(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103312499 B
(45)授权公告日 2018.07.03

(21)申请号 201210063650.1

(22)申请日 2012.03.12

(65)同一申请的已公布的文献号
申请公布号 CN 103312499 A

(43)申请公布日 2013.09.18

(73)专利权人 西安西电捷通无线网络通信股份有限公司
地址 710075 陕西省西安市高新区科技二路68号西安软件园秦风阁A201

(72)发明人 杜志强 曹军 铁满霞 李毅

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

审查员 解淑瑄

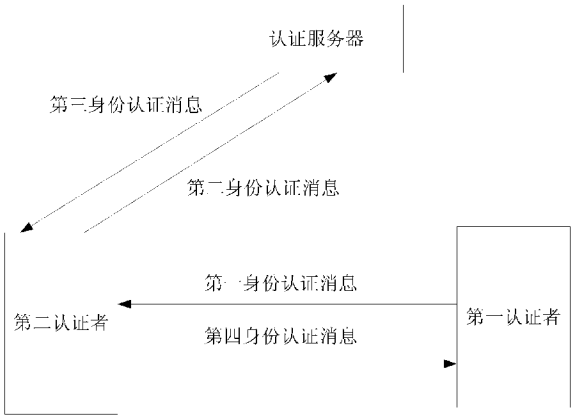
权利要求书6页 说明书10页 附图1页

(54)发明名称

一种身份认证方法及系统

(57)摘要

本发明提供的一种身份认证方法及其系统，属于身份认证领域，解决了现有的身份认证技术无法保护个人隐私，且包含个人隐私的认证技术又必须提供可跟踪能力的技术问题。该身份认证方法主要包括第一认证者向第二认证者发送第一身份认证消息，第二认证者向认证服务器发送第二身份认证消息，认证服务器根据第二身份认证消息验证第二认证者所处安全域的合法性，认证服务器向第二认证者返回第三身份认证消息，第二认证者收到第三身份认证消息后，向第一认证者发送第四身份认证消息，第一认证者对第四身份认证消息进行验证。该认证系统主要包括第一认证者、第二认证者、第二认证者所处的安全域一级认证服务器。



CN 103312499 B

1.一种身份认证方法,其特征在于,所述方法包括以下步骤:

1)第一认证者向第二认证者发送第一身份认证消息,所述第一身份认证消息中还包括第一认证者的标识;2)第二认证者向认证服务器发送第二身份认证消息,第二身份认证消息中包括第二认证者所处安全域的标识,所述第二身份认证消息中还包括第一认证者的标识;

3)认证服务器收到第二身份认证消息后,根据第二身份认证消息验证第二认证者所处安全域的合法性,产生对第二认证者所处安全域的验证结果;所述认证服务器还根据第二身份认证消息验证第一认证者的合法性而产生对第一认证者的验证结果;

4)认证服务器向第二认证者返回第三身份认证消息,第三身份认证消息中包括第二认证者所处安全域的验证结果以及认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息;所述第三身份认证消息中还包括第一认证者的验证结果以及认证服务器对包含第一认证者的验证结果在内信息的身份认证信息;或者,第三身份认证消息中还包括第一认证者的验证结果,且第三身份认证消息中的认证服务器的身份认证信息中进一步包含第一认证者的验证结果;

5)第二认证者收到第三身份认证消息后,向第一认证者发送第四身份认证消息,第四身份认证消息中包括第二认证者所处安全域的标识、第二认证者所处安全域的验证结果、认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息以及第二认证者对包含第一认证者的标识符在内信息的身份认证信息;

6)第一认证者收到第四身份认证消息后,对第四身份认证消息进行验证并根据验证情况确定第二认证者身份的合法性;

7)第一认证者向第二认证者发送第五身份认证消息,第五身份认证消息中包括第一认证者对包含第二认证者标识符在内信息的身份认证信息;

8)第二认证者收到第五身份认证消息后,验证第一认证者身份的合法性。

2.如权利要求1所述的身份认证方法,其特征在于:所述步骤3)中,认证服务器根据第二身份认证消息验证第二认证者所处安全域的合法性的具体步骤包括:

若第二身份认证消息中的第二认证者所处安全域的标识为第二认证者所处安全域的标识符,则认证服务器查找第二认证者所处安全域的公开认证信息,若查找到,则确定第二认证者所处安全域合法,否则,确定第二认证者所处安全域非法;或者

若第二身份认证消息中的第二认证者所处安全域的标识为第二认证者所处安全域的身份证明信息,则认证服务器检查其身份证明信息的有效性,若有效,则确定第二认证者所处安全域合法,否则,确定第二认证者所处安全域非法。

3.如权利要求1所述的身份认证方法,其特征在于:所述步骤6)中,第一认证者对第四身份认证消息进行验证并根据验证情况确定第二认证者的合法性,其具体实现方式包括如下步骤:

6.1)第一认证者验证认证服务器的身份认证信息是否有效,若是,则执行步骤6.2),否则,确定第二认证者非法;

6.2)第一认证者若根据第二认证者所处安全域的验证结果判断第二认证者所处安全域合法有效,则执行步骤6.3),否则,确定第二认证者非法;

6.3)第一认证者获取第二认证者所处安全域的公开认证信息,根据该公开认证信息验

证第二认证者的身份认证信息是否有效、并检查第一认证者的标识符与包含在第二认证者的身份认证信息中的第一认证者的标识符是否一致，若全部为是，则确定第二认证者合法，否则，确定第二认证者非法。

4.如权利要求1所述的身份认证方法，其特征在于：

所述步骤1)中的第一身份认证消息中进一步包括第一时变参数，第一时变参数由第一认证者产生；

所述步骤2)中的第二身份认证消息中进一步包括第一时变参数；

所述步骤4)中的第三身份认证消息的认证服务器的身份认证信息中，进一步包含第一时变参数；

所述步骤5)中的第四身份认证消息的第二认证者的身份认证信息中，进一步包含第一时变参数；

所述步骤6)中，第一认证者对第四身份认证消息进行验证并根据验证情况确定第二认证者的合法性，其具体实现方式包括如下步骤：

6.1)第一认证者验证认证服务器的身份认证信息是否有效，并验证第一身份认证消息中第一认证者产生的第一时变参数与包含在认证服务器的身份认证信息中的第一时变参数是否相符，若均为是，则执行步骤6.2)，否则，确定第二认证者非法；

