



(12) 发明专利申请

(10) 申请公布号 CN 103856438 A

(43) 申请公布日 2014. 06. 11

(21) 申请号 201210497240. 8

(22) 申请日 2012. 11. 28

(71) 申请人 卡巴斯克

地址 瑞典哥特堡

(72) 发明人 林茂聪 P·史柏格

(74) 专利代理机构 上海一平知识产权代理有限公司 31266

代理人 须一平

(51) Int. Cl.

H04L 29/06 (2006. 01)

H04L 9/32 (2006. 01)

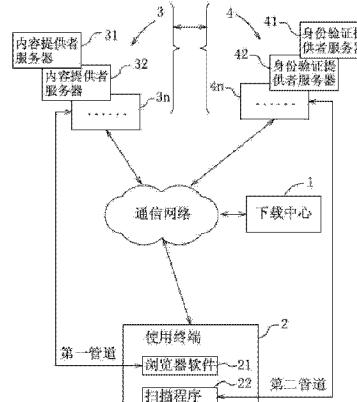
权利要求书1页 说明书6页 附图5页

(54) 发明名称

具安全性保护的自动转址及网络身份验证方法

(57) 摘要

一种具安全性保护的自动转址及网络身份验证方法，应用于一内容提供服务器、一身份验证服务器、一使用终端及一下载中心，该方法包括下述步骤：日常使用时，使用终端浏览内容提供服务器的网站，内容提供服务器的网站提供一脚本给使用终端，该脚本内含内容提供者委托帮其做身份认证的身份验证服务器的网页位址，该脚本受该使用终端触发后，使用终端的扫描程序便和该身份验证服务器相连，要求身份验证服务器下传前述经下载中心的私钥签过名的该身份验证服务器的网页位址，并用使用终端内存的下载中心的公钥来辨别其是否真正来自下载中心，若是，终端扫描程序便扫描使用终端产生一硬件扫描资料并上传该身份验证服务器储存以供后续使用者的身份比对。



1. 一种具安全性保护的自动转址及网络身份验证方法,应用于一内容提供者服务器、一身份验证提供者服务器、一使用终端及一下载中心,其特征在于:所述方法包括下述步骤:

(a) 该身份验证提供者服务器取得该下载中心事先用一非对称私钥签过名的该身份验证提供者服务器的网页位址,且该使用终端已从该下载中心下载内含有该下载中心的一非对称公钥及一扫描程序;

(b) 该使用终端浏览该内容提供者服务器的网站,该内容提供者服务器的网站提供一脚本给使用终端,该脚本内含该内容提供者服务器的业者委托进行身份认证的该身份验证提供者服务器的网页位址;及

(c) 该脚本受该使用终端触发后,该使用终端的扫描程序和该身份验证提供者服务器相连并要求身份验证提供者服务器下传前述经该下载中心的私钥签过名的该身份验证提供者服务器的网页位址,并用该使用终端内存该下载中心的公钥来辨别其是否真正来自该下载中心,若结果是真实,该扫描程序便扫描该使用终端且产生一硬件扫描资料并上传给该身份验证提供者服务器储存以供后续使用者的身份比对。

2. 如权利要求1所述的具安全性保护的自动转址及网络身份验证方法,其特征在于:所述使用终端随时直接和该下载中心相连,并请求该下载中心辨识取得的签过名的身份验证提供者服务器的网页位址是否真实,或下载其他新的公钥以防止黑客攻击或非签约的身份验证提供者服务器非法使用其技术及服务。

3. 如权利要求2所述的具安全性保护的自动转址及网络身份验证方法,其特征在于:所述扫描程序是扫描包括该使用终端的一中央处理单元、一基本输入输出系统单元、一储存装置、一网络界面、一主机板的识别码及一有线或无线近距离连接的外接装置的其中至少二硬件元件的识别码组合。

4. 如权利要求3所述的具安全性保护的自动转址及网络身份验证方法,其特征在于:所述扫描程序还对所扫描的所述硬件元件的地理位置进行定位,并在该身份验证提供服务器查验身份时,判断当时扫描的所述硬件元件是否处于相同的地理位置以决定使用者身份。

5. 如权利要求1所述的具安全性保护的自动转址及网络身份验证方法,其特征在于:所述内容提供者服务器提供数个不同的身份验证提供者让使用者选择,且提供给该使用终端的脚本内含该使用者所选择的身份验证提供者服务器的网页位址以进行身份登录及验证。

