证服务器用私钥签名验证结果后转发给浏览器认证插件。

[0068] 云认证服务器接收用户终端认证APP发送的验证结果,云认证服务器验证验证结果上的用户终端认证APP私钥签名的有效后,当验证结果中包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号时,云认证服务器在验证结果后添加域名,用自己的私钥签名验证结果后,将云认证服务器私钥签名后的验证结果转发给浏览器认证插件。

[0069] 当验证结果中包括验证不通过信息,则云认证服务器将验证不通过信息发送给浏览器认证插件。

[0070] 步骤S250、浏览器认证插件将验证结果作为凭证发送给登录的网站过滤器;

[0071] 浏览器认证插件接收云认证服务器私钥签名后的验证结果后,将验证结果存储到Cookie域,并将云认证服务器私钥签名后的验证结果作为凭证发送给登录的网站过滤器。

[0072] 浏览器认证插件接收云认证服务器发送的验证不通过信息后,将验证不通过信息发送给移动终端。

[0073] 步骤S260、网站过滤器允许拥有签名真实、凭证有效、IP地址和有效期有效、浏览器与系统正确的用户登录该网站。

[0074] 本发明实施例提供的一种网站过滤器的处理流程图如图6所示,网站过滤器从证书权威处获取云认证服务器的公钥证书,用该云认证服务器的公钥证书验证验证结果上的云认证服务器私钥签名的真实性。验证成功后,确定上述凭证有效,即确定上述验证结果上的云认证服务器私钥签名有效。

[0075] 网站过滤器验证验证结果中的登录主机的IP地址、有效期的有效性,验证浏览器名称与版本号、操作系统名称与版本号的正确性;

[0076] 网站过滤器验证所述验证结果中的登录主机的IP地址、有效期的有效性通过,并且验证所述验证结果中的浏览器名称与版本号、操作系统名称与版本号的正确性通过后,允许所述用户终端登录所述网站。即允许拥有签名真实、凭证有效、IP地址和有效期有效、浏览器与系统正确的用户登录该网站。

[0077] 实施例二

[0078] 广域网中用户终端身份认证的通用工作流程包括:

[0079] 浏览器认证阶段,包括获取认证信息、会话密钥协商、加密、解密、通信;

[0080] 网站过滤阶段,包括过滤、证书管理;

[0081] 云认证服务阶段,包括解析转发、私钥签名、证书管理;

[0082] 智能手机认证APP认证阶段,包括通信、会话密钥协商、加密、解密、认证、密码管理。

[0083] 该实施例提供了一种广域网中对用户终端进行身份认证的系统中的信息交互时序图如图7所示,其中,浏览器能够请求与展示Web网站信息,Web网站包括Web应用服务器、Web应用程序,实名智能手机具有IP地址,能够接入TCP/IP网络,广域网包括路由器与交换

机,可以传送和路由网络流量。上述系统的具体实现结构如图8所示,具体可以包括如下的模块:网站过滤器81、浏览器认证插件82、云认证服务器83和用户终端认证APP84。

[0084] 所述的浏览器认证插件82,用于在用户终端通过浏览器登录网站后,获取所述用户终端的认证信息,将所述认证信息发送给云认证服务器,所述认证信息包括所述用户终端的号码、密码、IP地址、浏览器信息和操作系统信息;在接收到所述云认证服务器返回的验证结果后,将所述认证信息发送给所述网站的网站过滤器;

[0085] 所述云认证服务器83,用于通过与所述用户终端进行数据通信交互,对所述认证信息进行验证,验证通过后,将验证结果发送给所述浏览器认证插件;

[0086] 所述的网站过滤器验证81,用于对所述认证信息中的IP地址、浏览器信息和操作系统信息正确后,允许所述用户终端登录所述网站。

[0087] 所述的用户终端认证APP84,用于在用户终端通过自带的浏览器登录网站后,在网站页面上输入用户终端的基本信息,该基本信息包括用户终端的号码、密码、IP地址与云认证服务器域名;通过云认证服务器与浏览器认证插件协商会话密码;

[0088] 所述的浏览器认证插件,用于接收所述用户终端的基本信息,获取所述用户终端的认证信息,该认证信息包括:用户终端的号码、密码、IP地址、云认证服务器域名、浏览器的名称与版本号、操作系统名称与版本号;

