(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 101867912 A
(43)申请公布日 2010.10.20

(21)申请号 201010197288.8

(22)申请日 2010.06.07

(71)申请人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地 B 区 2 号楼

(72)发明人 张乾春

(51)Int.Cl.
H04W 8/04(2009.01)
H04W 12/06(2009.01)
H04W 84/12(2009.01)
H04L 29/06(2006.01)

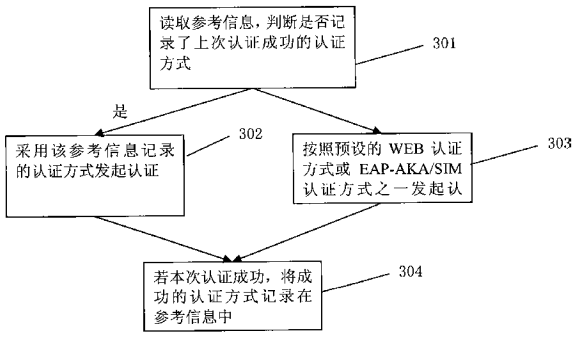
权利要求书 1 页 说明书 6 页 附图 3 页

(54)发明名称

一种接入网络的认证方法及终端

(57)摘要

本发明公开了一种接入网络的认证方法及终端。该方法包括,读取参考信息,若该参考信息记录了上次接入网络认证成功的认证方式,则采用该参考信息记录的认证方式发起认证,若该参考信息没有记录,按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证;若本次认证成功,将成功的认证方式记录在参考信息中。相应的,本发明实施例还提供一种应用上述方法的终端。通过本发明实施例提供的接入网络的认证方法和终端,运营商可利用现有的 WiFi WEB 认证网络兼容 WEB 认证和 EAP-AKA/SIM 认证方式,不需要增加任何网络设备,实施起来方便可靠。



CN 101867912 A

1. 一种接入网络的认证方法，适用于 WiFi WEB 认证网络，其特征在于，该认证方法包括：

读取参考信息，若该参考信息记录了上次接入网络认证成功的认证方式，则采用该参考信息记录的认证方式发起认证，若该参考信息没有记录，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；

若本次认证成功，将成功的认证方式记录在参考信息中。

2. 如权利要求 1 所述的认证方法，其特征在于，所述按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证之后还包括，

若认证失败，按照 WEB 和 EAP-SIM/AKA 中、预设的认证方式之外的另一种认证方式发起用户识别卡的认证。

3. 如权利要求 2 所述的认证方法，其特征在于，所述 EAP-SIM/AKA 认证方式中，终端在收到请求该终端上报身份信息之前，先关联到 Open 模式的 WLAN 网络。

4. 如权利要求 1 至 3 任一项所述的认证方法，其特征在于，若收到认证失败的消息，向用户提示认证失败，根据用户的指示终止认证或发起再次认征。

5. 如权利要求 4 所述的认证方法，其特征在于，在向用户提示认证失败后，若在设定的时间过后，仍然没有收到用户的指示，自动重新读取参考信息，若该参考信息记录了上次接入网络认证成功的认证方式，则采用该参考信息记录的认证方式发起认证，若该参考信息没有记录，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；若本次认证成功，将成功的认证方式记录在参考信息中。

6. 一种终端，通过带有 SIM 卡的数据卡或 WLAN 网卡接入网络，其特征在于，该终端包括：

读取单元，用于读取参考信息，并判断该参考信息是否记录了上次接入网络认证成功的认证方式；

认证单元，用于在已记录的情况下，采用该参考信息记录的认证方式发起认证，在没有记录的情况下，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；

存储单元，用于存储参考信息，并在本次认证成功时，将成功的认证方式记录在参考信息中。

7. 如权利要求 6 所述的终端，其特征在于，所述认证单元还用于，在按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证失败后，按照 WEB 和 EAP-SIM/AKA 中、预设的认证方式之外的另一种认证方式发起用户识别卡的认证。

8. 如权利要求 7 所述的终端，其特征在于，所述认证单元还包括，关联子单元，用于在终端在收到请求该数据卡上报身份信息之前，先关联到 Open 模式的 WLAN 网络。

9. 如权利要求 6-8 任一项所述的终端，其特征在于，该终端还包括，提醒单元，用于在收到认证失败的消息时，向用户提示认证失败；

指令接收单元，用于接收用户根据该认证失败提示返回的指令，若该指令为重新发起认证，则触发所述读取单元启动新一轮的认证。

10. 如权利要求 9 所述的终端，其特征在于，该终端还包括，定时单元，用于在所述提醒单元向用户提示认证失败后开始计时，若所述指令接收单元在达到设定的时间后仍然没有收到用户的指示，则触发所述读取单元启动新一轮的认证。