6.2)第一认证者若根据第二认证者所处安全域的验证结果判断第二认证者所处安全域合法有效，则执行步骤6.3)，否则，确定第二认证者非法；

6.3)第一认证者获取第二认证者所处安全域的公开认证信息，根据该公开认证信息验证第二认证者的身份认证信息是否有效、并检查第一认证者的标识符与包含在第二认证者的身份认证信息中的第一认证者的标识符是否一致、并检查第一身份认证消息中第一认证者产生的第一时变参数与包含在第二认证者的身份认证信息中的第一时变参数是否一致，若全部为是，则确定第二认证者合法，否则，确定第二认证者非法。

5.如权利要求1所述的身份认证方法，其特征在于：所述步骤3)中，认证服务器还根据第二身份认证消息验证第一认证者的合法性，具体步骤包括：

若第二身份认证消息中的第一认证者的标识为第一认证者的标识符，则认证服务器查找第一认证者的公开认证信息，若查找到，则确定第一认证者合法，否则，确定第一认证者非法；或者

若第二身份认证消息中的第一认证者的标识为第一认证者的身份证明信息，则认证服务器检查其身份证明信息的有效性，若有效，则确定第一认证者合法，否则，确定第一认证者非法。

6.如权利要求1所述的身份认证方法，其特征在于：所述步骤8)中，第二认证者验证第一认证者的合法性的具体步骤包括：

8.1)第二认证者验证认证服务器对包含第一认证者的验证结果在内信息的身份认证信息是否有效，若是，则执行8.2)，否则，确定第一认证者非法；

8.2)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行8.3)，否则，确定第一认证者非法；

8.3)第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者

的身份认证信息中的第二认证者所处安全域的标识符是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

7.如权利要求1所述的身份认证方法，其特征在于：

在所述步骤5)中，在第二认证者向第一认证者发送第四身份认证消息之前，第二认证者验证认证服务器对包含第一认证者的验证结果在内信息的身份认证信息是否有效；并在验证认证服务器对包含第一认证者的验证结果在内信息的身份认证信息有效时，向第一认证者发送第四身份认证消息；

所述步骤8)中，第二认证者验证第一认证者的合法性的具体步骤包括：

8.1)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行步骤8.2)，否则，确定第一认证者非法；

8.2)第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

8.如权利要求1所述的身份认证方法，其特征在于：

在所述步骤2)中，第二身份认证消息中可进一步包含第二时变参数，第二时变参数由第二认证者产生；

在所述步骤3)中，第三身份认证消息的认证服务器对包含第一认证者的验证结果在内信息的身份认证信息中，进一步包含第二时变参数；

所述步骤8)中，第二认证者验证第一认证者的合法性的具体步骤包括：

8.1)第二认证者验证认证服务器对包含第一认证者的验证结果的身份认证信息是否有效，并检查第二认证消息中第二认证者产生的第二时变参数与包含在认证服务器对包含第二时变参数在内信息的身份认证信息中的第二时变参数是否相符，若相符则执行8.2)，否则，确定第一认证者非法；

8.2)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行8.3)，否则，确定第一认证者非法；

8.3)第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效、检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致、并检查第五身份认证消息中第二认证者产生的第二时变参数与包含在第二认证者的身份认证信息中的第二时变参数是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

9.如权利要求1所述的身份认证方法，其特征在于：

在所述步骤2)中，第二身份认证消息中可进一步包含第二时变参数，第二时变参数由第二认证者产生；

在所述步骤3)中，第三身份认证消息的认证服务器对包含第一认证者的验证结果在内信息的身份认证信息中，进一步包含第二时变参数；

在所述步骤5)中，在第二认证者向第一认证者发送第四身份认证消息之前，第二认证者首先验证认证服务器对包含第一认证者的验证结果的身份认证信息是否有效、检查第二身份认证消息中第二认证者产生的第二时变参数与包含在验证认证服务器对包含第一认

证者的验证结果的身份认证消息中的第一时变参数是否相符，若均为是，向第一认证者发送第四身份认证消息；

所述步骤8）中，第二认证者验证第一认证者的合法性的具体步骤包括：

8.1）第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行步骤8.2），否则，确定第一认证者非法；

8.2）第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致、并检查第五身份认证消息中第二认证者产生的第二时变参数与包含在第二认证者的身份认证信息中的第二时变参数是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

10.如权利要求1或2或3或4所述的身份认证方法，其特征在于：所述身份认证方法还包括：

步骤0）第二认证者发送第零身份认证消息给第一认证者，第零身份认证消息中包括第二认证者所处安全域的标识；

所述步骤1）中的第一身份认证消息中还包括第一认证者的标识；

所述步骤2）中的第二身份认证消息中还包括第一认证者的标识；

所述步骤3）中，认证服务器还根据第二身份认证消息验证第一认证者的合法性而产生对第一认证者的验证结果；

在所述步骤4）中，第三身份认证消息中还包括第一认证者的验证结果以及认证服务器对包含第一认证者的验证结果在内信息的身份认证信息；或者，第三身份认证消息中还包括第一认证者的验证结果，且第三身份认证消息中的认证服务器的身份认证信息中进一步包含第一认证者的验证结果；

在所述步骤5）中，去除第四身份认证消息中的第二认证者所处安全域的标识；并且在第二认证者发送第四身份认证消息之前，对第三身份认证消息进行验证并根据验证情况确定第一认证者的合法性。

11.如权利要求10所述的身份认证方法，其特征在于：所述步骤3）中，认证服务器还根据第二身份认证消息验证第一认证者的合法性，具体步骤包括：

若第二身份认证消息中的第一认证者的标识为第一认证者的标识符，则认证服务器查找第一认证者的公开认证信息，若查找到，则确定第一认证者合法，否则，确定第一认证者非法；或者