[0089] 使用密钥交换算法通过云认证服务器与用户终端认证APP协商会话密码,使用协商得到的会话密钥加密除用户终端的号码外的其它认证信息,得到认证信息密文,将所述认证信息密文和用户终端的号码发送给云认证服务器。

[0090] 进一步地,所述的云认证服务器83,具体用于与用户终端认证APP之间通过使用椭圆曲线算法验证私钥签名,定期相互进行认证身份,相互认证身份成功后,接收用户终端认证APP定期发送的用户终端基本信息,将接收到的基本信息关联存储在映射表中,该映射表中存储的信息包括:用户终端的号码、用户终端IP、公钥证书格式符合X.509证书标准;

[0091] 接收浏览器认证插件发送的用户终端的号码和认证信息密文后,根据用户终端的号码查询所述映射表,获取所述用户终端的号码对应的用户终端IP地址,根据获取的用户终端IP地址将认证信息密文和用户终端的号码转发给用户终端认证APP;

[0092] 所述的用户终端认证APP84,具体用于用所述协商得到的会话密钥解密所述认证信息密文,得到认证信息明文,验证用户终端的号码与认证信息明文的正确性,生成验证结果,将验证结果用私钥签名后发送给云认证服务器,所述验证结果包括用户终端的号码、登录主机IP地址、有效期、浏览器名称与版本号、操作系统名称与版本号。

[0093] 进一步地,所述的云认证服务器83,具体用于接收用户终端认证APP发送的验证结果,验证所述验证结果上的用户终端认证APP私钥签名有效后,在所述验证结果上添加自己的域名,用自己的私钥签名所述验证结果,将签名后的验证结果发送给浏览器认证插件。

[0094] 进一步地,所述的浏览器认证插件82,具体用于接收到云认证服务器私钥签名后的验证结果后,将验证结果存储到Cookie域,并将云认证服务器私钥签名后的验证结果作为凭证发送给所述网站的网站过滤器;

[0095] 所述的网站过滤器81,具体用于从证书权威处获取云认证服务器的公钥证书,用该云认证服务器的公钥证书验证所述验证结果上的云认证服务器私钥签名的真实性,验证成功后,确定所述凭证有效;

[0096] 验证所述验证结果中的登录主机的IP地址、有效期的有效性通过，并且验证所述验证结果中的浏览器名称与版本号、操作系统名称与版本号的正确性通过后，允许所述用户终端登录所述网站。

[0097] 用本发明实施例的系统进行广域网中对用户终端进行身份认证的具体过程与前述方法实施例类似，此处不再赘述。

[0098] 综上所述，本发明实施例提供了一种广域网中对用户终端进行身份认证的方法，通过浏览器认证插件获取用户终端的认证信息，将认证信息发送给云认证服务器和浏览器认证插件，采用基于实名用户终端的云身份认证技术，可以将登录网站的用户与实名的用户终端捆绑在一起，间接使用户终端实名化，克服了Web SSO方法中存在的缺点，能够快速、简单、有效地验证Web用户终端身份的真实性，以保证网络Web应用的安全性与可用性，给网络用户一个安全、可用的网络应用环境。

[0099] 本发明实施例的对用户终端进行身份认证的方法没有使用Cookie技术，可以在不泄漏用户个人信息与上网行为等隐私信息的前提下，快速、简单、有效地认证登录网站的用户终端身份的真实性的同时，也保证了审计信息的线下可追踪性。

[0100] 本领域普通技术人员可以理解：附图只是一个实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

[0101] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机、服务器、或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0102] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置或系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的装置及系统实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0103] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