一种接入网络的认证方法及终端

技术领域

[0001] 本发明涉及移动通信应用领域，特别涉及一种接入网络的认证方法及终端。

背景技术

[0002] 无线上网卡（又称数据卡）通过计算机客户端软件可以实现综合接入，一方面数据卡可以接入 2G/3G 网络，同时也可以通过计算机上的无线高保真 WiFi 芯片接入 WiFi 网络。

[0003] 对于大多数 WiFi 网络，数据卡在接入时一般需要在 IE 浏览器中输入用户名 / 密码才能通过认证，这种方式被称之为 WEB 认证。对于 2G/3G 网络，数据卡在接入时则是通过用户识别卡（即 SIM 卡）中的标识完成认证。对于一些同时运营 WiFi 网络和 2G/3G 网络的运营商，如果能够直接利用 SIM 卡完成认证，而不需要用户手动的通过 WEB 界面进行输入，将会是一种理想方案。

[0004] 为了支持 WiFI 网络采用 3G SIM 卡鉴权，IETF RFC 4187 定义了 EAP-AKA(Extensible Authentication Protocol Method for 3G Authenticationand Key Agreement) 协议。然而，支持该方案的终端较少。手机也只有少数厂家的少数机型支持，而且 WinXP/Vista/MacOS/Linux 等计算机操作系统业不支持该方案，在数据卡上也没有实现该方案。另外，该方案并不兼容采用 WEB 认证的无线局域网 WLAN 网络，在 WEB 认证的情况下，接入点 AP 的工作模式是 open，而在 EAP-AKA 认证的情况下，AP 的工作模式必须是 WPA-EAP 模式或 802.1x 模式。在 2G 的网络中，2G SIM 卡鉴权采用的是 EAP-SIM(Extensible Authentication Protocol Method for GSM SubscriberIdentity Modules) 认证方式。

[0005] 发明人在实现本发明的过程中发现，现有技术至少具体如下问题：现有的兼容 WiFi 和 2G/3G 网络认证的方案，实现起来较复杂，另外，为了使数据卡同时支持 WEB 认证和 EAP-AKA/SIM 认证，在现有 WiFi WEB 认证的网络的情况下，运营商还需要新建专门的 EAP-AKA/SIM 认证的网络，这样一来，并不能充分利用现有的网络，造成了资源的浪费。

发明内容

[0006] 针对现有技术中兼容 WiFi 和 2G/3G 网络认证的方案实现复杂和未能充分利用资源的问题，本发明实施例提供了一种接入网络的认证方法及终端。通过本发明实施例提供的认证方法和终端，运营商可以免去新建专门 EAP-AKA/SIM 认证的网络，用户在使用时，也只使用一个服务集标识 SSID，操作起来更为方便。

[0007] 一方面，本发明实施例提供的接入网络的认证方法，用于 WiFi WEB 认证网络，该认证方法包括：

[0008] 读取参考信息，若该参考信息记录了上次接入网络认证成功的认证方式，则采用该参考信息记录的认证方式发起认证，若该参考信息没有记录，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；

[0009] 若本次认证成功，将成功的认证方式记录在参考信息中。

[0010] 另一方面，本发明实施例提供一种终端，通过带有 SIM 卡的数据卡或 WLAN 网卡接入网络，该终端包括：

[0011] 读取单元，用于读取参考信息，并判断该参考信息是否记录了上次接入网络认证成功的认证方式；

[0012] 认证单元，用于在已记录的情况下，采用该参考信息记录的认证方式发起认证，在没有记录的情况下，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；

[0013] 存储单元，用于存储参考信息，并在本次认证成功时，将成功的认证方式记录在参考信息中。

[0014] 由上述方案可以看出，通过本发明实施例提供的接入网络的认证方法和终端，运营商可利用现有的 WiFi WEB 认证网络兼容 WEB 认证和 EAP-AKA/SIM 认证方式，不需要增加任何网络设备，实施起来方便可靠。

附图说明

[0015] 图 1 为 WEB 认证的流程示意图；

[0016] 图 2 为 EAP-AKA 认证的流程示意图；

[0017] 图 3 为本发明实施例一认证方法的流程示意图；

[0018] 图 4 为本发明实施例二认证方法的流程示意图。

具体实施方式

[0019] 本发明实施例提供的接入网络的认证方法及数据卡，基于现有的 WiFiWEB 认证的网络，不需要增加新的网络设备，即可实现 EAP-AKA/SIM 认证，而且用户在使用时也只需使用原 WEB 认证的 SSID，因此易于实现且使用方便，以下结合附图对具体实施方式加以说明。