若第二身份认证消息中的第一认证者的标识为第一认证者的身份证明信息，则认证服务器检查其身份证明信息的有效性，若有效，则确定第一认证者合法，否则，确定第一认证者非法。

12.如权利要求10所述的身份认证方法，其特征在于：所述步骤5）中，第二认证者对第三身份认证消息进行验证并根据验证情况确定第一认证者的合法性的具体步骤包括：

5.1）第二认证者验证认证服务器对包含第一认证者的验证结果在内信息的身份认证信息是否有效，若是，则执行5.2），否则，确定第一认证者非法；

5.2）第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行5.3），否则，确定第一认证者非法；

5.3)第二认证者获取第一认证者的公开认证信息,根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致,若均为是,则确定第一认证者合法,否则,确定第一认证者非法。

13.如权利要求10所述的身份认证方法,其特征在于:

在所述步骤0)中,第零身份认证消息中可进一步包括第三时变参数,第三时变参数由第二认证者产生;

在所述步骤1)中,第一身份认证消息还包括第三时变参数,第一认证者的身份认证信息中进一步包括第三时变参数;

所述步骤5)中,第二认证者对第三身份认证消息进行验证并根据验证结果确定第一认证者的合法性的具体步骤包括:

5.1)第二认证者验证认证服务器对包含第一认证者的验证结果在内信息的身份认证信息是否有效,若是,则执行5.2),否则,确定第一认证者非法;

5.2)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效,则执行5.3),否则,确定第一认证者非法;

5.3)第二认证者获取第一认证者的公开认证信息,根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致,校验第零身份认证消息中第二认证者产生的第三时变参数与包含在第一认证者的身份认证消息中的第三时变参数是否一致,若均为是,则确定第一认证者合法,否则,确定第一认证者非法。

14.一种身份认证系统,其特征在于,所述系统包括:第一认证者、第二认证者、第二认证者所处的安全域、认证服务器;在第一认证者与第二认证者之间的身份认证过程中,第一认证者仅与第二认证者进行信息交互,认证服务器仅与第二认证者交互信息;具体是:

第一认证者向第二认证者发送第一身份认证消息,所述第一身份认证消息中还包括第一认证者的标识;

第二认证者向认证服务器发送第二身份认证消息,第二身份认证消息中包括第二认证者所处安全域的标识,所述第二身份认证消息中还包括第一认证者的标识;

认证服务器收到第二身份认证消息后,根据第二身份认证消息验证第二认证者所处安全域的合法性,产生对第二认证者所处安全域的验证结果;所述认证服务器还根据第二身份认证消息验证第一认证者的合法性而产生对第一认证者的验证结果;

认证服务器向第二认证者返回第三身份认证消息,第三身份认证消息中包括第二认证者所处安全域的验证结果以及认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息;所述第三身份认证消息中还包括第一认证者的验证结果以及认证服务器对包含第一认证者的验证结果在内信息的身份认证信息;或者,第三身份认证消息中还包括第一认证者的验证结果,且第三身份认证消息中的认证服务器的身份认证信息中进一步包含第一认证者的验证结果;

第二认证者收到第三身份认证消息后,向第一认证者发送第四身份认证消息,第四身份认证消息中包括第二认证者所处安全域的标识、第二认证者所处安全域的验证结果、认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息以及第二认

证者对包含第一认证者的标识符在内信息的身份认证信息；

第一认证者收到第四身份认证消息后，对第四身份认证消息进行验证并根据验证情况确定第二认证者身份的合法性；

第一认证者还向第二认证者发送第五身份认证消息，第五身份认证消息中包括第一认证者对包含第二认证者标识符在内信息的身份认证信息；

第二认证者收到第五身份认证消息后，验证第一认证者身份的合法性。

一种身份认证方法及系统

技术领域

[0001] 本发明涉及身份认证领域，尤其是一种身份认证方法及系统。

背景技术

[0002] 当今社会，人们越来越重视对自身隐私的保护，在很多要验证居民身份的场合，人们并不希望在自己身份合法性被验证的同时又将自己的身份信息公开给对方，从而充分保护自己的隐私。例如，在对一些敏感事件进行表决时，表决人既希望以合法的身份完成表决，又不希望暴露自己的身份；在一些消费场合，消费者在进行支付时并不希望商户知道自己的个人信息；网络用户在以可管控的身份登录网络后，在很多时候并不希望自己的身份信息暴露给公众。目前，这类隐私保护的需求越来越明显。

[0003] 提供身份认证服务的技术有多种，目前通常采用的是基于公钥密码技术的身份认证方法，这种方法通过数字签名完成对被认证者身份合法性的验证，同时被认证者的身份信息也将公开给认证者，很明显这类技术在为上述应用场合提供认证服务时有明显的局限性，因为它无法保护用户的隐私。另一方面，提供隐私保护的身份认证技术，又必须提供可追踪能力，便于管理者在必要时的管控。

发明内容

[0004] 本发明为解决背景技术中存在的目前的身份认证技术无法保护个人隐私，且包含个人隐私的认证技术又必须提供可跟踪能力的问题，提出一种身份认证方法及系统。

[0005] 本发明的技术解决方案是：

[0006] 一种身份认证方法，包括以下步骤：

[0007] 1)第一认证者向第二认证者发送第一身份认证消息；

[0008] 2)第二认证者向认证服务器发送第二身份认证消息，第二身份认证消息中包括第二认证者所处安全域的标识；

[0009] 3)认证服务器收到第二身份认证消息后，根据第二身份认证消息验证第二认证者所处安全域的合法性，产生对第二认证者所处安全域的验证结果；

[0010] 4)认证服务器向第二认证者返回第三身份认证消息，第三身份认证消息中包括第二认证者所处安全域的验证结果以及认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息；

[0011] 5)第二认证者收到第三身份认证消息后，向第一认证者发送第四身份认证消息，第四身份认证消息中包括第二认证者所处安全域的标识、第二认证者所处安全域的验证结果、认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息以及第二认证者对包含第一认证者的标识符在内信息的身份认证信息；

