(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
2009 年6 月25 日 (25.06.2009)

PCT

(10) 国际公布号
WO 2009/076879 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2008/073389

(22) 国际申请日: 2008 年12 月9 日 (09.12.2008)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200710199241.3
2007 年12 月14 日 (14.12.2007) CN

(71) 申请人 (对除美国外的所有指定国): **西安西电捷通无线网络通信有限公司 (CHINA IWNCOMM CO., LTD)** [CN/CN]; 中国陕西省西安市高新区科技二路68号西安软件园秦风阁A201, Shaanxi 710075 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **铁满霞 (TIE, Manxia)** [CN/CN]; 中国陕西省西安市高新区科技二路68号西安软件园秦风阁A201, Shaanxi 710075 (CN)。 **曹军 (CAO, Jun)** [CN/CN]; 中国陕西省西安市高新区科技二路68号西安软件园秦风阁A201, Shaanxi 710075 (CN)。 **黄振海 (HUANG, Zhenhai)** [CN/CN]; 中国陕西省西安市高新区科技二路68号西安软件园秦风阁A201, Shaanxi 710075 (CN)。 **赖晓龙 (LAI, Xiaolong)** [CN/CN]; 中国陕西省西安市高新区科技二路68号西安软件园秦风阁A201, Shaanxi 710075 (CN)。

(74) 代理人: **北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW)**; 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (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, 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,

[见续页]

(54) **Title:** AN ENTITY BIDIRECTIONAL AUTHENTICATION METHOD AND SYSTEM

(54) **发明名称:** 一种实体双向鉴别方法和系统

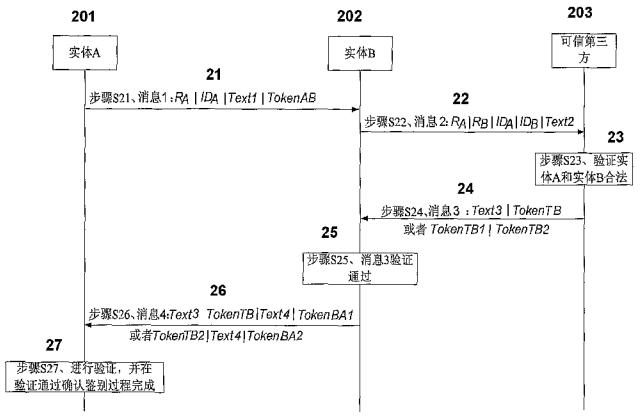

图 2 / Fig. 2

201 ENTITY A
202 ENTITY B
203 CREDIBLE THIRD PARTY
21 STEP S21, MESSAGE 1: R_A| ID_A| Text 1| Token AB
22 STEP S22, MESSAGE 2: R_A| R_B| ID_A| ID_B| Text 2
23 STEP S23, VERIFY THE LEGALITY OF THE ENTITY A AND ENTITY B
24 STEP S24, MESSAGE 3: Text 3| Token TB OR Token TB1| Token TB2
25 STEP S25, THE VERIFICATION OF MESSAGE 3 IS PASSED
26 STEP S26, MESSAGE 4: Text 3 Token TB| Text 4| Token BA1 OR Token TB2| Text 4| Token BA2
27 STEP S27, VERIFY, AND AFFIRM THE ACCOMPLISHMENT OF AUTHENTICATION PROCESS AFTER PASSING THE VERIFICATION

(57) **Abstract:** An entity bidirectional authentication method and system, the method involves: the first entity sends the first message; the second entity sends the second message to the credible third party after receiving the said first message; the said credible third party returns the third message after receiving the second message; the said second entity sends the fourth message after receiving the third message and verifying it; the said first entity receives the said fourth message and verifies it, completes the authentication. Compared with the conventional authentication mechanism, the invention defines an on-line retrieval and authentication mechanism of a public key, realizes the centralized management for it, simplifies the operating condition of the protocol, and facilitates the application and implement.

[见续页]

WO 2009/076879 A1

LT, LU, LY, MA, MD, ME, 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, 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, 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。

(57) 摘要：

一种实体双向鉴别方法和系统，该方法包括：第一实体发送第一消息；第二实体接收到所述第一消息后，向可信第三方发送第二消息；所述可信第三方收到第二消息后，返回第三消息；所述第二实体收到第三消息后，进行验证后，发送第四消息；所述第一实体接收所述第四消息并进行验证，完成鉴别。本发明相比传统鉴别机制，定义了公开密钥的在线检索和鉴别机制，实现了对它的集中管理，简化了协议的运行条件，便于其应用实施。

一种实体双向鉴别方法和系统

本申请要求于 2007 年 12 月 14 日提交中国专利局、申请号为 200710199241.3、发明名称为“一种实体双向鉴别方法”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。

技术领域

本发明涉及一种实体双向鉴别方法和系统。

背景技术

采用非对称密码技术的实体鉴别方法可分为两种类型，即单向鉴别和双向鉴别。鉴别的唯一性或时效性由时变参数进行标识，常被用作时变参数的有时间标记、顺序号和随机数等。若采用时间标记或顺序号作为时变参数，则单向鉴别只需要采用一次消息传递，双向鉴别需要采用两次消息传递；若采用随机数作为时变参数，则单向鉴别需要采用两次消息传递，双向鉴别需要采用三次消息传递或四次消息传递（即两次消息传递的并行鉴别）。

