

## (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  
2007年8月2日 (02.08.2007)

PCT

(10) 国际公布号  
WO 2007/085175 A1

(51) 国际专利分类号:

H04L 9/32 (2006.01)

(21) 国际申请号:

PCT/CN2006/003601

(22) 国际申请日:

2006年12月26日 (26.12.2006)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

200610033377.2

2006年1月24日 (24.01.2006)

CN

200610074902.5

2006年4月4日 (04.04.2006)

CN

200610079252.3

2006年4月20日 (20.04.2006)

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

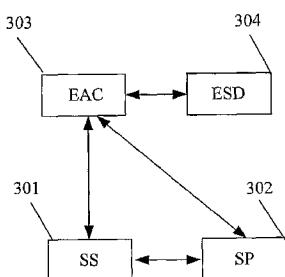
(75) 发明人/申请人 (仅对美国): 位继伟(WEI, Jiwei) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。范絮妍(FAN, Xuyan) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。李超(LI, Chao) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京德琦知识产权代理有限公司(DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

[见续页]

(54) Title: AUTHENTICATION METHOD, SYSTEM AND AUTHENTICATION CENTER BASED ON END TO END COMMUNICATION IN THE MOBILE NETWORK

(54) 发明名称: 基于移动网络端到端通信的认证方法、系统及认证中心



(57) Abstract: An authentication method based on end to end communication in the mobile network includes: the first service entity negotiates an authentication mode with an entity authentication center, in which the authentication mode includes: the authentication method between the first service entity and the entity authentication center, the authentication method between the second service entity and the entity authentication center, the method for looking up the authentication of the entity authentication center and the method for generating derived key, and the mutual authentication method between the first and the second service entity; said first and second service entity and entity authentication center carry out authentication for each other according to authentication mode respectively; when the first service entity requests the service provided by second service, said entity authentication center provides authentication inquiry to first and second service entity according to authentication mode and generates shared derived key between them the first and second service entity carry out mutual authentication using said shared derived key according to the authentication mode and generates conversation key.

(57) 摘要:

一种基于移动网络端到端通信的认证方法，该方法包括：第一业务实体与实体认证中心协商认证模式，该认证模式包括：该第一业务实体与实体认证中心之间的认证方法、第二业务实体与该实体认证中心之间的认证方法、该实体认证中心的认证查寻方法及衍生密钥生成方法、以及该第一和第二业务实体之间的互认证方法；所述第一和第二业务实体分别按该认证模式与该实体认证中心进行互认证；当该第一业务实体请求第二业务实体提供的业务时，所述实体认证中心按该认证模式为该第一和第二业务实体提供认证查询并生成二者之间的共享衍生密钥；该第一和第二业务实体使用所述共享衍生密钥按该认证模式进行互认证并生成会话密钥。

WO 2007/085175 A1



- (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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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。

所引用双字母代码及其它缩写符号, 请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

# 基于移动网络端到端通信的认证方法、系统及认证中心

## 技术领域

本发明属于网络通信服务技术领域，特别涉及一种基于移动网络端到端通信的认证方法及系统、业务实体的认证方法及系统、以及认证中  
5 心。

## 发明背景

目前，大多数应用服务器在向移动用户提供某一业务时，都首先与该移动用户建立相互信任的关系，例如：移动用户与认证代理之间、移动用户与公钥基础设施（PKI，Public Key Infrastructure）证书机构之间、  
10 移动用户与内容提供服务器之间等的信任关系。一般来说，这种信任关系是在移动用户与应用服务器之间的双向认证过程中确立的。

在第三代无线通信标准中，通用鉴权框架（GAA，General Authentication Architecture）是多种应用业务实体使用的一个用于对用户身份进行验证的通用结构，应用通用鉴权框架可实现对应用业务的用户  
15 进行检查和验证身份。上述多种应用业务可以是多播/广播业务、用户证书业务、信息即时提供业务等，也可以是代理业务。

图 1 为 GAA 的结构示意图，GAA 通常由用户 101、执行用户身份初始检查验证的实体（BSF）102、用户归属签约服务器（HSS，Home Subscriber Server）103 和网络应用功能实体（NAF，Network Application Function）104 组成。BSF 102 用于与用户 101 互验证身份，同时生成 BSF 102 与用户 101 的共享密钥；HSS 103 中存储用于描述用户信息的  
20 描述（Profile）文件，同时 HSS 103 还兼有产生鉴权信息的功能。

用户需要使用某种业务时，如果其知道该业务需要到 BSF 进行互鉴权过程，则直接到 BSF 进行互鉴权，否则，用户会首先和该业务对应的 NAF 联系，如果该 NAF 使用通用鉴权框架，并且发现发出请求的用户还未到 BSF 进行互认证过程，则通知发出请求的用户到 BSF 进行身份验证。  
5 验证。

用户与 BSF 之间鉴权成功后，用户和 BSF 之间互相认证了身份并且同时生成了共享密钥 K<sub>s</sub>，BSF 为这个密钥 K<sub>s</sub> 定义了一个有效期限，以便 K<sub>s</sub> 进行更新。之后，BSF 分配一个会话事务标识（B-TID，Bootstrapping Transaction Identifier）给用户，在将 B-TID 发送给用户设备（UE）的同时发送 K<sub>s</sub> 的有效期限，该 B-TID 是与 K<sub>s</sub> 相关联的。共享密钥 K<sub>s</sub> 是作为根密钥来使用的，不会离开用户的 UE 和 BSF，当用户和 NAF 通信时，将使用由 K<sub>s</sub> 衍生出的密钥 K<sub>s\_NAF</sub> 来进行通信保护。  
10  
15

该通用鉴权框架的缺点是：1、用户与BSF认证只支持一种认证方法（即AKA的认证方法）。2、该认证机制没有提供BSF与NAF的认证，容易使攻击者假冒NAF窃取用户的一些机密信息。

在3GPP2中，也存在一种通用的鉴权框架，参见图2。图2为现有的3GPP2中的通用鉴权框架图。3GPP2中的通用鉴权框架由移动节点（MN，Mobile Node）201，网络应用功能实体（NAF，Network Application Function）202，执行用户身份初始检查验证的实体（BSF）203，用户归属网络服务器（HSS）204，用户归属位置寄存器/鉴权中心（HLR/AC），和认证授权计费（AAA，Authentication Authorization Accounting）服务器组成。  
20  
25

MN若要使用NAF提供的业务，首先要与BSF进行互认证，互认证方法有三种（包括：AKA、基于CAVE的认证方法、基于AAA的认证方法），可以根据MN以及网络支持情况，以及运营商本地策略灵活选择认证方

法。

但是，该3GPP2的通用鉴权框架有以下缺点：1、它只支持三种认证方法，其不能适用于业务实体与多种网络之间的互认证。2、该认证机制仍然没有提供BSF与NAF的认证，容易使攻击者假冒NAF窃取用户的一些机密信息。  
5

综上所述，现有的通用鉴权框架仅能应用在所属的标准中，受到网络中业务实体与网络的限制，具有一定的局限性。

## 发明内容

本发明实施例的主要目的在于，为不同类型的实体之间建立相互信任关系提供一个适用于不同移动网络标准的通用认证框架。  
10

本发明实施例的技术方案如下：

本发明实施例公开了一种基于移动网络端到端通信的认证方法，应用于包括：请求业务的第一业务实体、提供业务的第二业务实体和实体认证中心的系统，该方法包括：

15 所述第一业务实体与所述实体认证中心协商认证模式，该认证模式包括：该第一业务实体与实体认证中心之间的认证方法、该第二业务实体与该实体认证中心之间的认证方法、该实体认证中心的认证查询方法及衍生密钥生成方法、以及该第一业务实体与该第二业务实体之间的互认证方法；

20 所述第一业务实体和第二业务实体分别按协商得到的认证模式中定义的认证方法与该实体认证中心进行互认证；

当第一业务实体请求第二业务实体提供的业务时，所述实体认证中心按该协商得到的认证模式中定义的认证查询方法为该第一业务实体和第二业务实体提供认证查询并按该协商得到的认证模式中定义的衍

生密钥生成方法生成二者之间的共享衍生密钥；

该第一业务实体和第二业务实体使用所述共享衍生密钥按该协商得到的认证模式中定义的二者之间的互认证方法进行互认证并生成保护本次业务的会话密钥。

5 本发明实施例还公开了一种业务实体认证方法，应用于业务实体和实体认证中心之中，该方法包括：

所述业务实体与所述实体认证中心协商认证模式，该认证模式至少用于定义：该业务实体与实体认证中心之间的认证方法；

该业务实体按协商得到的认证模式中定义的认证方法与该实体认  
10 证中心进行互认证。

本发明实施例公开了一种认证查询方法，应用于包括：用于请求业  
务的第一业务实体、用于提供业务的第二业务实体和实体认证中心的系  
统；所述第一业务实体和第二业务实体分别与所述实体认证中心进行互  
认证，该实体认证中心分别为该第一业务实体和第二业务实体分配临时  
15 身份信息，并分别获得自身与该第一业务实体和第二业务实体之间的共  
享密钥材料；所述第一业务实体与所述实体认证中心协商认证模式，该  
认证模式至少用于定义该实体认证中心的认证查询方法及衍生密钥生  
成方法，该方法包括：

当第一业务实体请求第二业务实体提供的业务时，所述实体认证中  
20 心使用协商得到的认证模式中定义的认证查询方法、按该第一业务实体  
和第二业务实体的临时身份信息对二者权限进行认证；

使用该协商得到的认证模式中定义的衍生密钥生成方法、以及该第  
一业务实体和第二业务实体的临时身份信息和该第一业务实体的共享  
密钥材料，计算得到用于保护该第一业务实体和第二业务实体之间通信  
25 的共享衍生密钥。

本发明实施例公开了一种基于移动网络端到端通信的认证系统，包括：用于请求业务的第一业务实体、用于提供业务的第二业务实体和实体认证中心；

所述第一业务实体用于与所述实体认证中心协商认证模式，该认证模式用于定义与认证相关的方法，按协商得到的认证模式的定义与该实体认证中心进行互认证，向所述第二业务实体请求业务，按该协商得到的认证模式的定义、使用与该第二业务实体之间的共享衍生密钥与该第二业务实体进行互认证；

所述第二业务实体用于按该协商得到的认证模式的定义与该实体认证中心进行互认证，在该第一业务实体请求业务时按该协商得到的认证模式的定义、使用与该第二业务实体之间的共享衍生密钥与该第一业务实体进行互认证；

所述实体认证中心用于按该协商得到的认证模式的定义分别与该第一业务实体和第二业务实体进行互认证，在该第一业务实体请求业务时按该协商得到的认证模式的定义为该第一业务实体和第二业务实体提供认证查询并生成二者的共享衍生密钥。

本发明实施例还公开了一种业务实体认证系统，包括业务实体和实体认证中心；

所述业务实体用于与实体认证中心协商认证模式，该认证模式至少用于定义该业务实体与该实体认证中心之间的认证方法，该业务实体使用协商得到的认证模式中定义的认证方法与该实体认证中心进行互认证。

本发明实施例公开了一种认证查询系统，包括：用于请求业务的第一业务实体、用于提供业务的第二业务实体和实体认证中心，所述第一业务实体与所述实体认证中心协商认证模式，该认证模式至少用于定义

该实体认证中心的认证查询方法及衍生密钥生成方法；

所述实体认证中心用于在所述第一业务实体请求业务时使用协商得到的认证模式中定义的认证查询方法对该第一业务实体和所述第二业务实体的权限进行认证，并使用该协商得到的认证模式中定义的衍生密钥生成方法生成二者共享的衍生密钥。

本发明实施例还公开了一种认证中心，包括：

第一单元，用于协商业务实体的认证模式，该认证模式至少用于定义：业务实体与实体认证中心之间的认证方法；

第二单元，用于按所述第一单元协商得到的认证模式中定义的认证方法与所述业务实体进行互认证。

本发明技术方案带来的有益效果是：本发明提出了一个真正意义上的通用鉴权框架，其中提供的认证机制可以对多种认证方法和认证模型进行协商和选择，增加了认证机制的灵活性和通用性。在本发明框架中，业务提供者可以是移动网络中的应用服务器，也可以是开放网络中的应用服务器，还可以是功能强大的移动终端，使得业务签约者可使用的业务资源更丰富。该认证方案支持移动终端升级为业务提供者的情况，很好的满足了功能强大的移动终端需要提供业务服务的需求。

## 附图简要说明

图 1 为通用鉴权框架（GAA）的结构示意图。

图 2 是现有技术中 3GPP2 中的通用鉴权框架图。

图 3 为基于本发明的基于移动网络的端到端通信认证框架的示意图。

图 4 为本发明一实施例中业务实体与实体认证中心之间的认证方法协商及互认证过程的流程图。

图 5 为本发明一实施例中业务实体与实体认证中心的认证查询过程的流程图。

图 6 为与 Kerberos 模型相结合的端到端认证模型示意图。

图 7 为与 Kerberos 模型相结合的认证查询过程的框图。

5 图 8 为与 Mediation 模型相结合的端到端认证模型示意图。

图 9 为与 Mediation 模型相结合的认证查询过程的框图。

图 10 为本发明一实施例中业务实体认证方法的流程图。

图 11 为本发明一实施例中业务实体在 3GPP 标准规范的无线网络中认证方法的流程图。

10 图 12 为本发明一实施例中业务实体在 3GPP2 标准规范的无线网络中认证方法的流程图。

图 13 为本发明一实施例中 SP 为银行时与实体认证中心互认证的流程图。

图 14 为本发明认证装置一实施例的结构图。

15 图 15 所示为本发明一实施例中业务签约者与认证中心间的认证流程图。

图 16 所示为本发明一实施例中业务签约者与业务提供者间的互认流程图。

20 图 17 所示为本发明一实施例中业务签约者与业务提供者重新利用认证结果生成会话密钥的流程图。

图 18 所示为本发明端到端通信认证装置一实施例的结构示意图。

## 实施本发明的方式

为了使本发明实施例的目的、技术方案和优点更加清楚明白，以下举实施例并参照附图，对本发明实施例进行进一步详细的说明。

图3显示了依据本发明的基于移动网络的端到端通信认证框架。该框架适用于不同移动网络标准，其作用在于为不同类型的业务实体之间建立相互信任关系，是一个真正意义上的通用鉴权框架。该通用鉴权框架涉及到的网络元素除了两种业务实体：业务签约者（SS，Service Subscriber）301和业务提供者（SP，Service Provider）302以外，在运营商网络中，还存在实体认证中心（EAC，Entity Authentication Center）303和实体签约信息数据库（ESD，Entity Subscription Database）304。在此框架中，SS与SP之间可进行通信，SS和SP可分别与EAC通信以完成各自的认证，而EAC可与ESD连接以从ESD中获取认证所需信息。在本发明实施例中，业务实体可以是业务签约者（SS），也可以是业务提供者（SP）。其中，SS可相当于3GPP通用鉴权框架中的用户或3GPP2通用鉴权框架中的MN；SP可相当于3GPP通用鉴权框架或3GPP2通用鉴权框架中的NAF；EAC可相当于3GPP通用鉴权框架或3GPP2通用鉴权框架中的BSF。

