(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1885768 B
(45)授权公告日 2010.07.21

(21)申请号 200510079607.4

(22)申请日 2005.06.23

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 单长虹 黄迎新

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 宋志强 麻海明

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/12(2006.01)

(56)对比文件
CN 1464402 A,2003.12.31, 全文.
JP 特开 2002-91918 A,2002.03.29, 说明书第[0009]段-第[0030]段,附图1-5.
CN 1595948 A,2005.03.16, 说明书第2页第11行-第3页第24行,第4页第21行-第7页第6行,附图1,2.
US 2005/0132192 A1,2005.06.16, 全文.

审查员 郭风顺

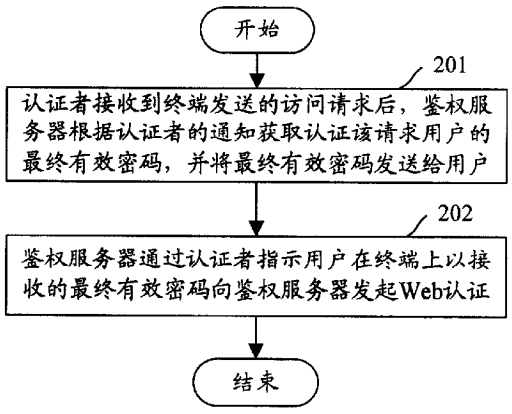
权利要求书 2 页 说明书 8 页 附图 4 页

(54)发明名称

一种环球网认证方法

(57)摘要

本发明公开了一种环球网认证方法,该方法包括:A、认证者在接收到终端发送的访问请求后,鉴权服务器根据认证者的通知获取认证该请求用户的最终有效密码,并将最终有效密码发送给用户;B、鉴权服务器通过认证者指示用户在终端上以接收的最终有效密码向鉴权服务器发起环球网Web认证。本发明中,由鉴权服务器获取用户的最终有效密码,并将该最终有效密码发送给用户,用户使用该最终有效密码发起Web认证,使得用户的密码能够动态更新,提高了Web认证的安全性;此外本发明中,不仅提供了用户每次登录都更改密码的实现形式,还提供了用户可以选择的以有效期为周期进行密码更改的实现形式,增加了业务实现方式,提高了竞争力。



CN 1885768 B

1. 一种环球网认证方法，其特征在于，该方法包括以下步骤：

A、认证者在接收到终端发送的访问请求后，向鉴权服务器发送通知，鉴权服务器根据认证者的通知获取用于认证该请求终端的最终有效密码，并将最终有效密码发送给所述终端；

B、鉴权服务器向认证者返回认证失败消息，该消息中包括网络给终端生成了新密码的信息；

认证者接收到认证失败消息后，根据认证失败消息中网络给终端生成了新密码的信息，将该认证失败消息对应的终端的更新密码标识更改为已更新，并向门户服务器发起取入口地址请求；

门户服务器接收到取入口地址请求后，向认证者返回取入口地址响应，其中包含入口地址；

认证者接收到入口地址后向终端下推访问入口地址的认证页面，指示用户在终端上以接收的最终有效密码向鉴权服务器发起环球网认证，并在接收到终端上报的访问入口地址请求消息后，判断终端的更新密码标识是否为已更新，若是，则继续执行后续环球网认证过程，并将终端的更新密码标识更改为未更新。

2. 根据权利要求 1 所述的方法，其特征在于，步骤 A 中所述将最终有效密码发送给用户的方法为：

鉴权服务器获取认证该请求用户的最终有效密码后，将该最终有效密码通过认证者发送给发起访问请求的终端，用户通过该终端获取密码。

3. 根据权利要求 1 所述的方法，其特征在于，步骤 A 中所述的访问请求中包括：用户标识信息；

步骤 A 中所述鉴权服务器获取认证该请求用户的最终有效密码之前进一步包括：

A01、认证者向鉴权服务器上报所述用户标识信息；

A02、鉴权服务器根据该用户标识信息判断对应的密码是否超过了有效期，如果超过了有效期，则执行所述的获取认证该请求用户的最终有效密码的步骤。

4. 根据权利要求 3 所述的方法，其特征在于，步骤 A 中所述的访问请求中进一步包括：密码；

步骤 A01 中进一步包括：认证者向鉴权服务器上报所述密码；

步骤 A02 中所述鉴权服务器判断对应的密码是否超过了有效期之前进一步包括：鉴权服务器对接收的用户标识信息和密码进行认证，如果认证通过，执行所述的判断对应的密码是否超过了有效期的步骤；否则通过认证者向终端返回拒绝请求消息，然后结束该流程。