具安全性保护的自动转址及网络身份验证方法

技术领域

[0001] 本发明涉及一种网络身份验证方法,特别是涉及一种经由第三方下载中心提供给内容提供者 (Internet Content Provider, 以下简称 ICP) 及身份验证提供者 (Identity Provider, 以下简称 IDP) 使用的安全、有弹性及让使用者方便的身份认证方式,亦让内容提供者可自由选择所信赖的身份验证提供者来确认使用者身份的具安全性保护的自动转址及网络身份验证方法。

背景技术

[0002] 蓬勃的各种网络服务,尤其是云端服务将带来各种今天仍没见到的新网络加值服务,但安全的身份验证而且能被普遍使用是使这些未来的便利的服务能成为事实的先决条件。

[0003] 然而,现有的各种硬件身份验证产品,如 :装有 PKI 证书的 USB 装置、IC 电子卡,或动态密码电子令牌 (token) 等身份验证硬件产品,但是整体的成本太高。另外,现有的网络身份验证,仍然是各网络服务商各自有自己的用户名和密码库及相对的身份验证产品,对于各网络业者而言,造成了重复投资的问题;而对于使用者而言,使用者得同时记住各种不同用户名密码及需要购买各种不同身份验证硬件产品,降低使用意愿。

发明内容

[0004] 目前的网络身份验证因市场已经往专业的独立第三方验证的身份验证提供者的系统发展,这样可避免各内容提供者的系统管理使用者身份验证资料的成本支出,使用者也免去记忆不同 ID 及密码的麻烦及购买各种不同身份验证硬件产品。

[0005] 因此,本发明是在提供一种具有前述优点的具安全性保护的自动转址及网络身份验证方法。

[0006] 本发明具安全性保护的自动转址及网路身份验证方法是应用于一内容提供者服务器、一身份验证提供者服务器、一使用终端及一下载中心,该方法包括下述步骤:(a) 该身份验证提供者服务器取得该下载中心事先用一非对称私钥签过名的该身份验证提供者服务器的网页位址,且该使用终端已从该下载中心下载内含有该下载中心的一非对称公钥及一扫描程序;(b) 该使用终端浏览该内容提供者服务器的网站,该内容提供者服务器的网站提供一脚本给使用终端,该脚本内含该内容提供者服务器的业者委托进行身份认证的该身份验证提供者服务器的网页位址;(c) 该脚本受该使用终端触发后,该使用终端的扫描程序和该身份验证提供者服务器相连并要求身份验证提供者服务器下传前述经该下载中心的私钥签过名的该身份验证提供者服务器的网页位址,并用该使用终端内存该下载中心的公钥来辨别其是否真正来自该下载中心,若结果是真实,该扫描程序便扫描该使用终端且产生一硬件扫描资料并上传给该身份验证提供者服务器储存以供后续使用者的身份比对。

[0007] 较佳的,该使用终端可随时直接和该下载中心相连,并请求该下载中心辨识取得

的签过名的身份验证提供者服务器的网页位址是否真实,或下载其他新的公钥以防止黑客攻击或非签约的身份验证提供者服务器非法使用其技术及服务。

[0008] 较佳的,该扫描程序是扫描包括该使用终端的一中央处理单元、一基本输入输出系统单元、一储存装置、一网络界面、一主机板的识别码及一有线或无线近距离连接的外接装置的其中至少二硬件元件的识别码组合。

[0009] 较佳的,该扫描程序还可取得对于所扫描的这些硬件元件的地理位置进行定位,并在该身份验证提供服务器查验身份时,判断当时扫描的这些硬件元件是否处于相同的地理位置以决定使用者身份。

[0010] 较佳的,该内容提供者服务器可提供数个不同的身份验证提供者让使用者选择,且提供给该使用终端的脚本内含该使用者所选择的身份验证提供者服务器的网页位址以进行身份登录及验证

[0011] 本发明具安全性保护的自动转址及网络身份验证方法的功效在于:内容提供者服务器、身份验证提供者服务器及使用终端可利用同一下载中心及同一扫描程序来做身份认证,免去重复投资,且内容提供者服务器及使用者都可自由选择身份验证提供者服务器,避免远端的网络黑客盗用身份资料,以及配合多重身份验证方式加强确认使用者本人的真实身份,因此,可加强验证使用者身份安全的保障,并且无需额外的身份识别硬件成本及维护,可增加业者及使用者的意愿。

附图说明

[0012] 图 1 是说明本发明具安全性保护的自动转址及网络身份验证方法的相关应用装置的系统方块图;

[0013] 图 2 是说明本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例中,下载中心 1 对应不同身份验证提供者服务器提供用其非对称私钥签过名的 IDP 网页位址以及提供不同使用终端来下载共用的扫描程序及相对的公钥的流程图;