[0012] 6)第一认证者收到第四身份认证消息后，对第四身份认证消息进行验证并根据验证情况确定第二认证者身份的合法性。

[0013] 本发明还提供一种身份认证系统，其特殊之处在于，所述系统包括：第一认证者、

第二认证者、第二认证者所处的安全域、认证服务器；在第一认证者与第二认证者之间的身份认证过程中，第一认证者仅与第二认证者进行信息交互，认证服务器仅与第二认证者交互信息。

[0014] 本发明的有益效果在于：

[0015] 在认证过程中使得第二认证者在匿名的情况下完成认证活动，在第二认证者被认证的同时也保护了第二认证者的隐私。

附图说明

[0016] 图1为本发明的示意图。

具体实施方式

[0017] 本发明的系统包括第一认证者、第二认证者、第二认证者所处的安全域、认证服务器。所述第一认证者和第二认证者可互为认证者与被认证者；所述第一认证者具有自己的公开认证信息和私有认证信息，私有认证信息用来产生供其他认证者认证第一认证者的身份认证信息，公开认证信息对外公开用于其他认证者验证第一认证者的身份认证信息，第一认证者具有标识，该标识可以是第一认证者的标识符，也可以是第一认证者的身份证明信息；所述安全域是一种带有边界性质且边界内实体共享某一公开认证信息的逻辑划分，安全域内的实体各自具有自己的私有认证信息，用来生成供其他认证者认证该实体的身份认证信息，安全域的公开认证信息对外公开便于其他认证者验证该实体的身份认证信息，安全域具有标识，该标识可以是安全域的标识符，也可以是安全域的身份证明信息；所述认证服务器用来为认证者提供来自可信第三方的认证服务，帮助认证者完成对被认证者的身份认证，认证服务器具有私有认证信息以及相应的公开认证信息，公开认证信息用于公开给其他实体，用于验证认证服务器利用私有认证信息产生的身份认证信息。在本发明系统实现第一认证者与第二认证者之间的身份认证过程中，第一认证者仅与第二认证者进行信息交互(信息交互具体内容参照本发明提供的身份认证方法)，认证服务器仅与第二认证者交互信息(信息交互具体内容参照本发明提供的身份认证方法)。

[0018] 本发明身份认证方法，包括以下步骤：

[0019] 步骤一、第一认证者向第二认证者发送第一身份认证消息；

[0020] 步骤二、第二认证者向认证服务器发送第二身份认证消息，消息中包括第二认证者所处安全域的标识；

[0021] 步骤三、认证服务器收到第二身份认证消息后，根据第二认证者所处安全域的标识认证第二认证者所处安全域的合法性；

[0022] 步骤四、认证服务器向第二认证者返回第三身份认证消息，消息中包括对第二认证者所处安全域的验证结果以及认证服务器对包含第二认证者所处安全域的验证结果在内信息的身份认证信息；

[0023] 步骤五、第二认证者收到第三身份认证消息后，向第一认证者发送第四身份认证消息，消息中包括第二认证者所处安全域的标识、认证服务器对第二认证者所处安全域的验证结果、认证服务器对包括第二认证者所处安全域的验证结果在内信息的身份认证信息以及第二认证者对包含第一认证者的标识符在内信息的身份认证信息；

[0024] 步骤六、第一认证者收到第四身份认证消息后，对该消息进行验证，并根据验证情况确定第二认证者身份的合法性。

[0025] 在一种实施方式中，第一身份认证消息中可进一步包含第一时变参数，第一时变参数由第一认证者产生，第一时变参数可以是时间标记、顺序号或随机数；在第二身份认证消息中，可进一步包含第一时变参数；在第三身份认证消息的认证服务器的身份认证信息中，可进一步包含第一时变参数；在第四身份认证消息的第二认证者的身份认证信息中，可进一步包含第一时变参数。

[0026] 具体地，

[0027] 上述步骤三中，认证服务器检查第二认证者所处安全域的合法性可采用如下方法：

[0028] 如果第二身份认证消息中第二认证者所处安全域的标识为第二认证者所处安全域的标识符，则认证服务器查找第二认证者所处安全域的有效公开认证信息；或者，如果第二认证者所处安全域的标识为第二认证者所处安全域的身份证明信息，则认证服务器检查第二认证者所处安全域的身份证明信息的有效性。

[0029] 上述步骤五中，第一认证者对第四身份认证消息进行验证并根据验证情况确定第二认证者的合法性，其具体实现方式可以包括如下步骤：

[0030] 1)第一认证者验证认证服务器的身份认证信息是否有效，并在认证服务器的身份认证信息中包含第一时变参数时验证第一身份认证消息中第一认证者产生的第一时变参数与包含在认证服务器的身份认证信息中的第一时变参数是否相符，若均为是，则执行步骤2)；否则，确定第二认证者非法；

[0031] 2)第一认证者若根据认证服务器对第二认证者所处安全域的验证结果判断第二认证者所处安全域合法有效，则执行步骤3)，否则，确定第二认证者非法；

[0032] 3)第一认证者获取第二认证者所处安全域的公开认证信息，根据该公开认证信息验证第二认证者的身份认证信息是否有效、并检查第一认证者的标识符与包含在第二认证者的身份认证信息中的第一认证者的标识符是否一致、并在第二认证者的身份认证信息中包含第一时变参数时检查第一身份认证消息中第一认证者产生的第一时变参数与包含在第二认证者的身份认证信息中的第一时变参数是否一致，若全部为是，则确定第二认证者合法，否则，确定第二认证者非法。

[0033] 进一步地，在第一身份认证消息中还包括第一认证者的标识；第二身份认证消息中还包括第一认证者的标识；认证服务器还根据第一认证者的标识验证第一认证者的合法性，并产生认证服务器对第一认证者的验证结果；并在第三身份认证消息增加认证服务器对第一认证者的验证结果；