5. 根据权利要求 1 至 4 中任一所述的方法，其特征在于，步骤 A 中所述鉴权服务器根据认证者的通知获取认证该请求用户的最终有效密码包括：

A1、认证者指示终端将用户标识信息和需要更改密码的信息发送给鉴权服务器；

A2、鉴权服务器根据接收的需要更改密码的信息获取对应用户的最终有效密码，记录所述用户标识信息与所述最终有效密码的对应关系。

6. 根据权利要求 5 所述的方法，其特征在于，步骤 A1 中所述的需要更改密码的信息为：用户标识信息后用于标识需要更改密码的域名。

7. 根据权利要求 5 所述的方法，其特征在于，步骤 A1 中所述的用户标识信息为用户的

唯一合法标识。

8. 根据权利要求 5 所述的方法，其特征在于，步骤 A2 中所述获取对应用户的最终有效密码为：

鉴权服务器为对应用户生成新密码作为最终有效密码；

或为：鉴权服务器将终端与需要更改密码的信息一起上报的密码作为本次认证的最终有效密码。

9. 根据权利要求 5 所述的方法，其特征在于，步骤 A 中所述将最终有效密码发送给用户的方法为：

鉴权服务器获取本次认证所需的最终有效密码后，将该最终有效密码发送给用户标识信息所对应的终端，用户通过该终端获取密码。

10. 根据权利要求 1 至 4 中任一所述的方法，其特征在于，步骤 B 所述后续环球网认证过程包括：

B1、向鉴权服务器上报包括所述最终有效密码作为密码的信息发起认证；

B2、鉴权服务器根据认证者上报的信息进行认证，并将认证结果信息发送给认证者；

B3、认证者将认证结果信息转发给所述门户服务器，门户服务器根据认证结果信息向用户终端下发对应的认证结果页面。

11. 根据权利要求 10 所述的方法，其特征在于，步骤 B1 中所述向鉴权服务器上报包括所述最终有效密码的信息发起认证之前进一步包括：

B11、认证者向门户服务器转发访问门户服务器入口地址请求；

B12、门户服务器接收到该请求后，向认证者发送挑战请求；

B13、认证者向门户服务器上报挑战值、挑战标识；

B14、门户服务器根据所述挑战值、挑战标识和访问门户服务器入口地址请求中的密码生成挑战密码，并将生成的挑战密码发送给认证者；

所述认证者向鉴权服务器发起认证所上报的最终有效密码为所述挑战密码；所述认证者向鉴权服务器发起认证所上报的信息中进一步包括：挑战值、挑战标识。

一种环球网认证方法

技术领域

[0001] 本发明涉及通信系统认证技术领域，特别是指一种环球网（Web）认证方法。

背景技术

[0002] 随着无线技术的发展，如全球接入互操作（WiMAX）网络、无线局域网（WLAN）等现令热门的无线接入网络，市场前景越来越好。但是随着应用越来越广泛，无线接入网络所受到的攻击也越来越多，因此现有的无线接入网络大多采用 Web 认证的方式来增强网络的安全性。

[0003] Web 认证方式是指终端（MSS、WLAN User Terminal.....）在访问服务之前，首先通过认证者（Authenticator、AC.....）获取门户服务器（PortalServer）的入口地址，然后认证者向终端下发访问门户服务器入口地址（PortalURL）的认证页面，终端在该认证页面输入用户名和密码，并将这些信息通过认证者上报给鉴权服务器（RADIUS or Diameter Server、AS.....）进行认证，在认证通过后 MSS 才可以访问 Portal Server 上的服务。

[0004] 下面以 WiMAX 网络中的 Web 认证流程对 Web 认证方式进行详细说明。如图 1 所示，WiMAX 网络中的 Web 认证流程包括以下步骤：

[0005] 步骤 101、终端（MSS）向认证者（Authenticator）发送访问请求消息，该消息中包括终端所要访问的服务的相关信息，如域名信息等。

[0006] 步骤 102、Authenticator 在接收到 MSS 发送的接入请求消息后，向所要访问的服务的相关信息对应的门户服务器（Portal Server）发送消息请求 Portal Server 的入口地址（Portal URL）。

[0007] 步骤 103 ～ 104、Portal Server 将自身的 Portal URL 发送给 Authenticator，该 Portal URL 可以是网址或者 IP 地址等，Authenticator 在接收到 Portal Server 发送的 Portal URL 后，向 MSS 下推访问该 Portal URL 的认证页面。

[0008] 步骤 105、用户在 Authenticator 下发的认证页面上输入用户名和密码后，终端通过 HTTPS 协议将用户输入的用户名和密码信息提交给 Authenticator。

[0009] 步骤 106、Authenticator 在接收到 MSS 提交的用户名和密码后，将该用户名和密码通过认证请求消息发送给 RADIUS or Diameter Server（AAAServer）为该用户进行认证。

[0010] 步骤 107、AAA Server 在接收到认证请求消息后，对该消息中的用户名和密码进行认证，并将认证成功或失败的结果信息通过认证请求响应消息返回给 Authenticator。

[0011] 步骤 108、Authenticator 在接收到 AAA Server 返回的认证请求响应消息后，将其中的认证结果信息发送给 Portal Server。

[0012] 步骤 109 ～ 111、Portal Server 在接收到 Authenticator 发送的认证结果信息后，判断该认证结果信息是否为认证成功，如果是则向 MSS 发送认证成功的页面，此后终端就可以对需要的服务进行访问了，然后执行步骤 112；否则，向 MSS 返回认证失败页面，以提示用户认证没有通过，然后执行步骤 112。

[0013] 步骤 112、Portal Server 将向终端下发认证成功或失败页面的信息发送给

Authenticator，然后结束该流程。

[0014] 通过上述流程就完成了终端接入的 Web 认证，保证了只有使用正确的用户名和密码的用户才能够访问服务。但是在这种 Web 认证方式中采用固定的用户名和密码进行认证，固定的用户名和密码很容易被他人获取，所以上述现有技术的 Web 认证方法中安全性很差。

发明内容

[0015] 有鉴于此，本发明的目的在于提供一种环球网认证方法，能够提高 Web 认证的安全性。

[0016] 为了达到上述目的，本发明提供了一种环球网认证方法，包括以下步骤：

[0017] A、认证者在接收到终端发送的访问请求后，向鉴权服务器发送通知，鉴权服务器根据认证者的通知获取认证该请求用户的最终有效密码，并将最终有效密码发送给用户；

[0018] B、鉴权服务器向认证者返回认证失败消息，该消息中包括网络给终端生成了新密码的信息；

[0019] 认证者接收到认证失败消息后，根据认证失败消息中网络给终端生成了新密码的信息，将该认证失败消息对应的终端的更新密码标识更改为已更新，并向门户服务器发起取入口地址请求；

[0020] 门户服务器接收到取入口地址请求后，向认证者返回取入口地址响应，其中包含入口地址；

[0021] 认证者接收到入口地址后向终端下推访问入口地址的认证页面，指示用户在终端上以接收的最终有效密码向鉴权服务器发起环球网认证，并在接收到终端上报的访问入口地址请求消息后，判断终端的更新密码标识是否为已更新，若是，则继续执行后续环球网认证过程，并将终端的更新密码标识更改为未更新。

[0022] 步骤 A 中所述将最终有效密码发送给用户的方法可以为：

[0023] 鉴权服务器获取认证该请求用户的最终有效密码后，将该最终有效密码通过认证者发送给发起访问请求的终端，用户通过该终端获取密码。

[0024] 步骤 A 中所述的访问请求中可以包括：用户标识信息；

[0025] 则步骤 A 中所述鉴权服务器获取认证该请求用户的最终有效密码之前可以进一步包括：

[0026] A01、认证者向鉴权服务器上报所述用户标识信息；

[0027] A02、鉴权服务器根据该用户标识信息判断对应的密码是否超过了有效期，如果超过了有效期，则执行所述的获取认证该请求用户的最终有效密码的步骤。

[0028] 步骤 A 中所述的访问请求中可以进一步包括：密码；

[0029] 则步骤 A01 中进一步包括：认证者向鉴权服务器上报所述密码；

[0030] 步骤 A02 中所述鉴权服务器判断对应的密码是否超过了有效期之前进一步包括：鉴权服务器对接收的用户标识信息和密码进行认证，如果认证通过，执行所述的判断对应的密码是否超过了有效期的步骤；否则通过认证者向终端返回拒绝请求消息，然后结束该流程。