[0020] 图 1 为 WEB 认证的流程示意图，图中所示的方法适用于 WLAN 用户使用数据卡进行 WEB 认证。该认证的过程包括：

[0021] 101. 客户端软件通过 WLAN 网卡关联到 Open 模式的 WLAN 网络。

[0022] 102. 用户在计算机上打开 WEB 浏览器，输入任意网址，发起 http 请求，该请求被 AC 强制重定向到 Portal 服务器。

[0023] 103.Portal 服务器把 WEB 认证页面推送到 WEB 浏览器中。

[0024] 104. 用户在 WEB 认证页面上输入用户名、密码后，提交到 Portal 服务器。

[0025] 105.Portal 服务器向 AAA 服务器查询用户信息。

[0026] 106.AAA 服务器返回用户信息及用户连接时长相关信息给 Portal 服务器。

[0027] 107.Portal 服务器根据用户信息比较用户名密码判断是否认证通过，如果查询失败，直接给出提示信息，结束认证。

[0028] 108.Portal 服务器通知 AC 认证通过。

[0029] 109.AC 给 Portal 服务器确认认证通过，并打开该用户的上网权限。

[0030] 110.Portal 服务器判断该用户所属的域。

[0031] 111.Portal 服务器给用户推送所属域的认证通过的 WEB 页面。

[0032] 图 2 为 EAP-AKA 认证的流程示意图，图中所示的方法适用于 WLAN 用户通过数据卡进行 EAP-AKA 认证。该认证的过程包括：

[0033] 201. 用户设备 UE 通过 WLAN 网卡关联到 WPA-Enterprise 模式或 802.1X 模式的 WLAN 网络。

[0034] 202.UE 收到 EAP-Request/Identity 的报文，请求 UE 上报身份信息。

[0035] 203.UE 回复 EAP-Response/Identity 的报文给 AAA，上报身份信息。

[0036] 204.AAA 根据 Identity 向 HLR 查询用户信息。

[0037] 205.HLR 返回用户认证信息给 AAA。

[0038] 206.AAA 根据用户认证信息，发送 EAP-Request/AKA-Challenge 报文给 UE，请求 UE 回复认证挑战。

[0039] 207.UE 回复 EAP-Response/AKA-Challenge 报文给 AAA。

[0040] 上述 SIM 卡鉴权过程为 3G SIM 卡鉴权，EAP-SIM 的认证过程也类似，此处不再赘述。

[0041] 图 3 为本发明实施例一提供的接入网络的认证方法，该方法适用于现有的 WiFi WEB 认证网络，需要说明的是，本实施例一的方法由装载在计算机内的客户端执行，客户端利用与计算机连接的带有 SIM 卡的数据卡进行网络连接，或者是利用与计算机连接的带有 SIM 卡的 WLAN 网卡进行网络连接。

[0042] 该认证方法包括：

[0043] 301. 读取参考信息，若该参考信息记录了上次接入网络认证成功的认证方式，转步骤 302；若该参考信息没有记录，转步骤 303；

[0044] 302. 采用该参考信息记录的认证方式发起认证，转步骤 304；

[0045] 303. 按照预设的 WEB 认证方式或 EAP-AKA/SIM 认证方式之一发起认证，转步骤 304；

[0046] 304. 若本次认证成功，将成功的认证方式记录在参考信息中。

[0047] 本发明实施例提供了一种接入网络的认证方法，通过该方法，运营商可利用现有的 WiFi WEB 认证网络兼容 WEB 认证和 EAP-AKA/SIM 认证方式，不需要增加任何网络设备，实施起来方便可靠。

[0048] 图 4 为本发明实施例二提供的接入网络的认证方法，该方法适用于现有 WiFi WEB 认证网络，需要说明的是，本实施例二的方法由装载在计算机内的客户端执行，客户端利用与计算机连接的带有 SIM 卡的数据卡进行网络连接，或者是利用与计算机连接的带有 SIM 卡的 WLAN 网卡进行网络连接。

[0049] 该认证方法包括：

[0050] 401. 客户端在发起认证前，读取参考信息，若该参考信息中记录了上次接入网络认证成功的认证方式，转步骤 402；若该参考信息未记录认证方式，转步骤 403。