[0034] 相应的，在步骤五中第一认证者确定第二认证者身份合法之后，第一认证者可向第二认证者发送第五身份认证消息，消息中包括第一认证者的身份认证信息；第二认证者收到第五身份认证消息后，对第五身份认证消息进行验证，并根据验证情况确定第一认证者身份的合法性。

[0035] 进一步地，在其他实施方式中，第二身份认证消息中可进一步包含第二时变参数，第二时变参数由第二认证者产生，第二时变参数可以是时间标记、顺序号或随机数；在第三身份认证消息的认证服务器对包含第一认证者的验证结果在内信息的身份认证信息中，可

进一步包含第二时变参数。

[0036] 上述第二认证者对第五身份认证消息进行验证并根据验证结果确定第一认证者的合法性，其具体实现方式可以采用如下两种方式：

[0037] 第一种，包括如下步骤：

[0038] 1)第二认证者验证认证服务器对包含第一认证者的验证结果的身份认证信息是否有效，并在认证服务器的身份认证信息中包含第二时变参数时检查第二认证消息中第二认证者产生的第二时变参数与包含在认证服务器对包含第二时变参数在内信息的身份认证信息中的第二时变参数是否相符，若相符则执行2)，否则，确定第一认证者非法；

[0039] 2)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行3)，否则，确定第一认证者非法；

[0040] 3)第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效，检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致，并在第二认证者的身份认证信息中包含第二时变参数时检查第五身份认证消息中第二认证者产生的第二时变参数与包含在第二认证者的身份认证信息中的第二时变参数是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

[0041] 第二种，在第二认证者向第一认证者发送第四身份认证消息之前，第二认证者首先验证认证服务器对包含第一认证者的验证结果的身份认证信息是否有效，并在认证服务器的身份认证消息中包含第二时变参数时检查第二身份认证消息中第二认证者产生的第二时变参数与包含在验证认证服务器对包含第一认证者的验证结果的身份认证消息中的第二时变参数是否相符，若均为是，则向第一认证者发送第四身份认证消息。于是，第二认证者验证第一认证者包括如下步骤：

[0042] 1)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行步骤2)，否则，确定第一认证者非法；

[0043] 2)第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致，并检查第五身份认证消息中第二认证者产生的第二时变参数与包含在第二认证者的身份认证信息中的第二时变参数是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

[0044] 前述步骤三中，认证服务器根据第二认证者所处安全域的标识认证第二认证者所处安全域的合法性，可采用两种方式：

[0045] 方式一，若第二身份认证消息中的第二认证者所处安全域的标识为第二认证者所处安全域的标识符，则认证服务器查找第二认证者所处安全域的公开认证信息，若查找到，则确定第二认证者所处安全域合法，否则，确定第二认证者所处安全域非法；

[0046] 方式二，若第二身份认证消息中的第二认证者所处安全域的标识为第二认证者所处安全域的身份证明信息，则认证服务器检查其身份证明信息的有效性，若有效，则确定第二认证者所处安全域合法，否则，确定第二认证者所处安全域非法。

[0047] 另外，在其他实施方式中，可在步骤一之前由第二认证者向第一认证者发送第零身份认证消息，第零身份认证消息中包括第二认证者所处安全域的标识。相应的，去除第四

身份认证消息中的第二认证者所处安全域的标识；第一身份认证消息中还包括第一认证者的标识；第二身份认证消息中还包括第一认证者的标识；认证服务器还根据第二身份认证消息验证第一认证者的合法性而产生对第一认证者的验证结果；对第三身份认证消息做如下调整：第三身份认证消息中增加第一认证者的验证结果以及认证服务器对包含第一认证者的验证结果在内信息的身份认证信息，或者，第三身份认证消息中增加第一认证者的验证结果且第三身份认证消息中的认证服务器的身份认证信息中进一步包含第一认证者的验证结果；在第二认证者发送第四身份认证消息之前，对第三身份认证消息进行验证并根据验证结果确定第一认证者的合法性。进一步地，可在第零身份认证消息中增加第二认证者产生的第三时变参数第二时变参数可以是时间标记、顺序号或随机数；在第一身份认证消息中增加第三时变参数，第一身份认证消息中第一认证者的身份认证信息中进一步包括第三时变参数。于是，本段中所述的“在第二认证者发送第四身份认证消息之前，对第三身份认证消息进行验证并根据验证结果确定第一认证者的合法性”的具体实现步骤包括：

[0048] 5.1)第二认证者验证认证服务器对包含第一认证者的验证结果在内信息的身份认证信息是否有效，若是，则执行5.2)，否则，确定第一认证者非法；

[0049] 5.2)第二认证者若根据认证服务器对第一认证者的验证结果判断第一认证者合法有效，则执行5.3)，否则，确定第一认证者非法；

[0050] 5.3)第二认证者获取第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证信息是否有效、并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证信息中的第二认证者所处安全域的标识符是否一致，当第一认证者的身份认证消息中保护第三时变参数时校验第零身份认证消息中第二认证者产生的第三时变参数与包含在第一认证者的身份认证消息中的第三时变参数是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。

[0051] 本发明中，第一身份认证消息、第二身份认证消息和第三身份认证消息还可分别包括可选字段。

[0052] 为便于理解本发明的身份认证方法，以下提供了三个较佳实施例。

[0053] 第一较佳实施例

[0054] 第一较佳实施例是实现第一认证者对第二认证者的身份认证的较佳实施例，包括如下步骤：

[0055] 步骤1、第一认证者发送第一身份认证消息到第二认证者，第一身份认证消息包括第一认证者产生的第一时变参数及第一可选字段；

[0056] 步骤2、第二认证者向认证服务器发送第二身份认证消息，第二身份认证消息包括第一时变参数、第二认证者所处安全域的标识及第二可选字段；

[0057] 步骤3、认证服务器收到第二身份认证消息后，根据第二认证者所处安全域的标识检查第二认证者所处安全域的合法性；

[0058] 认证服务器检查第二认证者所处安全域的合法性可采用如下方法：

[0059] 在第二身份认证消息中，如果第二认证者所处安全域的标识为第二认证者所处安全域的标识符，则认证服务器查找第二认证者所处安全域的有效公开认证信息；如果第二认证者所处安全域的标识为第二认证者所处安全域的身份证明信息，则认证服务器检查第二认证者所处安全域的身份证明信息的有效性。