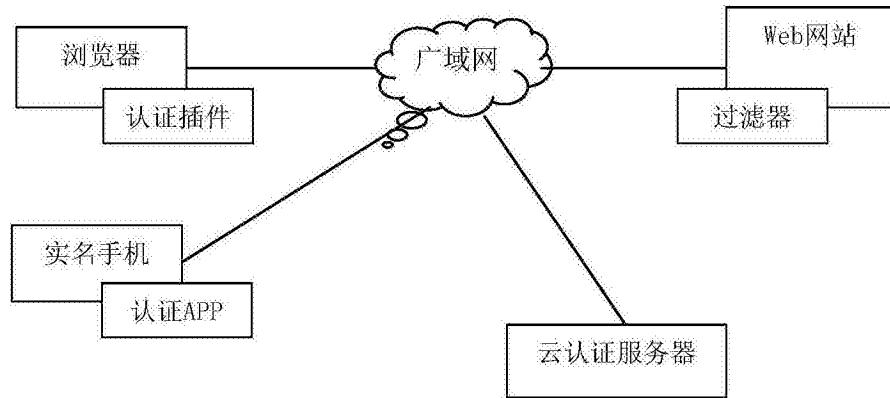
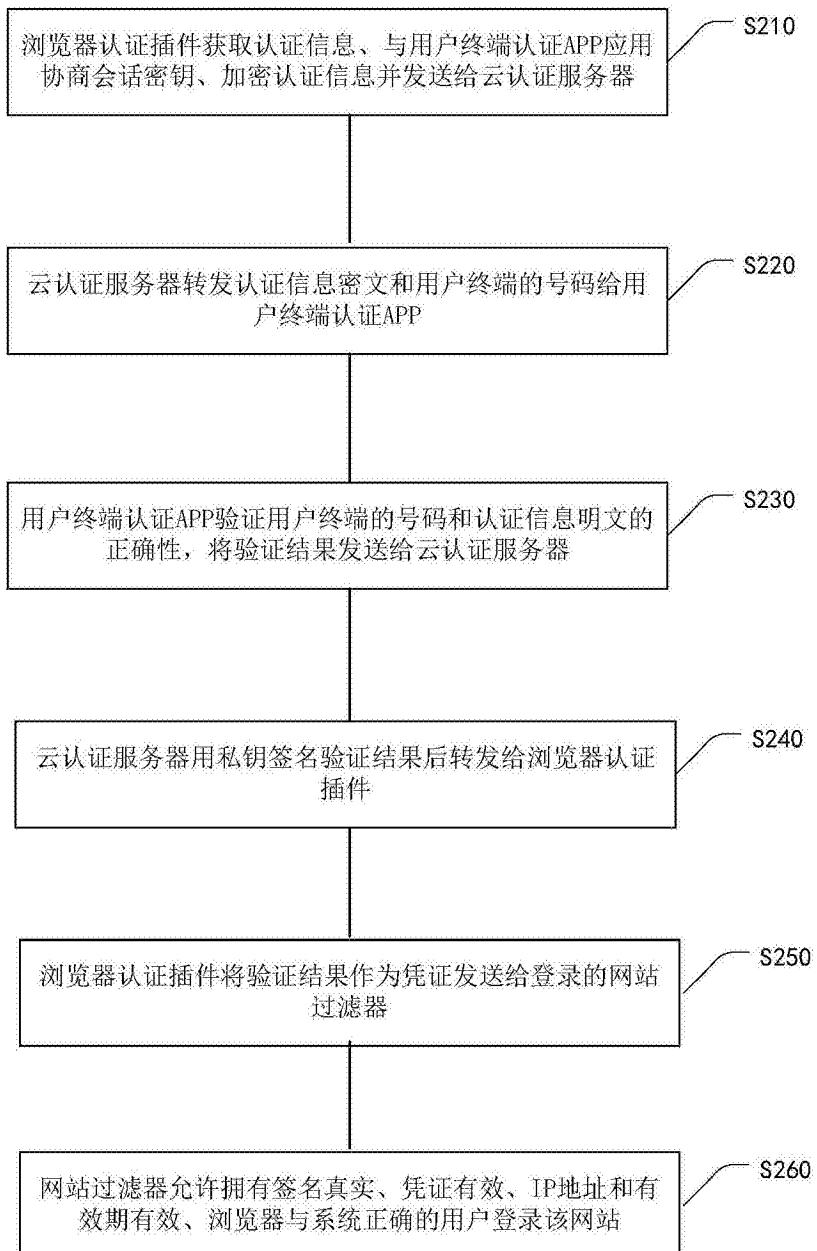


