# (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2010 年 1 月 7 日 (07.01.2010)

PCT

(10) 国际公布号
WO 2010/000185 A1

(51) 国际专利分类号:
*H04W 12/06* (2009.01) *H04W 12/04* (2009.01)

(21) 国际申请号: PCT/CN2009/072447

(22) 国际申请日: 2009 年 6 月 25 日 (25.06.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810068193.9 2008 年 6 月 30 日 (30.06.2008) CN



(71) 申请人 (对除美国外的所有指定国): **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **宫小玉 (GONG, Xiaoyu)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **李洪广 (LI, Hongguang)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京凯特来知识产权代理有限公司 (BEIJING CATALY IP ATTORNEY AT LAW)**; 中国北京市海淀区大柳树路甲 2 号中铁科大厦 8 层南区郑立明, Beijing 100081 (CN)。



(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。


(54) **Title**: A METHOD, APPARATUS, SYSTEM AND SERVER FOR NETWORK AUTHENTICATION

(54) **发明名称**: 一种网络认证的方法、装置、系统及服务器

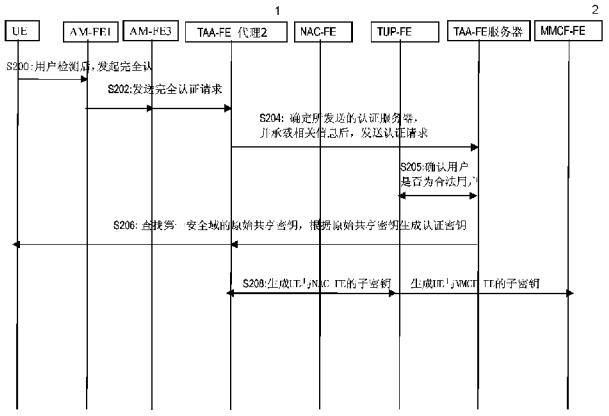


图2 / Fig. 2

S200 AFTER USER DETECTING, INITIATING THE FULL AUTHENTICATION
S202 SENDING THE FULL AUTHENTICATION REQUEST
S204 AFTER CONFIRMING THE AUTHENTICATION SERVER TO SEND AND CARRYING THE ASSOCIATED INFORMATION, TRANSMITTING THE AUTHENTICATION REQUEST
S205 VALIDATING THE USER AUTHENTICATED OR NOT
S206 SEARCHING FOR THE ORIGINAL SHARED KEY OF THE FIRST SECURITY DOMAIN, GENERATING THE AUTHENTICATION KEY BASED ON THE ORIGINAL SHARED KEY
S208 GENERATING THE SUB KEY BETWEEN UE AND NAC-FE, GENERATING THE SUB KEY BETWEEN UE AND MMCF-FE
1 TAA-FE AGENT PROXY2
2 TAA-FE SERVER


(57) **Abstract**: A method, apparatus, system and server for network authentication are provided. The method includes that: receiving a user authentication request from and forwarded by a second access management function entity, when the user is attached to the second access management function entity from a first access management function entity; obtaining a authentication key of the security domain of the second access management function entity, according to the user authentication request; authenticating the user based on the authentication key. The problem of losing packets of the user service and even interrupting the service temporarily in prior arts, caused by the long consuming time and weak security during the user intra-domain or inter-domain handover, is resolved, the safe authentication of the user intra-domain or inter-domain roaming is realized, the security and reliability of user authentication are improved.

(57) **摘要**: 本发明提供了一种网络认证的方法、装置、系统及服务器。本发明所述方法包括：当用户从第一接入管理功能实体附着到第二接入管理功能实体时，接收来自所述第二接入管理功能实体转发的用户认证请求；根据所述用户认证请求，获得所述第二接入管理功能实体的安全域的认证密钥；根据所述认证密钥，对用户进行认证。解决了现有技术中用户在域内和域间切换时，耗时长，且安全性差，导致用户业务的丢包甚至暂时中断业务的问题，实现了用户在域内或者域间移动的安全的认证，提高了用户认证的安全性、可靠性。



WO 2010/000185 A1

# 说明书

## 一种网络认证的方法、装置、系统及服务器

[1] 本申请要求于2008年06月30日提交中国专利局、申请号为200810068193.9、发明名称为“一种网络认证的方法、装置、系统及服务器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

[2] 技术领域

[3] 本发明涉及通信领域的网络技术，具体指一种网络认证的方法、装置、系统及服务器。

[4] 发明背景

[5] 目前，在下一代网络（Next Generation Network，NGN）的网络架构中，强调了固定和移动的网络融合，基于这个融合的网络，当用户切换到新的网络附着点的时候，从安全角度考虑需要进行安全认证。当用户通过安全认证之后，才能够被网络接纳，同时，在用户和网络之间建立子密钥，保护后续用户和网络侧的信息交互。因此，当用户在不同网络附着点间移动的时候，给用户提供更好的业务体验，快速、低时间延迟的无缝切换是非常有必要的。

[6] 对于移动用户，存在两种认证需求。一个是网络接入认证(network access service authentication)需求, 另一个是移动认证(mobility service authentication)。网络接入认证已经在ITU、TISAPAN 都有相应的标准，称为网络附着子系统（Network Attachment Control Functions，NACF），规定了用户在接入到网络之前所需要的认证，例如用户的IP地址分配，向用户设备发布其他的网络配置参数等过程。移动认证是移动业务认证，通过移动认证的用户，才可以在网络间进行漫游和切换。从二者实现方式上看，可以分为融合式和独立式两种。独立式是指网络接入认证和移动认证各自独立，采用不同的认证系统独立认证互不影响。网络接入认证就用现在ITU Y.NACF，TISPAN NASS等类似的网络附着功能来实现，移动认证则另外采用独立的认证功能实体