不论上述哪种鉴别机制，在运行之前或运行当中，验证者必须具有声称者的有效公开密钥，否则鉴别过程会受到损害或不能成功完成。在此，以双向鉴别的三次传递方法为例进行说明：

参见图 1，权标 $TokenAB=R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)$，$TokenBA=R_B||R_A||A||Text5||sS_B(R_B||R_A||A||Text4)$。其中，$X$ 为实体区分符，该鉴别系统有 A 和 B 两个鉴别实体；$Cert_X$ 表示实体 X 的证书；sS_X 表示实体 X 的签名；R_X 表示实体 X 产生的随机数；$Text$ 为可选文本字段。

三次传递鉴别机制运行过程详述如下：

步骤 S11、实体 B 发送随机数 R_B、可选项文本 $Text1$ 给实体 A；

步骤 S12、实体 A 发送权标 $TokenAB$、可选项证书 $Cert_A$ 给实体 B；

步骤 S13、实体 B 通过检验实体 A 的证书或通过别的方式确保拥有实体 A 的有效公开密钥。

步骤 S14、实体 B 获取实体 A 的公钥后，验证步骤 S12 中的 $TokenAB$ 的签名，校验区分符 B 的正确性，并检查步骤 S11 中发送的随机数 R_B 和 $TokenAB$

中的随机数 R_B 是否相符；实体 *B* 完成对实体 *A* 的验证;

步骤 S15、实体 *B* 发送权标 *TokenBA*、可选项证书 $Cert_B$ 给实体 *A*;

步骤 S16、实体 A 通过检验实体 *B* 的证书或通过别的方式确保拥有实体 *B* 的有效公开密钥;

步骤 S17、实体 A 获取实体 *B* 的公钥后，验证 S15 中的 *TokenBA* 的签名，校验区分符 A 的正确性，并检查步骤 S12 中发送的随机数 R_A 和 *TokenBA* 中的随机数 R_A 是否相符及 S11 中收到的随机数 R_B 和 *TokenBA* 中的随机数 R_B 是否相符；实体 *A* 完成对实体 *B* 的验证。

可见，三次传递鉴别机制欲运行成功必须确保实体 A 和 *B* 分别拥有对方的有效公开密钥，而如何获得对方公开密钥及其有效性，协议本身并没有涉及。这一保障需求条件在目前很多应用环境下都不能满足，比如通信网络通常采用实体鉴别机制实现用户接入控制功能，在鉴别机制成功完成前，禁止用户访问网络，因而在鉴别之前用户无法或难以访问证书机构获得对端实体——网络接入点公开密钥的有效性，导致鉴别过程无法进行。

发明内容

有鉴于此，本发明提供一种实体双向鉴别方法和系统，以解决现有技术由于在鉴别成功前无法访问网络而导致鉴别过程无法进行的问题。

本发明实施例提供的实体双向鉴别方法包括以下步骤:

第一实体发送携带有时变参数 R_A、身份标识 ID_A 和签名的第一消息;

第二实体收到所述第一消息后，向可信第三方发送携带有时变参数 R_A 和 R_B、所述第一实体的身份标识 ID_A 和本身的身份标识 ID_B 的第二消息;

所述可信第三方收到所述第二消息后，向所述第二实体返回携带自身签名及时变参数 R_A 和时变参数 R_B 的第三消息;

所述第二实体收到所述第三消息后，在可信第三方签名验证通过且时变参数 R_B 与本地存储的时变参数 R_B 相符时，获取第一实体的验证结果，当验证结果指示所述第一实体合法有效时，获取所述第一实体的公钥以验证所述第一消息中所述第一实体的签名，在验证通过时，发送携带所述可信第三方签名、第

二实体签名和时变参数 R_A 的第四消息;

所述第一实体收到所述第四消息后，在可信第三方签名验证通过且时变参数 R_A 与本地存储的时变参数 R_A 相符时，获取第二实体的验证结果，当验证结果指示所述第二实体合法有效时，获取所述第二实体的公钥以验证所述第四消息中所述第二实体的签名，完成鉴别过程。

优选的，上述方法中，所述第三消息是在完成所述第一实体和第二实体的合法性验证时发送的。

优选的，上述方法中，所述第一实体和第二实体合法的条件为：所述第二消息中的所述第一实体和第二实体的身份标识为证书，且所述证书有效。

优选的，上述方法中，所述第一实体和第二实体合法的条件为：所述第二消息中的所述第一实体和第二实体的身份标识为区分符，且所述第一实体和第二实体的公钥存在并有效。

优选的，上述方法中，所述时变参数可为随机数、时间标记或顺序号。

本发明实施例同时还公开了一种三元对等鉴别系统，包括：第一实体、第二实体和作为可信第三方的第三实体，其中：

第一实体用于：向所述第二实体发送携带时变参数 R_A、自身身份标识 ID_A 及签名的第一消息；在接收所述第二实体发送的携带第三实体签名、第二实体签名和时变参数 R_A 的第四消息后，在第三实体签名验证通过且时变参数 R_A 与本地存储的时变参数 R_A 相符时，获取第二实体的验证结果，并当该验证结果指示第二实体合法时，获取所述第二实体的公钥，以对所述第四消息中的第二实体的签名进行验证;