[0031] 步骤 A 中所述鉴权服务器根据认证者的通知获取认证该请求用户的最终有效密

码可以包括：

[0032] A1、认证者指示终端将用户标识信息和需要更改密码的信息发送给鉴权服务器；

[0033] A2、鉴权服务器根据接收的需要更改密码的信息获取对应用户的最终有效密码，记录所述用户标识信息与所述最终有效密码的对应关系。

[0034] 较佳地，步骤 A1 中所述的需要更改密码的信息为：用户标识信息后用于标识需要更改密码的域名。

[0035] 较佳地，步骤 A1 中所述的用户标识信息为用户的唯一合法标识。

[0036] 步骤 A2 中所述获取对应用户的最终有效密码可以为：

[0037] 鉴权服务器为对应用户生成新密码作为最终有效密码；

[0038] 或可以为：鉴权服务器将终端与需要更改密码的信息一起上报的密码作为本次认证的最终有效密码。

[0039] 步骤 A 中所述将最终有效密码发送给用户的方法还可以为：

[0040] 鉴权服务器获取本次认证所需的最终有效密码后，将该最终有效密码发送给用户标识信息所对应的终端，用户通过该终端获取密码。

[0041] 步骤 B 所述后续环球网认证过程可以包括：

[0042] B1、向鉴权服务器上报包括所述最终有效密码作为密码的信息发起认证；

[0043] B2、鉴权服务器根据认证者上报的信息进行认证，并将认证结果信息发送给认证者；

[0044] B3、认证者将认证结果信息转发给所述门户服务器，门户服务器根据认证结果信息向用户终端下发对应的认证结果页面。

[0045] 步骤 B1 中所述向鉴权服务器上报包括所述最终有效密码的信息发起认证之前可以进一步包括：

[0046] B11、认证者向门户服务器转发访问门户服务器入口地址请求；

[0047] B12、门户服务器接收到该请求后，向认证者发送挑战请求；

[0048] B13、认证者向门户服务器上报挑战值、挑战标识；

[0049] B14、门户服务器根据所述挑战值、挑战标识和访问门户服务器入口地址请求中的密码生成挑战密码，并将生成的挑战密码发送给认证者；

[0050] 所述认证者向鉴权服务器发起认证所上报的最终有效密码为所述挑战密码；所述认证者向鉴权服务器发起认证所上报的信息中进一步包括：挑战值、挑战标识。

[0051] 从以上方案可以看出，本发明中，在进行 Web 认证过程中，由鉴权服务器获取用户的最终有效密码，并将该最终有效密码发送给用户，用户使用该最终有效密码发起 Web 认证，使得用户的密码能够动态更新，提高了 Web 认证的安全性；

[0052] 本发明中，不仅提供了用户每次登录都更改密码的实现形式，还提供了用户可以选择的以有效期为周期进行密码更改的实现形式，增加了业务实现方式，提高了竞争力。

[0053] **附图说明**

[0054] 图 1 为现有技术中 Web 认证的流程图；

[0055] 图 2 为本发明的总体流程图；

[0056] 图 3 为本发明第一实施例的流程图；

[0057] 图 4 为本发明第二实施例的流程图；

[0058] 图 5 为本发明在 WiMAX 网络中的框架图；

[0059] 图 6 为本发明在 WLAN 网络中的框架图。

[0060] **具体实施方式**

[0061] 为使本发明的目的、技术方案和优点更加清楚，下面结合附图对本发明作进一步的详细描述。

[0062] 本发明的总体流程如图 2 所示，具体步骤如下：

[0063] 步骤 201、认证者在接收到终端发送的访问请求后，鉴权服务器根据认证者的通知获取认证该请求用户的最终有效密码，并将最终有效密码发送给用户；

[0064] 步骤 202、鉴权服务器通过认证者指示用户在终端上以接收的最终有效密码向鉴权服务器发起 Web 认证。

[0065] 在上述步骤 201 中，鉴权服务器获取本次认证的最终有效密码，可以是自身生成新的密码作为最终有效密码，也可以是把终端上报的密码作为最终有效密码。鉴权服务器将最终有效密码发送给用户，可以是由鉴权服务器与短消息服务器进行交互，通过短消息服务器以短消息的形式将密码发送给上述用户标识信息对应的终端；也可以是鉴权服务器通过与其他服务器进行交互，以其他形式将密码发送给上述用户标识信息对应的终端，如以多媒体消息形式，或电子邮件方式等。此外，还可以是鉴权服务器通过认证者直接发送给发送访问请求消息的终端。

[0066] 此外，为了进一步增加 Web 认证的安全性，本发明中还可以在鉴权服务器与 Portal Server 之间增加挑战握手认证 (CHAP) 交互流程。

[0067] 下面通过本发明在 WiMAX 网络中的两种实现方式作为具体实施例对本发明进行详细说明。

[0068] 在本发明的第一实施例中，预先在 Authenticator 中为用户设定更新密码标识，用来标识是否已经为该用户更新了密码。例如设定该标识的初始值为 0，代表没有进行密码更新，而在 AAA Server 为用户更新密码之后，将该值更改为 1，代表已经进行了密码更新。

[0069] 如图 3 所示，为本实施例的具体实现流程，步骤如下：

[0070] 步骤 301、MSS 向 Authenticator 发送访问请求，其中包括所要访问的 Portal Server 相关信息，该信息可以是该 Portal Server 对应的域名信息，例如 www.google.com。

[0071] 步骤 302、Authenticator 接收到 MSS 发送的访问 Portal Server 请求后，向 MSS 下发 OTP 认证页面，在该页面上提示用户输入用户标识信息 (MSISDN)@ 域名形式的用户名。其中用户标识信息是指唯一能够标识用户名所对应的合法终端的标识信息，如可以是 MSISDN 或其他信息，在本实施例中以 MSISDN 为例进行说明；域名可以是 OTP 字段或其他标识该用户标识信息是用来进行 OTP 认证的字段，在本实施例中以 OTP 字段为例进行说明。

[0072] 步骤 303、MSS 在用户输入了 MSISDN@OTP 形式的用户名后，通过 HTTP 协议或者 HTTPS 协议将包括该用户名的认证请求消息上报给 Authenticator。