[0014] 图 3 是说明本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例中的身份登录过程的流程图;

[0015] 图 4 是说明本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例中的身份验证过程的流程图;

[0016] 图 5 是说明本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例中,提供多种不同身份验证提供者的选项供使用终端选择以进行身份登录过程的流程图;

[0017] 图 6 是说明本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例中,提供多种不同身份验证提供者的选项供使用终端选择以进行身份验证过程的流程图。

具体实施方式

[0018] 下面结合附图及实施例对本发明进行详细说明。在本发明被详细描述之前,要注意的是,在以下的数个较佳实施例的详细说明内容中,类似的元件是以相同的编号来表示。

[0019] 参阅图 1,本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例,是应用于一下载中心 1、一使用终端 2、一内容提供者服务器群集 3 及一身份验证提供者服务器群集 4,各装置分别介绍如下。

[0020] 内容提供者服务器群集 3 包括多数个分别属于不同网站服务业者的内容提供者服务器 31-3n, 例如 : 网络银行、拍卖网站、线上游戏业者等。身份验证提供者服务器群集 4 包括多数个分别属于不同 ID 管理业者的身份验证提供者服务器 41-4n, 也就是提供第三方网络身份验证服务的如 Google、Yahoo、Facebook 等系统。

[0021] 内容提供者服务器 31-3n、身份验证提供者服务器 41-4n、下载中心 1 及使用终端 2 以通信网络彼此连接及传递资料。

[0022] 使用终端 2 安装有一浏览器软件 21 及一扫描程序 22, 浏览器软件 21 是供使用者浏览内容提供者服务器 31-3n 的网站, 扫描程序 22 是用于扫描使用终端 2 的多个硬件元件成识别码记录成一硬件扫描清单, 扫描程序 22 是由下载中心 1 下载。

[0023] 较佳的, 扫描程序 22 是扫描包括使用终端 2 的一中央处理单元、一基本输入输出系统单元、一储存装置、一网络界面、一主机板的识别码及一有线或无线近距离连接的外接装置的其中至少二硬件元件的识别码组合 ; 此外, 扫描程序 22 还可取得对于所扫描的这些硬件元件的地理位置进行定位, 并在该身份验证提供者服务器 41-4n 查验身份时, 判断当时扫描的这些硬件元件是否处于相同的地理位置以决定使用者身份。

[0024] 本发明具安全性保护的自动转址及网络身份验证方法的原理包括下述步骤 : 使用终端 2 经一第一管道浏览该内容提供者服务器 41 的网站, 内容提供者服务器 41 的网站由此第一管道提供一脚本 (如 : JAVA Script) 内含内容提供者委托帮其做身份认证的身份验证提供者服务器 41 的网页位址 (URL) 给使用终端 2, 该脚本受该使用终端 2 触发后, 使用终端 2 的扫描程序 22 便经由一不同于该第一管道的第二管道链结至该对应的身份验证提供者, 要求该身份验证提供者下传上述经下载中心 1 私钥签过名的该身份验证提供者服务器 41 的网页位址, 并用其内存下载中心 1 的公钥来辨别其是否真正来自下载中心 1, 若结果是真实, 扫描程序 22 便扫描使用终端 2, 产生一硬件扫描资料, 并经由上述第二管道上传给该身份验证提供者服务器 41 储存以供后续使用者的身份比对。

[0025] 本发明具安全性保护的自动转址及网络身份验证方法的较佳实施例包括如图 2 的网页位址签名及公钥分送程序、如图 3 的身份登录程序及如图 4 的身份验证程序, 以下配合图 1 的装置将本发明方法的各程序介绍如下。

[0026] 参阅图 2, 下载中心 1 是对应不同的身份验证提供者服务器 41、42 提供经其非对称私钥签过名的各身份验证提供者服务器 41、42 的网页位址, 在本实施例中, 下载中心 1 首先产生一非对称密钥对, 例如 : 符合非对称公钥技术的一公钥及一私钥, 并对每一签过约的身份验证提供者服务器 41、42 提供经下载中心 1 私钥签过名的身份验证提供者服务器 41、42 的网页位址给身份验证提供者服务器 41 (步骤 S201) 及身份验证提供者服务器 42 (步骤 S202) 以及在使用终端 2 由下载中心 1 下载扫描程序 22 时提供该公钥给该使用终端 2 (步骤 S203 及步骤 S204) 。