[0051] 可以将参考信息初始化一个值，如果在发起认证前读取到参考信息中存的仍然是初始值，就判断该参考信息没有存上次认证成功的认证方式，如果该参考信息中的内容已经发生了变化，并且现在的内容为约定的数值（例如约定 WEB 认证方式用 001 代表，约定 EAP-AKA/SIM 认证方式用 002 代表），就按照该数值对应的认证方式发起认证。参考信息可以存储在计算机客户端软件的配置文件中。对于发起的是 EAP-AKA 还是 EAP-SIM 认证，由 SIM 卡本身的特性决定，如果是 2G 的 SIM 卡，则发起 EAP-SIM，如果是 3G 的 SIM 卡，则发起 EAP-AKA 认证。

[0052] 402. 采用该参考信息中的认证方式发起认证，转步骤 405。

[0053] 如果参考信息记录的是 WEB 认证，就可采用图 1 所示的认证流程；类似的，如果参考信息记录的是 EAP-AKA/SIM，需要将 201 步骤替换为“关联到 Open 模式的 WLAN”，然后使用就可采用图 2 所示的 202-210 认证流程。

[0054] 403、按照预设的 WEB 认证方式或 EAP-AKA/SIM 认证方式之一发起认证，若收到认证成功的消息，则转步骤 406；若收到认证失败的消息，则转步骤 404。

[0055] 此处可以由用户手动或者由数据卡厂商 /WLAN 网卡厂商，又或者是运营商来设定预设的认证方式，该预设的认证方式是在没有记录上次认证成功的认证方式时，第一次尝试认证的方式。假设首次认证预设的是 EAP-AKA 认证，则发起流程如图 2 的 EAP-AKA 认证请求，除了将步骤 201 替换为“关联到 Open 模式的 WLAN”，步骤 202-210 不需改变，如果该次 EAP-AKA 认证失败，则自动发起流程如图 1 的 WEB 认证请求。由于具体内容与前面相同，此处不再赘述。

[0056] 404、按照 WEB 和 EAP-AKA/SIM 中、预设的认证方式之外的另一种认证方式发起用户识别卡的认证，转步骤 405。

[0057] 由于按照预设的认证方式没有成功，数据卡再采用第一次没有尝试过的认证方式进行认证。具体来说，如果步骤 403 中采用的是 WEB 认证，这次就采用 EAP-AKA/SIM 认证，反之也类似。由于 EAP-AKA 和 EAP-SIM 并不能同时存在，也就是说对于 2G 的 SIM 卡，此处可选认证方式只有 WEB 和 EAP-SIM 两种，步骤 403 选择了其一进行认证，如果认证失败，步骤 404 选择另一个方式进行认证。对于 3G 的 SIM 卡，此处可选的认证方式只有 WEB 和 EAP-AKA 两种，步骤 403 选择了其一进行认证，如果认证失败，步骤 404 采用另一个方式进行认证。

[0058] 405、如果收到认证成功的消息，确定已完成用户识别卡认证，转步骤 406；若收到认证失败的消息，终止本次认证，向用户提示认证失败。

[0059] 若两次认证都失败，可设置自动停止认证，还可设置根据用户的指示进行重新发起认证，即回到步骤 401 重新执行。若两次认证都失败，也可以设置设定的时间后，如果用户没有指示，认证自动从步骤 401 开始直至认证完成，如果认证仍然失败，可以设置重新认证的最大次数。如果达到最大次数，将停止认证。

[0060] 406. 将本次成功的认证方式记录在参考信息中。

[0061] 最后，在认证成功后，将成功的认证方式记录在配置文件中以备下次认证时选择。

[0062] 本发明实施例提供了一种接入网络的认证方法，通过该方法，运营商可利用现有的 WiFi WEB 认证网络兼容 WEB 认证和 EAP-AKA/SIM 认证方式，不需要增加任何网络设备，实施起来方便可靠，同时在认证失败后还提供多样化的再次认证方式，提高了认证的成功率，降低了用户的操作复杂程度。

[0063] 本发明实施例三提供一种终端，用于执行上述实施例一的方法步骤。该终端通过带有 SIM 卡的数据卡或 WLAN 网卡接入网络，该终端包括：

[0064] 读取单元，用于读取参考信息，并判断该参考信息是否记录了上次接入网络认证成功的认证方式；

[0065] 认证单元，用于在已记录的情况下，采用该参考信息记录的认证方式发起认证，在没有记录的情况下，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；

[0066] 存储单元，用于存储参考信息，并在本次认证成功时，将成功的认证方式记录在参

考信息中。

[0067] 可以理解，上述单元的部分或全部功能可以由装载在终端（如计算机）内的客户端软件执行。

[0068] 通过本发明实施例提供的终端，运营商可利用现有的 WiFi WEB 认证网络兼容 WEB 认证和 EAP-AKA/SIM 认证方式，不需要增加任何网络设备，实施起来方便可靠。