[0073] 在本实施例中，还可以用户只输入 MSISDN，然后通过认证页面上提供的下拉框或其他形式选择进行 OTP 认证的域名 @OTP。

[0074] 步骤 304、Authenticator 在接收到 MSS 发送的认证请求消息后，通过 OTP 后缀识别出该次认证请求消息为 OTP 认证请求后，将包括用户名为 MSISDN@OTP，密码为空的认证请求消息发送给 AAA Server。

[0075] 步骤 305、AAA Server 在接收到 Authenticator 上报的用户名为 MSISDN@OTP，密码为空的认证请求信息，识别出用户名中包括 OTP 后缀后，为该 MSISDN 对应的用户生成新密码，并用该新密码替换原有的旧密码，然后执行步骤 306 和步骤 307。

[0076] 步骤 306、AAA Server 将新密码发送给 MSISDN 对应的 MSS。

[0077] 本步骤中 AAA Server 可以首先与短消息中心进行交互，然后通过短消息中心将密码以短消息的形式发送给 MSS。

[0078] 步骤 307、AAA Server 向 Authenticator 返回认证失败消息，该消息中包括网络给 MSS 生成了新密码的信息，该信息可以通过设定认证失败消息中的失败原因值 (failure-Code) 为 Push-Authentication-Code 的形式实现，然后执行步骤 308。

[0079] 步骤 308、Authenticator 在接收到 AAA Server 返回的认证失败消息，识别出失败原因值为 Push-Authentication-Code 后，将该消息对应终端的更新密码标识的值更改为 1，然后根据步骤 302 中接收的访问请求消息中的 PortalServer 信息向 Portal Server 发起取 Portal URL 请求。

[0080] 步骤 309、Portal Server 接收到取 Portal URL 请求后，向 AAA Server 返回取 Portal URL 响应，其中包括 Portal Server 的 Portal URL 地址。

[0081] 步骤 310、Authenticator 在接收到 Portal Server 返回的 Portal URL 地址后，向 MSS 下推访问 Portal URL 的认证页面，以通知用户输入用户名和新密码以访问 Portal URL，这里的用户名可以为正常形式的用户名，如用户 ID 等。

[0082] 步骤 311、MSS 接收认证页面，将认证页面显示给用户，并在用户输入了用户名和新密码后，通过 HTTPS 协议向 Authenticator 发送包括用户名和新密码的访问 Portal URL 请求消息。

[0083] 步骤 312、Authenticator 接收到 MSS 上报的访问 Portal URL 请求消息后，识别出其中包括用户名和密码信息后，判断该 MSS 是否已经进行了密码更新，如果是则执行步骤 313；否则，返回执行步骤 302。

[0084] 本步骤中，判断该 MSS 是否已经进行了密码更新即判断该 MSS 对应的更新密码标识的值是否为 1。

[0085] 步骤 313、Authenticator 将接收到访问 Portal URL 请求消息转发给 PortalServer，并将更新密码标识的值更改为 0。

[0086] 步骤 314、Portal Server 在接收到 Authenticator 转发的访问 Portal URL 请求消息后，向 Authenticator 发送挑战请求。本步骤中，Portal Server 向 Authenticator 发送挑战请求是为了在 Portal Server 和 AAA Server 之间进行 CHAP 认证，以确定 Portal Server 的合法性。

[0087] 步骤 315、Authenticator 接收到挑战请求后，进行计算获得挑战值 (Challenge)，并向 Portal Server 返回包括该 Challenge 和挑战标识 (ChallengeID) 的挑战响应消息 (ACK_Challenge)。

[0088] 步骤 316、Portal Server 对密码和 Authenticator 发送的 Challenge ID 和 Challenge 以 MD5 算法计算获得挑战密码 (Challenge-Password)，然后将该 Challenge-Password 和用户名一起发送给 Authenticator，发起认证请求。

[0089] 步骤 317、Authenticator 将接收到的认证请求中的用户名和

Challenge-Password 以及 Challenge ID 和 Challenge 通过认证请求消息发送给 AAA Server 进行认证。

[0090] 步骤 318、AAA Server 在接收到 Authenticator 发送的认证请求消息后，对其中的信息进行认证，并将认证是否成功的结果信息通过认证请求响应消息发送给 Authenticator。

[0091] 本步骤中，AAA Server 对 Authenticator 发送的认证请求消息中的信息进行认证包括，根据 Challenge ID、Challenge 和自身中用户名对应的密码通过 MD5 算法生成 Challenge-Password，然后将认证者上报的 Challenge-Password 和生成的 Challenge-Password 进行比较是否相同。

[0092] 步骤 319、Authenticator 在接收到认证请求响应消息后，将认证结果信息发送给 Portal Server。

[0093] 步骤 320 ～ 321、Portal Server 根据接收的认证结果信息向 MSS 下发认证成功页面或认证失败页面，并将已经向 MSS 下发了认证成功或认证失败页面的信息发送给 Authenticator，然后结束该流程。

[0094] 以上是对本发明第一实施例的说明，在本发明第一实施例中提供了每次 Web 认证都更改密码的流程，在这种每次认证都更改密码的流程中，用户需要频繁地输入用户名和密码。此外，在该实施例中，更新后的密码完全由 AAA Server 生成，生成的密码不方便用户记忆。为方便用户，增加本发明的实现方式，并为用户提供更多的业务实现方式，提出了本发明的第二实施例，以下进行说明。

[0095] 在本发明第二实施例中，预先在 AAA Server 中为用户设置对应的密码更新时长或同一密码登录次数，用户可以通过定制的方式定制不同的密码更新时长或同一密码登录次数，以实现在一定的时间段内或一定的登录次数内不必更新密码。对于前者，还需要在 AAA Server 中设置密码更新时间，则通过判断用当前时间减去密码更新时间所得的时间是否小于密码更新时长，就可以判断出该次登录是否在上次密码更新后设置的密码更新时长内，如果是则该用户的密码在有效期内，不需要更新密码；否则需要更新密码，并将密码更新时间更改为该次更新密码的时间。对于后者，还需要在 AAA Server 中设置同一密码登录剩余次数，该同一密码登录剩余次数的初始值与同一密码登录次数相同，用户每登录一次该同一密码登录剩余次数值减一，如果用户的同一密码登录剩余次数值大于 0，则该用户的密码在有效期内，不需要更新密码；否则需要更新密码，更新密码后，同一密码登录剩余次数值恢复为用户定制的同一密码登录次数的值。