[0027] 参阅图 3, 本发明方法的登录程序中, 使用终端 2 使用浏览器软件 21 浏览内容提供者服务器 31 的网站, 且使用终端 2 是经由一第一管道传递一登录资料 (例如, 使用者 ID 及密码) 给内容提供者服务器 31 (步骤 S301), 内容提供者服务器 31 验证登录资料无误后, 即提供脚本内含 ICP 委托帮其做身份认证的身份验证提供者服务器 41 的网页位址给使用终端 2 (步骤 S302) 并同时请求该身份验证提供者服务器 41 进行用户身份登录工作 (步骤 S303) ; 该脚本受该使用终端触发后, 使用终端 2 扫描程序 22 便经由一不同于该第一管道的

第二管道链结至该对应身份验证提供者服务器 41(步骤 S304),要求该身份验证提供者服务器 41 下传前述经下载中心 1 私钥签过名的该身份验证提供者服务器 41 的网页位址(步骤 S305);并用其内存下载中心 1 的公钥来辨别其是否真正来自下载中心 1(步骤 S306),若结果是真实,扫描程序 22 便扫描使用终端 2 产生一硬件扫描资料(步骤 S307),再经由上述第二管道传递硬件扫描资料给身份验证提供者服务器 41 储存以供后续使用者的身份比对(步骤 S308),身份验证提供者服务器 41 并同通知内容提供者服务器 31 登录已经成功(步骤 309)。

[0028] 由于身份验证提供者服务器 41 留存有对应不同使用者的登录资料相对应的使用终端 2 的硬件扫描资料,由于使用者利用随身的使用终端 2 的硬件扫描资料作为身份验证之用,让第三人无法轻易窃取或盗用。此外,使用终端 2 可随时直接和下载中心 1 相连,并请求下载中心 1 辨识取得的签过名的身份验证提供者服务器 41 的网页位址是否真实,或下载其他新的公钥以防止黑客攻击或非签约的身份验证提供者服务器 41 非法使用其技术及服务

[0029] 参阅图 4,当使用终端 2 完成如图 3 的身份登录程序后,在下一次使用浏览器软件 21 浏览内容提供者服务器 31 的网站时,使用终端 2 经由第一管道传递该登录资料(例如,使用者 ID 及密码)给内容提供者服务器 31(步骤 S401),内容提供者服务器 31 验证登录资料无误后,即提供脚本内含内容提供者委托帮其做身份认证的身份验证提供者服务器 41 的网页位址给使用终端 2(步骤 S402) 并同时请求该身份验证提供者服务器 41 做用户身份认证工作(步骤 403);该脚本受该使用终端 2 触发后,使用终端 2 的扫描程序 22 便经由一不同于该第一管道的第二管道链结至该对应身份验证提供者服务器 41(步骤 S404);要求该身份验证提供者服务器 41 下传前述经下载中心 1 私钥签过名的该身份验证提供者服务器 41 的网页位址(步骤 S405);并用其内存下载中心 1 的公钥来辨别其是否真正来自下载中心 1(步骤 S406),若结果是真实,扫描程序 22 便扫描使用终端 2 产生一硬件扫描资料(步骤 S407),再经由上述第二管道传递硬件扫描资料给身份验证提供者服务器 41(步骤 S408);身份验证提供者服务器 41 查验使用终端 2 的硬件扫描资料与该使用终端 2 预存的硬件扫描资料是否相符(步骤 S409),借此,身份验证提供者服务器 41 将查验结果回传给内容提供者服务器 31(步骤 S410) 以决定是否允许使用终端 2 登录内容提供者服务器 31。

[0030] 参阅图 5,本发明方法的登录程序还可提供多个身份验证提供者服务器 41、42 的选项给使用者,其方式为:使用终端 2 使用浏览器软件 21 浏览内容提供者服务器 31 的网站,且使用终端 2 是经由第一管道传递一登录资料(例如,使用者 I D 及密码)给内容提供者服务器 31(步骤 S501),内容提供者服务器 31 验证登录资料无误后,即提供身份验证提供者服务器 41、42 的选项(步骤 S502),使用终端 2 即可发送选取身份验证提供者服务器 42 的指令给内容提供者服务器 31(步骤 S503);内容提供者服务器 31 并同时请求该身份验证提供者服务器 42 做用户身份登录工作(步骤 S504)。

[0031] 接着,内容提供者服务器 31 提供一脚本内含身份验证提供者服务器 42 的网页位址给使用终端 2(步骤 S505),使用终端 2 触发脚本后,使用终端扫描程序 22 便经由一不同于该第一管道的第二管道链结至该对应身份验证提供者(步骤 S506);要求该身份验证提供者服务器 42 下传前述经下载中心 1 私钥签过名的该身份验证提供者服务器 42 的网页位址(步骤 S507);并用其内存下载中心 1 的公钥来辨别其是否真正来自下载中心 1(步骤