[0069] 本发明实施例四还提供一种终端，用于执行上述实施例二的方法步骤。该终端通过带有 SIM 卡的数据卡或 WLAN 网卡接入网络，该终端包括：

[0070] 读取单元，用于读取参考信息，并判断该参考信息是否记录了上次接入网络认证成功的认证方式；

[0071] 认证单元，用于在已记录的情况下，采用该参考信息记录的认证方式发起认证，在没有记录的情况下，按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证；其中的预设认证方式，此处可以由用户手动或者由数据卡 /WLAN 网卡厂商，又或者是运营商来设定预设，该预设的认证方式是在没有记录上次认证成功的认证方式时，第一次尝试认证的方式。

[0072] 存储单元，用于存储参考信息，并在本次认证成功时，将成功的认证方式记录在参考信息中。

[0073] 具体的，认证单元还用于，在按照预设的 WEB 认证方式或 EAP-SIM/AKA 认证方式之一发起认证失败后，按照 WEB 和 EAP-SIM/AKA 中、预设的认证方式之外的另一种认证方式发起用户识别卡的认证。

[0074] 可选的，所述认证单元还包括，关联子单元，用于在终端在收到请求该终端上报身份信息之前，先关联到 Open 模式的 WLAN 网络。如果参考信息记录的是 WEB 认证，认证单元就可采用图 1 所示的认证流程；类似的，如果参考信息记录的是 EAP-AKA/SIM，需要将 201 步骤替换为“关联到 Open 模式的 WLAN”，这部分功能由此处的关联子单元完成，然后认证单元就可执行图 2 所示的 202-210 认证流程。

[0075] 可选的，该终端还包括，提醒单元，用于在收到认证失败的消息时，向用户提示认证失败；指令接收单元，用于接收用户根据该认证失败提示返回的指令，若该指令为重新发起认证，则触发所述读取单元启动新一轮的认证。

[0076] 可选的，定时单元，用于在所述提醒单元向用户提示认证失败后开始计时，若所述指令接收单元在达到设定的时间后仍然没有收到用户的指示，则触发所述读取单元启动新一轮的认证。

[0077] 需要说明的是，关于本实施例终端，可以将参考信息初始化一个值，如果在发起认证前读取到参考信息中存的仍然是初始值，就判断该参考信息没有存上次认证成功的认证方式，如果该参考信息中的内容已经发生了变化，并且现在的内容为约定的数值（例如约定 WEB 认证方式用 001 代表，约定 EAP-AKA/SIM 认证方式用 002 代表），就按照该数值对应的认证方式发起认证。参考信息可以由存储单元存储在计算机客户端软件的配置文件中。对于发起的是 EAP-AKA 还是 EAP-SIM 认证，由 SIM 卡本身的特性决定，如果是 2G 的 SIM 卡，则发起 EAP-SIM，如果是 3G 的 SIM 卡，则发起 EAP-AKA 认证。

[0078] 本发明实施例提供了一种终端，通过该终端，运营商可利用现有的 WiFiWEB 认证网络兼容 WEB 认证和 EAP-AKA/SIM 认证方式，不需要增加任何网络设备，实施起来方便可

靠，同时在认证失败后还提供多样化的再次认证方式，提高了认证的成功率，降低了用户的操作复杂程度。

[0079] 可以理解，本发明实施例虽然多以数据卡为例进行说明，但是该方法或终端也同样适用于装有用户身份识别模块的 WLAN 网卡，由于实施的方法类似，故不再重复。

[0080] 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步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，实施的步骤与方法相同，所述的存储介质，如 :ROM/RAM、磁碟、光盘等。

[0081] 以上是对本发明具体实施例的说明，在具体的实施过程中可对本发明的方法进行适当的改进，以适应具体情况的具体需要。因此可以理解，根据本发明的具体实施方式只是起示范作用，并不用以限制本发明的保护范围。