来实现。在融合式模式下，移动用户通过一套认证系统一次认证来同时解决网络接入认证和移动认证。一旦用户被认证通过，即可认为网络接入认证和移动认证都通过了，用户可以接入到网络，可以在网络间进行移动。由于用户在移动过程中在目标切换网络的认证相对目标网络来讲，也是一次网络接入认证，因此二者存在一定的内在关联，故而基于融合式认证的方法更容易被接受。

[7] 在实现本发明的过程中，发明人发现现有技术至少存在如下问题：

[8] 上述的认证过程，需要被认证者和网络侧认证功能实体多次交互才能完成。特别是在移动场景中，用户需要在同种甚至异种接入网络中进行切换，如果每次都需要复杂的完整的认证过程，那么用户在域内和域间切换时就会非常耗时，且安全性差，导致用户业务的丢包甚至暂时中断业务，影响用户的体验。

[9] 发明内容

[10] 有鉴于此，本发明实施例的主要目的在于提供一种网络认证的方法、装置、系统及服务器，用以解决用户在域内和域间切换时，耗时长，且安全性差的问题。

[11] 为实现上述目的，本发明实施例提供如下的技术方案：

[12] 一种网络认证方法，包括：当用户从第一接入管理功能实体附着到第

[13] 二接入管理功能实体时，所述方法包括：接收来自所述第二接入管理功能实体转发的用户认证请求；根据所述用户认证请求，获得所述第二接入管理功能实体的安全域的认证密钥；根据所述第二接入管理功能实体的安全域的认证密钥，对用户进行认证。

[14] 一种网络认证系统，包括：接入管理功能实体、传送层认证功能实体代理；所述接入管理功能实体，用于与传送层认证功能实体代理进行信息交互，发送用户认证请求给传送层认证功能实体代理；所述传送层认证功能实体代理，用于根据所述用户认证请求，获得用户附着的安全域的认证密钥；根据所述用户附着的安全域的认证密钥，对用户进行认证。

[15] 一种传送层认证功能实体代理装置，包括：存储单元，用于存储接入管理功能实体的安全域的认证密钥；处理单元，用于根据存储单元存储的认证密钥，为所述安全域的其他接入管理功能实体和用户之间的信息交互派生密钥，并将所

述派生的密钥发送给认证单元；认证单元：用于根据处理单元发送的所述派生的密钥，对用户进行认证。

[16] 一种网络认证服务器，包括：请求接收单元，用于接收用户认证请求；请求响应单元，用于响应所述用户认证请求，并向传送层认证功能实体代理发送响应信息，所述响应信息包括用户附着的认证结果、用户附着的根认证密钥、接入管理功能实体所属安全域的认证密钥；所述安全域的认证密钥由所述用户附着根密钥信息和安全域的标识ID、域名信息派生。

[17] 本发明实施例能够解决现有技术中用户在域内和域间切换时，耗时长，且安全性差，导致用户业务的丢包甚至暂时中断业务的问题，实现了用户在域内或者域间移动的安全认证，提高了用户认证的安全性、可靠性。

[18] 附图简要说明

[19] 图1-1为本发明实施方式中一种跨安全域的组网示意图；

[20] 图1-2为本发明实施方式中一种安全域内的组网示意图；

[21] 图2为本发明实施方式中一种跨安全域的网络认证方法流程图；

[22] 图3为本发明实施方式中一种安全域内的网络认证方法流程图；

[23] 图4为本发明实施方式中一种网络认证系统的结构图；

[24] 图5为本发明实施方式中一种传送层认证功能实体代理装置结构图；

[25] 图6为本发明实施方式中一种网络认证服务器的组成结构图。

[26] 实施本发明的方式

[27] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明的实施例作进一步地详细描述。

[28] 本发明实施例提供了一种网络认证方法，当用户从接入管理功能实体附着到第二接入管理功能实体时，接收来自所述第二接入管理功能实体转发的用户认证请求；根据所述用户认证请求，获得所述第二接入管理功能实体的安全域的认证密钥；根据所述第二接入管理功能实体的安全域的认证密钥，对用户进行认证。所述认证请求具体为：用户第一次接入安全域的完全认证和用户在安全域内的重新认证；所述第二接入管理功能实体的安全域的认证密钥具体根据第一接入管理功能实体和所述第二接入管理功能实体是否属于同一安全域而不同。

[29] 本发明实施例的应用场景为，用户的业务签约地在家乡网（Home Network），所述用户的移动业务相关信息存储在家乡网，当用户漫游到拜访网（Visited Network），在拜访地进行域内切换和跨域（即域间）切换。

[30] 所述移动业务相关信息为配置信息，共享密钥（即原始会话协商密钥），移动业务配置参数等信息。所述拜访网的安全域（也称“接入管理域”）是根据每个域按照唯一一组管理实体组成来划分的，所述管理实体组包括移动管理功能子系统（Mobility Management Control Functions，MMCF）、传送层认证授权功能实体（Transport Authentication Funtional Entity，TAA-FE）、接入管理功能实体（Access Management Functional Entity，AM-FE）的一种或几种的组合。