所述第二实体用于：在接收到所述第一消息后，向所述第三实体发送携带有时变参数 R_A 和 R_B、第一实体身份标识 ID_A、自身身份标识 ID_B 的第二消息，在接收所述第三实体返回的携带所述第三实体签名及时变函数 R_A 和时变参数 R_B 的第三消息后，在所述的第三实体签名验证通过且所述第三消息中的时变参数 R_B 与本地存储的时变参数 R_B 相符时，获取第一实体的验证结果，并当所述验证结果指示所述第一实体合法有效时，获取所述第一实体的公钥以验证所

述第一消息中所述第一实体的签名，在验证通过时发送所述第四消息；

所述第三实体用于：接收所述第二消息，向所述第二实体返回所述第三消息。

优选的，上述系统中，所述第三消息是在完成所述第一实体和第二实体的合法性验证时发送的。

优选的，上述系统中，所述第一实体和第二实体合法的条件为：所述第二消息中的所述第一实体和第二实体的身份标识为证书，且所述证书有效。

优选的，上述系统中，所述第一实体和第二实体合法的条件为：所述第二消息中的所述第一实体和第二实体的身份标识为区分符，且所述第一实体和第二实体的公钥存在并有效。

优选的，上述系统中，所述时变参数可为随机数、时间标记或顺序号。

本发明采用三实体构架，鉴别实体在鉴别之前需获得可信第三方的的公钥或证书，并获得可信第三方颁发给自己的用户证书或将自己的公钥交给可信第三方保管，而无需事先知晓对端鉴别实体的有效公开密钥。在协议运行中，鉴别实体的公开密钥及其有效性通过可信第三方的搜索和验证，自动传递给所需的对端。本发明相比传统鉴别机制，定义了公开密钥的在线检索和鉴别机制，实现了对它的集中管理，简化了协议的运行条件，便于其应用实施。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为现有技术中三次传递鉴别机制的鉴别示意图；

图 2 为本发明实施例提供的双向鉴别方法的示意图；

图 3 为图 2 所示方法中实体 B 验证过程示意图；

图 4 为图 2 所示方法中实体 A 验证过程示意图；

图 5 为本发明实施例提供的三元对等鉴别系统的结构示意图。

具体实施方式

为了使本领域技术人员能够清楚理解本发明的技术方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整的描述。显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，均属于本发明保护的范围。

参见图 2，为本发明实施例提供的实体双向鉴别方法的示意图。

本发明实施例的方法涉及三个实体，两个鉴别实体 *A* 和 *B*，一个可信第三方 *TTP*（Trusted Third Party），可信第三方 *TTP* 为鉴别实体 *A* 和 *B* 的可信第三方。将这种通过可信第三方 *TTP* 实现两实体 *A*、*B* 之间对等鉴别的系统，称之为三元对等鉴别 TePA（Tri-element Peer Authentication）系统。$Valid_X$ 表示证书 $Cert_X$ 的有效性；$PublicKey_X$ 为实体 *X*（*X* 代表 *A* 或 *B*）的公钥；ID_X 为实体 *X* 的身份标识，由证书 $Cert_X$ 或者实体的区分符 *X* 表示；Pub_X 表示实体 *X* 的验证结果，由证书 $Cert_X$ 及其有效性 $Valid_X$ 组成或者由实体 *X* 及其公钥 $PublicKey_X$ 组成，*Token* 为权标字段，定义如下：

$TokenAB = sS_A(R_A||ID_A||Text1)$

$TokenTB = R_A||R_B||Pub_A||Pub_B||sS_{TP}(R_A||R_B||Pub_A||Pub_B||Text3)$

$TokenTB1 = R_B||Pub_A||Text5||sS_{TP}(R_B||Pub_A||Text5)$

$TokenTB2 = R_A||Pub_B||Text6||sS_{TP}(R_A||Pub_B||Text6)$

$TokenBA1 = sS_B(Text3||TokenTB||Text4||)$

$TokenBA2 = sS_B(TokenTB2||Text4)$

其具体流程如下：

步骤 S21、实体 *A* 发送消息 1 给实体 *B*，消息 1 包括时变参数 R_A、身份标识 ID_A、权标 *TokenAB*、可选项文本 *Text1*；

步骤 S22、实体 *B* 收到消息 1 后，向可信第三方 *TTP* 发送消息 2，消息 2 包括时变参数 R_A 和 R_B、身份标识 ID_A 和 ID_B 以及可选项文本 *Text2*；

步骤 S23、可信第三方 *TTP* 收到消息 2 后，检查实体 *A* 和实体 *B* 是否合法；

其中：若消息 2 中实体 *A* 和实体 *B* 的身份标识为证书，则检查实体 *A* 和实体 *B* 证书的有效性；若无效，则直接丢弃消息 2 或返回消息 3；若有效，返回消息 3；

若消息 2 中实体 *A* 和实体 *B* 的身份标识为区分符，则搜索并检查实体 *A* 和实体 *B* 相应的公钥及其有效性；若公钥未搜索到或无效，则直接丢弃消息 2 或返回消息 3；若公钥搜索到且有效，返回消息 3；