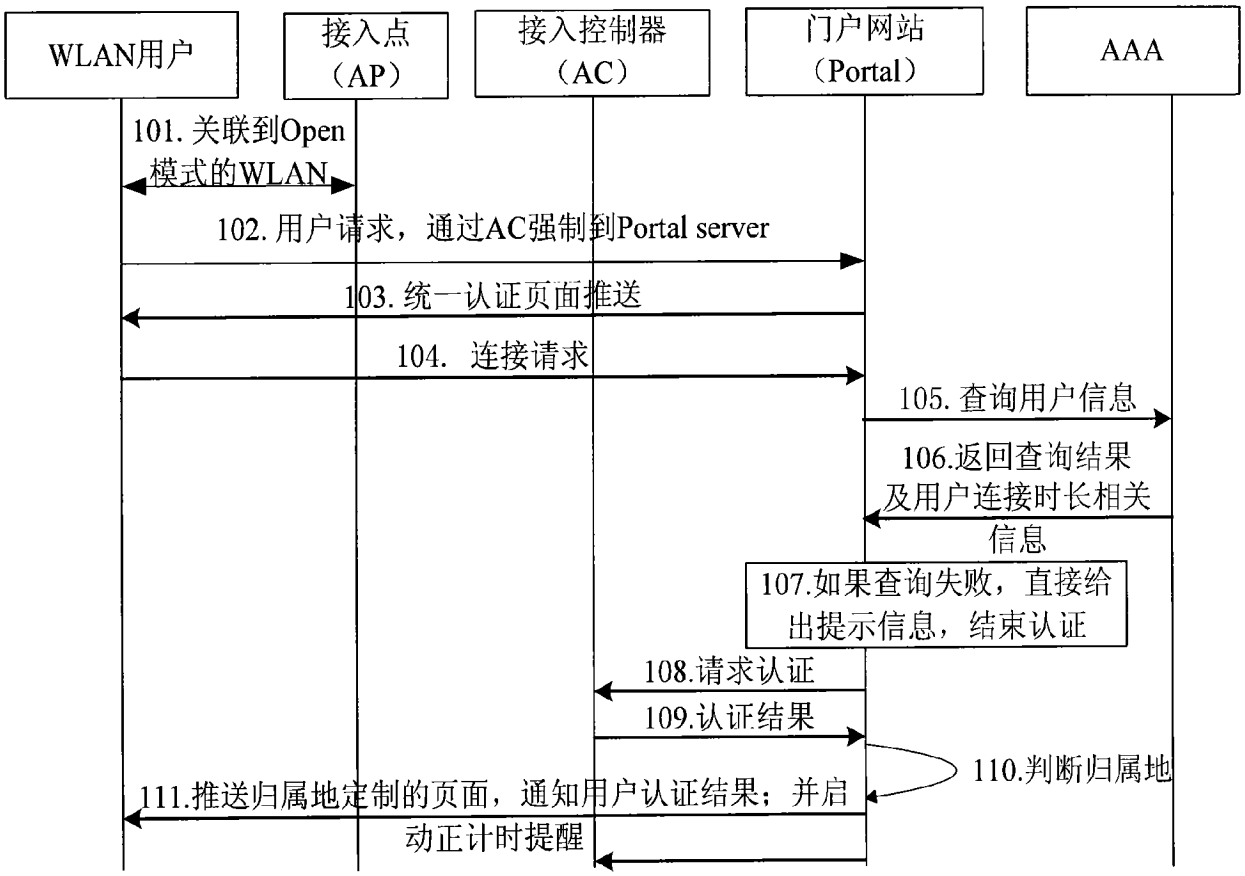

WLAN用户
接入点（AP）
接入控制器（AC）
门户网站（Portal）
AAA
101. 关联到Open模式的WLAN
102. 用户请求，通过AC强制到Portal server
103. 统一认证页面推送
104. 连接请求
105. 查询用户信息
106.返回查询结果及用户连接时长相关信息
107.如果查询失败，直接给出提示信息，结束认证
108.请求认证
109.认证结果
110.判断归属地
111.推送归属地定制的页面，通知用户认证结果；并启动正计时提醒