[0096] 如图 4 所示为本实施例的实现流程，具体步骤如下：

[0097] 步骤 401、MSS 向 Authenticator 发送访问请求消息，在该访问请求消息中包括用户标识信息和密码，以及所要访问的门户服务器的相关信息，如域名信息。

[0098] 步骤 402、Authenticator 接收到访问请求后，将该访问请求转发给 AAAServer。

[0099] 步骤 403、AAA Server 接收到访问请求后，对该访问请求中的用户名和密码进行认证，判断是否合法，如果是执行步骤 404；否则通过 Authenticator 向 MSS 返回拒绝请求消息，然后结束该流程。

[0100] 步骤 404、AAA Server 判断该访问请求所对应用户的密码是否在有效期内如果在有效期内执行步骤 405；否则执行步骤 406。

[0101] 步骤 405、向 Authenticator 返回访问回复消息，在该消息中包括认证成功消息，然后执行步骤 407。

[0102] 本步骤中，如果用户定制的密码更新周期是同一密码登录次数，则还需将同一密码登录剩余次数值减一。

[0103] 步骤 406、向 Authenticator 返回访问回复消息，在该消息中包括需要用户更新密码的信息，然后执行步骤 407。

[0104] 步骤 407、Authenticator 判断 AAA Server 返回的访问回复消息中的信息是否为需要用户更新密码，如果是执行步骤 408；否则 Authenticator 根据步骤 401 中用户上报的接入请求信息向对应的 Potral Server 发送 Portal URL 请求消息，并在获得 Portal URL 后，将用户上报的用户标识信息和密码发送给 Portal Server，然后执行步骤 419 及其后步骤。

[0105] 步骤 408、Authenticator 向 MSS 下推认证页面，提示用户更新密码。在该认证页面中提供 OTP 后缀，用户可以直接选择该后缀然后重新发起认证。

[0106] 步骤 409、用户在认证页面上的用户名中输入 MSISDN@OTP 形式的用户名后，MSS 向 Authenticator 上报该用户名。

[0107] 步骤 410、Authenticator 接收到用户上报的信息后，识别出用户名带有 OTP 后缀，则判断出该信息是更新密码请求，然后向 AAA Server 发送更新密码请求消息，在该消息中包括 MSISDN@OTP 形式的用户名。

[0108] 步骤 411、AAA Server 接收到更新密码请求消息后，根据带有 OTP 后缀形式的用户名识别出该请求为更新密码请求，则为用户生成新的密码，并保存该密码与 MSISDN 的对应关系。

[0109] 此外，在本步骤中，如果用户定制的密码更新周期是密码更新时长，则还需要将该用户对应的密码更新时间更改为当前时间；如果用户定制的密码更新周期是同一密码登录次数，则还需要将该用户对应的同一密码登录剩余次数值更改为该用户定制的同一密码登录次数的值。

[0110] 步骤 412、AAA Server 向 Authenticator 返回更新密码请求响应消息，在该消息中包括更新密码成功的信息并携带新的密码。

[0111] 步骤 413、Authenticator 在接收到更新密码请求响应消息后，识别出更新密码成功后，根据步骤 401 中用户上报的接入请求信息向对应的 PotralServer 发送 Portal URL 请求消息。

[0112] 步骤 414、Portal Server 在接收到 Portal URL 请求消息后，将自身的 PortalURL 发送给 Authenticator。

[0113] 步骤 415、Authenticator 在接收到 Portal Server 返回的 Portal URL 后，将密码更新成功信息、新的密码和用户请求的 Portal URL 一起发送给 MSS，并再次向 MSS 下推包括 Portal URL 的认证页面，提示用户输入用户名和新密码。

[0114] 步骤 416、MSS 在用户输入用户名和密码后，通过 HTTPS 协议向 Authenticator 发送包括用户名和密码的访问 Portal URL 的请求消息。

[0115] 步骤 417、Authenticator 判断该访问 Portal URL 请求消息所对应的用户是否已经进行了密码更新，如果是执行步骤 418；否则返回执行步骤 402。本步骤中判断用户是否

已经进行了密码更新的方法与第一实施例中相同，即通过对预先为用户设定的更新密码标识值进行判断来确定是否进行了密码更新，另外，对密码更新标识值的设定和更改方法也与第一实施例中相同，这里不再详细说明。

[0116] 步骤 418、Authenticator 将 MSS 上报的 HTTPS 协议形式的访问 PortalURL 请求消息发送给 Portal Server。

[0117] 步骤 419、Portal Server 接收到该访问 Portal URL 请求消息后发起 CHAP 过程，与 Authenticator 进行交互，在 CHAP 认证通过后，Portal Server 将用户名和挑战密码 (Challenge-Password) 发送给 Authenticator。

[0118] 本步骤中的 CHAP 过程的具体实现与第一实施例相同，即本步骤包括了图 3 中的步骤 314 至步骤 316。

[0119] 步骤 420、Authenticator 向 AAA Server 上报包括 Challenge ID、Challenge、Challenge-Password 和用户名的信息的认证请求消息。

[0120] 步骤 421、AAA Server 在接收到认证请求消息后，判断其中的信息是否合法，并将判断后获得的认证是否成功的结果信息通过认证响应消息发送给 Authenticator。

[0121] 步骤 422、Authenticator 将 AAA Server 返回的认证响应消息中的信息发送给 Portal Server。

[0122] 步骤 423、Portal Server 在接收到 Authenticator 发送的认证响应消息后，判断其中的认证结果信息是否为认证成功，如果是则向 MSS 发送认证成功的页面；否则向用户返回认证失败页面。

[0123] 步骤 424、Portal Server 向 Authenticator 发送已经向 MSS 发送认证成功或认证失败页面的信息，然后结束该流程。

[0124] 在上述步骤 409 中，用户也可以在认证页面上输入密码，然后 MSS 将用户输入的密码也上报给 Authenticator，则在步骤 410，Authenticator 在接收到 MSS 上报的请求信息后，判断请求信息中是否有密码，如果有则将该密码也上报给 AAA Server，在步骤 411，AAA Server 接收到认证请求消息，并识别出该消息中包括密码后，并不生成新的密码，而是将用户上报的密码作为新的密码，存储用户信息与该新密码的对应关系，并将该用户上报的密码下发给 Authenticator。