图1



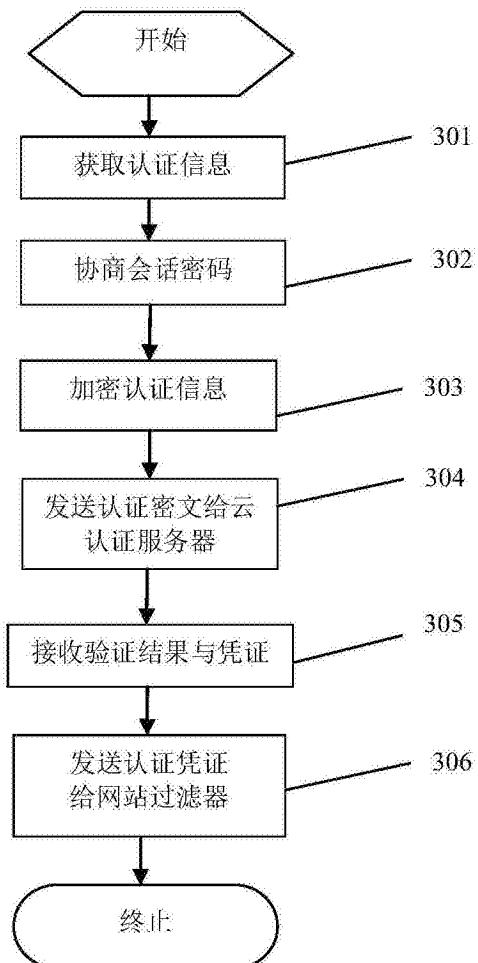


图3

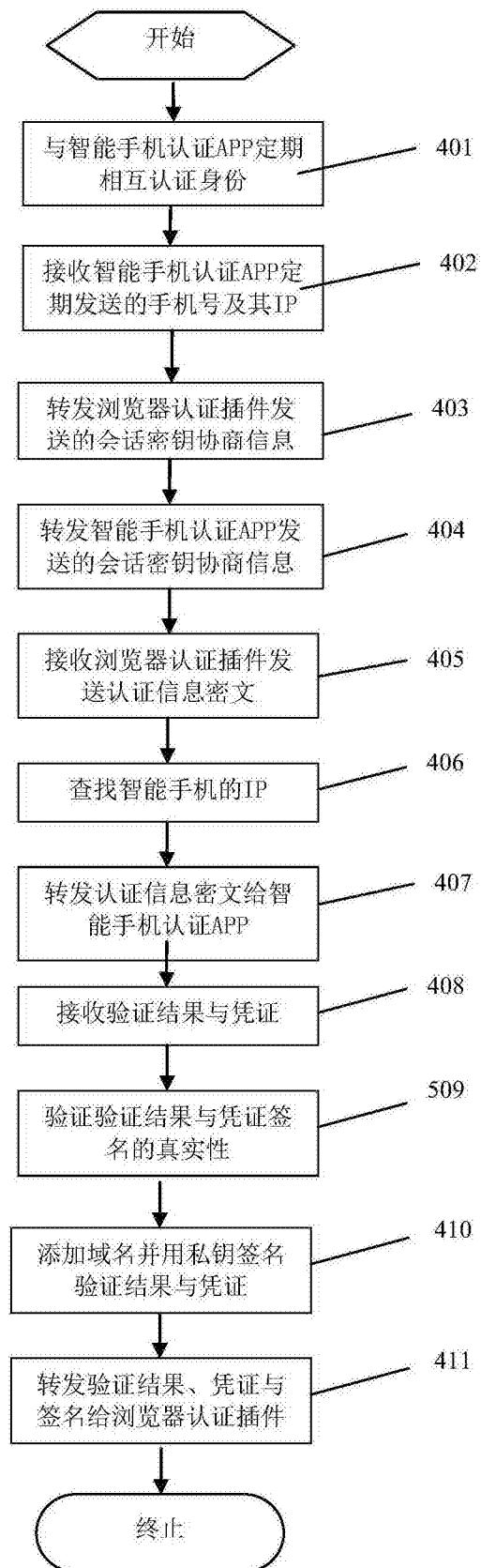