图 1

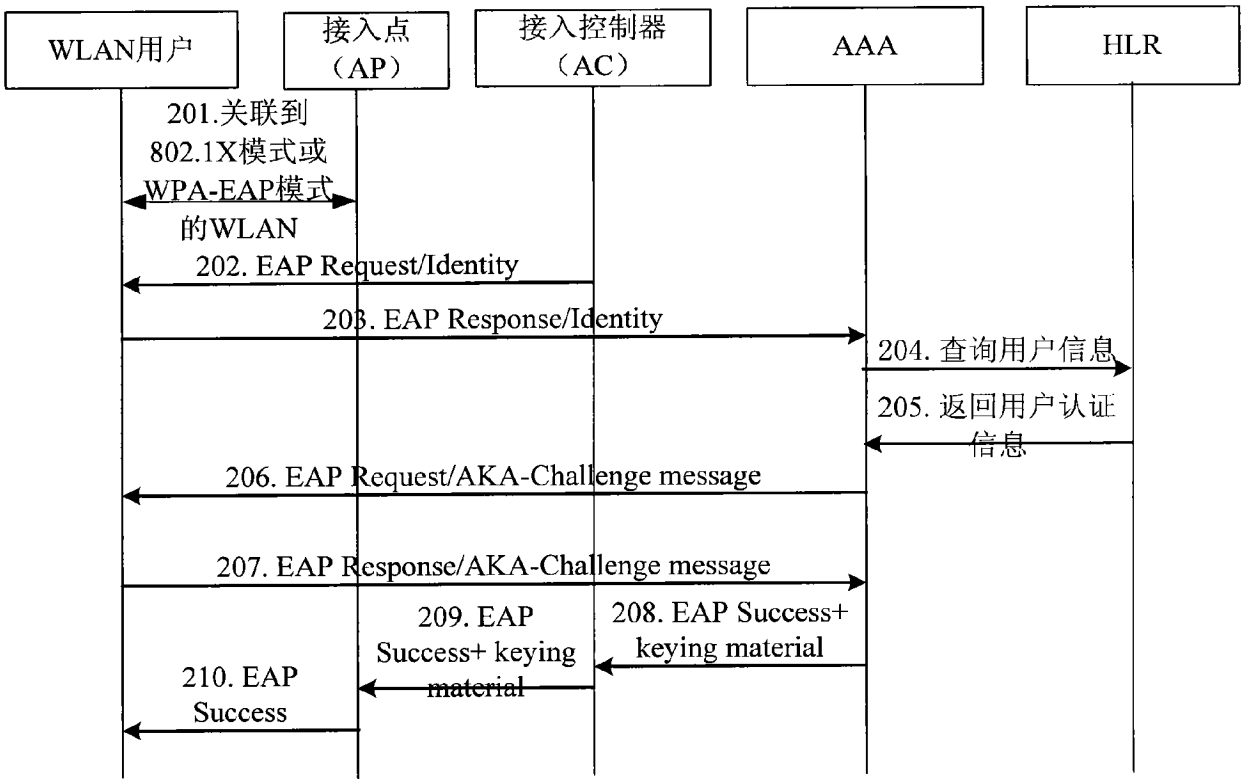

WLAN用户
接入点（AP）
接入控制器（AC）
AAA
HLR
201.关联到802.1X模式或WPA-EAP模式的WLAN
202. EAP Request/Identity
203. EAP Response/Identity
204. 查询用户信息
205. 返回用户认证信息
206. EAP Request/AKA-Challenge message
207. EAP Response/AKA-Challenge message
208. EAP Success+ keying material
209. EAP Success+ keying material
210. EAP Success

图 2

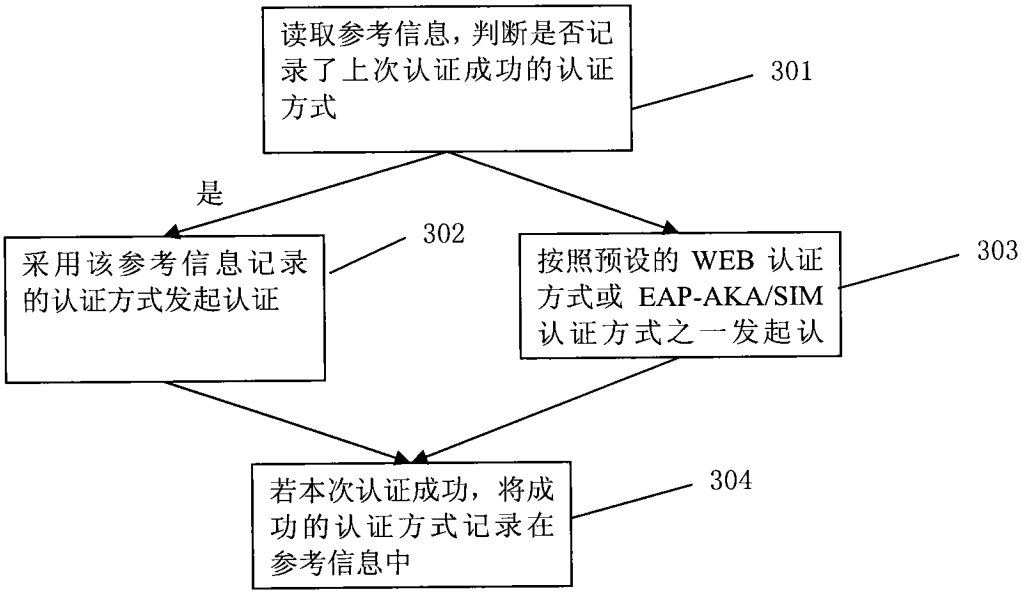

读取参考信息，判断是否记录了上次认证成功的认证方式
301
是
采用该参考信息记录的认证方式发起认证
302
按照预设的 WEB 认证方式或 EAP-AKA/SIM 认证方式之一发起认
303
若本次认证成功，将成功的认证方式记录在参考信息中
304