[31] 下面具体结合下面的附图进行详细说明

[32] 请参阅图1-1所示一种跨安全域的组网示意图，结合图2对本发明实施方式中一种跨安全域的网络认证方法流程图作具体介绍。

[33] 所述图1-1为用户10从所在第一安全域20附着至第二安全域30的组网示意图。用户10从所在第一安全域20的接入管理功能实体2002（Access Management Functional Entity，AM-FE1）移动至第二安全域30的接入管理功能实体3002（AM-FE3），第二安全域30的传送层认证授权功能实体代理3006（Transport Authentication and Authorization Functional Entity，TAA-FEproxy2）根据用户发送的完全认证请求，确定第二安全域的认证密钥，根据所述第二安全域的认证密钥，对所述用户进行完全认证。结合图2对网络认证的方法作进一步地详细描述。

[34] 在步骤S200中，用户（UE）发起完全认证请求。

[35] 用户在跨域认证前需要判断附着点AM-FE1和AM-FE3是在同一安全域内还是在不同的安全域，具体判断步骤如下：

[36] 用户向周边发起二层链路扫描，发现周边的接入点，并获得周边接入点（Access Point，AP）或基站（Base Station，BS）的标识；然后用户携带备选或目标接入点的标识信息，向当前所

在网络发起查询，获得备选或目标接入点所属的接入域信息，即本发明实施例中AM-FE3的信息；若用户根据查询结果，检测到AM-FE1和AM-FE3在不同的安全域，则用户发起完全认证请求；若AM-FE1和AM-FE3在相同的安全域，则用户发起重新认证请求。本发明实施例的图2流程图即为AM-FE1和AM-FE3在不同的安全域，即域间切换认证的场景，即发起完全认证请求。所述用户为移动用户，例如手机终端等；所述完全认证请求为预先完全认证（Pre-Authentication）。所述认证请求包括用户名、密码、用户初始门控信息、家乡域信息、用户标识等。

[37] 步骤S202中：AM-FE1将所述完全认证请求发送给AM-FE3，所述AM-FE3转发给TAA-FE proxy2。

[38] 步骤S204中：所述TAA-FE proxy2将用户相关的信息承载在所述认证请求中，判断并发送所述完全认证请求给TAA-FE sever进行安全认证。

[39] 所述认证服务器TAA-FE sever位于家乡网，TAA-FE proxy2位于拜访网的第二安全域中，因此所述TAA-FE proxy2根据接收的完全认证请求信息中的家乡网信息将所述完全认证请求发送给家乡网的TAA-FE sever并将AM-FE3的域名或域标识(ID)等用户相关的信息承载在所述完全认证请求中。

[40] 所述认证请求包括：用户附着的安全域的标识（ID）或者域名信息的一种或多种的任意组合，也可以包括用户协商的序列号（SEQ）等信息。

[41] 步骤S205中：所述TAA-FE sever根据认证请求，与第一安全域内的传送层用户配置库功能实体（TUP-FE）进行信息交互，确认用户是否为合法用户。

[42] 具体为：所述认证服务器根据认证请求，与第一安全域内的传送层用户配置库功能实体（TUP-FE）进行信息交互，获取第一安全域内TUP-FE的移动配置信息；根据所述移动配置信息，通过挑战字协商，原始共享密钥等对所述用户身份信息（ID）进行认证，确认所述用户是否为合法用户。

[43] 所述传送层用户配置库功能实体（TUP-FE）存储所述用户的移动配置信息，

所述移动配置信息包括：传送用户标识、支持的认证方法列表、密钥、移动用户的网络配置信息(如：IP地址)、最大接入带宽、网络切换策略等信息的一种或多种。

[44] 步骤S206：所述TAA-FE

sever根据所述安全认证请求携带的用户信息和AM-FE3所在安全域的域ID或域名，生成用户附着根密钥信息并派生出所在安全域的认证密钥（DSRK），并存储当前域的认证密钥，同时，将所述安全域的认证密钥返回给TAA-FE proxy2。

[45] 具体为：所述TAA-FE

sever根据所述安全认证请求中携带的用户信息和AM-FE3所在安全域的域ID或域名，生成AM-FE3所在安全域的认证密钥（DSRK），将所述认证密钥发送给所述第二安全域内的第二传送层认证功能实体代理TAA-FE proxy2。由TAA-FE proxy2分层次生成该用户和本安全域的其他功能实体之间的认证密钥，使得系统便于统一管理和存储安全域的认证密钥信息。

[46] 步骤S208：TAA-FE

proxy2根据认证服务器返回的认证密钥，对用户进行认证。

[47] 所述TAA-FE

proxy2接收到当前安全域的认证密钥（DSRK）并保存，同时，所述TAA-FE proxy2根据所述认证密钥(DSRK)，与用户进行协商，生成所述用户和所述第二安全域内的其他功能实体之间的子密钥；并将相应的子密钥配置到相应的功能实体，即所述TAA-FE

proxy2根据接收到当前域的认证密钥（DSRK），生成用户与NAC-FE之间的子密钥，以及生成用户与MMCF之间的子密钥；同时，所述TAA-FE proxy2将相应的子密钥分别配置到相应的功能实体上，建立起用户到各个功能实体之间的安全通道，完成初始化用户认证，以充分保证后续过程信息交互的安全性和可靠性。所述子密钥也可以理解为所述用户和所述第二安全域内的其他功能实体之间的安全联盟。所述第二安全域内的其他功能实体至少包括：网络地址配置功能实体NAC-FE、和移动管理功能子系统MMCF，即完成用户的完全认证，以充分保证后续过程信息交互的安全性和可靠性。