步骤 S24、可信第三方 *TTP* 检查完实体 *A* 和实体 *B* 的合法性后，向实体 *B* 返回消息 3，消息 3 包括权标 *TokenTB* 和可选项文本 *Text3* 或者包括权标 *TokenTB1* 和 *TokenTB2*；

步骤 S25、实体 *B* 收到消息 3 后，进行验证；

实体 B 进行验证的具体过程如图 3 所示，包括以下步骤：

步骤 S31、验证 *TokenTB* 或 *TokenTB1* 的可信第三方 *TTP* 的签名，如果验证成功，则进入步骤 S32；否则，结束流程；

步骤 S32、检查消息 2 中的时变参数 R_B 与 *TokenTB* 或 *TokenTB1* 中的时变参数 R_B 是否相符，相符则执行步骤 S32，否则结束流程；

步骤 S33、得到实体 *A* 的验证结果 Pub_A；若实体 *A* 合法有效，则执行步骤 S34，否则结束流程；

步骤 S34、获取实体 *A* 的公钥，验证消息 1 中的 *TokenAB* 的实体 *A* 的签名，如果签名正确，则确定验证通过。

需要说明的是，在其他实施例中，验证 *TokenTB* 或 *TokenTB1* 的可信第三方 *TTP* 的签名的操作，可以在检查消息 2 中的时变参数 R_B 与 *TokenTB* 或 *TokenTB1* 中的时变参数 R_B 是否相符的操作之后进行。

另外，还需要说明的是，步骤 S33 中，在实体 A 为不合法的情况下，也可以直接执行步骤 S26。

步骤 S26、实体 *B* 完成对消息 3 的验证后，向实体 *A* 发送消息 4，消息 4

包括权标 *TokenTB*、*TokenBA1*、可选项文本 *Text3* 和 *Text4* 或者包括权标 *TokenTB2*、*TokenBA2* 和可选项文本 *Text4*；需要说明的是，若消息 3 包括权标 *TokenTB* 和可选项文本 *Text3* 时，则消息 4 包括权标 *TokenTB*、*TokenBA1*、可选项文本 *Text3* 和 *Text4*；若消息 3 包括权标 *TokenTB1* 和 *TokenTB2*，则消息 4 包括权标 *TokenTB2*、*TokenBA2* 和可选项文本 *Text4*。

步骤 S27、实体 *A* 收到消息 4 后，进行验证；

实体 A 进行验证的具体过程如图 4 所示，包括以下步骤：

步骤 S41、验证 *TokenTB* 或 *TokenTB2* 的可信第三方 *TTP* 的签名，如果验证成功，则进入步骤 S42；否则，结束流程；

步骤 S42、检查消息 1 中的时变参数 R_A 与 *TokenTB* 或 *TokenTB2* 中的时变参数 R_A 是否相符，相符则执行步骤 S43，否则，结束流程；

步骤 S43、得到实体 *B* 的验证结果 Pub_B，若实体 *B* 合法有效，则执行步骤 S44，否则结束；

步骤 S44、获取实体 *B* 的公钥，验证 *TokenBA1* 或 *TokenBA2* 的实体 *B* 的签名，验证通过则完成鉴别。

需要说明的是，验证 *TokenTB* 或 *TokenTB2* 的可信第三方 *TTP* 的签名的操作，可以在检查消息 1 中的时变参数 R_A 与 *TokenTB* 或 *TokenTB2* 中的时变参数 R_A 是否相符的操作之后进行。

另外，还需说明的是，本发明中时变参数可为随机数、时间标记或顺序号。

针对上述方法，本发明实施例同时还提供了一种实现上述方法的系统，即三元对等鉴别 TePA（Tri-element Peer Authentication）系统，该系统的结构如图 5 所示，包括：第一实体 51、第二实体 52 和第三实体 53，其中：

第三实体 53 为第一实体 51 和第二实体 52 的可信第三方；

第一实体 51 用于：向第二实体发送携带时变参数 R_A、自身身份标识 ID_A 及权标 *TokenAB* 的第一消息；并在接收第二实体 52 发送的携带权标 *TokenTB* 和 *TokenBA1* 或者携带权标 *TokenTB2* 和 *TokenBA2* 的第四消息，对所述权标 *TokenTB* 或 *TokenTB2* 的第三实体 53 签名进行验证，并验证时变参数 R_A 与

TokenTB 或 *TokenTB2* 中的时变参数 R_A 是否相符，若均相符，则获取第二实体 52 的验证结果，当所述验证结果指示所述第二实体 52 合法有效时，获取第二实体 52 的公钥以验证所述第四消息中的权标 *TokenBA1* 或 *TokenBA2* 的第二实体 52 签名进行验证;

所述第二实体 52 用于：在接收到所述第一消息后，向所述第三实体 53 发送携带有时变参数 R_A 和 R_B、第一实体 51 身份标识 ID_A、自身身份标识 ID_B 的第二消息，并接收所述第三实体 53 返回的携带权标 *TokenTB* 或者携带权标 *TokenTB1* 和 *TokenTB2* 的第三消息，对所述权标 *TokenTB* 或 *TokenTB1* 的第三实体 53 签名进行验证，并验证时变参数 R_B 与 *TokenTB* 或 *TokenTB1* 中的时变参数 R_B 是否相符，若均相符，则获取第一实体 51 的验证结果，当所述验证结果指示所述第一实体 51 合法有效时，获取第一实体 51 的公钥以验证所述第一消息中的 *TokenAB* 的第一实体 51 的签名，并在验证通过时发送所述第四消息;