S508),若结果是真实,扫描程序 22 便扫描使用终端 2 产生一硬件扫描资料(步骤 S509),再经由上述第二管道传递硬件扫描资料给身份验证提供者服务器 42 储存以供后续使用者的身份比对(步骤 S510),身份验证提供者服务器 42 并通知内容提供者服务器 31 身份登录成功(步骤 S511)。

[0032] 参阅图 6,当使用终端 2 完成如图 5 的身份登录程序后,在下一次使用浏览器软件 21 浏览内容提供者服务器 31 的网站时,使用终端 2 经由第一管道传递该登录资料(例如,使用者 ID 及密码)给内容提供者服务器 31(步骤 S601),内容提供者服务器 31 验证登录资料无误后,即提供身份验证提供者服务器 41、42 的选项(步骤 S602),使用终端 2 即可发送选取身份验证提供者服务器 42 的指令给内容提供者服务器 31(步骤 S603)。

[0033] 然后,内容提供者服务器 31 即提供一脚本内含身份验证提供者服务器 42 的网页位址给使用终端 2(步骤 S604)并同时请求该身份验证提供者做用户身份认证工作(步骤 S605),该脚本受使用终端 2 触发后,使用扫描程序 22 便经由一不同于该第一管道的第二管道链结至该对应身份验证提供者服务器 42(步骤 S606);要求该身份验证提供者服务器 42 下传前述经下载中心 1 私钥签过名的该身份验证提供者服务器的网页位址(步骤 S607);并用其内存下载中心 1 的公钥来辨别其是否真正来自下载中心 1(步骤 S608),若结果是真实,扫描程序 22 便扫描使用终端 2 产生一硬件扫描资料(步骤 S609),再经由上述第二管道传递硬件扫描资料给身份验证提供者服务器 42(步骤 S610);身份验证提供者服务器 42 查验使用终端 2 的硬件扫描资料与该使用终端 2 预存的硬件扫描资料是否相符(步骤 S611),借此,身份验证提供者服务器 42 将查验结果回传给内容提供者服务器 31(步骤 S612)以决定是否允许使用终端 2 登录内容提供者服务器 31,如此一来,即提供使用终端 2 更为多元的身份验证提供者服务器 41-4n 的不同选择来进行身份验证。

[0034] 从长远来看,本发明可改变网络身份认证产业生态,提供一个各身份验证提供者在相同条件下自由竞争,提供各有特色及不同价值的安全认证服务,使用者有选择权,且随时可更换身份验证提供者业者,内容提供者可以专注于其核心业务,把身份认证交给第三方身份验证提供者及让其使用者选择自己信任的身份验证提供者,本发明真正用到互联网这样一个开放环境且符合其精神可以自由竞争,自由选择的安全身份认证。

[0035] 综合以上所述,本发明具安全性保护的自动转址及网络身份验证方法的有益效果在于:

[0036] 1. 本发明是借由使用终端 2 的扫描程序 22 来扫描使用终端 2 的硬件资料进行身份认证,不用另外购买各种不同身份验证硬件产品。

[0037] 2. 本发明连接使用终端 2 和内容提供者服务器 31-3n 的管道和连接使用终端和身份验证提供者服务器 41-4n 的管道并不一样,是一个双管道的认证架构,黑客不容易攻击。

[0038] 3. 使用者只需从下载中心 1 下载一扫描程序 22,各个内容提供者服务器 31-3n 及身份验证提供者服务器 41-4n 皆可使用同一扫描程序 22 来做身份认证。

[0039] 4. 内容提供者服务器 31-3n 可选择不同身份验证提供者服务器 41-4n 的业者帮其做身份认证,亦可随时更换身份验证提供者服务器 41-4n 的业者,不用考虑更换身份验证提供者服务器 41-4n 时所需的各种费用,时间及给使用者带来的麻烦。

[0040] 5. 身份验证提供者服务器 41-4n 的业者可利用同一架构及技术对不同客户(内容提供者服务器 31-3n) 提供不同附加价值,不同价格及特色的认证服务。