[48] 在本发明实施例中，通过用户检测到第一接入管理功能实体与第二接入管理功能实体属于不同安全域时，向位于家乡域的认证服务器发起完全认证请求；所述认证服务器根据传送层认证功能实体代理携带的用户信息和第二接入管理功能实体所属的域的标识（ID）或者域名，生成所属附着安全域的认证密钥(该安全域的认证密钥DSRK)，并发送给该安全域的传送层认证功能实体代理，该安全域的传送层认证功能实体代理与用户交互并生成保护用户与其它各功能实体信息交互子密钥，完成用户跨域的完全认证，在充分保证了用户在域间移动的安全性和可靠性的基础上，降低了用户在域内移动中的认证延时，使得用户体验到更为平滑的网络切换效果。

[49] 请参阅图1-2为一种安全域内的组网示意图，结合图3对本发明实施方式中一种安全域内的网络认证方法流程图作具体介绍。

[50] 所述图1-2为用户10从所在第一安全域20内的接入管理功能实体2002（Access Management Functional Entity，AM-FE1）附着至第一安全域20内的接入管理功能实体2004（AM-FE2）时的组网示意图。传送层认证授权功能实体代理2006（Transport Authentication and Authorization Functional Entity，TAA-FEproxy1）根据所述用户10发送的重新认证请求，确定第一安全域20的认证密钥；根据所述认证密钥对用户进行重新认证，结合图3对网络认证的方法作进一步地详细描述。

[51] 步骤S300：当用户在第一安全域内从AM-FE1附着至第一安全域内的

[52] AM-FE2时，用户发送重新认证请求。

[53] 具体为：用户在域内认证前需要判断附着点AM-FE1和AM-FE2是否在同一安全域内，具体判断步骤如下：

[54] 用户向周边发起二层链路扫描，发现周边的接入点，并获得周边接入点（Access Point，AP）或基站（Base Station，BS）的标识；然后用户携带备选或目标接入点的标识信息，向当前所在网络发起查询，获得备选或目标接入点所属的接入域信息，即本发明实施例中AM-FE2的信息；若用户通过判断结果，检测到AM-FE1和AM-FE2在相同的安

全域，则用户发起重认证请求；所述认证请求包括：用户附着的安全域的标识（ID）或者域名信息的一种或多种的任意组合，也可以包括用户协商的序列号（SEQ）等信息。

[55] 步骤S302中：AM-FE1将所述重新认证请求发送给AM-FE2，所述AM-FE2转发给TAA-FE proxy1。

[56] 步骤S304中：所述TAA-FE

proxy1接收到所述用户发送的重新认证请求时，根据所述第一安全域的认证密钥，对用户进行认证。

[57] TAA-FE

proxy1接收到所述用户发送的重新认证请求时，根据所述用户的重新认证请求，直接查找出所述用户与TAA-FE

proxy1之前的附着过程中协商好的认证密钥，即AM-FE1所在域的认证密钥；根据所述认证密钥，与功能实体NAC-FE、MMCF进行协商，生成相应的多个子密钥，并将多个子密钥配置到相应的功能实体，使得通过TAA-FE

proxy1，建立起用户到各个功能实体之间的子密钥，完成用户在第一安全域内从AM-FE1附着至第一安全域内的AM-FE2的重新认证，以充分保证后续过程信息交互的安全性和可靠性。

[58] 其中，所述第一安全域的认证密钥是用户首次接入安全域时完成完全认证过程中，由认证服务器生成并发送给TAA-FE proxy1，所述TAA-FE

proxy1保存所述第一安全域的认证密钥，当用户从同一安全域内的AM-FE1移动到AM-FE2时，直接查询获取AM-FE1所在安全域的认证密钥，并派生出其他子密钥（如用户和网络的传送子密钥，用户和NAC-FE的交互子密钥，用户和移动管理功能MMCF的交互子密钥）等等。

[59] 在本发明实施例中，通过TAA-FE

proxy1根据用户所在域的认证密钥（DSRK），对用户进行域内认证，实现了用户在域内一次认证成功后即可通过移动业务认证，使其在保证用户在域内移动的安全性和可靠性的基础上，降低了用户在域内移动中的重认证延时，使得用户体验到更为平滑的网络切换效果。

[60] 请参阅图4，为本发明实施方式中一种网络认证系统的组成结构示意图。

[61] 一种网络认证系统40，包括：接入管理功能实体402、传送层认证功能实体代理404。

[62] 所述接入管理功能实体402，用于与传送层认证功能实体代理404进行信息交互，发送用户认证请求给传送层认证功能实体代理404；进一步而言，所述接入管理功能实体402支持用户网络接入的预认证，所述预认证为本发明实施例提到的用户重新认证和用户完全认证。

[63] 所述传送层认证功能实体代理404，用于转发所述用户认证请求，并获得用户附着的安全域的认证密钥；根据所述用户附着的安全域的认证密钥，生成用户与各个网络实体交互的子密钥（如用户和网络的传送子密钥，用户和NAC-FE的交互子密钥，用户和移动管理功能MMCF的交互子密钥）并对用户进行认证。即所述子密钥由所述安全域的传送层认证功能实体代理根据安全域的认证密钥派生。所述用户附着的安全域为与所述接入管理功能实体的安全域相同的其它接入管理功能实体的安全域；和/或所述用户附着的安全域为与所述接入管理功能实体的安全域不相同的其它接入管理功能实体的安全域。

[64] 所述传送层认证功能实体代理404支持对一个用户会话的，来自不同的接入管理功能实体的多个关联绑定状态。多个关联绑定状态中，有一个是Active状态，其他是Proactive状态，并能根据移动切换状态的情况进行关联状态转换。