图 3

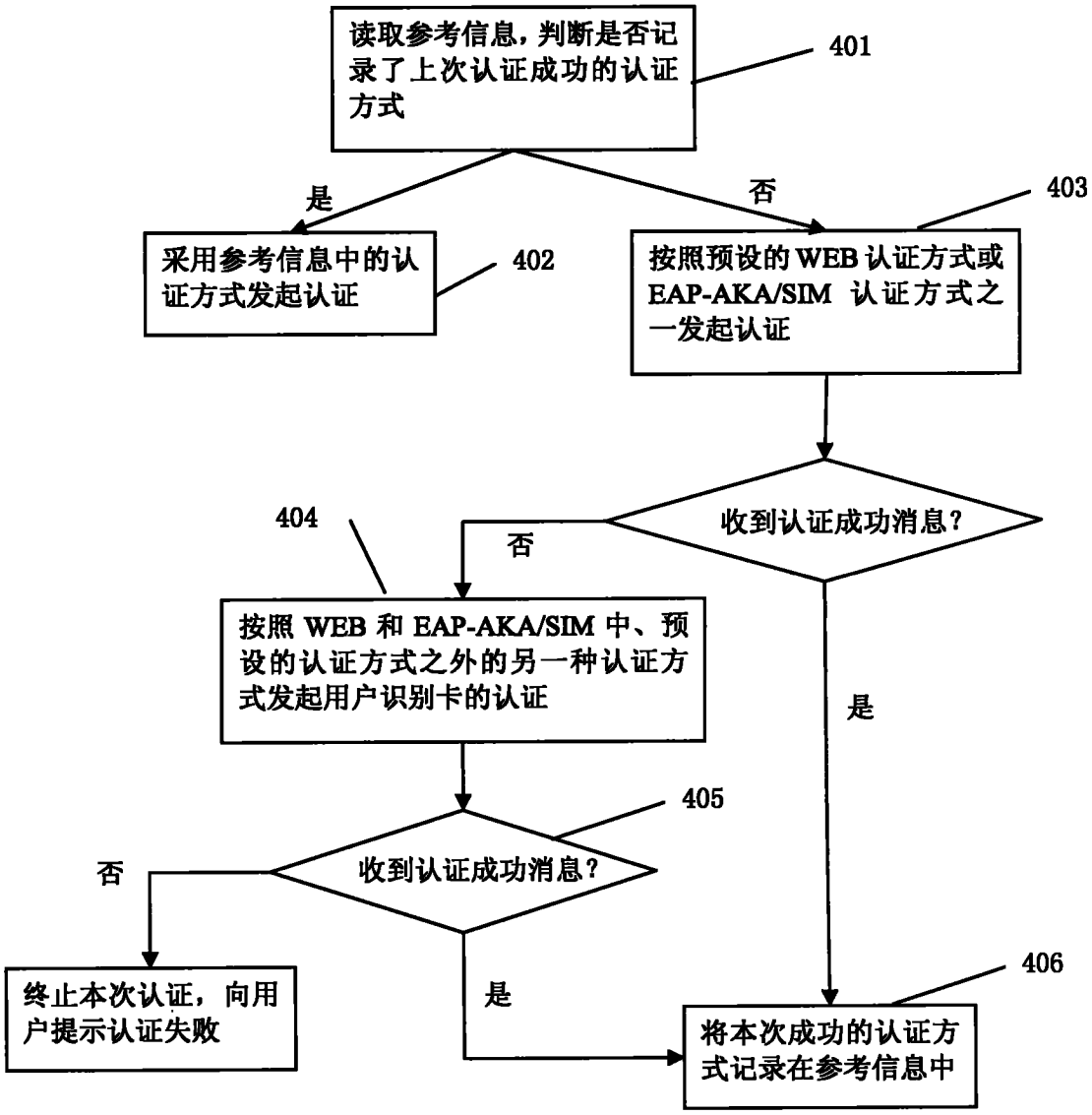

读取参考信息，判断是否记录了上次认证成功的认证方式
401
是
否
采用参考信息中的认证方式发起认证
402
按照预设的WEB认证方式或EAP-AKA/SIM 认证方式之一发起认证
403
收到认证成功消息？
404
否
是
按照 WEB 和 EAP-AKA/SIM 中、预设的认证方式之外的另一种认证方式发起用户识别卡的认证
405
收到认证成功消息？
否
是
终止本次认证，向用户提示认证失败
将本次成功的认证方式记录在参考信息中
406

图 4