大多数应用服务器在向移动用户提供某一项业务时，都首先与用户建立相互信任的关系（例如移动用户与认证代理之间，移动用户与PKI证书机构之间，移动用户与内容提供服务器之间等建立信任关系）。一般来说，这种信任关系是在移动用户与应用服务器之间进行的双向认证过程中确立的。随着移动网络的发展，业务的类型也越来越多样化：业务提供者不再是单纯的运营商网络本身，还可以是运营商网络以外的第三方内容提供者，甚至可以是移动用户本身。也就是说某些移动用户不仅可以不仅限于使用网络提供的应用服务，还可以向网络中其他用户提供一些服务。本发明实施例中业务提供者可以有三种：运营商网络的AS、第三方AS以及移动用户，业务签约者有两种：一般普通移动用户或第三方AS。这样移动用户既可以是业务签约者又可以是业务提供者，而第

三方 AS 既可以是业务提供者又可以是业务签约者。因此，原来将业务实体划分为用户和业务提供者，而本发明实施例中分为三种：1、SS，其为单纯的业务签约者，它只能申请业务（一般为普通的移动用户）；2、SP，其为单纯的业务提供者（运营商网络的 AS 或外部网络的 SP）；3、  
5 业务签约者和业务提供者（又称为 SSP, Service Subscriber and Provider），SSP 既是业务签约者又是业务提供者（可以是普通的移动用户，也可以是第三方的 AS）。

在图 3 所示的框架中，EAC 用于完成与业务实体进行认证方法协商及认证的过程，并且对端到端的通信实体的身份以及实体请求或提供业务权限的合法性进行检验，还具有生成衍生密钥等功能。ESD 保存有实体的签约信息，签约信息包括：该实体签约的服务类型和/或该实体提供的服务类型，以及该实体支持的认证方法及认证资料等。其中，实体的签约信息与实体的私有身份标识一起保存。业务提供者在向其它实体提供业务或者业务签约者向其它实体请求业务之前，需要与网络存在签约  
10 关系，并将签约信息存放于 ESD 中。  
15

本发明提供的认证流程包括如下几个阶段：

第一阶段（称为实体认证流程）：网络中每个业务签约者与业务提供者进行通信之前，业务实体需要先到 EAC 协商认证方法，并完成对身份的认证。

20 其中，认证方法的协商过程由业务实体发起，并在请求消息中携带自身身份标识，以及业务的安全等级需求。EAC 根据安全等级、网络支持情况和实体签约信息，选择一种认证方法，并将相应信息返回给认证请求者。其中业务的安全等级不同所选择的认证方法也不同。请求者发确认消息表示协商过程结束。

25 业务实体与 EAC 按照协商的方法进行认证。该认证是双向的。认

证结束后，认证请求实体（即请求认证的业务实体）和 EAC 生成共享的密钥材料，并且 EAC 将会根据认证请求实体的签约信息情况给其分配临时身份标识以及相应的有效期：1) 如果该认证请求实体是 SS，则 EAC 将向其分配一个中间业务请求标识 (ISR-ID, Interim Service Request Identifier); 2) 如果该认证请求实体是 SP，则 EAC 将向其分配一个中间认证查询标识 (IAC-ID—Interim Authentication Check Identifier)。

EAC 将业务实体的临时身份标识以及有效期发送给请求认证的业务实体，此后该请求认证的业务实体与 EAC 之间的通信都可以采用认证过程生成的业务实体与 EAC 间的共享密钥材料进行保护。

10 第二阶段（称为认证查询流程）：

业务签约者完成与 EAC 之间的认证后，便可向业务提供者请求业务。

其中，SP 或 SSP 收到业务请求以后，如果已经完成与 EAC 之间的认证并获得有效的 IAC-ID，便可向 EAC 查询业务签约者的认证情况；  
15 否则，首先到 EAC 进行认证以及密钥协商后，再向 EAC 请求查询业务签约者的认证情况，其中，查询请求中携带业务签约者的 ISR-ID 以及自身的 IAC-ID。EAC 收到查询请求后，首先根据业务签约者的标识以及业务提供者的标识查询二者是否有相应的权限，然后根据二者的相关信息，利用 SS/SSP 到 EAC 协商的  $K_s$  为二者计算一个用于保护业务签约者和提供者之间业务通信的衍生密钥，并发送给业务提供者。同时，业务签约者也由相同的参数以及算法计算出衍生密钥。业务实体与 EAC 之间认证所建立的信任关系存在一个有效期。有效期快要过期或已经过期，业务实体需要到 EAC 之间进行重认证过程，建立新的信任关系。

25 第三阶段（称为业务实体之间的互认证流程）：当 SS 与 SP 获得共享的衍生密钥后，在开始每次业务通信之前，还可以先利用所述衍生密

钥在双方间进行互认证，并进一步生成保护本次通信安全的会话密钥 Kr-SS-SP，然后利用该会话密钥保护本次业务通信。

下面结合附图对本发明提出的认证流程的各个阶段加以详细说明。

图 4 为本发明一实施例中业务实体与实体认证中心之间的认证方法协商及互认证流程图。本实施例中，业务实体与 EAC 间的认证方法协商和互认证过程由业务实体发起，如图 4 所示，包括如下步骤：

步骤 401：业务实体自动选择所请求的业务或所提供的业务（如视频会议业务）对应认证方法的安全等级需求（例如，高安全等级）。

步骤 402：该业务实体向 EAC 发送认证请求，该认证请求中携带该业务实体的身份标识以及其所选择的认证方法的安全等级等相关信息；

步骤 403：该 EAC 收到该认证请求后，查找本地保存的安全等级列表，找到符合该安全等级需求的当前网络支持的认证方法，包括：认证协议、加密算法。例如，Http AKA 是一种无线网络中的网络与终端的互鉴权协议，执行这个协议能够使通信的双方互相认证对方的身份，并且在通信的双方生成相同的密钥。

步骤 404：该 EAC 根据业务实体的身份标识在 ESD 存储的签约信息中查询该业务实体的认证信息，例如该业务实体支持的认证方法，包括：认证协议、加密算法和其它相关参数。

步骤 405：该 ESD 向该 EAC 返回该业务实体的认证能力信息（即所支持的认证协议和加密算法等）和其它相关参数。

步骤 406：该 EAC 根据本地策略匹配网络和该业务实体所支持的认证协议和加密算法，确定出符合安全等级需求的并且双方都支持的认证协议和加密算法（即认证方法），如果没有符合安全等级需求的并且双方都支持的认证协议和加密算法，则向该业务实体返回错误指示，结束

本流程。

步骤 407: 该 EAC 将选定的认证方法, 包括认证协议和加密算法, 返回给该业务实体;

5 步骤 408: 该业务实体收到该 EAC 返回的信息后, 确认认证方法, 向该 EAC 返回确认响应。

步骤 409: 该业务实体和该 EAC 应用所选的认证协议和加密算法进行互认证, 并在认证成功后, 双方获得共享密钥材料 (也称为共享密秘信息)。

如果业务实体是一个移动终端的话, 那么共享密钥材料就可以是共享密钥 ( $K_s$ ), 如果业务实体是一个移动核心网域的应用服务器 (AS), 那么业务实体和 EAC 在互认证过程中可能协商出的共享密钥材料为安全关联 (SA, Security Association) 即因特网协议安全 (IPSec, Internet Protocol Security) 协议中业务实体双方协商的安全通信的密钥以及密钥算法信息。

15 步骤 410: 该 EAC 向该业务实体返回认证成功响应, 并分配业务实体临时身份标识以及相应的有效期, 包括: 1) 如果向 EAC 发出认证请求的业务实体是业务签约者 (SS/SSP), 则 EAC 将向其分配一个中间业务请求标识 (ISR-ID), 以在向其它实体请求业务时使用; 2) 如果向 EAC 发出认证请求的业务实体是业务提供者 (SP/SSP), 则 EAC 将向其分配 20 一个中间业务查询标识 (IAC-ID), 以在需要向 EAC 查询 SS 的认证情况时使用。

步骤 411: 该 EAC 和该业务实体侧分别将共享密钥材料与对应的安全等级关联并保存起来, 包括: 关联并保存 ISR-ID/IAC-ID、密钥材料

及认证方法和安全等级。

图 5 为本发明一实施例中业务实体与实体认证中心的认证查询过程的流程图。本实施例中，在完成了互认证之后，业务实体与实体认证中心要进行认证查询过程，具体处理如图 5 所示：

5 步骤 501：SS（或 SSP）向能够提供服务的 SP（或另一个 SSP）提出业务请求。该业务请求中包括了 SS 前面认证得到的中间业务请求标识（ISR-ID，）以及 SP 的公开身份标识（UID），该公开身份标识是其它业务实体联系的身份标识。

10 同一业务实体提供的不同的业务对应不同的 UID，即可以利用 UID 区分出不同的业务。

步骤 502：该 SP 收到业务请求后，查找本地是否保存有 SS 的 ISR-ID，以识别该 SS；如果保存有该 ISR-ID 以及与其关联的有效的衍生密钥和业务实体真实身份信息等，双方开始利用衍生密钥保护它们之间的业务，若 SP 发现该衍生密钥或该 ISR-ID 等信息处于次操作状态或已被撤销或销毁，则该 SP 指示该 SS 发起重认证请求，关于重认证发起的具体处理详见下文描述，结束本流程；如果没有保存该 ISR-ID，则向 EAC 发出认证查询请求，并在认证查询请求中携带该 SS 的 ISR-ID 以及自身的 IAC-ID 和 UID，然后执行步骤 503；

20 步骤 503：该 EAC 收到认证查询请求后，首先查询并判断其中携带的 IAC-ID 是否有效以及该 SP 是否有权提供该项业务，然后再查询并判断该认证查询请求携带的 ISR-ID 是否有效以及该 SS 是否有权请求此项业务，如果上述判断 IAC-ID 有效且该 SP 有权提供该项业务、并且判断 ISR-ID 有效且该 SS 有权请求此项业务（即验证通过），则该 EAC 为该 SS 和 SP 生成衍生密钥。

25 步骤 504：该 EAC 向该 SP 返回认证查询响应，该响应携带步骤 503

生成的衍生密钥和密钥有效期。其中，如果步骤 503 中的认证查询成功（即查询并判断为是），则在返回的认证查询响应中携带新生成的衍生密钥，该衍生密钥通过该 SP 与 EAC 的共享密钥材料加密获得；否则，返回错误消息，并由该 EAC 通知相应的业务实体到 EAC 进行重认证，  
5 重认证发起的具体处理详见下文描述，结束本流程。

步骤 505：该 SP 从该认证查询响应中解密得到新生成的衍生密钥，并将该衍生密钥、有效期、该 SS 的 ISR-ID 以及该 SP 的 UID 关联并保存在本地。

步骤 506：该 SP 向该 SS 返回业务请求响应；

10 步骤 507：该 SS 在本地利用相同的参数和密钥算法计算出相同的衍生密钥；其中，该密钥算法可以采用：数据加密标准（DES）、三重 DES（3-DES）、高级加密标准（AES）256、AES1024 等，其中 256 和 1024 代表密钥长度。

步骤 508：该 SS 与该 SP 利用该衍生密钥保护它们之间的业务。

15 由于，业务实体与 EAC 之间通过认证所建立的信任关系存在一个有效期（如共享密钥材料具有、衍生密钥具有有效期、临时身份标识具有的有效期）。当有效期快要过期或已经过期时，业务实体需要与 EAC 进行二者的重认证以建立新的信任关系。

另外，根据共享密钥材料或临时身份标识所处的情况不同，业务实体可以具有以下状态：1、次操作状态：共享密钥材料、衍生密钥或临时身份标识快要过期，此时不能再用此共享密钥材料进行加密运算但能够用其解密以及验证实体身份；2、撤销状态：共享密钥材料、衍生密钥或临时身份标识已经过期，并且解除了共享密钥材料或临时身份与该实体的真实身份的对应关系；3、销毁状态：共享密钥材料、衍生密钥或临时身份标识的相关记录被删除。这样，当满足下列情况之一时，需  
20  
25

要发起重认证过程：

1、EAC 根据本地相关策略发现业务实体与 EAC 的共享密钥材料或临时身份标识处于次操作状态，EAC 指示该业务实体发起重认证请求；

5 2、EAC 根据本地相关策略发现共享密钥材料或临时身份标识处于撤销或销毁状态，EAC 指示该业务实体发起重认证请求；

3、EAC 不能根据临时身份标识查找到相关的身份信息和密钥信息时（即处于销毁状态），EAC 指示该业务实体发起重认证请求；

4、SP 根据本地相关策略发现衍生密钥处于次操作状态时，SP 指示该 SS 发起重认证请求；

10 5、SP 根据本地相关策略发现衍生密钥处于撤销或销毁状态时，SP 指示该 SS 发起重认证请求；

6、SP 不能根据临时身份标识查找到相应的身份信息和密钥信息时（即处于销毁状态），SP 指示该 SS 发起重认证请求。

在上述 EAC 指示业务实体发起重认证请求时，该指示中标明有重  
15 认证的原因。如果重认证的原因是共享密钥材料或临时身份标识处于次操作状态，那么该业务实体在所发起的重认证请求中以临时身份标识自己。EAC 收到该重认证请求后，根据该临时身份标识，确定无需协商认证方法，直接采用原来使用的认证方法进行互认证。如果重认证的原因是共享密钥材料或临时身份标识处于撤销或销毁状态，或是需要使用密  
20 钥材料时却不能根据临时身份查找到，那么该业务实体在所发起的重认证请求中以私有身份标识自己。EAC 收到该重认证请求后，根据该私有身份标识，确定需要重新协商认证方法，该重新协商认证方法过程与图 4 所示的初始的认证过程相同。

同样，在上述 SP 指示 SS 发起重认证请求中，该指示标明有重认证  
25 的原因。如果该重认证的原因是临时身份标识处于次操作状态，那么该

SS 在所发起的重认证请求中以临时身份标识自己；EAC 收到请求后，根据该临时身份标识，确定无需协商认证方法，直接采用原来使用的认证方法进行互认证。如果该重认证的原因是临时身份标识处于撤销或销毁状态，那么该 SS 在所发起的重认证请求中以私有身份标识自己；EAC 5 收到请求后，根据该私有身份标识，确定需要重新协商认证方法，该重新协商认证方法过程与图 4 所示的初始的认证过程相同。