[65] 所述系统进一步还包括：认证服务器406，和/或其它功能实体408。

[66] 所述认证服务器406：用于接收用户认证请求，根据用户认证请求向所述传送层认证功能实体代理404发送响应信息，所述响应信息包括用户附着的认证结果、用户附着的接入管理功能实体的安全域的认证密钥的一种或多种。所述认证密钥根据安全域的标识ID和/或域名信息以及用户附着根密钥信息而生成。

[67] 所述其它功能实体408，所述其它功能实体408与用户之间具有基于所述认证密钥派生的子密钥，其中，所述其它功能实体408包括网络地址配置功能实体、传送层用户配置功能实体和移动管理功能子系统的一个或多个功能实体。其中，网络地址配置功能实体，用于实现IP地址和接入参数的配置；传送层用户配置功能实体，用于保存用户移动相关的配置信息及用户订制的配置文件，例如：不

同接入技术下允许支持的最大接入带宽，网络切换策略，移动位置管理器地址等；移动管理功能子系统，用于实现用户的地址绑定更新功能；还可以包括：传送位置管理功能实体，用于支持一个用户会话的多个关联绑定状态，并能根据移动切换的情况，进行状态转化，并将目标或备选接入点的位置信息（如接入点AP信息或基站BS信息，以及目标或备选接入管理功能实体的信息或接入路由器的信息），作为位置信息，提供给资源接纳控制功能子系统。

[68] 请参阅图5，为本发明实施方式中一种传送层认证功能实体代理装置的组成结构示意图，包括：

[69] 存储单元502：用于存储第一接入管理功能实体所属安全域的认证密钥，所述认证密钥由认证服务器TAA-Server
在用户认证通过后生成的用户附着根密钥信息生成；

[70] 处理单元504：用于根据存储单元存储的所述认证密钥，为本安全域的其他接入管理功能实体和用户之间的信息交互派生密钥，并将所述派生的密钥发送给认证单元；

[71] 认证单元506：用于根据处理单元发送的所述派生的密钥，对用户进行认证。

[72] 请参阅图6，为本发明实施方式中一种网络认证服务器的组成结构示意图。

[73] 一种网络认证服务器60，其特征在于，包括：请求接收单元602，用于接收用户认证请求；请求响应单元604，用于响应所述用户认证请求，并向传送层认证功能实体代理发送响应信息，所述响应信息包括用户附着的认证结果、用户附着的接入管理功能实体所属安全域的域认证密钥；其中，所述安全域的认证密钥由所述用户附着的根密钥信息和安全域的标识ID、域名等信息派生而来。

[74] 综上所述，本发明实施例提出了一种网络认证的方法、装置、系统及服务器，克服了现有技术中用户在域内和域间切换时，耗时长，且安全性差，导致用户业务的丢包甚至暂时中断业务的问题，实现了用户在域内或者域间移动的快速、安全的认证，降低了用户在移动过程中的重新认证延时，提高了用户认证的安全性、可靠性，确保了无缝的、更为平滑的网络切换效果。

[75] 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，都应该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。

# 权利要求书

[1] 一种网络认证方法，其特征在于，当用户从第一接入管理功能实体附着到第二接入管理功能实体时，所述方法包括：

接收来自所述第二接入管理功能实体转发的用户认证请求；

根据所述用户认证请求，获得所述第二接入管理功能实体的安全域的认证密钥；

根据所述第二接入管理功能实体的安全域的认证密钥，对用户进行认证。

[2] 根据权利要求1所述的网络认证方法，其特征在于，所述第一接入管理功能实体，所述第二接入管理功能实体属于不同安全域，所述获得所述第二接入管理功能实体的安全域的认证密钥的步骤具体包括：

根据所述第二接入管理功能实体的安全域的标识ID和/或域名信息生成所述第二接入管理功能实体的安全域的认证密钥；和/或

将所述第二接入管理功能实体的安全域的标识ID和/或域名信息发送给认证服务器，并接收所述认证服务器返回的所述第二接入管理功能实体的安全域的认证密钥。

[3] 根据权利要求1所述的网络认证方法，其特征在于，所述第一接入管理功能实体和所述第二接入管理功能实体属于同一安全域，所述获得所述第二接入管理功能实体的安全域的认证密钥的步骤具体包括：

获得所述第一接入管理功能实体的安全域的认证密钥，将获得的所述第一接入管理功能实体的安全域的认证密钥作为所述第二接入管理功能实体的安全域的认证密钥。

[4] 根据权利要求1所述的网络认证方法，其特征在于，所述方法进一步包括：

根据所述认证密钥，与用户进行协商，生成所述用户和其他功能实体之间的子密钥；所述其他功能实体包括网络地址配置功能实体、传送层用户配置功能实体和移动管理功能子系统的一个或多个功能实体。

[5] 一种网络认证系统，其特征在于，包括：接入管理功能实体、传送层认证功能实体代理；

所述接入管理功能实体，用于与传送层认证功能实体代理进行信息交互，

发送用户认证请求给传送层认证功能实体代理；

所述传送层认证功能实体代理，用于根据所述用户认证请求，获得用户附着的安全域的认证密钥；根据所述用户附着的安全域的认证密钥，对用户进行认证。

[6] 根据权利要求5所述的网络认证系统，其特征在于，所述用户附着的安全域为其它接入管理功能实体的安全域，其中，所述其它接入管理功能实体的安全域与所述接入管理功能实体的安全域相同和/或不同。

[7] 根据权利要求5所述的网络认证系统，其特征在于，所述系统进一步包括：

认证服务器：用于接收用户认证请求，根据用户认证请求向所述传送层认证功能实体代理发送响应信息，所述响应信息包括用户附着的认证结果、用户附着的接入管理功能实体所属安全域的认证密钥。