[0041] 6. 下载中心 1 是独立于内容提供者的业者及身份验证提供者的业者以外的第三方, 可以事先大量的推出扫描程序 22 给使用者, 大量节省客服成本。

[0042] 7. 同一内容提供者服务器 31-3n 可同时提供不同身份验证提供者服务器 41-4n 让使用者选择, 使用者可以在不同内容提供者服务器 31-3n 选用同一身份验证提供者服务器 41-4n, 这样好的身份验证提供者服务器 41-4n 就可胜出, 淘汰不好的身份验证提供者服务器 41-4n。

[0043] 8. 不同的内容提供者服务器 31-3n 的业者及不同的身份验证提供者服务器 41-4n 的业者可与下载中心 1 的业者合作, 由第三方的业者提供下载中心 1 及扫描程序 22, 如此一来, 使用者以使用终端 2 可自由选择所信赖的身份验证提供者服务器 41-4n 来确认使用者身份。

[0044] 9. 当任一内容提供者服务器 31-3n 导向任一身份验证提供者服务器 41-4n 时, 由于各内容提供者服务器 31-3n 及各身份验证提供者服务器 41-4n 之间的传输通道已被加密, 可避免有心人士拦截及窜改网页位址的方式盗用个人资料。

[0045] 10. 除了内容提供者服务器 31-3n 使用传统的 ID 及密码的登录资料, 再利用多重的硬件扫描资料及地理位置的查验, 可加强确认使用者本人的真实身份, 避免被远端的黑客盗用身份资料, 故确实能达到本发明的目的。

[0046] 惟以上所述的内容, 只为本发明的较佳实施例而已, 应当不能以此限定本发明实施的范围, 即凡依本发明申请专利范围及发明说明内容所作的简单的等效变化与修饰, 皆仍属本发明专利涵盖的范围内。