其中，在使用临时身份标识（即ISR-ID/IAC-ID）或者与之关联存储的共享密钥材料（即Ks/Kp）时，业务实体（即SS或SP）或者EAC必须首先验证临时身份标识或者共享密钥材料是否处于次操作、撤销或销毁 10 状态。如果处于次操作、撤销或销毁状态，则业务实体或者EAC将触发相应的业务实体和EAC之间的实体重认证过程。在认证过程中，当收到标有失败原因的失败消息的时候，也可以触发实体的重认证过程。另外，若SP发现自身与SS之间的共享衍生密钥处于次操作、撤销或销毁状态，将向SS发送重认证请求，并在其中指明重认证原因。如果仅仅是共享衍生密钥处于次操作、撤销或销毁状态，而SS和SP的临时身份标识处于正常 15 状态，则SS和SP不必与EAC进行初始的实体认证，由SS向EAC发起认证查询，并由EAC为生成新的共享衍生密钥发送给SP，再由SS生成相同的衍生密钥。

其中，对有效期和次操作状态的举例说明如下：以共享密钥材料的有效期为例，假设共享密钥材料的有效期为 48 小时，并设定 44~48 小时范围内是处于次操作状态，若共享密钥材料已生存 45 小时，就可以判断该共享密钥材料已经处于生命周期的次操作状态了。

当实体认证中心（EAC）具有 Kerberos 服务器功能时，可以采用与 Kerberos 模型相结合的认证查询方法。图 6 为与 Kerberos 模型相结合的 25 端到端认证模型示意图。如图 6 所示，业务签约者（SS）向实体认证中

心(EAC)请求业务许可票据，并向该EAC提供该SS的ISR-ID和UID，实体认证中心检查该ISR-ID和IAC-ID的有效性，生成业务许可票据，并向业务签约者返回该业务许可票据。业务签约者在向业务提供者发出业务请求时携带该业务许可票据，该业务提供者按该业务许可票据生成  
5 衍生密钥再向该业务签约者返回服务响应。

图7为与图6所示Kerberos模型相结合的认证查询过程的流程图。如图7所示，具体步骤如下：

步骤701：当业务签约者(SS)需要获得某项业务时，首先查看本地是否保存了对应于此项业务的业务许可票据，如果有，则直接跳到步骤705；如果没有，则向实体认证中心(EAC)发送业务许可票据请求，该请求中携带该业务签约者(SS)的中间业务请求标识(ISR-ID)，以及该项业务的业务提供者(SP)的公开身份标识(UID)。  
10

步骤702：该EAC收到该业务许可票据请求后，进行身份和权限的合法性检查。首先通过查询该请求中携带的ISR-ID是否有效来判断该SS是否有权使用此项业务，然后根据该请求中携带的该SP的UID获得该SP的IAC-ID，并根据该IAC-ID是否有效判断该SP是否有权提供此  
15 项业务；

如果上述检查结果为该SP有权提供该项业务(即该SP合法)，该EAC根据该SS和SP的身份信息，以及该SS与该EAC的共享密钥材料计算出一个用于保护该SS和SP之间业务通信的衍生密钥K-SSP/SP，该EAC还产生一个包含衍生密钥、该SS的身份信息和该SP的身份信息的业务许可票据(SGT)，利用自身与该SP的共享密钥材料加密该业务许可票据。  
20

如果检查结果为该SP无权提供该项业务(即该SP不合法)，则发出错误信息，该EAC通知相应的实体重新到实体认证中心认证身份，  
25

结束本流程。

步骤 703：该 EAC 向该 SS 发送上述加密后的业务许可票据。

步骤 704：该 SS 收到该业务许可票据后在本地采用和该 EAC 相同的参数和算法产生一个相同的衍生密钥。

5 步骤 705：该 SS 向该 SP 发送业务请求，该业务请求携带该业务许可票据。

步骤 706：该 SP 解密该业务许可票据，获得衍生密钥。

步骤 707：该 SP 向该 SS 返回指示成功的业务请求响应。

步骤 708：该 SS 与该 SP 利用该衍生密钥保护它们之间的业务。

10 除了采用上述步骤外，EAC 也可以利用其与 SS 的共享密钥材料加密所述衍生密钥，并将加密后的衍生密钥发送给 SS，从而 SS 不是在本地重新计算得出衍生密钥，而是通过解密获得衍生密钥。

15 同样，SS 与 SP 获得共享的衍生密钥后，在开始每次业务通信之前，还可以先利用所述衍生密钥进行双方间的互认证，并进一步生成保护该次通信安全的会话密钥 Kr-SS-SP，然后利用所述会话密钥保护该次业务通信。

当实体认证中心(EAC)具有充当仲裁者身份的可信的第三方(TTP, Trusted Third Party)功能时，也可以采用与 Mediation 模型相结合的认证查询方法。图 8 为与 Mediation 模型相结合的端到端认证模型示意图。

20 如图 8 所示，业务签约者(SS)发送业务请求至实体认证中心(EAC)，请求业务提供者(SP)的业务；该 EAC 确定该 SS 合法后将业务请求转发至该 SP；该 SP 返回携带自身 IAC-ID 的业务请求响应给该 EAC；该 EAC 按此 IAC-ID 检查该 SP 的合法性，若该 SP 合法，则计算该 SS 和该 SP 之间的衍生密钥并发送给该 SP，同时返回业务请求响应给该 SS；  
25 该 SS 收到响应后计算得到同样的衍生密钥。

图 9 为与图 8 所示 Mediation 模型相结合的认证查询过程的流程图。

如图 9 所示，具体步骤如下：

步骤 901：业务签约者（SS）在需要使用业务提供者（SP）的某项业务时，首先向实体认证中心（EAC）提出业务请求，该业务请求中携带该 SS 的 ISR-ID 以及该 SP 的 UID。  
5

步骤 902：该 EAC 检查该 SS 的 ISR-ID 的有效性，以及该 SS 的签约信息，以确定该 SS 是否有请求此项业务的权限。

步骤 903：如果该 SS 是合法的，则该 EAC 为其转发业务请求给该 SP，执行步骤 904；如果该 SS 是不合法的，则该 EAC 向该 SS 发错误信息，通知该 SS 重新到该 EAC 认证身份，结束本流程。  
10

步骤 904：该 SP 返回业务请求响应，该响应中携带自身 IAC-ID。

步骤 905：该 EAC 检查该 IAC-ID 的有效性，以及该 SP 的签约信息，以确定该 SP 是否有权提供此项业务，如果该 SP 是合法的，则该 EAC 根据该 SS 和 SP 的身份信息，以及该 SS 与该 EAC 的共享密钥材料计算出一个用于保护该 SS 和 SP 之间业务通信的衍生密钥，执行步骤 906；如果该 SP 是不合法的，则该 EAC 向该 SP 发错误信息，通知该 SP 重新到该 EAC 认证身份，结束本流程。  
15

步骤 906：该 EAC 向该 SS 发送业务请求成功响应，并向该 SP 发送经由该 EAC 与 SP 的共享密钥材料加密的衍生密钥。

步骤 907：该 SS 收到该 EAC 发送的业务请求成功响应后，采用与该 EAC 相同的参数和算法计算得到衍生密钥。  
20

步骤 908：该 SS 与该 SP 使用该衍生密钥保护它们之间的业务。

同样，当 SS 与 SP 获得共享的衍生密钥后，在开始每次业务通信之前，还可以先利用所述衍生密钥进行双方间的互认证，并进一步生成保护本次通信安全的会话密钥 Kr-SS-SP，然后利用该会话密钥保护本次业  
25

务通信。

以上只是本发明的优选的典型的实施方式进行了描述，其它类似的情况，如 SSP 作为业务实体时，它在通信中的身份可以变化，当它处于请求业务情况下，它与上述 SS 的处理方式相同，当它处于提供业务的情况下，它与上述 SP 的处理方式相同。因此，本领域的技术人员在本发明范围内进行的通常变化和替换，都应包含在本发明保护的范围内。  
5

以下为基于本发明实施例通用鉴权框架的认证方法中若干第一阶段和第二阶段认证流程的实施例。

图10为本发明一实施例中业务实体认证方法的流程图。参见图10，

10 本发明所述的认证方法描述如下：

步骤1001：业务实体向实体认证中心（EAC）发送认证请求，该认证请求中携带业务实体的身份标识信息、安全等级信息、该业务实体所支持的认证方法信息（其中，如果与网络的签约信息中保存有该业务实体所支持的认证方法信息，则该认证方法信息可以不携带）等。

15 其中，身份标识信息可以包括：私有身份标识（PID）或公开身份标识UID等。对于安全等级的选取，可以考虑以下几种情况：1) 业务实体可以针对需要进行的业务类型查找本地保存的业务安全等级列表选择相应的安全等级；2) 当业务实体本地没有保存安全等级列表时，它可以根据通过人机界面由用户手动选择安全等级；3) 业务实体也可以  
20 不选择安全等级而只是将相应业务提供者（SP）的UID发送给EAC，该UID能够标识出该业务提供者提供的业务类型，然后该EAC能根据业务类型查找安全等级列表从而选择相应的安全等级。

步骤1002：该EAC收到该认证请求后，根据该请求中的身份标识查找ESD中保存的签约信息，并综合业务实体、网络对认证方法的支持情况以及安全等级，采用本地策略选择一种认证方法，这里标识为认证方  
25

法b。其中，所支持的认证方法可包括：AKA、基于SIM的认证、基于CAVE的认证方法、基于AAA的认证方法、TLS握手协议、DH交换、公钥证书认证、生物认证等。

当网络与业务实体都只支持一种认证方法时，无需认证协商，双方  
5 可直接采用此认证方法进行互认证。EAC选择安全等级时可以结合业务  
的安全等级需求也可以不结合，即安全等级这一条件对于认证协商过程  
是可选的。

步骤1003：该EAC向该业务实体发送认证初始化消息，该消息中携  
带步骤1002所选认证方法的标号、安全等级（如果在步骤1002的协商过  
10 程中考虑安全等级，则该安全等级应不低于业务实体所选择的安全等  
级）等。

如果后续的认证交互过程由EAC侧发起，则该认证初始化消息还应  
包括基于此认证方法的第一条认证消息所承载的信息。该第一条认证消  
息的内容对于AKA认证来说是认证向量，而对TLS认证方法就是Hello  
15 Request。

步骤1004：该业务实体获知认证方法。如果后续的认证由业务实体  
侧发起，则该业务实体计算认证信息；如果后续的认证由EAC侧发起，  
则该业务实体收到了相关认证信息，就计算响应值。

步骤1005：该业务实体与该EAC间进行基于所选认证方法的认证交  
20 互过程。

步骤1006：在认证结束后，该业务实体与EAC均具有了共享密钥材  
料，并且该EAC为业务实体分配临时身份标识（ISR-ID）或IAC-ID，该  
标识与共享密钥材料关联保存，其可作为查找共享密钥材料的一个索引  
或者是一个安全连接的会话标识（Session ID）。

25 图11为本发明一实施例中业务实体在3GPP标准规范的无线网络中

认证方法的流程图。参见图 11，本实施例中，业务实体为 SS，当 SS 为 3GPP 网络中的移动终端，即图 11 中的 UE，且只支持 AKA 认证时，认证流程如下：

步骤 1101：UE 向 EAC 发送 HTTP Digest 认证请求，该请求中携带其身份标识。  
5

步骤 1102：由于 3GPP 网络和 UE 都只支持 AKA 方法，因此双方不需要协商认证方法，直接采用 AKA 方法认证，该 EAC 到 ESD 获取该 UE 用户的认证向量 (RAND, AUTN, RES, CK, IK)。

步骤 1103：该 EAC 在 HTTP 的 401 消息（包含 Digest AKA challenge）中携带该认证向量中的 RAND 和 AUTN 给该 UE。  
10

步骤 1104：该 UE 计算并检验该 AUTN 的正确性，以确认该包含 Digest AKA challenge 的消息是否来自一个被授权的网络，同时该 UE 计算 CK、IK 和 RES。

步骤 1105：该 UE 发送 HTTP request 消息给该 EAC，其中包含 Digest  
15 AKA response 以及由上述 RES 计算的摘要值。

步骤 1106：该 EAC 验证上述计算的摘要值的正确性，以认证该 UE 的合法性。

步骤 1107：该 EAC 生成密钥材料  $K_s=CK||IK$  以及 ISR-ID，其中，该 ISR-ID 的生成方法以及格式与 3GPP 通用鉴权框架中的 B-TID 相同。

步骤 1108：该 EAC 发送 200 OK 消息，表示认证成功结束，该消息中包含密钥材料的有效期以及 ISR-ID，并经由  $K_s$  加密传送给该 UE。  
20

步骤 1109：该 UE 也生成同样的密钥材料  $K_s=CK||IK$ ，然后解密获得 ISR-ID 以及有效期，并和有效期认证方法等关联保存在本地。

图 12 为本发明一实施例中业务实体在 3GPP2 标准规范的无线网络  
25 中认证方法的流程图。本实施例中，业务实体为 SS，当该 SS 为一移动

终端(UE)且支持AKA认证、证书认证等认证方法，而网络侧是3GPP2的网络，其支持AKA认证、基于CAVE的认证方法以及基于MN-AAA的认证方法时，参见图12，认证流程如下：

步骤1201：UE向EAC发送HTTP认证请求，该认证请求中携带身份标识及支持的认证方法，如AKA认证、证书认证。  
5

步骤1202：该EAC根据该UE的身份标识到ESD查找其签约信息，再根据自身所支持的认证方法类型，如支持AKA认证、基于CAVE的认证方法以及基于MN-AAA的认证方法，采用本地策略最后确定双方采用AKA方法进行认证；该EAC到该ESD获取该UE用户的认证向量  
10 (RAND, AUTN, RES, CK, IK)。

步骤1203：该EAC在HTTP的401消息(包含Digest AKA challenge)中携带RAND和AUTN发给UE，并将认证方法标识放在payload信息中。

步骤1204：该UE计算并检验AUTN的正确性，以确认该包含  
15 challenge的消息是否来自一个被授权的网络，同时该UE计算CK、IK和RES。

步骤1205：该UE发送HTTP request消息给该EAC，其中包含有Digest AKA response以及经由RES计算的摘要值。

步骤1206：该EAC验证所述摘要值的正确性，以认证该UE的合  
20 法性。

步骤1207：该EAC生成密钥材料Ks=CK||IK以及ISR-ID，其中该ISR-ID生成方法以及格式与3GPP2通用鉴权框架中的B-TID相同。

步骤1208：EAC发送200 OK消息给UE，表示认证成功结束，该消息中包含密钥材料的有效期以及ISR-ID并经由Ks加密。

步骤 1209：该 UE 也生成同样的  $K_s=CK||IK$ ，然后解密获得 ISR-ID 以及有效期，并将其和有效期、认证方法等关联保存在本地。

如果 UE 也支持基于 CAVE 的认证方法，而且 EAC 收到认证请求后，根据身份标识查找签约信息，并结合自身支持的认证方法类型，采用本地策最后确定基于 CAVE 的认证方法进行互认证，则后面的认证流程与 5 3GPP2 通用鉴权框架中的基于 CAVE 的认证流程一样。而当确定采用 AAA 认证方法时也同理可以使用本发明方案的通用鉴权框架。