[0125] 此外，在上述步骤 412 中，AAA Server 也可以不将密码发送给 Authenticator，而是与第一实施例中相同，通过短消息中心将密码发送给用户。

[0126] 在本发明所举的两个具体实施例中，都是以本发明在如图 5 所示的 WiMAX 网络架构中的应用为例进行说明的。本发明还可以应用在除 WiMAX 外的 WLAN 或其他的采用三方认证模式的网络中，例如本发明在如图 6 所示的 WLAN 网络架构中应用时，只需要将具体实施例流程中的 MSS 替换成 WLAN 用户终端 (WLAN User Terminal)，将 Authenticator 替换成 WLAN 订阅者接入认证和服务控制点 (WLAN Subscriber AccessAuthentication Point and Service Control Point，AC)，将 AAA Server 替换成订阅者认证服务器 (RADIUS Subscribe Authentication Server，AS) 即可。

[0127] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

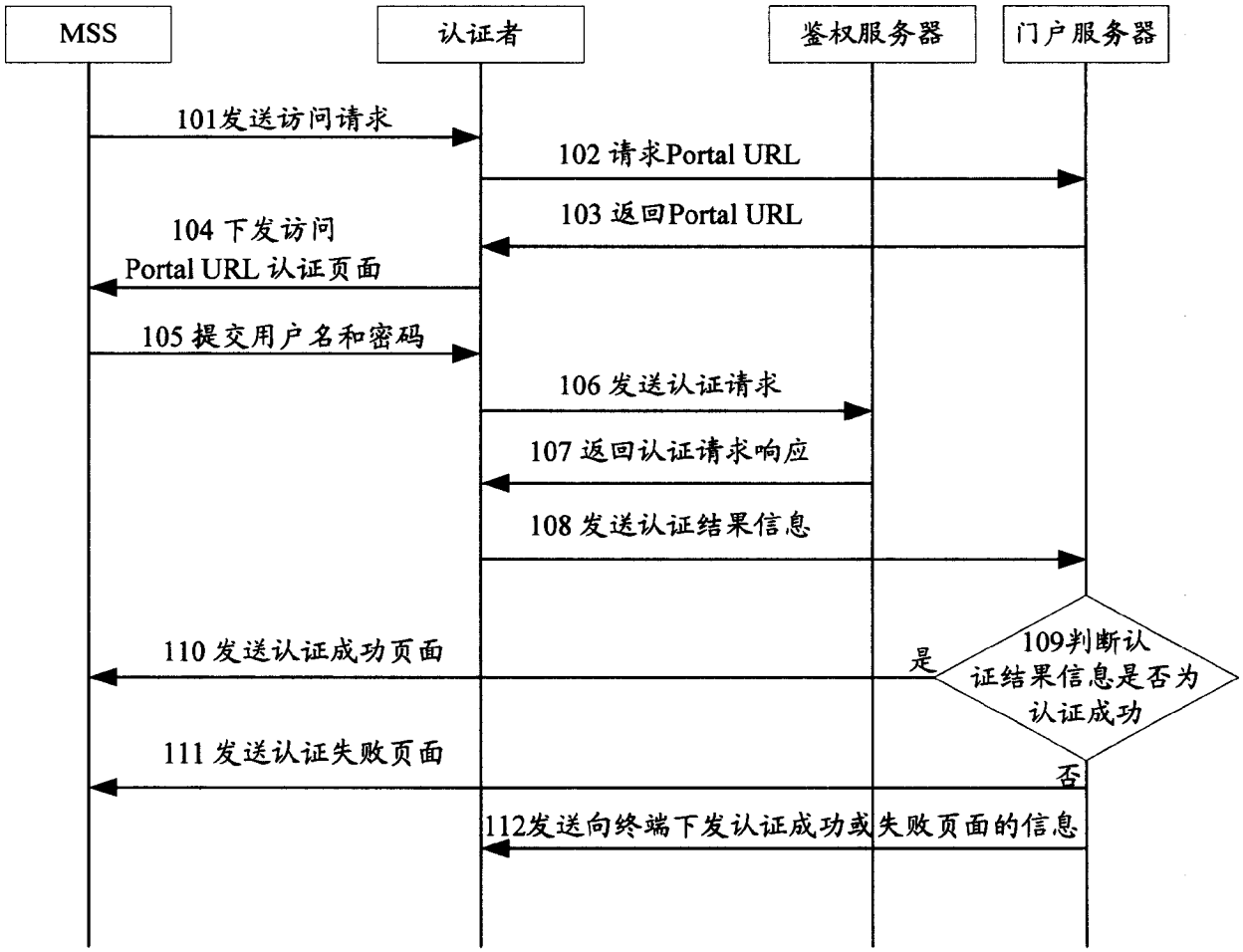

MSS
认证者
鉴权服务器
门户服务器
101发送访问请求
102 请求Portal URL
103 返回Portal URL
104 下发访问
Portal URL 认证页面
105 提交用户名和密码
106 发送认证请求
107 返回认证请求响应
108 发送认证结果信息
109判断认证结果信息是否为认证成功
是
否
110 发送认证成功页面
111 发送认证失败页面
112发送向终端下发认证成功或失败页面的信息

图 1

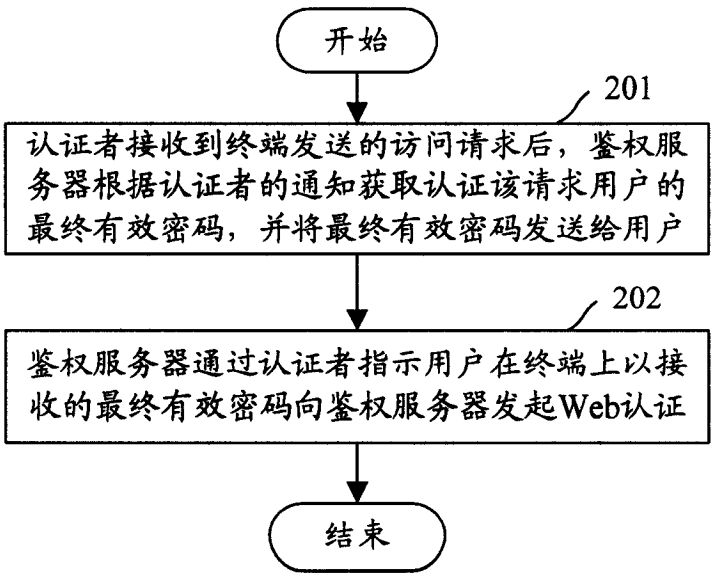

开始
201
认证者接收到终端发送的访问请求后，鉴权服务器根据认证者的通知获取认证该请求用户的最终有效密码，并将最终有效密码发送给用户
202
鉴权服务器通过认证者指示用户在终端上以接收的最终有效密码向鉴权服务器发起Web认证
结束