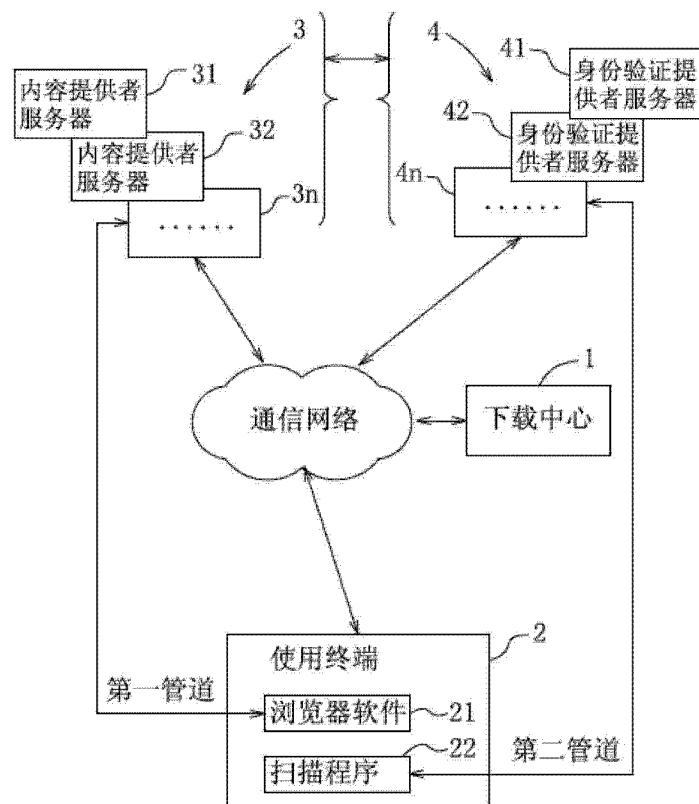


图 1

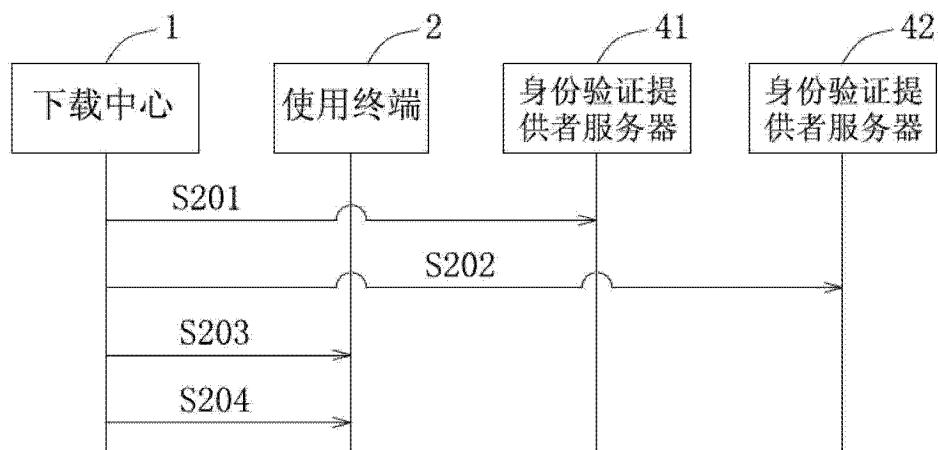


图 2

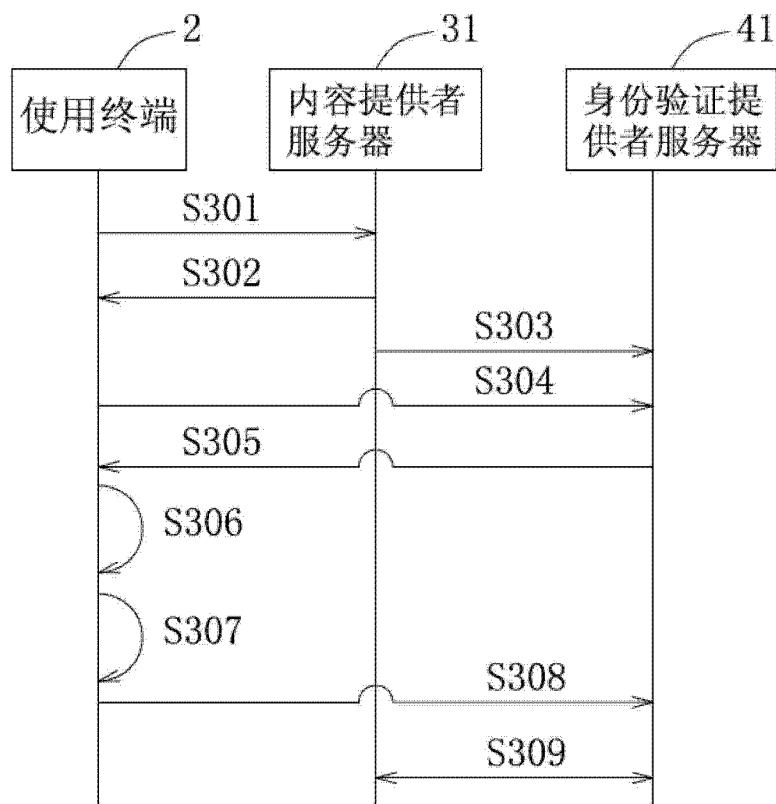


图 3