图 13 为本发明一实施例中 SP 为银行时与实体认证中心互认证的流程图。本实施例中，业务实体为银行 SP，当银行 SP 欲向 UE 提供业务 10 手机银行业务前，首先需要与 EAC 互认证生成共享密钥材料，并建立安全连接，参见图 13，认证流程如下：

步骤 1301：SP 向 EAC 发送认证请求，该认证请求中携带该 SP 的公开身份标识（UID）。

步骤 1302：该 EAC 根据该公开身份标识查找该 SP 的签约信息，确认 15 该 SP 有权提供此项业务后，获取该 SP 的认证能力信息，即该 SP 所支持的认证方法，如：证书、证书 TLS 认证、基于预共享密钥的 TLS 认证等。

然后，该 EAC 查找业务安全等级列表，确认该手机银行业务属于高安全等级，并且查找认证安全等级列表，找到符合高安全等级的网络 20 支持的认证方法有 HTTP Digest AKA、证书 TLS 认证等，最后匹配 SP 所支持的认证方法，确定所采用的认证方法进行互认证，本实施例中设定确定采用证书 TLS。

步骤 1303：该 EAC 向该 SP 发起 Hello Request 消息，该消息携带认证方法标识（本实施例中为证书 TLS 认证的标识）以及安全等级标识。

步骤 1304：该 SP 获知认证方法为证书 TLS，查找本地有无 Session ID: IAC-ID，其中，若以前已经通过 EAC 的证书 TLS 认证建立了 TLS 安全通道并且还在有效期内，则 Session ID 可以作为该 TLS 安全通道的索引。

5 步骤 1305：该 SP 向该 EAC 发送 Client Hello 消息。如果该 SP 没有保存有效的 Session ID，则该消息的 Session ID 字段为空；如果该 SP 保存有有效的 Session ID: IAC-ID，则该消息的 Session ID 字段为该 IAC-ID。

10 步骤 1306：该 EAC 收到该 Client Hello 消息后，查看 Session ID 字段是否为空，如果不为空且能够匹配到相关联的安全连接信息，则该 EAC 直接发送 Finished 消息给该 SP 以验证该安全连接的认证结果和共享密钥材料是否可用。该 SP 验证该 Finished 消息中的参数正确后，返回另一 Finished 消息给 EAC。该 EAC 验证该 Finished 消息参数正确后，双方重用该安全连接。

15 如果该 Session ID 字段为空或上述 Finished 消息有误，则该 EAC 根据本地策略配置消息中的参数，依次返回 Server certificate 消息、ServerKeyExchange 消息（可选）、CertificateRequest 消息。最后，EAC 返回 ServerHelloDone 消息，表示 ServerHello 以及相关消息已发送完毕。

20 步骤 1307：该 SP 在收到 ServerHelloDone 消息后，返回 Certificate 消息，然后发送 ClientKeyExchange 消息，通过这条消息双方获得了共享秘密参数。然后，该 SP 发送 CertificateVerify 消息给 EAC，便于其清楚地验证该 SP 的证书。最后，在发送了 ChangeCipherSpec 消息后该 SP 立即发送 Finished 消息给该 EAC，用于正式密钥交换和验证过程的成功。

步骤 1308：该 EAC 验证该 SP 的 Finished 消息中的信息是否正确，如果不正确，则中止当前握手过程；如果正确，则返回另一 Finished 消

息给该 SP。如果该 SP 验证该 Finished 消息中的信息正确，那么双方认证和密钥交换过程成功结束。

本实例提供了 3GPP/3GPP2 网络认证 NAF 的统一化过程方案，该方法同样基于本发明的通用鉴权框架。

5 基于上述本发明方法，本发明还提出了一种实体认证装置。图 14 为本发明认证装置一实施例的结构图。参见图 14，该实体认证装置包括：认证请求发送模块、协商模块和认证交互模块。

其中，认证请求发送模块用于为业务实体向实体认证中心发送认证请求，该认证请求的内容包括该业务实体的身份标识；协商模块用于在 10 收到认证请求后，为该实体认证中心根据其本地策略选择一种认证方法，并向该业务实体发送认证初始化消息；认证交互模块用于该业务实体与实体认证中心之间基于所选认证方法进行认证交互。这些模块实现具体功能的原理在前述方法流程中均有描述，这里不再赘述。

在上述认证方法的基础之上，本发明还提出了一种增强方案，包括： 15 首先定义认证模式，该认证模式从整体上对实体认证和认证查询流程做了定义，包括：业务实体与实体认证中心之间的认证方法、业务实体之间的认证方法及会话密钥的生成方法等。该认证方法简述如下：

### 一、首先定义认证模式

可定义 E2E 认证模式，其主要由 SS 与 EAC 的认证方法决定，有时也 20 由 SS 与 SP 的认证方法决定。在该认证模式中可设定：SS 和 EAC 的认证方法、SP 和 EAC 的认证方法、EAC 提供认证查询的方法及衍生密钥的生成方法、SS 和 SP 之间的认证方法以及会话密钥生成方法。其中，针对某些情况所定义的认证模式中可以只设定上述认证方法中的一种或者几种。例如，在 SS 和 SP 可以直接认证并建立安全连接的情况下，无需进行 SS 25 和 EAC 及 SP 和 EAC 的认证，则针对这种情况定义的认证模式中只需设定

SS和SP之间的认证方法以及会话密钥生成方法。

认证模式中还可设定每种认证方法的选择策略，其中包括该认证方法是否可选或必选以及该认证方法是否可以协商。

本发明可采用的端到端（E2E, End to End）认证模式有如下几种：

5 E2E\_3GPP\_AKA, E2E\_3GPP2\_AKA, E2E\_3GPP2\_CAVE ,  
E2E\_WLAN, E2E\_3GPP2\_MNAAA, E2E\_3GPP\_WLAN, E2E\_Kerberos,  
E2E\_Mediation, E2E\_TLS (但认证模式的定义并不限于这几种，还可以  
根据需要进行新的定义)。如下列出这几种认证模式的定义实例。

1、E2E\_3GPP\_AKA 模式定义如下：

10 E2E\_3GPP\_AKA ::= struct {  
    SS<->EAC认证方法 AKA,  
                                承载协议 HTTP Digest  
    SP<->EAC认证方法 TLS方法 (或IPSec通道等方法)  
    SS<->SP的认证方法 基本查询方法  
15                                承载协议 TLS (或其他)  
    会话密钥生成方法 是自定义的 (或其他, 可选)。  
}

2、E2E\_3GPP2\_CAVE模式的定义如下：

20 E2E\_3GPP2\_CAVE ::= struct {  
    SS<->EAC认证方法 Authentication based on CAVE,  
                                承载协议 HTTP Digest  
    SP<->EAC认证方法 TLS方法 (或IPSec通道等方法)  
    SS<->SP的认证方法 基本查询方法  
                                承载协议 TLS (或其他)  
25    会话密钥生成方法 是自定义的 (或其他, 可选)。

}

3、E2E\_WLAN ::= struct {

SS<->EAC认证方法 AKA(或SIM),

承载协议 EAP(Extensible Authentication

5 Protocol)可扩展认证协议

SP<->EAC认证方法 TLS方法 (或IPSec通道等方法)

SS<->SP的认证方法 基本查询方法

承载协议 TLS (或其他)

会话密钥生成方法 是自定义的 (或其他, 可选)。

10 }

4、E2E\_Kerberos模式的定义如下:

E2E\_Kerberos ::=struct {

SS<->EAC认证方法 (可协商, 如AKA, 基于CAVE的认证, 基于证书的认证)

15 SP<->EAC认证方法 IPSec通道 (或其他, 可选)

SS<->SP的认证方法 Kerberos (必选, 可协商采用那种Kerberos或Kerberos改进方案)

承载协议 TCP (或其他)

会话密钥生成方法 TLS-Krb5 (或其他, 可选)

20 }

5、E2E\_TLS模式的定义如下:

E2E\_TLS ::= struct {

SS<->EAC认证方法 无

SP<->EAC认证方法 无

25 SS<->SP的认证方法 TLS

会话密钥生成方法 TLS-PSK (或其他, 可选)

{}

6、E2E\_3G\_GAA 模式的定义如下:

SS 与 EAC 的认证方法为: SIM, AKA, CAVE, MN-AAA Key,

5 TLS-PSK, TLS-Cert 等方法中之一;

SP 和 EAC 互认证方法为: TLS, IKE;

认证查询和衍生密钥生成方法为: GBA;

SS 与 SP 的互认证方法为: TLS-PSK, TLS-Cert。

7、E2E\_KERBEROS 模式的定义如下:

10 SS 与 EAC 的认证方法为: 同 E2E\_3G\_GAA, 但在认证成功后 EAC

生成并发送 SGT 给业务实体;

SP 和 EAC 互认证方法为: NULL, TLS, IKE;

认证查询和衍生密钥生成方法为: Kerberos;

SS 与 SP 的互认证方法为: NULL, TLS-KBR5。

15 8、E2E\_Mediation 模式的定义如下:

SS 与 EAC 的认证方法为: 同 E2E\_3G\_GAA, 还可以是 IKE;

SP 和 EAC 互认证方法为: 同 E2E\_3G\_GAA;

认证查询和衍生密钥生成方法为: Mediation;

SS 与 SP 的互认证方法为: TLS-PSK。

20 9、E2E\_TLS 模式的定义如下:

SS 与 EAC 的认证方法为: NULL;

SP 和 EAC 互认证方法为: NULL;

认证查询和衍生密钥生成方法为: NULL;

SS 与 SP 的互认证方法为: TLS-Cert, TLS-PSK。

25 上述模式还可以根据业务需求进行新的认证方法设定, 本发明对于

认证模式所限定的具体认证方法、选择策略、密钥生成方法均不作限定。

图 15 所示为本发明一实施例中业务签约者与认证中心间的认证流程图。参见图 15，本实施例中，3GPP 网络中的移动用户 UE 使用 Internet 中的应用服务器（该服务器支持 Kerberos 认证协议）所提供的业务，具体过程如下：

步骤 1501：SS（即 UE）向实体认证中心（EAC）发送业务请求，该业务请求中携带用户 UE 的身份标识、认证能力标识、业务类型；该业务请求也可以不携带业务类型，而携带业务提供者（SP）的公开身份标识（UID）以使 EAC 通过该 UID 到实体签约数据库（ESD）中查找相应的业务类型。

步骤 1502：该 EAC 根据业务请求中的身份标识，并综合该 SS 以及 SP 的认证能力信息采用本地策略选取认证模式以及相应的认证方法。本实施例中设定选取的是 E2E\_Kerberos 模式。

该 EAC 能根据认证模式中认证方法的选择策略及本地策略确定每一种认证方法。其中，本地策略可以为：SS 和 SP 依据双方的认证能力以及业务类型等选取互认证方法以及会话密钥生成方法；由该 SS 和 SP 的互认证方法决定是否进行该 SP 与 EAC 的互认证，如果需要互认证则根据该 SP 和 EAC 的认证能力以及业务类型等选取认证方法。

步骤 1503：根据 E2E\_Kerberos 模式的定义，该 SS 与 EAC 认证方法为可协商，则依据本地策略（即双方的认证能力以及双方要进行的业务类型等）选择认证方法，本实施例设定中选择了 AKA 认证方法。其中，该 SP 与 EAC 的认证方法被设为 IPSec 通道或其他，并且可选，本实施例中设定选取为空，即不进行 SP 与 EAC 的认证。该 SS 与 SP 的认证方法被设为 Kerberos，则可协商采用 Kerberos 或 Kerberos 改进方案，也可以协商承载协议为 TCP 或其他。本实施例中设定依据双方的认证能力以及业务类型

等经过协商选取该 SS 与 SP 的认证方法为 Kerberos 且承载协议为 TLS-Krb5。另外，会话密钥生成方法被设为 TLS-Krb5 或其他，且可选，本实施例中设定选取会话密钥生成方法为 TLS-Krb5。

根据上述选定的各种认证方法，可以开始进行该 SS 和 EAC 之间的认证。如果该 SS 和 EAC 已经进行过 AKA 的互认证并且所生成的共享密钥和中间业务请求标识 (ISR-ID) 仍在有效期内，则不用执行该 AKA 的互认证步骤，直接跳到步骤 209 以生成业务许可票据 (SGT)。

步骤 1504：该 EAC 从 ESD 中获取用户的认证向量 (RAND,AUTN,RES,CK,IK)。

步骤 1505：该 EAC 在 HTTP 的 401 消息(含有 gest AKA chanllenge) 中携带 RAND 和 AUTN 并发送给该 UE，并将认证方法标识 a 放在 payload 信息中。

步骤 1506：该 UE 计算并检验所收到的 AUTN 的正确性，以确认所述 chanllenge 消息是否来自一个被授权的网络，同时该 UE 计算 CK、IK 和 RES。

步骤 1507：该 UE 发送 HTTP request 消息给该 EAC，其中包含有 Digest AKA response 以及经由 RES 计算的摘要值。

步骤 1508：该 EAC 验证计算的摘要值的正确性，用以认证该 UE 的合法性。

步骤 1509：该 EAC 生成共享密钥  $K_s=CK||IK$ ，以及中间业务请求标识 (ISR-ID)，然后利用共享密钥 (K<sub>s</sub>)、该 SS 的身份标识以及该 SP 的 UID 生成衍生密钥 (K<sub>sp</sub>)，并将所生成的衍生密钥放在业务许可票据 (SGT) 中，该票据的内容包括：衍生密钥 (K<sub>sp</sub>)、SS 的 ISR-ID、SP 的 UID、有效期、防重放攻击参数等，并且该票据经由 EAC 与 SP 的共享密钥加密。

步骤 1510：该 EAC 发送 200 OK 消息给 UE，表示认证成功结束，该 200 OK 消息中包含共享密钥的有效期、ISR-ID 以及经由共享密钥  $K_s$  加密的业务许可票据（SGT）。

步骤 1511：该 UE 也生成共享密钥  $K_s=CK||IK$  以及衍生密钥  $K_{sp}$ ，  
5 然后解密获得上述 200 OK 消息中的 ISR-ID、有效期以及业务许可票据（SGT），并将解密得到的这些信息连同认证模式信息关联保存在本地。

图 16 所示为本发明一实施例中业务签约者与业务提供者间的互认证流程图。参见图 16，业务签约者（SS）与业务提供者（SP）间进行互认证，具体过程如下：

10 步骤 1601：SS 向 SP 发送 ClientHello 消息，该消息中携带该 SP 的公开身份标识（UID）、该 SS 所支持的 TLS-KRB5 加密套件、以及认证模式 E2E\_Kerberos 的相应信息。

所谓认证模式 E2E\_Kerberos 的相应信息指该 E2E\_Kerberos 模式中定义的 SS 与 SP 的认证方法和会话密钥生成方法。

15 步骤 1602：该 SP 收到该 Client Hello 消息后，发现 Session ID 字段为空，则选择双方都支持的 TLS-KRB5 加密套件，先后发送 ServerRequest 消息 ServerHello 和 ServerHelloDone 消息给该 SS。