[0060] 步骤4、认证服务器检查完第二认证者所处安全域的合法性后，向第二认证者返回第三身份认证消息；第三身份认证消息包括认证服务器对第二认证者所处安全域的验证结果，以及认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第三可选字段在内信息的身份认证信息；

[0061] 步骤5、第二认证者收到第三身份认证信息后，向第一认证者发送第四身份认证消息；第四身份认证消息中包括第二认证者所处安全域的标识，认证服务器对第二认证者所处安全域的验证结果，认证服务器对包含第二认证者所处安全域验证结果、第一时变参数以及第三可选字段在内的身份认证信息，以及第二认证者对包含第二认证者所处安全域的标识符、第一时变参数及第六可选字段在内信息的身份认证信息。

[0062] 步骤6、第一认证者收到第四身份认证消息后，对第四身份认证消息进行验证并根据验证情况确定第二认证者身份的合法性，过程如下：

[0063] 6.1)第一认证者根据认证服务器的公开认证信息，验证认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第三可选字段在内信息的身份认证信息是否有效，并验证第一身份认证消息中第一认证者产生的第一时变参数与包含在认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第三可选字段在内的身份认证信息中的第一时变参数是否相符，若是则执行6.2)；否则，确定第二认证者非法；

[0064] 6.2)第一认证者得到第二认证者所处安全域的验证结果，若根该验证结果判断第二认证者所处安全域合法有效，则执行6.3)；否则，确定第二认证者非法；

[0065] 6.3)第一认证者获取第二认证者所处安全域的公开认证信息，根据该公开认证信息验证第二认证者的身份认证信息是否有效，校验第一身份认证消息中第一认证者产生的第一时变参数与包含在第二认证者的身份认证信息中的第一时变参数是否一致，若是，则确定第二认证者合法，否则，确定第二认证者非法。第一认证者完成对第二认证者的鉴别。

[0066] 通过上述的第一认证者对第二认证者的身份认证过程，可以实现第一认证者对第二认证者身份合法性的认证，并保护第二认证者的身份信息不被暴露。

[0067] 第二较佳实施例

[0068] 第二较佳实施例是实现第一认证者和第二认证者之间的双向身份认证的较佳实施例，包括如下步骤：

[0069] 步骤1、第一认证者发送第一身份认证消息给第二认证者，第一身份认证消息包括第一认证者产生的第一时变参数、第一认证者的标识及第一可选字段。

[0070] 步骤2、第二认证者收到第一身份认证消息后，向认证服务器发送第二身份认证消息，第二身份认证消息包括第一认证者产生的第一时变参数、第二认证者产生的第二时变参数、第二认证者所处安全域的标识、第一认证者的标识及第二可选字段。

[0071] 步骤3、认证服务器收到第二身份认证消息后，根据第二认证者所处安全域的标识和第一认证者的标识检查第二认证者所处安全域和第一认证者的合法性。

[0072] 认证服务器检查第二认证者所处安全域和第一认证者的合法性可采用如下方法：

[0073] 在第二身份认证消息中，如果第二认证者所处安全域的标识为第二认证者所处安全域的标识符，则认证服务器查找第二认证者所处安全域的有效公开认证信息；如果第二认证者所处安全域的标识为第二认证者所处安全域的身份证明信息，则认证服务器检查第二认证者所处安全域的身份证明信息的有效性；如果第一认证者的标识为第一认证者的标

识符，则认证服务器查找第一认证者的有效公开认证信息；如果第一认证者的标识为第一认证者的身份证明信息，则认证服务器检查第一认证者的身份证明信息的有效性。

[0074] 步骤4、认证服务器检查完第二认证者所处安全域和第一认证者的合法性后，向第二认证者返回第三身份认证信息，

[0075] 第三身份认证信息可以是包括认证服务器对第二认证者所处安全域的验证结果，认证服务器对第一认证者的验证结果，认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第四可选字段在内信息的身份认证信息，以及认证服务器对包含第一认证者的验证结果、第二时变参数及第五可选字段在内信息的身份认证信息的消息；

[0076] 第三身份认证消息还可以是包括认证服务器对第二认证者所处安全域的验证结果，认证服务器对第一认证者的验证结果，以及认证服务器对包含第二认证者所处安全域验证结果、第一时变参数、第一认证者的验证结果、第二认证者产生的第三时变参数以及第六可选字段在内信息的身份认证信息的消息；

[0077] 步骤5、第二认证者收到第三身份认证信息后，向第一认证者发送第四身份认证消息；该消息中包括第二认证者所处安全域的标识，第三时变参数，认证服务器对第二认证者所处安全域的验证结果，认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第四可选字段在内信息的身份认证信息，第二认证者对包含第一时变参数、第三时变参数、第一认证者的标识符、第二认证者所处安全域的标识符及第七可选字段在内信息的身份认证信息，以及第八可选字段；

[0078] 步骤6、第一认证者收到第四身份认证消息后，对该消息进行验证，过程如下：

[0079] 6.1)第一认证者根据认证服务器的公开认证信息，验证认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第四可选字段在内信息的身份认证信息或认证服务器对包含第二认证者所处安全域验证结果、第一时变参数、第一认证者的验证结果、第二时变参数及第六可选字段在内信息的身份认证信息是否有效，并检查第一身份认证消息中第一认证者产生的第一时变参数与包含在认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第四可选字段在内信息的身份认证信息或认证服务器对包含第二认证者所处安全域验证结果、第一时变参数、第一认证者的验证结果、第三时变参数及第六可选字段在内信息的身份认证信息中的第一时变参数是否相符，若是则执行6.2)；否则，确定第二认证者非法，并结束鉴别过程或执行步骤7；

[0080] 6.2)第一认证者得到认证服务器对第二认证者所处安全域的验证结果，若根据该结果判断第二认证者所处安全域合法有效，则执行6.3)，否则，确定第二认证者非法，并结束鉴别过程或执行步骤7；