图4

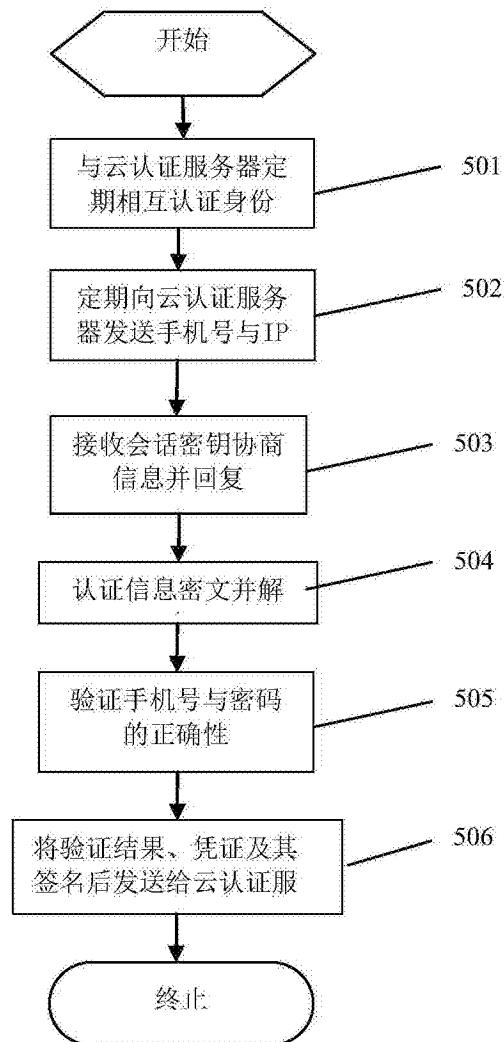


图5

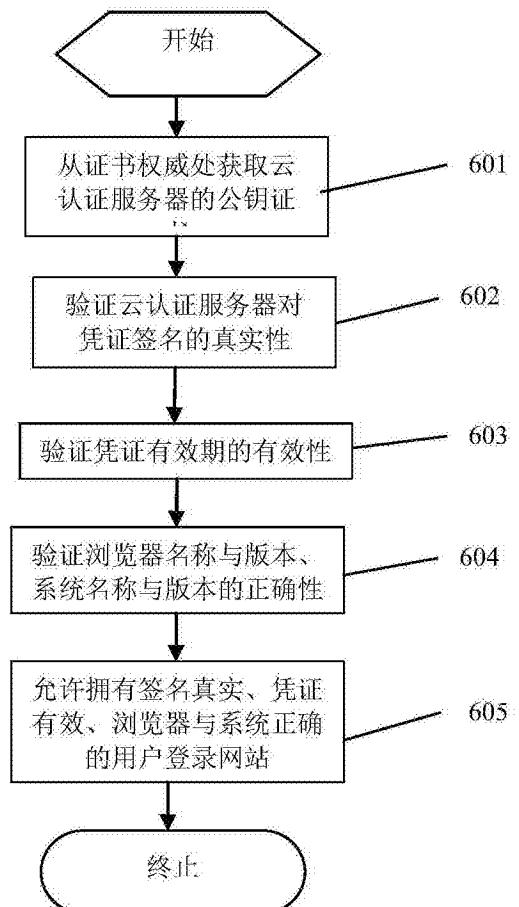