步骤 1603：收到该 ServiceHelloDone 消息后，该 SS 向该 SP 发送 ClientKeyExchange 消息，通过这条消息双方获得预共享秘密参数  
20（PreMasterSecret）；该 SS 利用该 PreMasterSecret 以及随机数生成会话密钥（MasterSecret）；然后，该 SS 在发出 ChangeCipherSpec 消息并随后发送 Finished 消息给该 SP，用于正式密钥交换和验证。

步骤 1604：该 SP 解密业务许可票据（SGT）并检验票据的有效性，  
25 获得共享衍生密钥（ $K_{sp}$ ），并利用共享衍生密钥（ $K_{sp}$ ）解密该 PreMasterSecret，然后由该 PreMasterSecret 以及随机数等生成该 SS 和

SP 的会话密钥 (MasterSecret); 然后该 SP 验证该 SS 的 Finished 消息中的信息是否正确，如果不正确，结束本流程；否则执行步骤 1605。

步骤 1605：该 SP 发送 ChangeCipherSpec 消息给该 SS 并随后将 Finished 消息返回给该 SS。

5 步骤 1606：该 SS 验证该来自 SP 的 Finished 消息中的信息的正确性，如果该 SS 验证该 Finished 消息的信息正确，那么双方的认证和密钥交换过程成功结束。

步骤 1607：该 SS 和 SP 开始传输业务通信数据。

当上述流程所建立的会话没有过期时，若 SS 再次向 SP 发送业务请求，  
10 则可以重用上次会话生成的 PreMasterSecret 来生成本次业务通信的新  
的会话密钥 (MasterSecret)。

图 17 所示为本发明一实施例中业务签约者与业务提供者重新利用  
认证结果生成会话密钥的流程图。参见图 17，具体流程如下：

步骤 1701：SS 向 SP 发送 Client Hello 消息，并携带上次会话的  
15 Session ID。

步骤 1702：该 SP 收到该 Client Hello 消息后，发现 Session ID 不为  
空，且能够匹配到相关联的安全连接信息，则重用该 Session ID 来标识  
会话，并向该 SS 发送 ServerHello 消息，该消息携带该 Session ID，然  
后发送 ServerHelloDone 消息给该 SS。

20 步骤 1703：该 SS 利用与该 SP 共享的 PreMasterSecret 生成会话密  
钥 (MasterSecret)。

步骤 1704：该 SS 向该 SP 发送 ChangeCipherSpec 消息，并随后发  
送 Finished 消息给该 SP。

步骤 1705：该 SP 检验接收到的 Finished 消息无误后，利用同样的  
25 PreMasterSecret 生成会话密钥 (MasterSecret)。

步骤 1706：该 SP 发送 ChangeCipherSpec 消息给该 SS，并随后返回 Finished 消息给该 SS。

步骤 1707：如果该 SS 收到的 Finished 消息无误，则双方互认证结束，开始传输本次业务通信数据。

5 根据上述基于认证模式的实体认证增强方案，本发明实施例还提出了另一种实体认证装置。该装置与图 14 所示装置类似。图 18 所示为本发明实施例端到端通信认证装置一实施例的结构示意图。参见图 18，该实体认证装置包括：发送模块（类似图 14 中的认证请求发送模块），用于为业务实体（SS 或 SP）向实体认证中心发送认证请求；选择模块（类似图 14 中的协商模块），用于按发送模块发送的认证请求，为实体认证中心选择认证模式并通知业务实体；认证模块（类似图 14 中的认证交互模块），用于业务实体和实体认证中心之间或业务实体之间根据选择模块所选择的认证模式进行认证。这些模块实现具体功能的原理在前述方法流程中均有描述，这里不再赘述。

10 15 当然，本发明实施例还能提供一种实体认证装置，能够实现前述两种装置的功能，该种装置可包括：第一模块，用于实现前述发送模块和认证请求发送模块的功能；第二模块，用于实现选择模块和协商模块的功能；第三模块，用于实现认证模块和认证交换模块的功能。这里就不再对此装置做进一步详述。

20 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、等同替换和改进等，均应包含在本发明的保护范围之内。

## 权利要求书

1、一种基于移动网络端到端通信的认证方法，应用于包括：请求业务的第一业务实体、提供业务的第二业务实体和实体认证中心的系统，其特征在于，该方法包括：

5 所述第一业务实体与所述实体认证中心协商认证模式，该协商得到的认证模式包括：该第一业务实体与实体认证中心之间的认证方法、该第二业务实体与该实体认证中心之间的认证方法、该实体认证中心的认证查询方法及衍生密钥生成方法、以及该第一业务实体与该第二业务实体之间的互认证方法；

10 所述第一业务实体和第二业务实体分别按协商得到的认证模式中定义的认证方法与该实体认证中心进行互认证；

当第一业务实体请求第二业务实体提供的业务时，所述实体认证中心按该协商得到的认证模式中定义的认证查询方法为该第一业务实体和第二业务实体提供认证查询并按该协商得到的认证模式中定义的衍生密钥生成方法生成二者之间的共享衍生密钥；

该第一业务实体和第二业务实体使用所述共享衍生密钥按该协商得到的认证模式中定义的二者之间的互认证方法进行互认证并生成保护本次业务的会话密钥。

2、根据权利要求 1 所述的方法，其特征在于，所述第一业务实体与所述实体认证中心协商认证模式，包括：

该第一业务实体向实体认证中心发送认证请求，该请求携带该第一业务实体的身份信息和当前请求的业务类型；

该实体认证中心按当前请求的业务类型确定提供该业务的第二业务实体，获取该第一业务实体和第二业务实体的认证能力，并按二者的认证能力选择认证模式。

3、根据权利要求 1 所述的方法，其特征在于，所述认证模式进一步定义：该第一业务实体和第二业务实体之间会话密钥的生成方法，

该第一业务实体和第二业务实体生成保护本次业务的会话密钥，包括：按协商得到的认证模式中定义的会话密钥生成方法生成所述会话密钥。

4、根据权利要求 1 所述的方法，其特征在于，所述业务实体按协商得到的认证模式中定义的认证方法与该实体认证中心进行互认证，包括：该业务实体与实体认证中心按所述认证方法进行相互认证并获得用于保护与该实体认证中心通信的共享密钥材料，该实体认证中心为该业务实体分配临时身份信息，该实体认证中心和该业务实体分别将所分配的临时身份信息和所获得的共享密钥材料关联保存；

所述实体认证中心为该第一业务实体和第二业务实体提供认证查询并生成所述共享衍生密钥，包括：

该实体认证中心按该第一和第二业务实体的临时身份信息分别对该第一和第二业务实体的权限进行认证，使用自身与该第一业务实体之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到用于保护第一和第二业务实体之间通信的共享衍生密钥，并返回该共享的衍生密钥给该第二业务实体；该第二业务实体关联保存该第一业务实体的临时身份信息、该共享的衍生密钥和当前请求的业务类型；该第一业务实体使用自身与该实体认证中心之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到该共享的衍生密钥。

5、根据权利要求 4 所述的方法，其特征在于，所述共享衍生密钥、共享密钥材料和临时身份信息具有有效期；该方法进一步包括：

当所述实体认证中心发现自身与所述第一和/或第二业务实体的共享密钥材料或该第一和/或第二业务实体的临时身份信息快过期或已过

期时，则指示该第一和/或第二业务实体发起重认证过程；和/或，

当所述第一和/或第二业务实体发现自身与所述实体认证中心的共享密钥材料或自身的临时身份信息快过期或已过期时，则向该实体认证中心发起重认证过程；和/或，

5 当所述实体认证中心发现所述第一和第二业务实体之间的共享衍生密钥快过期或已过期时，则指示该第一业务实体发起重认证过程；和/或，

10 当所述第二业务实体发现自身与第一业务实体的共享的衍生密钥或该第一业务实体的临时身份信息快过期或已过期时，则指示该第一业务实体发起重认证过程。

6、一种业务实体认证方法，应用于业务实体和实体认证中心之中，其特征在于，该方法包括：

所述业务实体与所述实体认证中心协商认证模式，该认证模式至少用于定义：该业务实体与实体认证中心之间的认证方法；

15 该业务实体按协商得到的认证模式中定义的认证方法与该实体认证中心进行互认证。

7、根据权利要求 6 所述的方法，其特征在于，所述实体认证中心与该业务实体协商认证模式，包括：

20 该业务实体向实体认证中心发送认证请求，该请求携带该业务实体的身份信息和当前请求的业务类型；

该实体认证中心按当前请求的业务类型确定提供业务的业务实体，获取该业务实体和提供该业务的业务实体的认证能力，并按二者的认证能力选择认证模式。

25 8、根据权利要求 7 所述的方法，其特征在于，所述获取该业务实体和提供业务的业务实体的认证能力，包括：

该请求业务的业务实体在所述认证请求中携带自身的认证能力，该实体认证中心在确定该提供业务的业务实体后按其身份信息查询签约数据得到该提供业务的业务实体的认证能力；或者，

该实体认证中心按该请求业务的业务实体的身份信息查询签约数  
5 据得到其认证能力，在确定该提供业务的业务实体后按其身份信息查询  
签约数据得到该提供业务的业务实体的认证能力。

9、根据权利要求 6 所述的方法，其特征在于，所述业务实体按协商得到的认证模式中定义的认证方法与该实体认证中心进行互认证，包括：  
10 该业务实体与实体认证中心按所述认证方法进行相互认证并获得用于保护与该实体认证中心通信的共享密钥材料，该实体认证中心为该业务实体分配临时身份信息，该实体认证中心和该业务实体分别将所分配的临时身份信息和所获得的共享密钥材料关联保存；

10、根据权利要求 9 所述的方法，其特征在于，所述共享密钥材料和临时身份信息具有有效期；该方法进一步包括：

15 当所述实体认证中心发现自身与所述业务实体的共享密钥材料或该业务实体的临时身份信息快过期或已过期时，则指示该业务实体发起重认证过程；和/或，

当所述业务实体发现自身与所述实体认证中心的共享密钥材料或自身的临时身份信息快过期或已过期时，则向该实体认证中心发起重认  
20 证过程。

11、一种认证查询方法，应用于包括：用于请求业务的第一业务实体、用于提供业务的第二业务实体和实体认证中心的系统；所述第一业务实体和第二业务实体分别与所述实体认证中心进行互认证，该实体认证中心分别为该第一业务实体和第二业务实体分配临时身份信息，并分别获得自身与该第一业务实体和第二业务实体之间的共享密钥材料；其  
25

特征在于，所述第一业务实体与所述实体认证中心协商认证模式，该认证模式至少用于定义该实体认证中心的认证查询方法及衍生密钥生成方法，该方法包括：

当第一业务实体请求第二业务实体提供的业务时，所述实体认证中心使用协商得到的认证模式中定义的认证查询方法、按该第一业务实体和第二业务实体的临时身份信息对二者权限进行认证；

使用该协商得到的认证模式中定义的衍生密钥生成方法、以及该第一业务实体和第二业务实体的临时身份信息和该第一业务实体的共享密钥材料，计算得到用于保护该第一业务实体和第二业务实体之间通信的共享衍生密钥。

12、根据权利要求 11 所述的方法，其特征在于，该方法包括：

该实体认证中心使用协商得到的认证模式中定义的认证查询方法、按该第一和第二业务实体的临时身份信息分别对该第一和第二业务实体的权限进行认证；使用该协商得到的认证模式中定义的衍生密钥生成方法、以及自身与该第一业务实体之间的共享密钥材料以及该第一和第二业务实体的临时身份信息，计算得到用于保护第一和第二业务实体之间通信的共享衍生密钥，并返回该共享的衍生密钥给该第二业务实体；

该第二业务实体关联保存该第一业务实体的临时身份信息、该共享的衍生密钥和当前请求的业务类型；

该第一业务实体使用自身与该实体认证中心之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到该共享的衍生密钥。

13、根据权利要求 11 所述的方法，其特征在于，该方法包括：

该第一业务实体在向该第二业务实体请求业务时，提供自身的临时身份信息；

该第二业务实体将自身的临时身份信息和该第一业务实体的临时身份信息提供给该实体认证中心；

该实体认证中心按该第一和第二业务实体的临时身份信息对二者的权限进行认证，使用自身与该第一业务实体之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到用于保护第一和第二业务实体之间通信的共享衍生密钥，并返回该共享的衍生密钥给该第二业务实体；

该第二业务实体关联保存该第一业务实体的临时身份信息、该共享的衍生密钥和当前请求的业务类型；

10 该第一业务实体使用自身与该实体认证中心之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到该共享的衍生密钥。

14、根据权利要求 11 所述的方法，其特征在于，该方法包括：

该第一业务实体在向所述实体认证中心请求业务许可票据时，提供自身的临时身份信息和当前请求的业务类型；

15 该实体认证中心按该第一业务实体的临时身份信息对其权限进行认证，根据当前请求的业务类型得到所述第二业务实体的临时身份信息，并按此临时身份信息对该第二业务实体的权限进行认证，使用自身与该第一业务实体之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到用于保护第一和第二业务实体之间通信的共享的衍生密钥，产生包含该衍生密钥、该第一业务实体和第二业务实体的临时身份信息的业务许可票据并发送至该第一业务实体；

该第一业务实体使用自身与该实体认证中心之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到该共享的衍生密钥，并在向该第二业务实体请求业务时，提供该业务许可票据；

该第二业务实体从该业务许可票据中得到自身与该第一业务实体之间的共享的衍生密钥，并关联保存该第一业务实体的临时身份信息、该共享的衍生密钥和当前请求的业务类型。

15、根据权利要求 11 所述的方法，其特征在于，该方法包括：

5 该第一业务实体向所述实体认证中心提出业务请求，并提供自身的临时身份信息和当前请求的业务类型；

该实体认证中心按该第一业务实体的临时身份信息对其权限进行认证，按当前请求的业务类型转发业务请求至该第二业务实体；

该第二业务实体向该实体认证中心返回自身的临时身份信息；

10 该实体认证中心按该第二业务实体的临时身份信息对该第二业务实体的权限进行认证，使用自身与该第一业务实体之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到用于保护第一和第二业务实体之间通信的共享的衍生密钥并发送至该第二业务实体；

15 该第二业务实体关联保存该第一业务实体的临时身份信息、该共享的衍生密钥和当前请求的业务类型；

该第一业务实体使用自身与该实体认证中心之间的共享密钥材料以及该第一和第二业务实体的临时身份信息计算得到该共享的衍生密钥。

16、根据权利要求 11 至 15 中任一项所述的方法，其特征在于，当 20 所述实体认证中心返回该共享的衍生密钥给该第二业务实体时，进一步包括：使用自身与该第二业务实体之间的共享密钥材料进行通信保护。

17、一种基于移动网络端到端通信的认证系统，包括：用于请求业务的第一业务实体、用于提供业务的第二业务实体和实体认证中心；其特征在于，

25 所述第一业务实体用于与所述实体认证中心协商认证模式，该认证

模式用于定义与认证相关的方法，按协商得到的认证模式的定义与该实体认证中心进行互认证，向所述第二业务实体请求业务，按该协商得到的认证模式的定义、使用与该第二业务实体之间的共享衍生密钥与该第二业务实体进行互认证；