所述第三实体 53 用于：接收所述第二消息，当完成所述第一实体 51 和第二实体 52 的合法性验证时，向所述第二实体 52 返回所述第三消息。

本实施例中，各实体之间的信息交互具体过程如有不详尽之处，请参照前文方法部分的描述。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求

1、一种实体双向鉴别方法，其特征在于，包括:

第一实体发送携带有时变参数 R_A、身份标识 ID_A 和签名的第一消息;

第二实体收到所述第一消息后，向可信第三方发送携带有时变参数 R_A 和 R_B、所述第一实体的身份标识 ID_A 和本身的身份标识 ID_B 的第二消息;

所述可信第三方收到所述第二消息后，向所述第二实体返回携带自身签名及时变参数 R_A 和时变参数 R_B 的第三消息;

所述第二实体收到所述第三消息后，在可信第三方签名验证通过且时变参数 R_B 与本地存储的时变参数 R_B 相符时，获取第一实体的验证结果，当验证结果指示所述第一实体合法有效时，获取所述第一实体的公钥以验证所述第一消息中所述第一实体的签名，在验证通过时，发送携带所述可信第三方签名、第二实体签名和时变参数 R_A 的第四消息;

所述第一实体收到所述第四消息后，在可信第三方签名验证通过且时变参数 R_A 与本地存储的时变参数 R_A 相符时，获取第二实体的验证结果，当验证结果指示所述第二实体合法有效时，获取所述第二实体的公钥以验证所述第四消息中所述第二实体的签名，完成鉴别过程。

2、根据权利要求 1 所述的实体双向鉴别方法，其特征在于，所述第三消息是在完成所述第一实体和第二实体的合法性验证时发送的。

3、根据权利要求 2 所述的实体双向鉴别方法，其特征在于，所述第一实体和第二实体合法的条件为: 所述第二消息中的所述第一实体和第二实体的身份标识为证书，且所述证书有效。

4、根据权利要求 2 所述的实体双向鉴别方法，其特征在于，所述第一实体和第二实体合法的条件为: 所述第二消息中的所述第一实体和第二实体的身份标识为区分符，且所述第一实体和第二实体的公钥存在并有效。

5、根据权利要求 1 所述的实体双向鉴别方法，其特征在于，所述时变参数可为随机数、时间标记或顺序号。

6、一种三元对等鉴别系统，其特征在于，包括: 第一实体、第二实体和

作为可信第三方的第三实体，其中：

第一实体用于：向所述第二实体发送携带时变参数 R_A、自身身份标识 ID_A 及签名的第一消息；在接收所述第二实体发送的携带第三实体签名、第二实体签名和时变参数 R_A 的第四消息后，在第三实体签名验证通过且时变参数 R_A 与本地存储的时变参数 R_A 相符时，获取第二实体的验证结果，并当该验证结果指示第二实体合法时，获取所述第二实体的公钥，以对所述第四消息中的第二实体的签名进行验证；

所述第二实体用于：在接收到所述第一消息后，向所述第三实体发送携带有时变参数 R_A 和 R_B、第一实体身份标识 ID_A、自身身份标识 ID_B 的第二消息，在接收所述第三实体返回的携带所述第三实体签名及时变函数 R_A 和时变参数 R_B 的第三消息后，在所述的第三实体签名验证通过且所述第三消息中的时变参数 R_B 与本地存储的时变参数 R_B 相符时，获取第一实体的验证结果，并当所述验证结果指示所述第一实体合法有效时，获取所述第一实体的公钥以验证所述第一消息中所述第一实体的签名，在验证通过时发送所述第四消息；

所述第三实体用于：接收所述第二消息，向所述第二实体返回所述第三消息。

7、根据权利要求 6 所述的系统，其特征在于，所述第三消息是在完成所述第一实体和第二实体的合法性验证时发送的。

8、根据权利要求 7 所述的系统，其特征在于，所述第一实体和第二实体合法的条件为：所述第二消息中的所述第一实体和第二实体的身份标识为证书，且所述证书有效。

9、根据权利要求 7 所述的系统，其特征在于，所述第一实体和第二实体合法的条件为：所述第二消息中的所述第一实体和第二实体的身份标识为区分符，且所述第一实体和第二实体的公钥存在并有效。

10、根据权利要求 6 所述的系统，其特征在于，所述时变参数可为随机数、时间标记或顺序号。


实体A
实体B
步骤S11、随机数RB、Text1
步骤S12、权标TokenAB、可选项证书CertA
步骤S13、确保拥有实体A的有效公开密钥
步骤S14、完成对实体A的验证
步骤S15、权标TokenAB、可选项证书CertB
步骤S16、确保拥有实体B的有效公开密钥
步骤S17、完成对实体B的验证