[8] 根据权利要求5、6或7所述的网络认证系统，其特征在于，所述安全域的认证密钥由安全域的标识ID和/或域名信息以及用户附着根密钥信息确定。

[9] 根据权利要求5所述的网络认证系统，其特征在于，所述系统进一步包括其它功能实体，所述其它功能实体与用户之间具有基于所述认证密钥的子密钥，其中，所述其它功能实体包括网络地址配置功能实体、传送层用户配置功能实体和移动管理功能子系统的一个或多个功能实体；

所述子密钥由所述安全域的传送层认证功能实体代理根据安全域的认证密钥派生。

[10] 一种传送层认证功能实体代理装置，其特征在于，包括：

存储单元：用于存储接入管理功能实体所属安全域的认证密钥；

处理单元：用于根据存储单元存储的认证密钥，为所述安全域的其他接入管理功能实体和用户之间的信息交互派生密钥，并将所述派生的密钥发送给认证单元；

认证单元：用于根据处理单元发送的所述派生的密钥，对用户进行认证。

[11] 一种网络认证服务器，其特征在于，包括：

请求接收单元，用于接收用户认证请求；

请求响应单元，用于响应所述用户认证请求，并向传送层认证功能实体代

理发送响应信息，所述响应信息包括用户附着的认证结果、用户附着的接入管理功能实体所属安全域的认证密钥；所述安全域的认证密钥由所述用户附着根密钥信息和安全域的标识ID、域名信息派生。

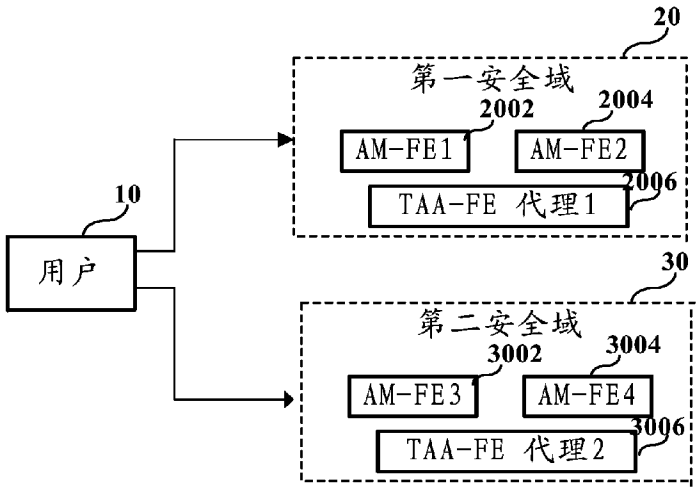
20
第一安全域
2002
2004
AM-FE1
AM-FE2
2006
TAA-FE 代理1
10
用户
30
第二安全域
3002
3004
AM-FE3
AM-FE4
3006
TAA-FE 代理2

图1-1

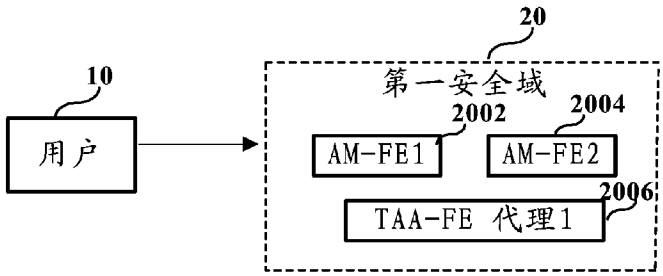
20
第一安全域
2002
2004
AM-FE1
AM-FE2
2006
TAA-FE 代理1
10
用户

图1-2

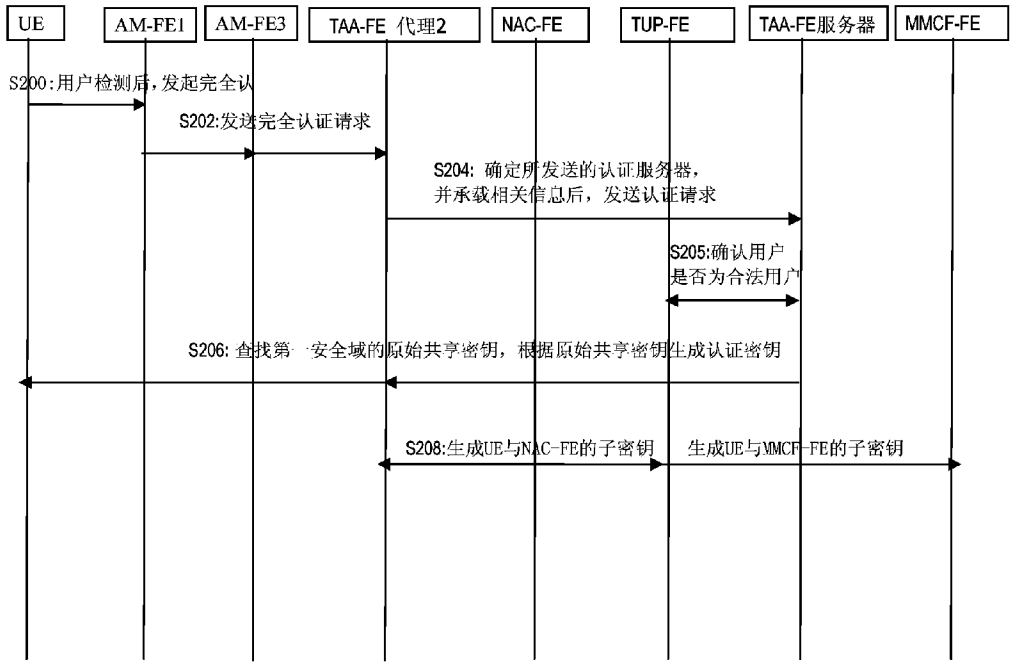
UE
AM-FE1
AM-FE3
TAA-FE 代理2
NAC-FE
TUP-FE
TAA-FE服务器
MMCF-FE
S200:用户检测后，发起完全认
S202:发送完全认证请求
S204: 确定所发送的认证服务器，
并承载相关信息后，发送认证请求
S205:确认用户
是否为合法用户
S206: 查找第一安全域的原始共享密钥，根据原始共享密钥生成认证密钥
S208:生成UE与NAC-FE的子密钥
生成UE与MMCF-FE的子密钥