5 所述第二业务实体用于按该协商得到的认证模式的定义与该实体认证中心进行互认证，在该第一业务实体请求业务时按该协商得到的认证模式的定义、使用与该第二业务实体之间的共享衍生密钥与该第一业务实体进行互认证；

10 所述实体认证中心用于按该协商得到的认证模式的定义分别与该第一业务实体和第二业务实体进行互认证，在该第一业务实体请求业务时按该协商得到的认证模式的定义为该第一业务实体和第二业务实体提供认证查询并生成二者的共享衍生密钥。

18、根据权利要求 17 所述的系统，其特征在于，该系统进一步包括：用于保存业务实体签约数据的数据库；

15 该实体认证中心在协商认证模式时，进一步用于按所述第一业务实体和第二业务实体的身份信息查询该数据库得到该第一业务实体和第二业务实体的认证能力，并按二者的认证能力选择所述认证模式。

19、根据权利要求 17 所述的系统，其特征在于，

20 所述实体认证中心在分别与第一业务实体和第二业务实体进行互认证时，分别为该第一业务实体和第二业务实体分配临时身份信息，并分别获得自身与该第一业务实体和第二业务实体之间的共享密钥材料；在为该第一业务实体和第二业务实体提供认证查询时，使用该第一业务实体和第二业务实体的临时身份信息和该第一业务实体的共享密钥材料、按所述协商得到的认证模式的定义，计算得到用于保护该第一业务实体和第二业务实体之间通信的共享衍生密钥并返回给该第二业务实

体；

该第一业务实体在请求业务时使用自身的共享密钥材料和临时身份信息、该第二业务实体的临时身份信息、按所述协商得到的认证模式的定义，计算得到共享衍生密钥；

5 该第二业务实体进一步用于关联保存该第一业务实体的临时身份信息、所收到的共享衍生密钥和当前第一业务实体请求的业务类型。

20、一种业务实体认证系统，包括业务实体和实体认证中心；其特征在于，

所述业务实体用于与实体认证中心协商认证模式，该认证模式至少  
10 用于定义该业务实体与该实体认证中心之间的认证方法，该业务实体使用协商得到的认证模式中定义的认证方法与该实体认证中心进行互认  
证。

21、根据权利要求 20 所述的系统，其特征在于，该系统进一步包  
括：用于保存业务实体签约数据的数据库；

15 该实体认证中心在协商认证模式时，进一步用于按所述请求业务的  
业务实体和所述提供业务的业务实体的身份信息查询该数据库得到这  
两个业务实体的认证能力，并按二者的认证能力选择认证模式。

22、一种认证查询系统，包括：用于请求业务的第一业务实体、用  
于提供业务的第二业务实体和实体认证中心，其特征在于，所述第一业  
20 务实体与所述实体认证中心协商认证模式，该认证模式至少用于定义该  
实体认证中心的认证查询方法及衍生密钥生成方法；

所述实体认证中心用于在所述第一业务实体请求业务时使用协商  
得到的认证模式中定义的认证查询方法对该第一业务实体和所述第二  
业务实体的权限进行认证，并使用该协商得到的认证模式中定义的衍生  
25 密钥生成方法生成二者共享的衍生密钥。

23、根据权利要求 22 所述的系统，其特征在于，

所述实体认证中心用于按所述第一业务实体和第二业务实体的临时身份信息对该第一业务实体和第二业务实体的权限进行认证，使用第一业务实体的共享密钥材料、该第一业务实体和第二业务实体的临时身份信息计算得到共享的衍生密钥并返回给该第二业务实体；

所述第一业务实体用于按自身的共享密钥材料和临时身份信息、以及该第二业务实体的临时身份信息计算得到所述共享的衍生密钥；

所述第二业务实体用于关联保存该第一业务实体的临时身份信息、该共享的衍生密钥和当前请求的业务类型。

10 24、一种认证中心，其特征在于，包括：

第一单元，用于协商业务实体的认证模式，该认证模式至少用于定义：业务实体与实体认证中心之间的认证方法；

第二单元，用于按所述第一单元协商得到的认证模式中定义的认证方法与所述业务实体进行互认证。

15 25、根据权利要求 24 所述的认证中心，其特征在于，所述第一单元包括：

第一模块，用于查询签约数据分别得到请求业务的业务实体和提供业务的业务实体的认证能力；

第二模块，用于按所述第一模块得到的该请求业务的业务实体和提供业务的业务实体的认证能力选择一种认证模式。

20 26、根据权利要求 24 或 25 所述的认证中心，其特征在于，所述认证模式进一步用于定义：所述实体认证中心的认证查询方法及衍生密钥生成方法；该认证中心进一步包括：

第三单元，用于在业务实体请求业务时使用所述协商得到的认证模式中定义的认证查询方法和衍生密钥生成方法为该请求业务的业务实

体和提供业务的业务实体提供认证查询并生成二者的共享衍生密钥。

27、根据权利要求 26 所述的认证中心，其特征在于，  
所述第二单元用于生成业务实体的共享密钥材料和临时身份信息；  
所述第三单元用于使用该第二单元生成的共享密钥材料、所述请求  
5 业务的业务实体及提供业务的业务实体的临时身份信息计算得到该请  
求业务的业务实体和该提供业务的业务实体之间的共享衍生密钥。