图 1

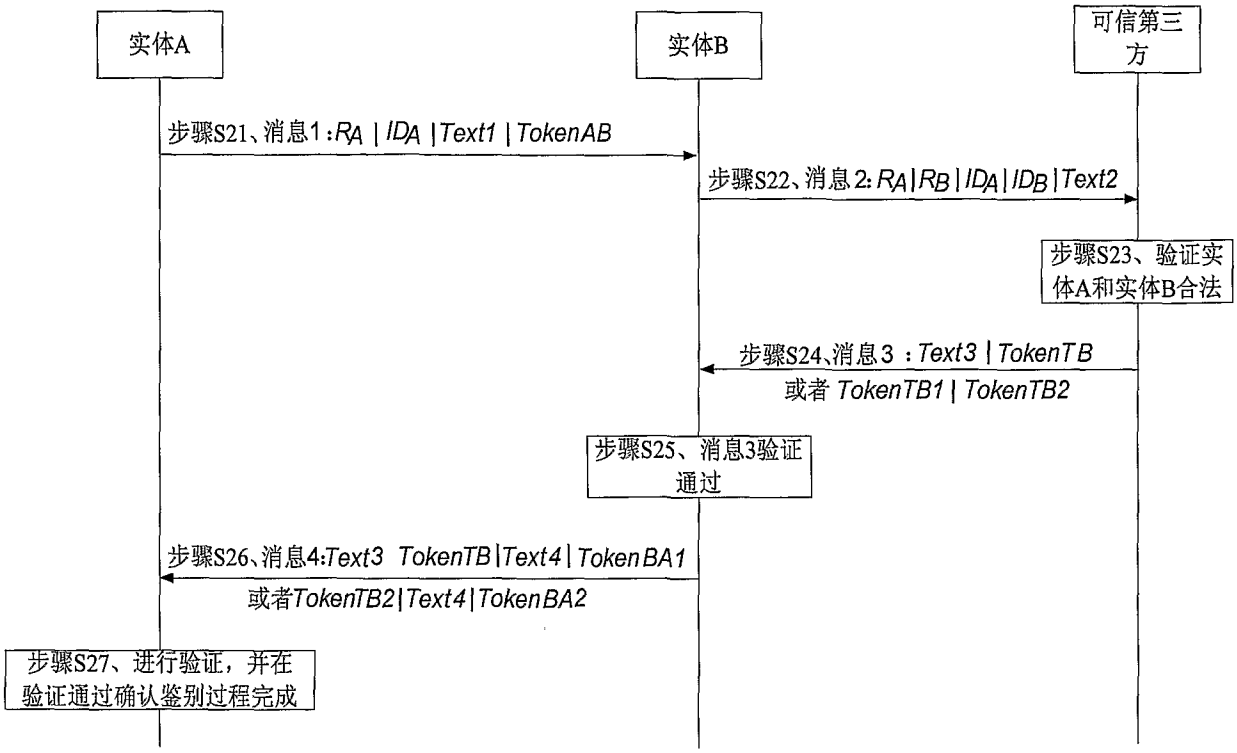
实体A
实体B
可信第三方
步骤S21、消息1：R_A | ID_A | Text1 | TokenAB
步骤S22、消息2: R_A | R_B | ID_A | ID_B | Text2
步骤S23、验证实体A和实体B合法
步骤S24、消息3 ：Text3 | TokenTB
或者 TokenTB1 | TokenTB2
步骤S25、消息3验证通过
步骤S26、消息4:Text3 TokenTB | Text4 | TokenBA1
或者TokenTB2 | Text4 | TokenBA2
步骤S27、进行验证，并在验证通过确认鉴别过程完成

图 2

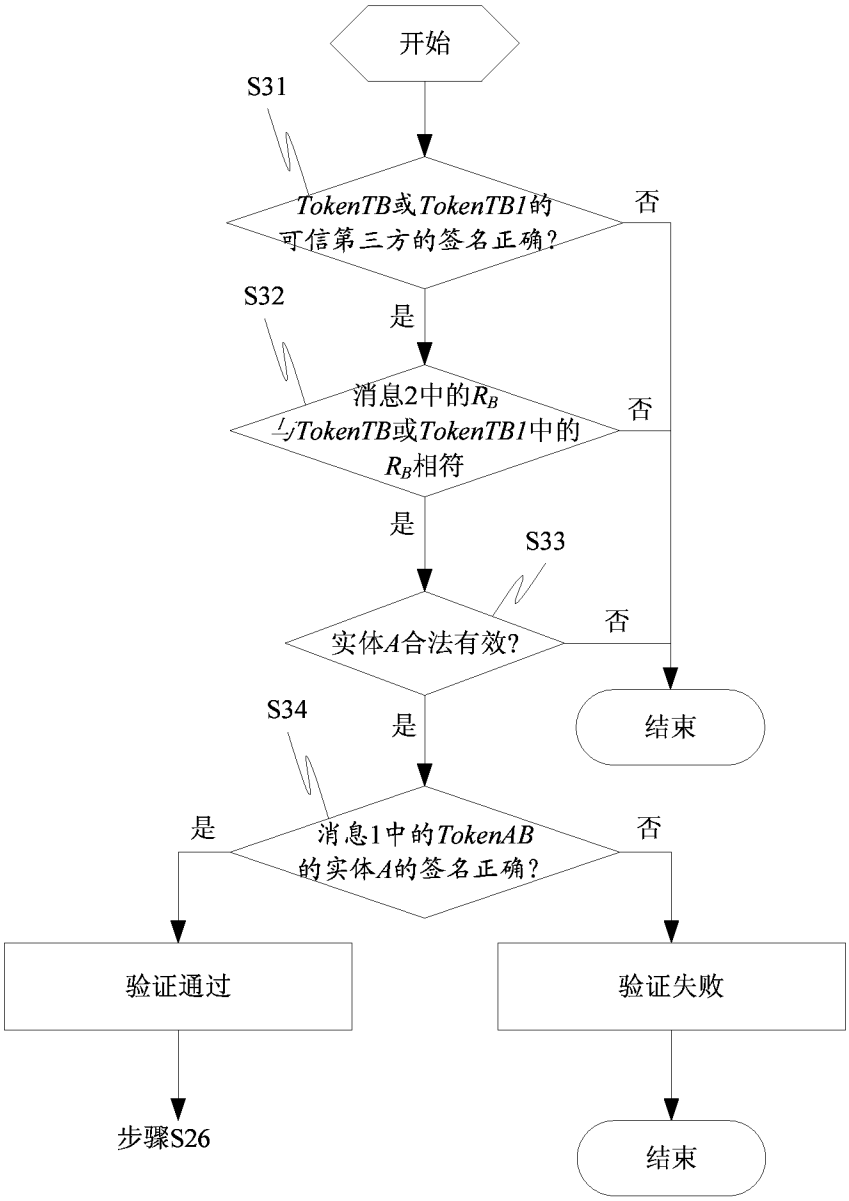
开始
S31
TokenTB或TokenTB1的可信第三方的签名正确?
否
是
S32
消息2中的R_B与TokenTB或TokenTB1中的R_B相符
否
是
S33
实体A合法有效?
否
是
S34
消息1中的TokenAB的实体A的签名正确?
是
否
验证通过
验证失败
步骤S26
结束
结束