图2

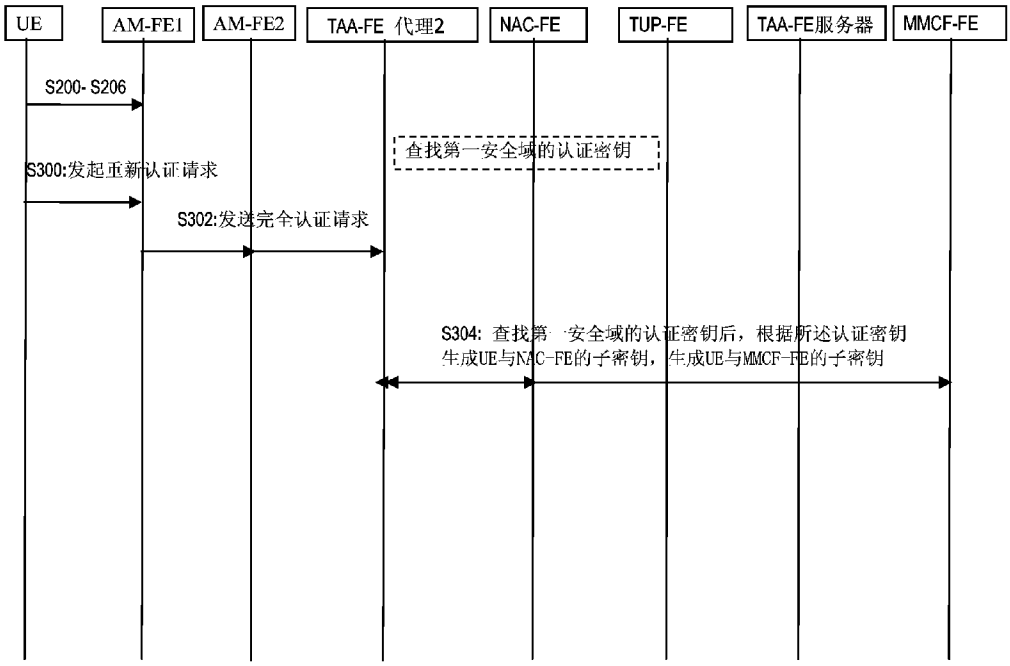
UE
AM-FE1
AM-FE2
TAA-FE 代理2
NAC-FE
TUP-FE
TAA-FE服务器
MMCF-FE
S200- S206
查找第一安全域的认证密钥
S300:发起重新认证请求
S302:发送完全认证请求
S304: 查找第一安全域的认证密钥后，根据所述认证密钥
生成UE与NAC-FE的子密钥，生成UE与MMCF-FE的子密钥

图3

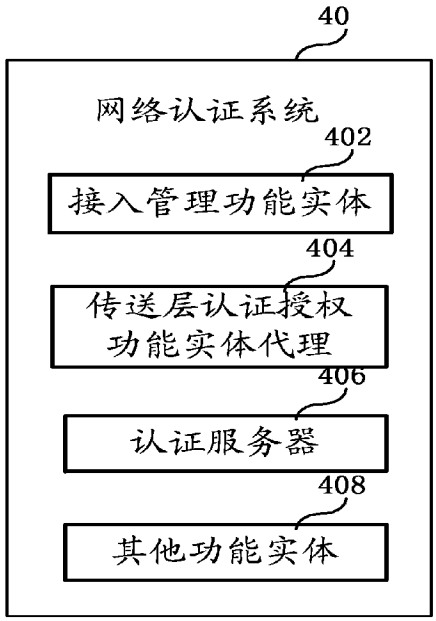
40
网络认证系统
402
接入管理功能实体
404
传送层认证授权
功能实体代理
406
认证服务器
408
其他功能实体

图4

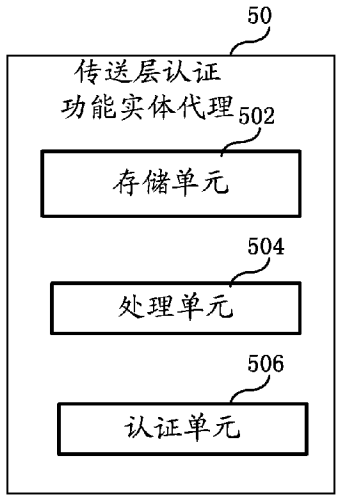
50
传送层认证
功能实体代理
502
存储单元
504
处理单元
506
认证单元