图 2

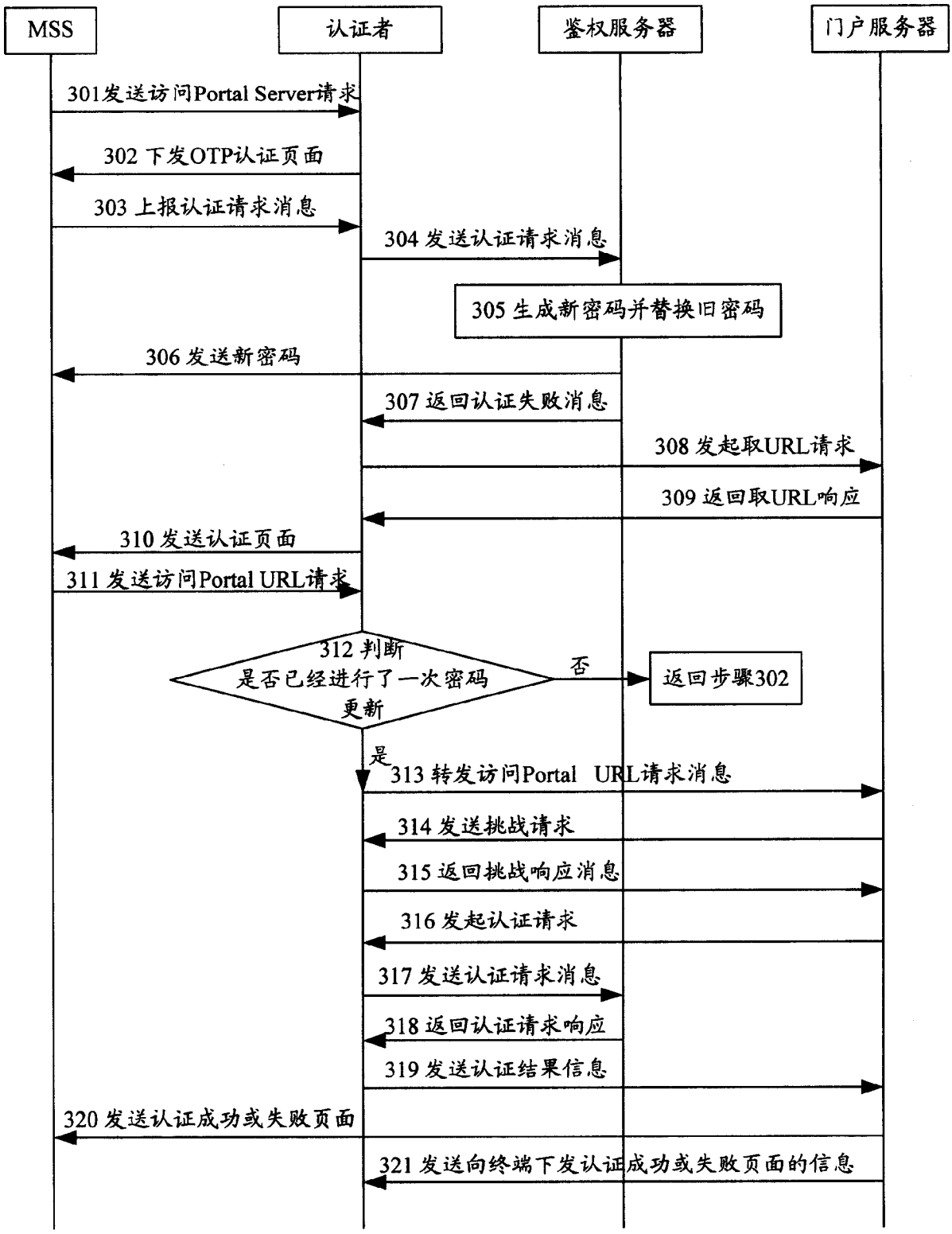

MSS
认证者
鉴权服务器
门户服务器
301发送访问Portal Server请求
302 下发OTP认证页面
303 上报认证请求消息
304 发送认证请求消息
305 生成新密码并替换旧密码
306 发送新密码
307 返回认证失败消息
308 发起取URL请求
309 返回取URL响应
310 发送认证页面
311 发送访问Portal URL请求
312 判断
是否已经进行了一次密码
更新
否
返回步骤302
是
313 转发访问Portal URL请求消息
314 发送挑战请求
315 返回挑战响应消息
316 发起认证请求
317 发送认证请求消息
318 返回认证请求响应
319 发送认证结果信息
320 发送认证成功或失败页面
321 发送向终端下发认证成功或失败页面的信息