图 3

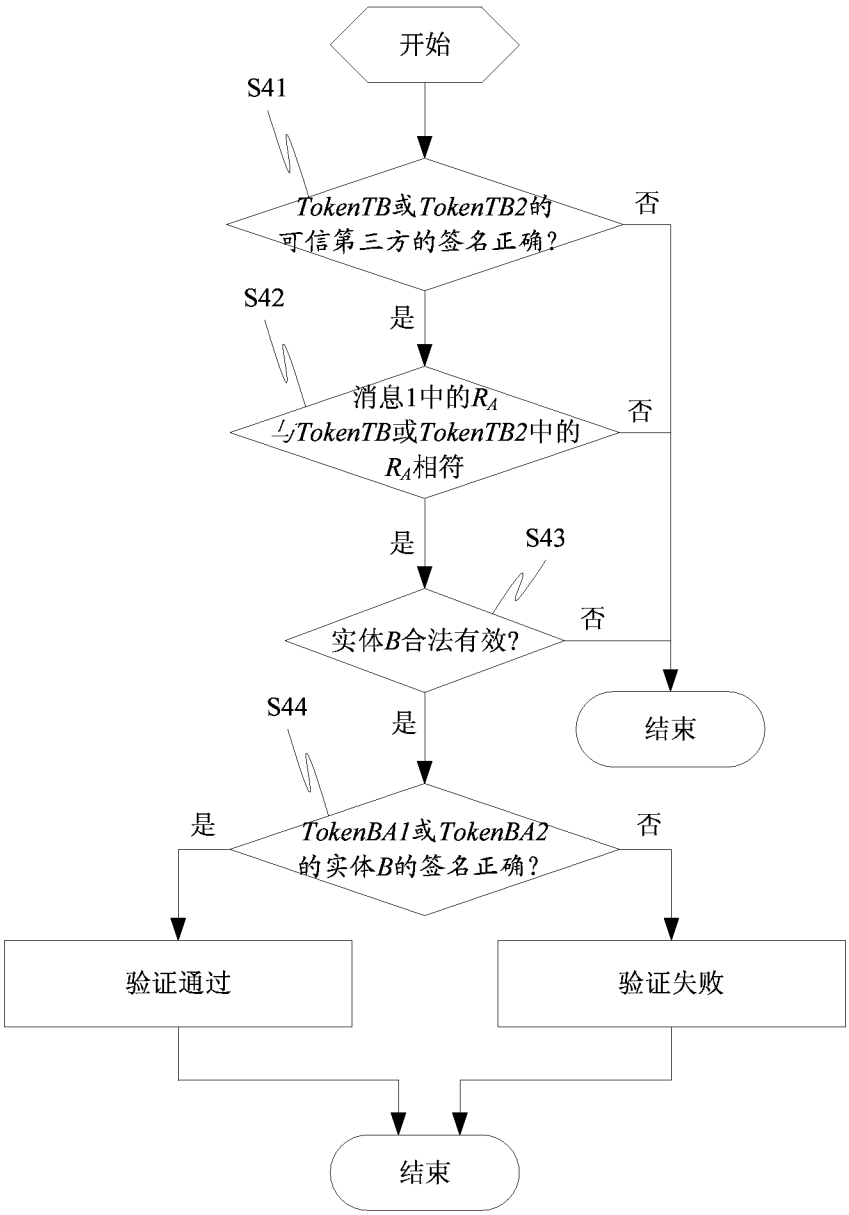
开始
S41
TokenTB或TokenTB2的可信第三方的签名正确?
否
是
S42
消息1中的R_A与TokenTB或TokenTB2中的R_A相符
否
是
S43
实体B合法有效?
否
是
结束
S44
TokenBA1或TokenBA2的实体B的签名正确?
是
否
验证通过
验证失败
结束