[0081] 6.3)第一认证者获取第二认证者所处安全域的公开认证信息，根据该公开认证信息验证第二认证者的身份认证信息是否有效，并检查第一认证者的标识符与包含在第二认证者的身份认证信息中的第一认证者的标识符是否一致，校验第一身份认证消息中第一认证者产生的第一时变参数与包含在第二认证者的身份认证信息中的第一时变参数是否一致，若是，则确定第二认证者合法，否则，确定第二认证者非法。第一认证者完成对第二认证者的鉴别，执行步骤7。

[0082] 步骤7、第一认证者向第二认证者发送第五身份认证消息，该消息为第一认证者对包含第一时变参数、第三时变参数、第一认证者的标识符、第二认证者所处安全域的标识符

及第九可选字段在内信息的身份认证消息；

[0083] 步骤8、第二认证者收到第五身份认证消息后，对该消息进行验证，过程可以为：

[0084] 8.1)利用认证服务器的公开认证信息验证认证服务器的身份认证消息是否有效，并检查第二身份认证消息中第二认证者产生的第一时变参数与包含在验证认证服务器的身份认证消息中的第一时变参数是否相符，并在验证认证服务器的身份认证消息是否有效、并检查检查第二身份认证消息中第二认证者产生的第一时变参数与包含在验证认证服务器的身份认证消息中的第一时变参数是否相符，若均为是，则执行8.2)；否则，确定第一认证者非法；

[0085] 8.2)第二认证者得到认证服务器对第一认证者的验证结果，若根据该验证结果判断第一认证者合法有效，则执行8.3)，否则，确定第一认证者非法；第二认证者完成对第一认证者的鉴别；

[0086] 8.3)第二认证者获得第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证消息是否有效，并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证消息中的第二认证者所处安全域的标识符是否一致，校验第四身份认证消息中第二认证者产生的第三时变参数与包含在第一认证者的身份认证消息中的第三时变参数是否一致，若是，则确定第一认证者合法，否则，确定第一认证者非法。第二认证者完成对第一认证者的鉴别。

[0087] 其中，上述8.1)可提前至上述步骤5中执行，即上述步骤5中第二认证者收到第三身份认证信息之后，第二认证者向第一认证者发送第四身份认证消息之前，先执行8.1)中的“利用认证服务器的公开认证信息验证认证服务器的身份认证消息是否有效，并检查第二身份认证消息中第二认证者产生的第一时变参数与包含在验证认证服务器的身份认证消息中的第一时变参数是否相符，并在验证认证服务器的身份认证消息是否有效、并检查检查第二身份认证消息中第二认证者产生的第一时变参数与包含在验证认证服务器的身份认证消息中的第一时变参数是否相符”，验证通过后再向第一认证者发送第四身份认证消息，且当执行到步骤8时，直接从步骤8.2)开始执行

[0088] 通过上述的第二认证者和第一认证者之间的双向认证过程，可以实现两实体间的双向身份合法性认证，并保护第二认证者的身份信息不被暴露。

[0089] 第三较佳实施例

[0090] 本实较佳施例是实现第一认证者和第二认证者之间的双向身份认证过程的较佳实施例，包括如下步骤：

[0091] 步骤0、第二认证者发送第零身份认证消息给第一认证者，第零身份认证消息中包括第二认证者产生的第三时变参数、第二认证者所处安全域的标识以及第一可选字段。

[0092] 步骤1、第一认证者发送第一身份认证消息给第二认证者，第一身份认证消息包括第一认证者产生的第一时变参数，第二认证者产生的第三时变参数，第二可选字段，以及第一认证者对包含第一认证者的标识、第一认证者产生的第一时变参数、第二认证者产生的第三时变参数、第二认证者所处安全域的标识及第三可选字段在内信息的身份认证消息。

[0093] 步骤2、第二认证者收到第一身份认证消息后，向认证服务器发送第二身份认证消息，第二身份认证消息包括第一认证者产生的第一时变参数、第二认证者产生的第二时变参数、第二认证者所处安全域的标识、第一认证者的标识及第四可选字段。

[0094] 步骤3、认证服务器收到第二身份认证消息后，根据第二认证者所处安全域的标识和第一认证者的标识检查第二认证者所处安全域和第一认证者的合法性。

[0095] 认证服务器检查第二认证者所处安全域和第一认证者的合法性可采用如下方法：

[0096] 在第二身份认证消息中，如果第二认证者所处安全域的标识为第二认证者所处安全域的标识符，则认证服务器查找第二认证者所处安全域的有效公开认证信息；如果第二认证者所处安全域的标识为第二认证者所处安全域的身份证明信息，则认证服务器检查第二认证者所处安全域的身份证明信息的有效性；如果第一认证者的标识为第一认证者的标识符，则认证服务器查找第一认证者的有效公开认证信息；如果第一认证者的标识为第一认证者的身份证明信息，则认证服务器检查第一认证者的身份证明信息的有效性。

[0097] 步骤4、认证服务器向第二认证者返回第三身份认证信息，

[0098] 第三身份认证信息可以是包括认证服务器对第二认证者所处安全域的验证结果，认证服务器对第一认证者的验证结果，认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第五可选字段在内信息的身份认证信息，以及认证服务器对包含第一认证者的验证结果、第二时变参数及第六可选字段在内信息的身份认证信息的消息；

[0099] 第三身份认证消息还可以是包括认证服务器对第二认证者所处安全域的验证结果，认证服务器对第一认证者的验证结果，以及认证服务器对包含第二认证者所处安全域验证结果、第一时变参数、第一认证者的验证结果、第二时变参数及第七可选字段在内信息的身份认证信息的消息；

[0100] 步骤5、第二认证者收到第三身份认证信息后，向第一认证者发送第四身份认证消息；第四身份认证消息中包括第二认证者所处安全域的标识，第三时变参数，认证服务器对第二认证者所处安全域的验证结果，认证服务器对包含第二认证者所处安全域验证结果、第一时变参数及第四可选字段在内信息的身份认证信息，第二认证者对包含第一时变参数、第三时变参数、第一认证者的标识符、第二认证者所处安全域的标识符及第七可选字段在内信息的身份认证信息，以及第八可选字段；其中，在发送第四身份认证消息之前，执行如下过程：