图 3

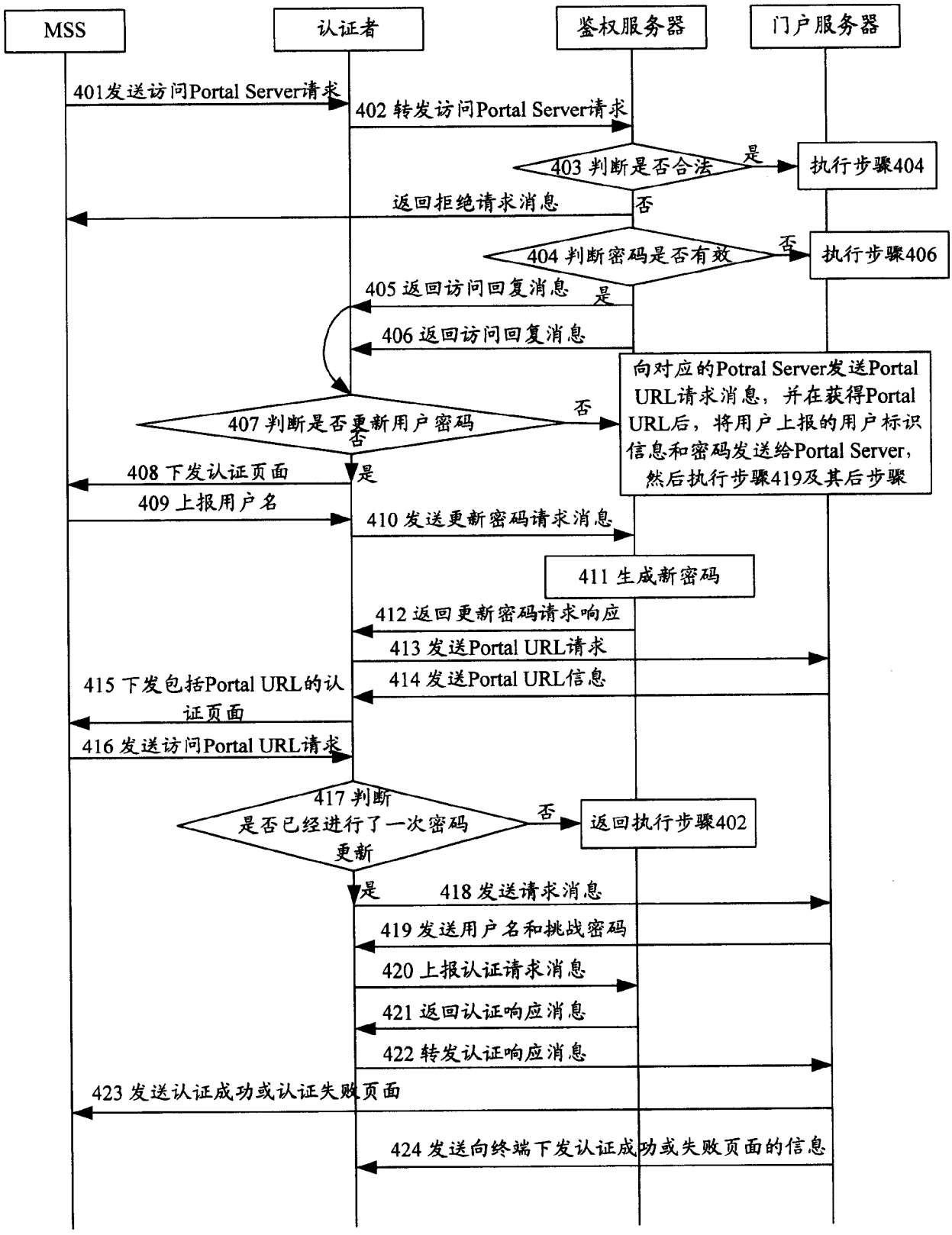

MSS
认证者
鉴权服务器
门户服务器
401发送访问Portal Server请求
402 转发访问Portal Server请求
403 判断是否合法
是
执行步骤404
返回拒绝请求消息
否
404 判断密码是否有效
否
执行步骤406
405 返回访问回复消息
是
406 返回访问回复消息
向对应的Potral Server发送Portal URL请求消息，并在获得Portal URL后，将用户上报的用户标识信息和密码发送给Portal Server，然后执行步骤419及其后步骤
407 判断是否更新用户密码
否
否
是
408 下发认证页面
409 上报用户名
410 发送更新密码请求消息
411 生成新密码
412 返回更新密码请求响应
413 发送Portal URL请求
414 发送Portal URL信息
415 下发包括Portal URL的认证页面
416 发送访问Portal URL请求
417 判断是否已经进行了一次密码更新
否
返回执行步骤402
是
418 发送请求消息
419 发送用户名和挑战密码
420 上报认证请求消息
421 返回认证响应消息
422 转发认证响应消息
423 发送认证成功或认证失败页面
424 发送向终端下发认证成功或失败页面的信息

图 4

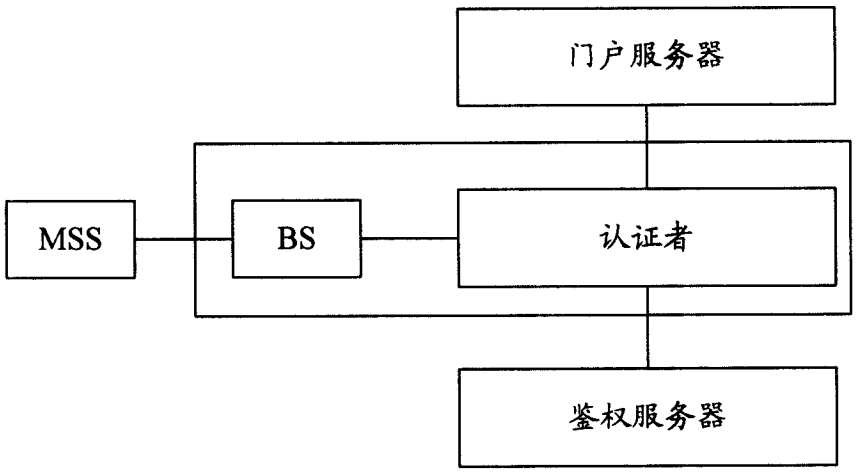


图 5

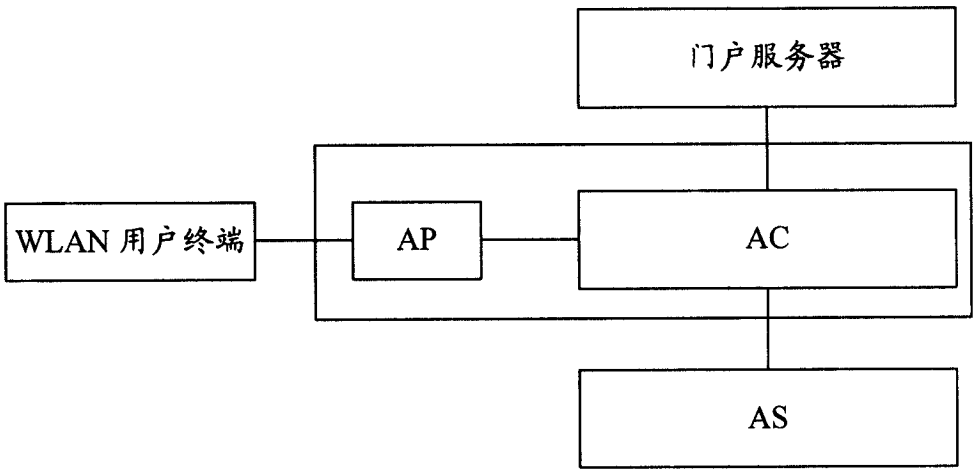


图 6