图 4

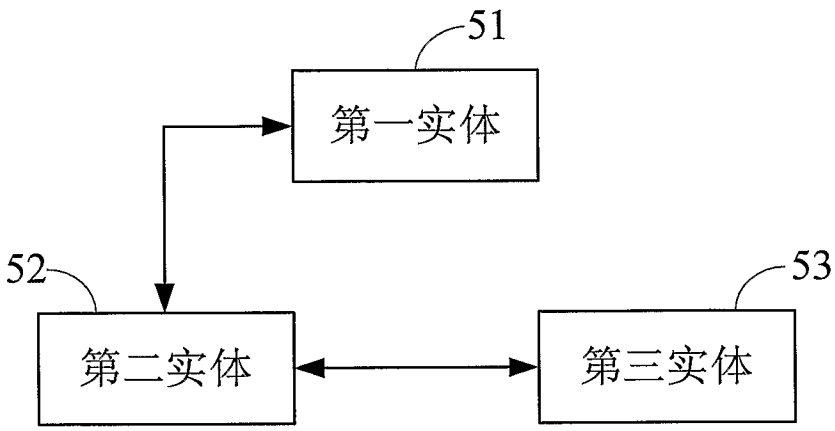

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2008/073389

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) 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: H04L 9/-; H04L 29/-

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)

CPRS, CNKI, WPI, EPODOC, PAJ: two w way, bi, dual, both, directional, direction, authenticat+, distinguish+, identity, identify+, legal, validity, third, three, tri, trusted, credible, creditable, believable, bilievable

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN101222328 A (XIAN XIDIAN JIETONG WIRELESS NETWORK COM) 16 Jul.2008 (16.07.2008) the whole document	1-10
PX	CN101247223 A (SIAN XIDIANJIETONG WIRELESS NETWORK COMMUNICATION CO LTD) 20 Aug.2008 (20.08.2008) the whole document	1-10
A	CN1345498 A (NOKIA NETWORKS OY) 17 Apr. 2002 (17.04.2002) the whole document	1-10
A	US2003041240 A1 (AMERICA ONLINE INC et al.) 27 Feb.2003 (27.02.2003) the whole document	1-10
A	US2007245414 A1 (MICROSOFT CORP) 18 Oct.2007 (18.10.2007) the whole document	1-10

☐ 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
06 Mar. 2009 (06.03.2009)	**19 Mar. 2009 (19.03.2009)**
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 SHAO Yuanyuan Telephone No. (86-10)62411433

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2008/073389

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101222328 A	16.07.2008	None	
CN101247223 A	20.08.2008	None	
CN1345498 A	17.04.2002	WO0048358 A1	17.08.2000
		AU2803800 A	29.08.2000
		EP1151578 A1	07.11.2001
		US2002164026 A1	07.11.2002
		JP2002541685 T	03.12.2002
		CA2362905 C	12.12.2006
US2003041240 A1	27.02.2003	WO03019378 A1	06.03.2003
		AU2002319692 A1	10.03.2003
US2007245414 A1	18.10.2007	None	

国际检索报告

国际申请号
PCT/CN2008/073389

A. 主题的分类

H04L 9/32 (2006.01) 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: H04L 9/-; H04L 29/-

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）)

CPRS,CNKI: 双向,鉴别,鉴权,区别,辨别,证书,验证,公钥,密钥,身份标识,合法,检查,三元,三,第三,可信,信任

WPI, EPODOC, PAJ: two w way, bi, dual, both, directional, direction, authenticat+, distinguish+, identity, identify+, legal, validity, third, three, tri, trusted, credible, creditable, believable, bilievable

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
PX	CN101222328 A (西安西电捷通无线网络通信有限公司) 16.7 月 2008 (16.07.2008) 全文	1-10
PX	CN101247223 A (西安西电捷通无线网络通信有限公司) 20.8 月 2008 (20.08.2008) 全文	1-10
A	CN1345498 A (诺基亚网络有限公司) 17.4 月 2002 (17.04.2002) 全文	1-10
A	US2003041240 A1 (AMERICA ONLINE INC 等) 27.2 月 2003 (27.02.2003) 全文	1-10
A	US2007245414 A1 (MICROSOFT CORP) 18.10 月 2007 (18.10.2007) 全文	1-10

☐ 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	国际检索报告邮寄日期
06.3 月 2009 (06.03.2009)	**19.3 月 2009 (19.03.2009)**

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	受权官员 **邵源渊** 电话号码：(86-10) **62411433**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2008/073389

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101222328 A	16.07.2008	无	
CN101247223 A	20.08.2008	无	
CN1345498 A	17.04.2002	WO0048358 A1	17.08.2000
		AU2803800 A	29.08.2000
		EP1151578 A1	07.11.2001
		US2002164026 A1	07.11.2002
		JP2002541685 T	03.12.2002
		CA2362905 C	12.12.2006
US2003041240 A1	27.02.2003	WO03019378 A1	06.03.2003
		AU2002319692 A1	10.03.2003
US2007245414 A1	18.10.2007	无	