[0101] 5.1)利用认证服务器的公开认证信息验证认证服务器的身份认证消息是否有效，并检查第二身份认证消息中第二认证者产生的第一时变参数与包含在验证认证服务器的身份认证信息中的第一时变参数是否相符，并在验证认证服务器的身份认证信息是否有效、并检查第二身份认证消息中第二认证者产生的第一时变参数与包含在认证服务器的身份认证消息中的第一时变参数是否相符，若均为是，则执行5.2)；否则，确定第一认证者非法；

[0102] 5.2)第二认证者得到认证服务器对第一认证者的验证结果，若根据该验证结果判断第一认证者合法有效，则执行5.3)，否则，确定第一认证者非法；

[0103] 5.3)第二认证者获得第一认证者的公开认证信息，根据该公开认证信息验证第一认证者的身份认证消息是否有效，并检查第二认证者所处安全域的标识符与包含在第一认证者的身份认证消息中的第二认证者所处安全域的标识符是否一致，校验第零身份认证消息中第二认证者产生的第三时变参数与包含在第一认证者的身份认证消息中的第三时变参数是否一致，若均为是，则确定第一认证者合法，否则，确定第一认证者非法。第二认证者完成对第一认证者的鉴别。

[0104] 步骤6、第一认证者收到第四身份认证消息后，对该消息进行验证，过程如下：

[0105] 6.1)第一认证者根据认证服务器的公开认证信息，验证认证服务器的身份认证信息是否有效，并检查第一身份认证消息中第一认证者产生的第一时变参数与包含在认证服务器的身份认证信息中的第一时变参数是否相符，若均为是，则执行6.2)；否则，确定第二认证者非法；

[0106] 6.2)第一认证者得到认证服务器对第二认证者所处安全域的验证结果，若根据该结果判断第二认证者所处安全域合法有效，则执行6.3)，否则，确定第二认证者非法；

[0107] 6.3)第一认证者获取第二认证者所处安全域的公开认证信息，根据该公开认证信息验证第二认证者的身份认证信息是否有效，并检查第一认证者的标识符与包含在第二认证者的身份认证信息中的第一认证者的标识符是否一致，校验第一身份认证消息中第一认证者产生的第一时变参数与包含在第二认证者的身份认证信息中的第一时变参数是否一致，若均为是，则确定第二认证者合法，否则，确定第二认证者非法。第一认证者完成对第二认证者的鉴别。

[0108] 通过上述的第二认证者和第一认证者之间的双向认证过程，可以实现两实体间的双向身份合法性认证，并保护第二认证者的身份信息不被暴露。

[0109] 前文中所出现的第一可选字段、第二可选字段、第三可选字段…的存在性和内容均是不确定的，其意义主要是考虑到实施者可以根据其具体需求自行定义可选字段内容以达到扩展的目的，因而，在其他实施例中，可选字段也可省去。

[0110] 前文中提到的第一认证者的私有认证信息可以是信息安全领域公钥密码体制中的私钥等信息。

[0111] 前文中提到的第二认证者的私有认证信息可以是信息安全领域公钥密码体制中的匿名签名密钥等信息。

[0112] 前文中所出现的第二时变参数和第三时变参数均为第二认证者产生的时变参数，二者可以相同，也可以不同。

[0113] 前文提及第一认证者或认证服务器的身份认证信息可以是利用私有认证信息，并采用数字签名等信息安全技术，计算生成的信息。

[0114] 前文提及第二认证者的身份认证信息可以是利用私有认证信息，并采用匿名数字签名等信息安全技术，计算生成的信息。

[0115] 尽管已描述了本发明的优选实施方式，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0116] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

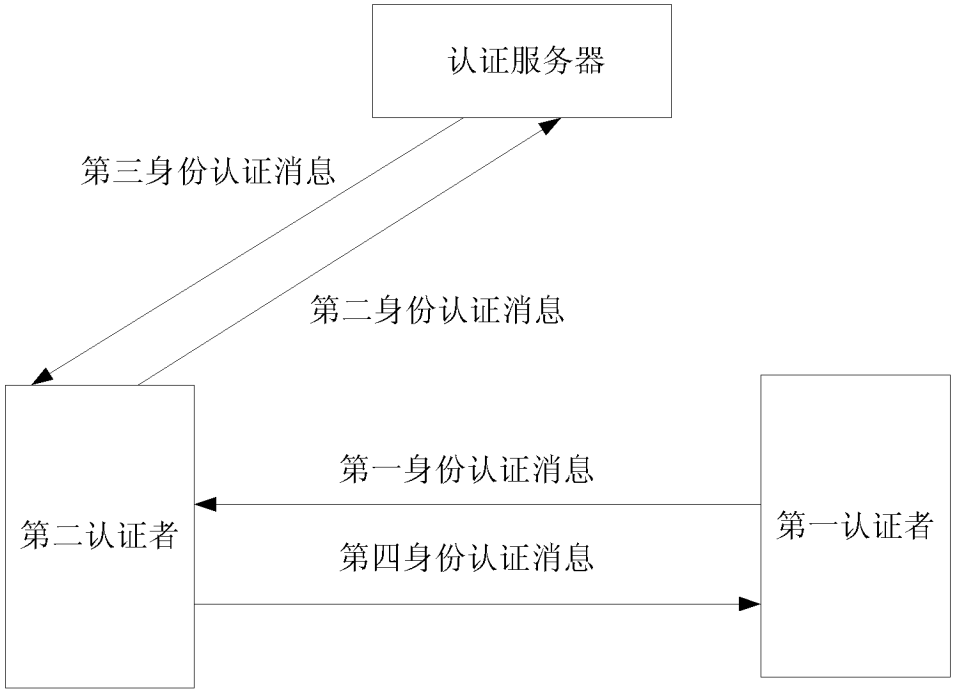


图1