1/15

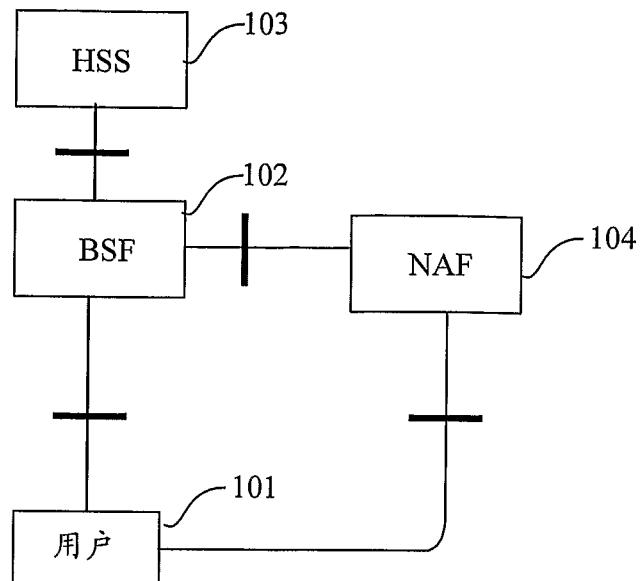


图 1

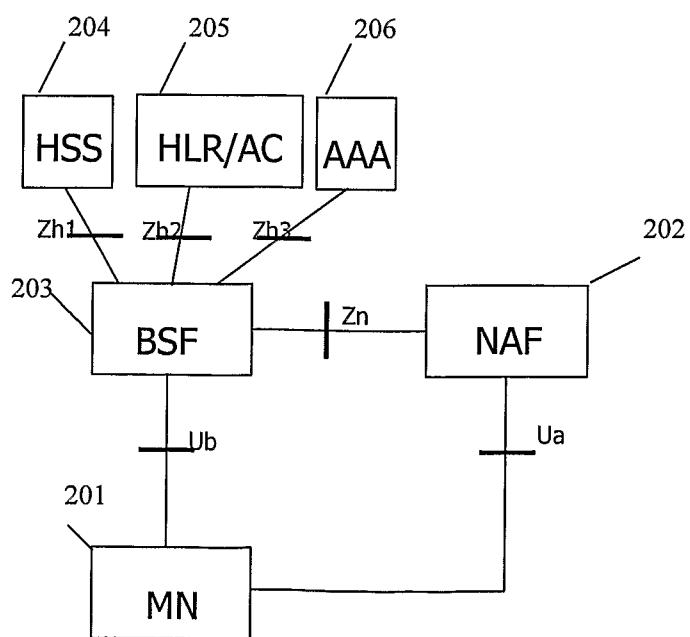


图 2

2/15

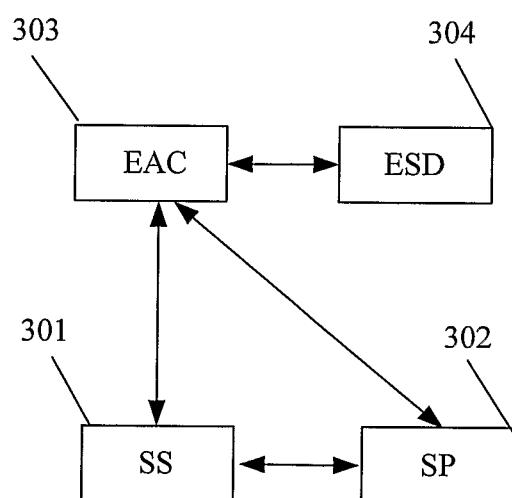


图 3

3/15

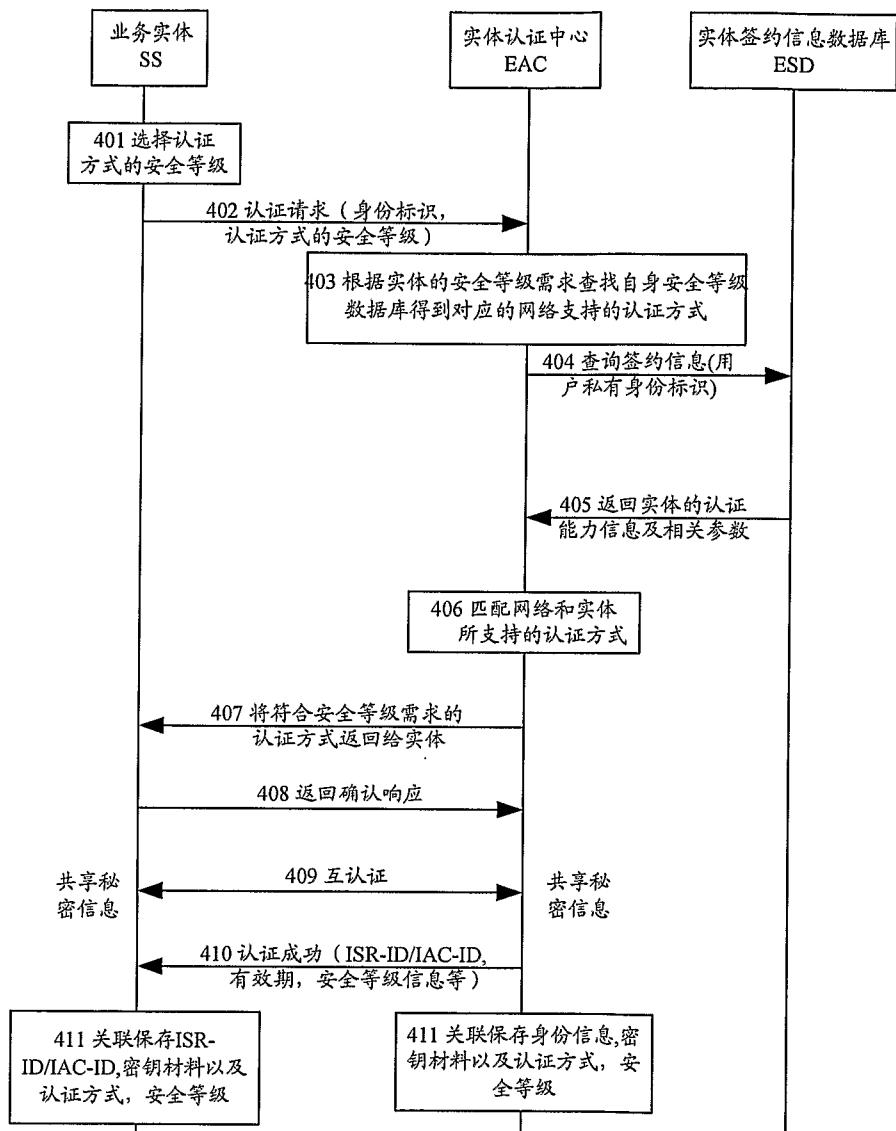


图 4

4/15

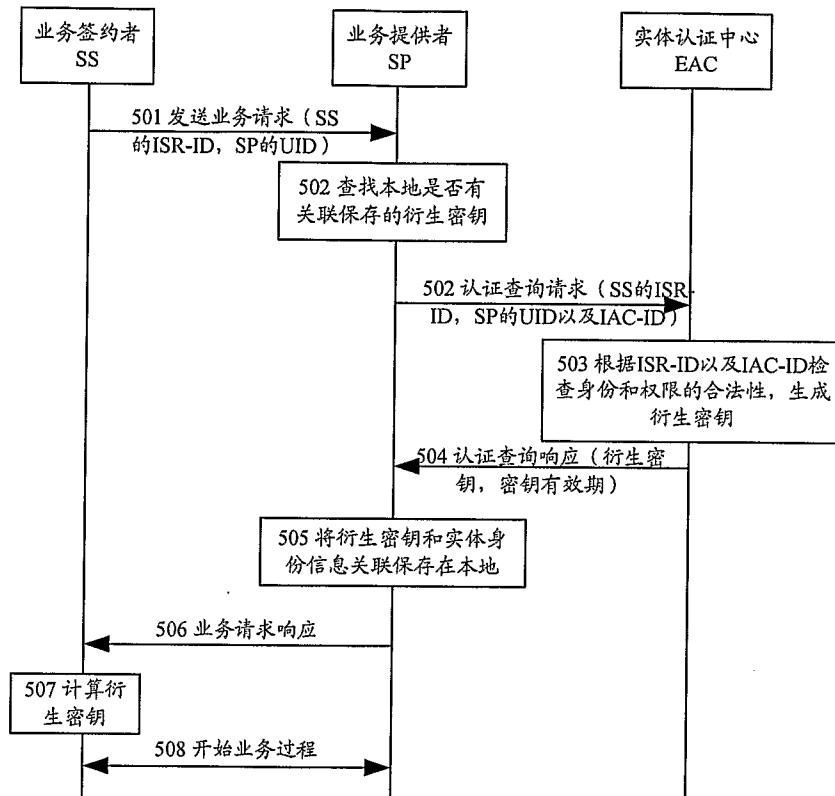


图 5

5/15

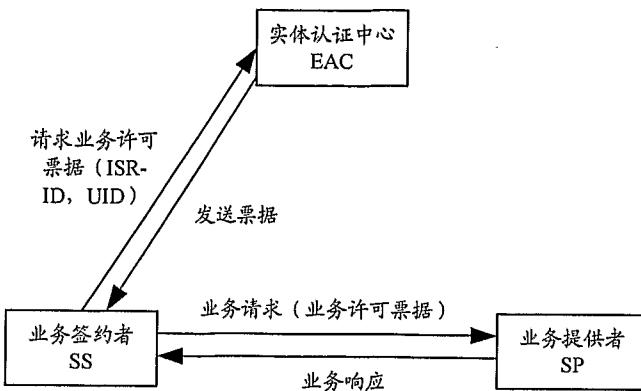


图 6

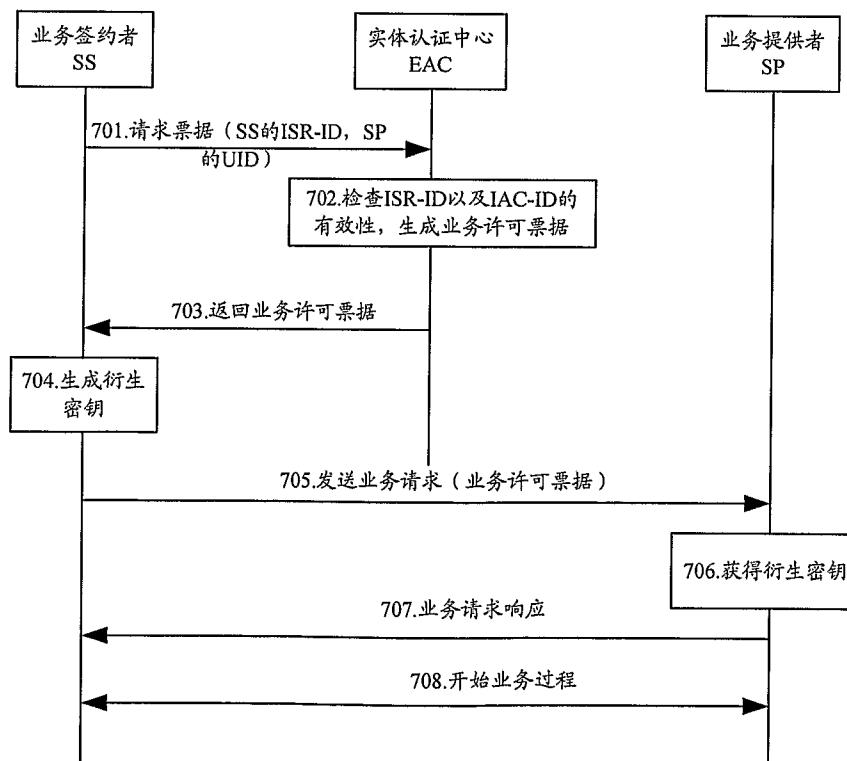


图 7

6/15

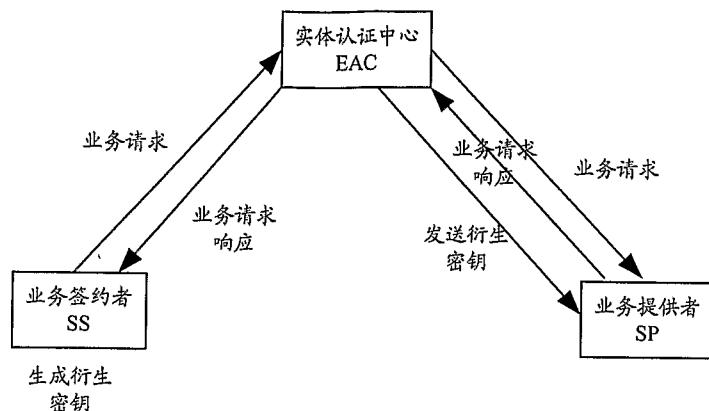


图 8

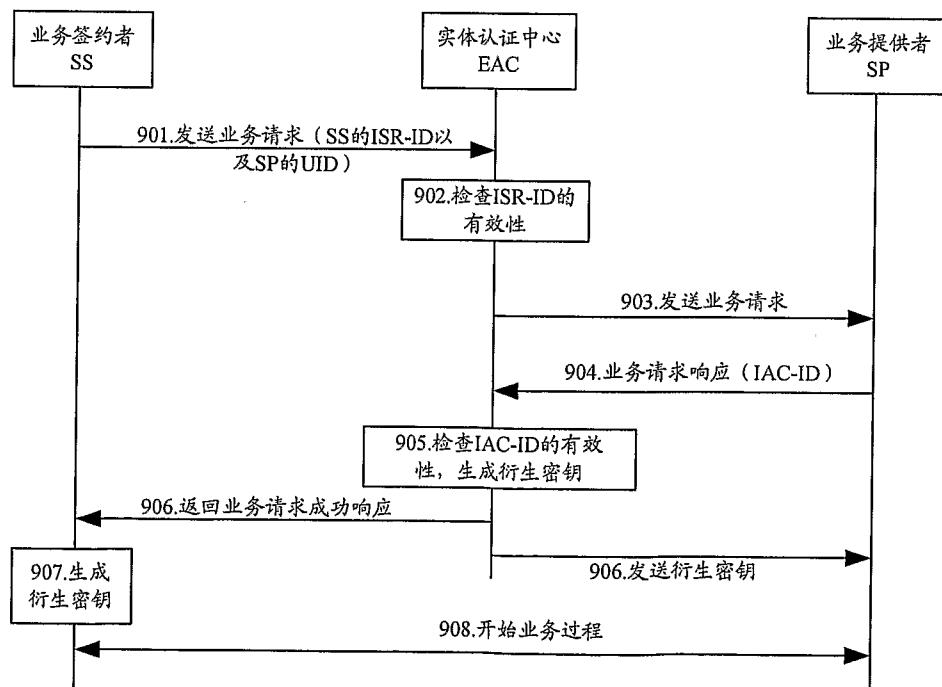


图 9

7/15

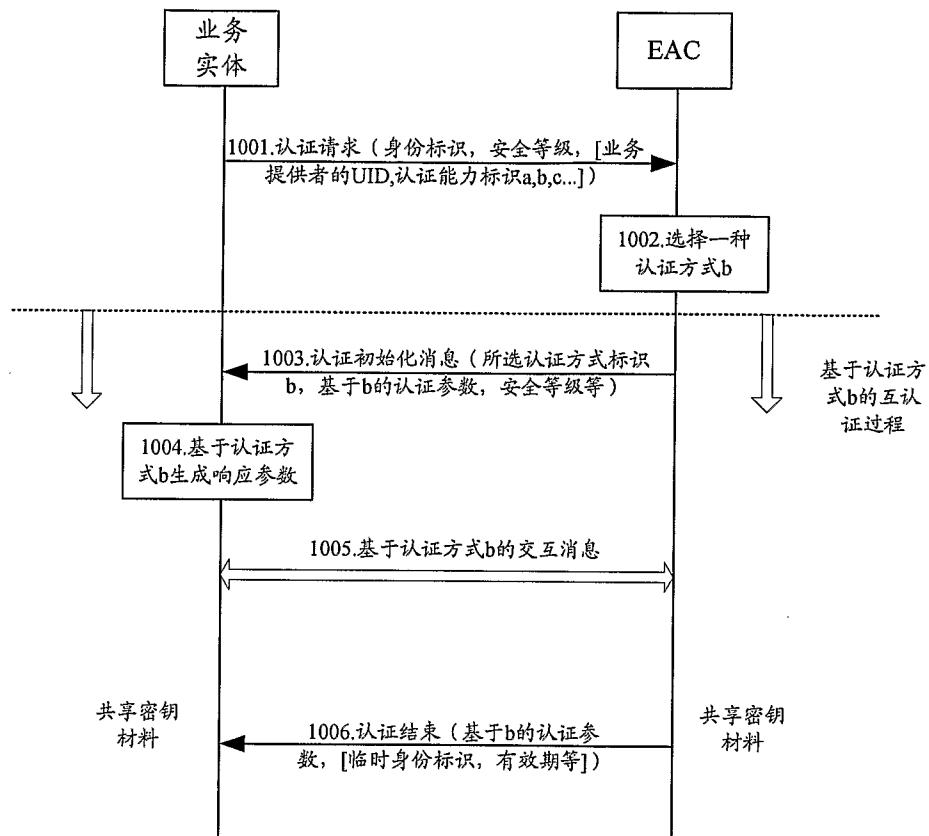


图 10

8/15

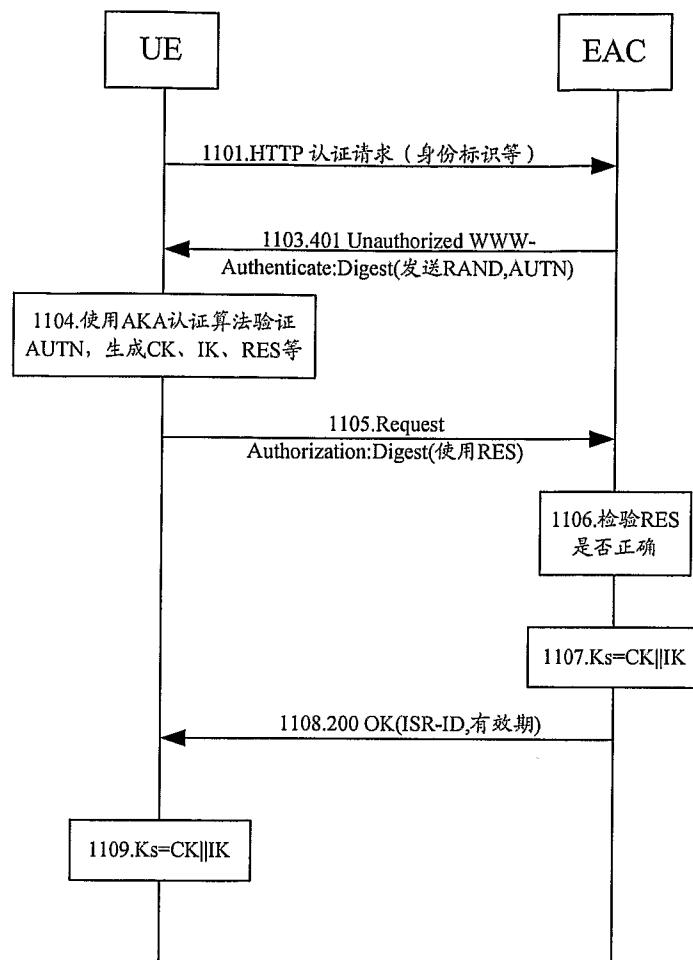


图 11

9/15

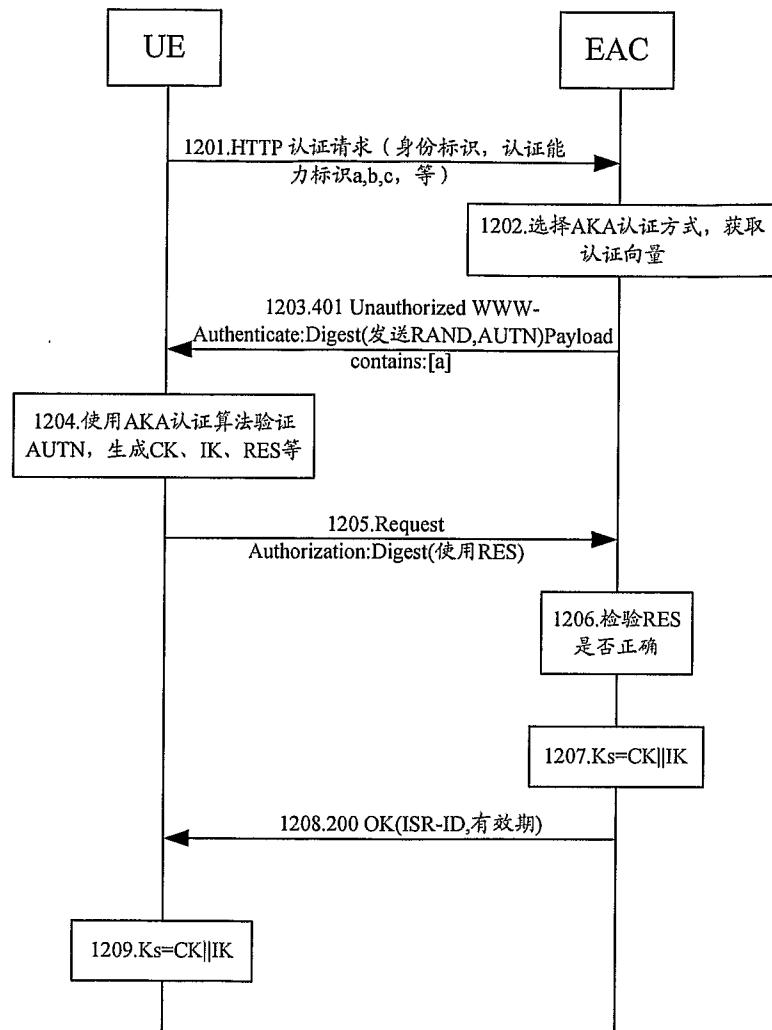


图 12

10/15

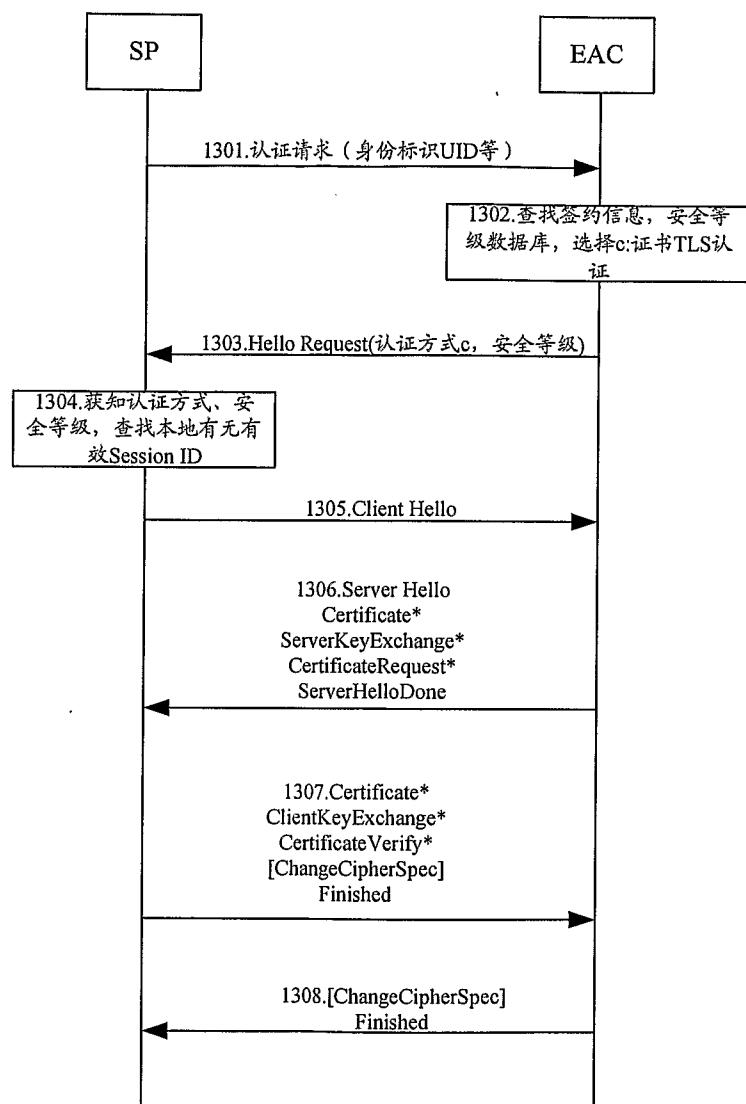


图 13

11/15

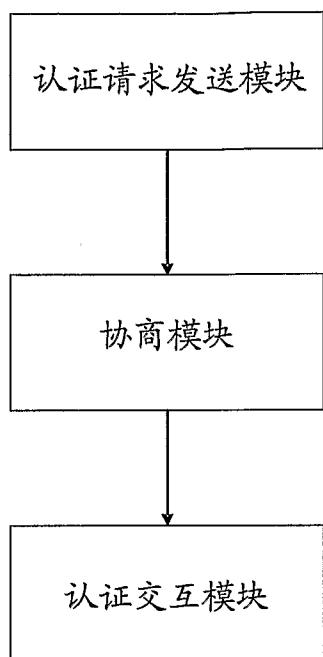


图 14

12/15

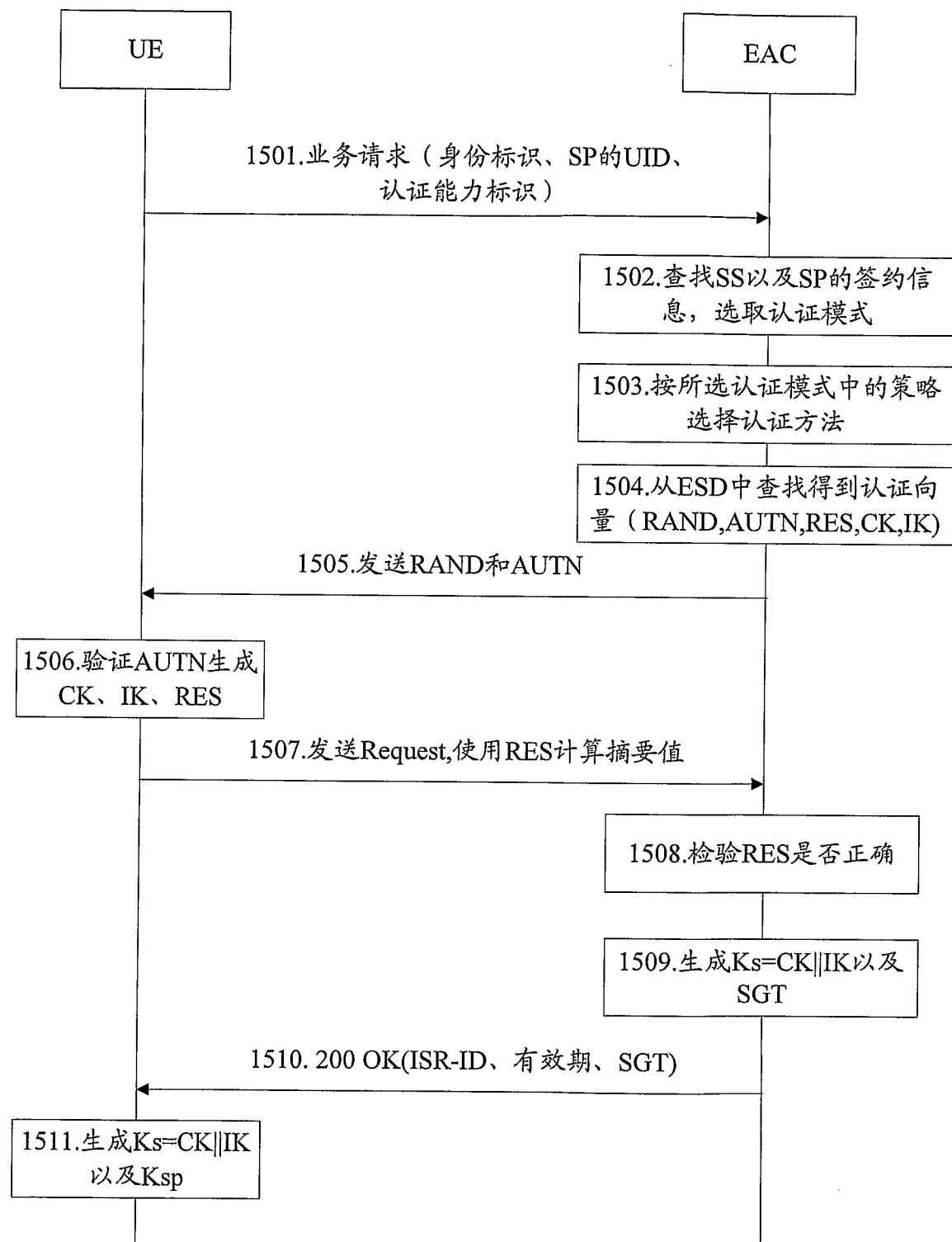


图 15

13/15

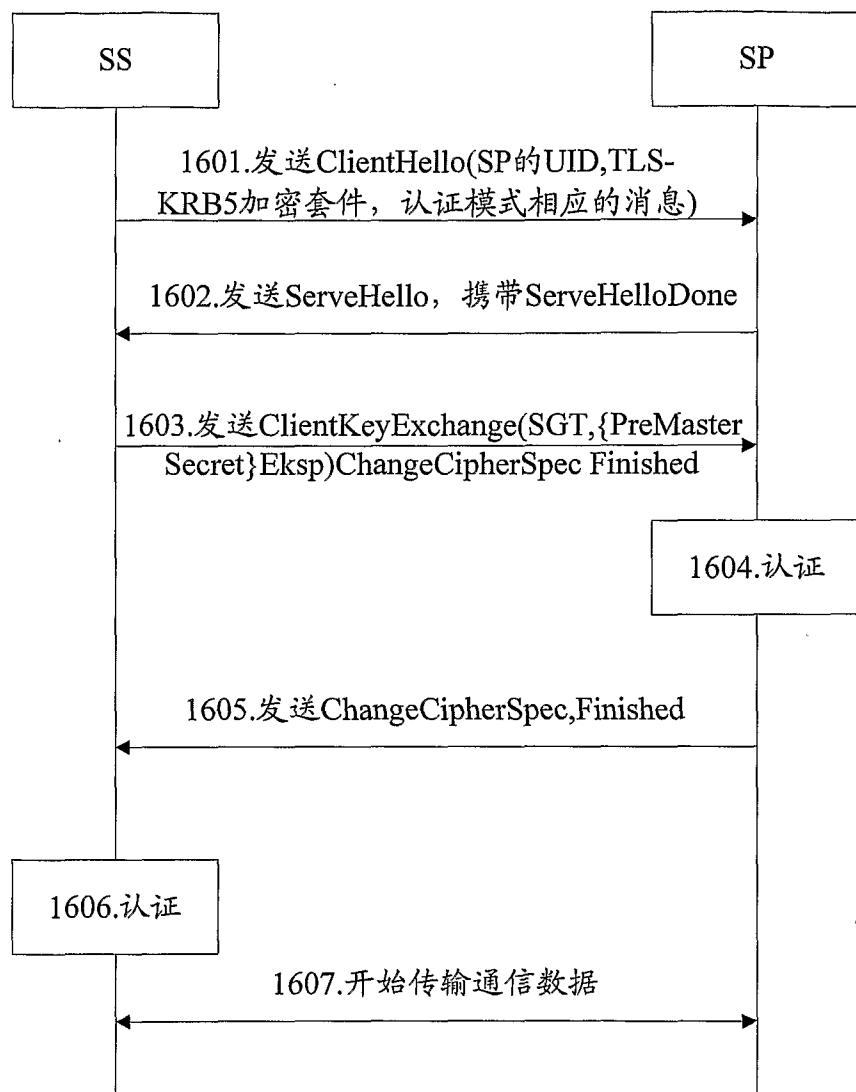


图 16

14/15

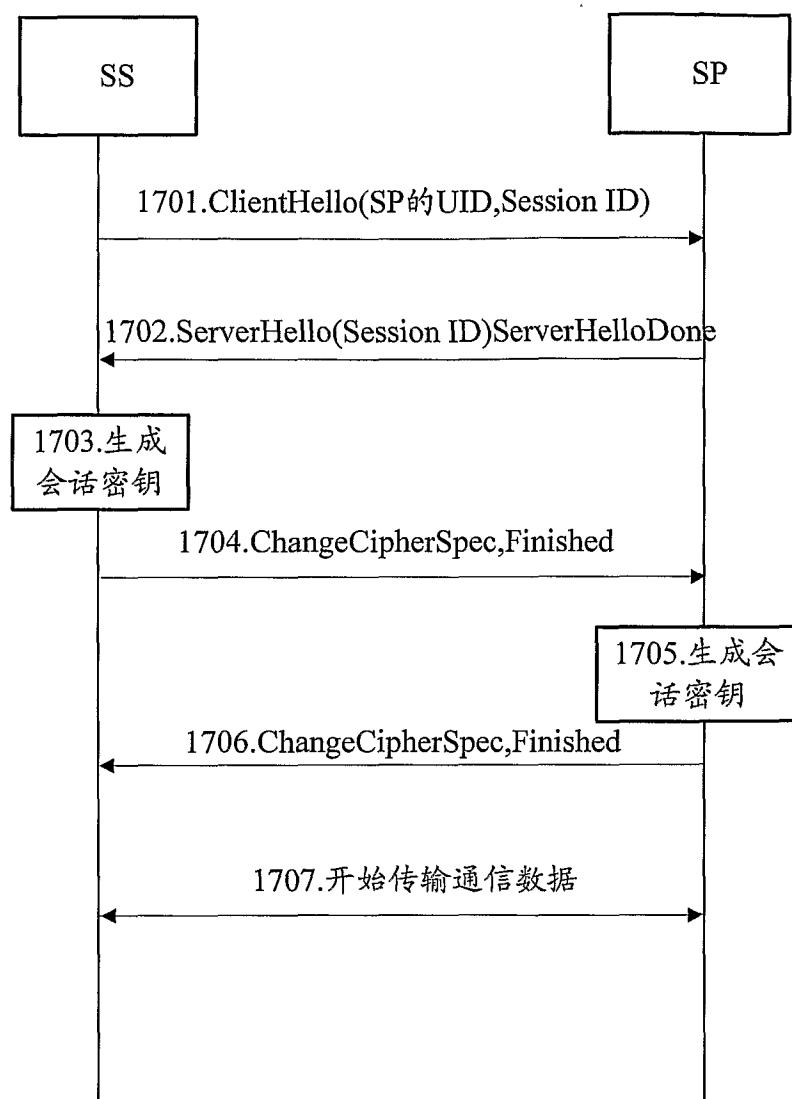


图 17

15/15

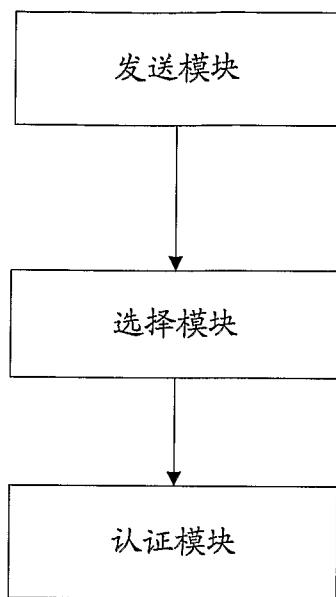


图 18

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2006/003601

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2007.01) i

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:H04L9/-;H04Q7/-

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)

WPI,EPODOC,PAJ,CNPAT: authentication, authorization, registration, adjust, change, vary, type, kind, sort, differ, service, provider, subscriber, entity, select+, auc, mode, method, service provider, subscriber, entity, center

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN1320344A (NOKIA NETWORKS OY) 31 Oct.2001 (31.10.2001) description: paragraphs 4,6 of page 3,paragraphs 3-5 of page 4	1, 6, 11, 17, 20, 22, 24
A	The whole document	2-5, 7-10, 12-16, 18, 19, 21, 23, 25-27
Y	CN1722658A(MICROSOFT CORP)18 Jan.2006(18.01.2006)description: paragraph 7 of page 2 to paragraph 8 of page 10	1, 6, 11, 17, 20, 22, 24
A	The whole document	2-5, 7-10, 12-16, 18, 19, 21, 23, 25-27

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

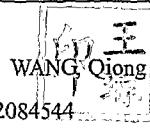
Date of the actual completion of the international search  
15 Mar.2007 (15.03.2007)

Date of mailing of the international search report