图6

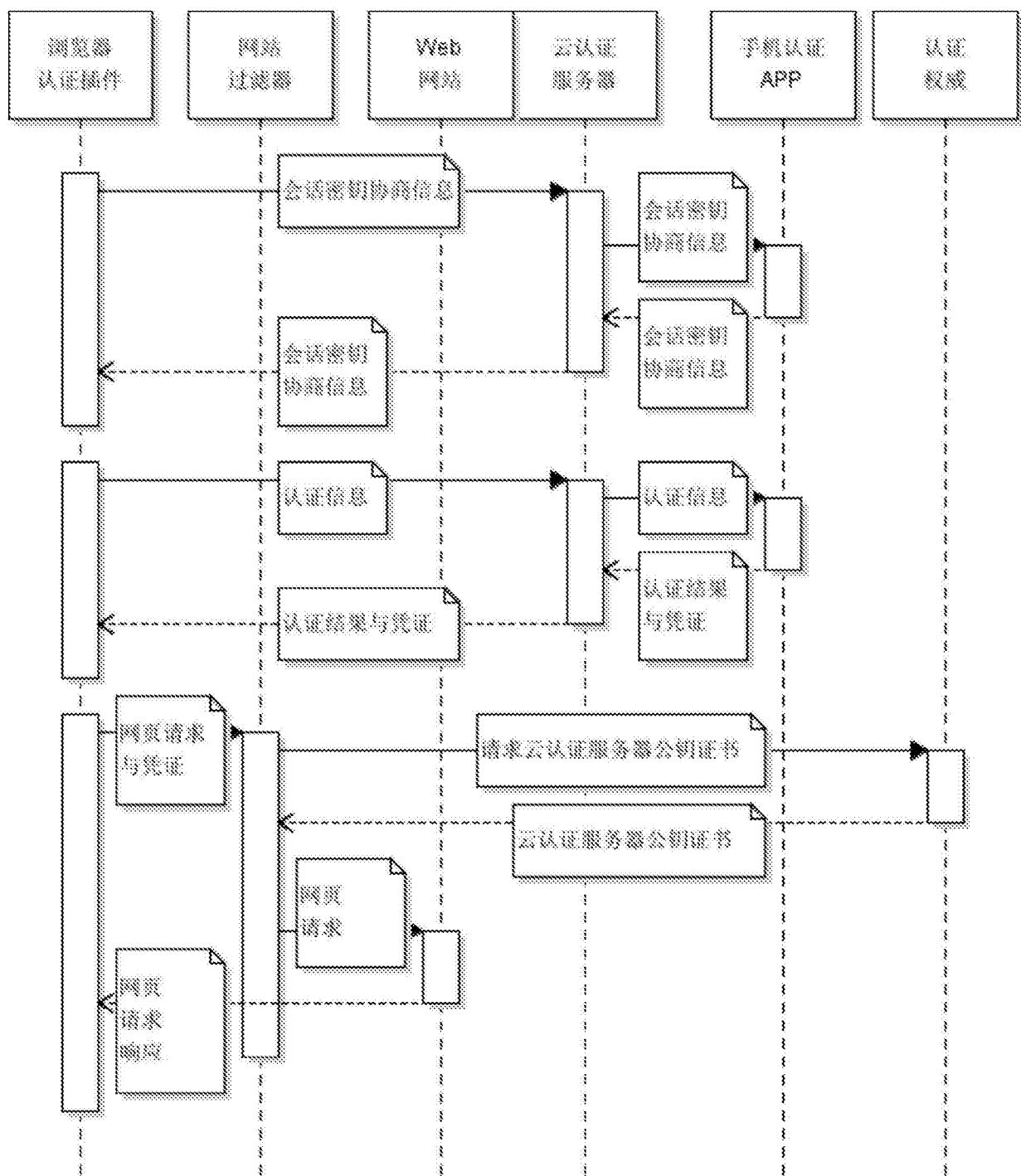


图7

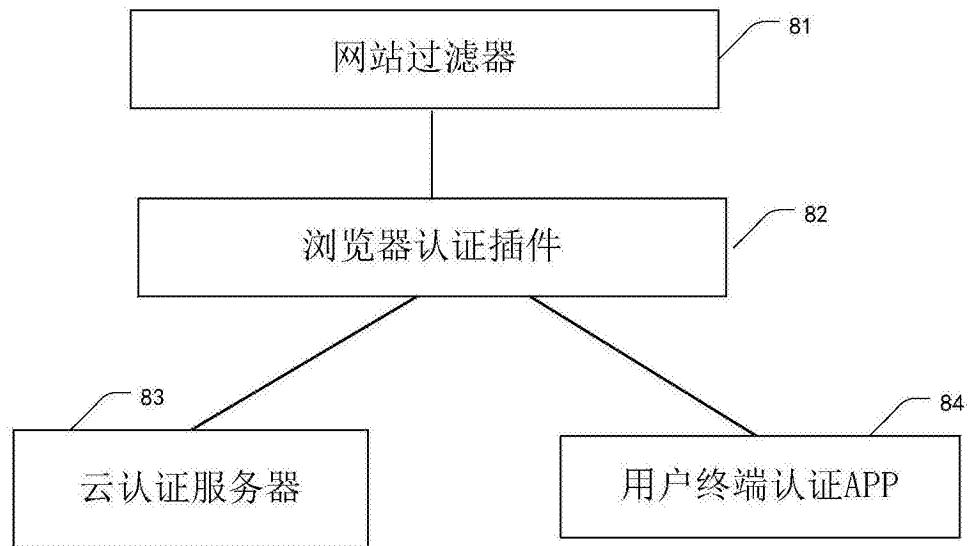


图8