图5

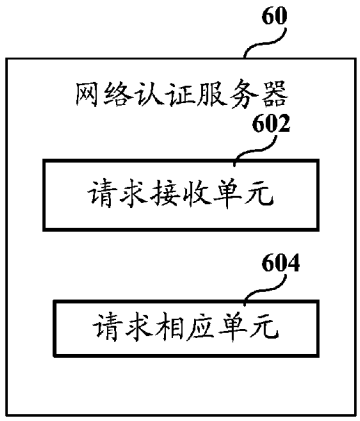


图6

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/072447

**A. CLASSIFICATION OF SUBJECT MATTER**

See extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, PAJ, IEEE: across w domain inter-domain intra-domain (safety or security) w domain? key? authenti+ authoriz+ handoff handover roam+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN1921379A (HUAWEI TECHNOLOGIES CO LTD), 28 Feb.2007(28.02.2007), See the description page 1 line 12 to page 2 line 24, page 8 line 3 to page 10 line 8, figures 1,4-5 | 1-11 |
| X | CN1794682A (HUAWEI TECHNOLOGIES CO LTD), 28 June 2006 (28.06.2006), See the description page 6 line 23 to page 10 line 4, figures 1-3 | 1-11 |
| X | CN1905734A (HUAWEI TECHNOLOGIES CO LTD), 31 Jan. 2007(31.01.2007), See the description page 2 lines 11-20, page 8 line 3 to page 10 line 8, figures 4-5 | 1-11 |
| A | WO2005015938A1 (DOCOMO COMMUNICATIONS LAB EURO GMBH), 17 Feb. 2005 (17.02.2005), The whole document | 1-11 |
| A | JP2008015696A (SOFTBANK MOBILE CORP ET-AL), 24 Jan. 2008(24.01.2008), The whole document | 1-11 |

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 08 Sep. 2009 (08.09.2009) | **01 Oct. 2009 (01.10.2009)** |
| Name and mailing address of the ISA/CN<br>The State Intellectual Property Office, the P.R.China<br>6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088<br>Facsimile No. 86-10-62019451 | Authorized officer<br>FU qi<br>Telephone No. (86-10)62411231 |

Form PCT/ISA /210 (second sheet) (July 2009)

# INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/072447

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN1921379A | 28.02.2007 | None | |
| CN1794682A | 28.06.2006 | None | |
| CN1905734A | 31.01.2007 | None | |
| WO2005015938A1 | 17.02.2005 | AU2003255352A1 | 25.02.2005 |
| | | EP1649715A1 | 26.04.2006 |
| | | JP2007515814T | 14.06.2007 |
| | | DE60317243E | 13.12.2007 |
| | | DE60317243T2 | 07.08.2008 |
| JP2008015696A | 24.01.2008 | None | |

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/072447

**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 12/06 (2009.01) i
H04W 12/04 (2009.01) i

# 国际检索报告

国际申请号
**PCT/CN2009/072447**

**A. 主题的分类**

参见附加页

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

**B. 检索领域**

检索的最低限度文献(标明分类系统和分类号)

IPC: H04W, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNKI, CNPAT：跨域 域间 域内 安全域 密钥 认证 鉴权 切换 漫游

WPI, EPODOC, PAJ, IEEE：across w domain inter-domain intra-domain (safety or security) w domain? key? authenti+ authoriz+ handoff handover roam+

**C. 相关文件**

| 类 型* | 引用文件，必要时，指明相关段落 | 相关的权利要求 |
|---|---|---|
| X | CN1921379A（华为技术有限公司），28.2 月 2007（28.02.2007），参见说明书第 1 页 12 行至第 2 页 24 行、第 8 页第 3 行至第 10 页第 8 行，图 1、4-5 | 1-11 |
| X | CN1794682A（华为技术有限公司），28.6 月 2006（28.06.2006），参见说明书第 6 页第 23 行至第 10 页第 4 行，图 1-3 | 1-11 |
| X | CN1905734A（华为技术有限公司），31.1 月 2007（31.01.2007），参见说明书第 2 页 11 至 20 行、第 8 页第 3 行至第 10 页第 8 行，图 4-5 | 1-11 |
| A | WO2005015938A1（DOCOMO COMMUNICATIONS LAB EURO GMBH），17.2 月 2005（17.02.2005），全文 | 1-11 |
| A | JP2008015696A（ SOFTBANK MOBILE CORP ET-AL），24.1 月 2008（24.01.2008），全文 | 1-11 |

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

| 国际检索实际完成的日期 | 国际检索报告邮寄日期 |
|---|---|
| 08.9 月 2009（08.09.2009） | **01.10 月 2009 (01.10.2009)** |
| ISA/CN 的名称和邮寄地址：<br>中华人民共和国国家知识产权局<br>中国北京市海淀区蓟门桥西土城路 6 号 100088<br>传真号： (86-10)62019451 | 受权官员<br>傅琦<br>电话号码：(86-10) **62411231** |

# 国际检索报告

关于同族专利的信息

国际申请号
**PCT/CN2009/072447**

| 检索报告中引用的专利文件 | 公布日期 | 同族专利 | 公布日期 |
|---|---|---|---|
| CN1921379A | 28.02.2007 | 无 | |
| CN1794682A | 28.06.2006 | 无 | |
| CN1905734A | 31.01.2007 | 无 | |
| WO2005015938A1 | 17.02.2005 | AU2003255352A1 | 25.02.2005 |
| | | EP1649715A1 | 26.04.2006 |
| | | JP2007515814T | 14.06.2007 |
| | | DE60317243E | 13.12.2007 |
| | | DE60317243T2 | 07.08.2008 |
| JP2008015696A | 24.01.2008 | 无 | |

# 国际检索报告

国际申请号
**PCT/CN2009/072447**

A. 主题的分类

H04W 12/06 (2009.01) i

H04W 12/04 (2009.01) i