**05 · APR 2007 (05 · 04 · 2007)**

Name and mailing address of the ISA/CN  
The State Intellectual Property Office, the P.R.China  
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China  
100088  
Facsimile No. 86-10-62019451

Authorized officer

WANG Qiong  


Telephone No. (86-10)62084544

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/CN2006/003601

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1320344A	31.10.2001	WO0113666A1 AU6573600A EP1121822A1	22.02.2001 13.03.2001 08.08.2001
CN1722658A	18.01.2006	EP1577736A2 JP2005269656A US2005210252A1 KR20060044410A	21.09.2005 29.09.2005 22.09.2005 16.05.2006

## 国际检索报告

国际申请号

PCT/CN2006/003601

**A. 主题的分类**

H04L 9/32 (2007.01) i

按照国际专利分类表(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:H04L9/-;H04Q7/-

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))

WPI, EPODOC, PAJ: authentication, authorization, registration, adjust, change, vary, type, kind, sort, differ, service, provider, subscriber, entity, select+, auc, mode, method, service provider, subscriber, entity, center

CNPAT 认证方法, 认证方式, 认证模式, 鉴权方法, 鉴权模式, 鉴权方式, 验证方法, 验证方式, 验证模式, 调整, 改变, 协商, 选择, 实体, 类型, 多种, 不同, 不同的认证方法, 协商认证方式, 选择认证方式, 调整认证方式, 调整认证模式, 选择认证模式, 选择认证方法, 认证中心

**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
Y	CN1320344A (诺基亚网络有限公司) 31.10月2001 (31.10.2001) 说明书第3页第4, 6段, 第4页第3-5段	1, 6, 11, 17, 20, 22, 24
A	全文	2-5, 7-10, 12-16, 18, 19, 21, 23, 25-27
Y	CN1722658A (微软公司) 18.1月2006 (18.01.2006) 说明书第2页第7段至第10页第8段	1, 6, 11, 17, 20, 22, 24
A	全文	2-5, 7-10, 12-16, 18, 19, 21, 23, 25-27

 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  
 “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 15.3 月 2007 (15.03.2007)	国际检索报告邮寄日期 05.4月2007 (05.04.2007)
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451	授权官员  电话号码: (86-10)62084544

国际检索报告  
关于同族专利的信息

国际申请号  
PCT/CN2006/003601

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1320344A	31.10.2001	WO0113666A1 AU6573600A EP1121822A1	22.02.2001 13.03.2001 08.08.2001
CN1722658A	18.01.2006	EP1577736A2 JP2005269656A US2005210252A1 KR20060044410A	21.09.2005 29.09.2005 22.09.2005 16.05.2006