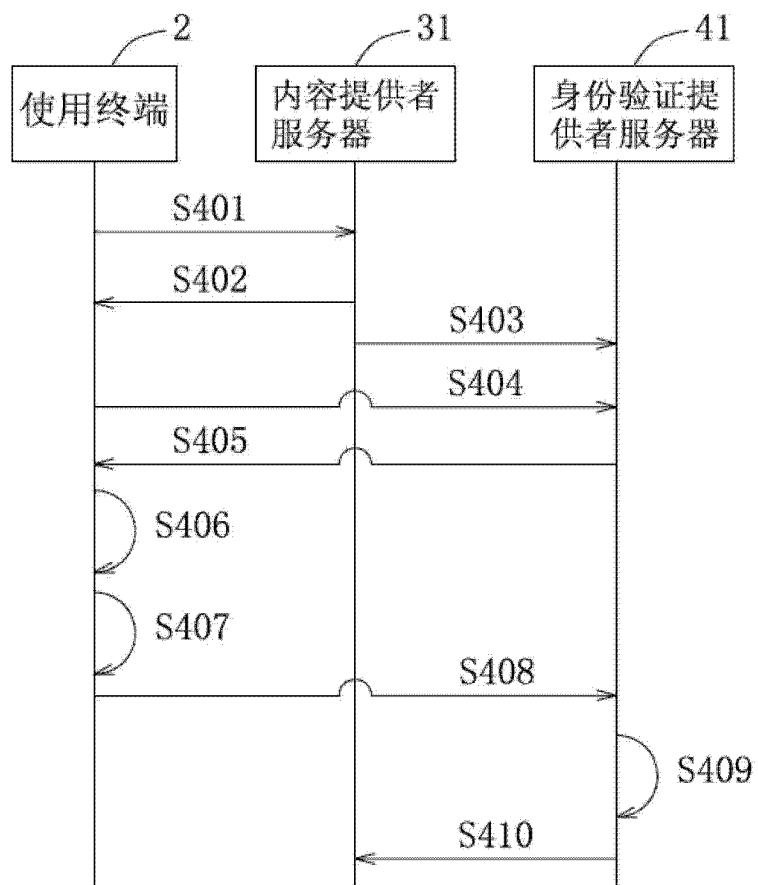


图 4

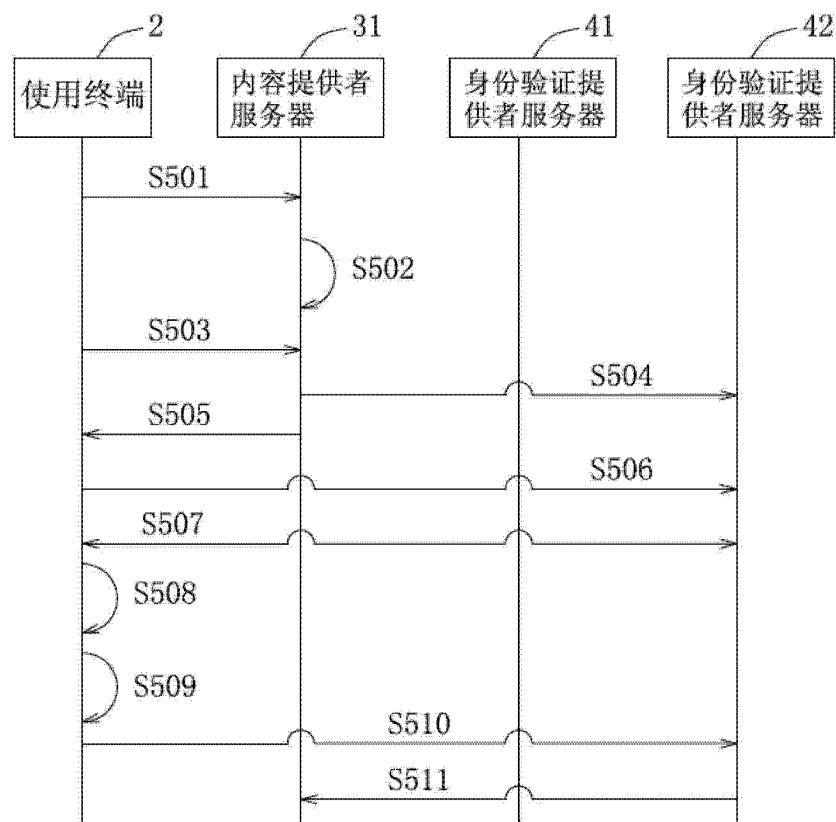


图 5

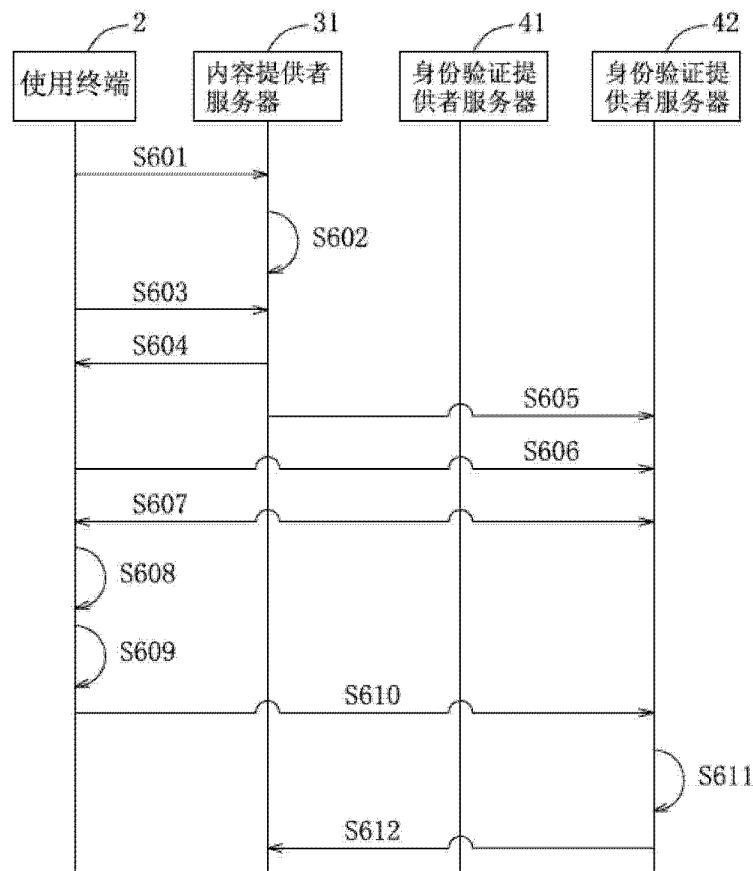


图 6