(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 1835436 B
(45)授权公告日 2010.04.14

(21)申请号 200510053868.9
(22)申请日 2005.03.14
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 黄迎新
(51)Int.Cl.
*H04L 9/32*(2006.01)
(56)对比文件
CN 1430441 A,2003.07.16, 全文.
US 2003/0097593 A1,2003.05.22, 全文.
WO 2004/084464 A2,2004.09.30, 全文.
CN 1414709 A,2003.04.30, 全文.
CN 1349723 A,2002.05.15, 全文.

审查员 李博

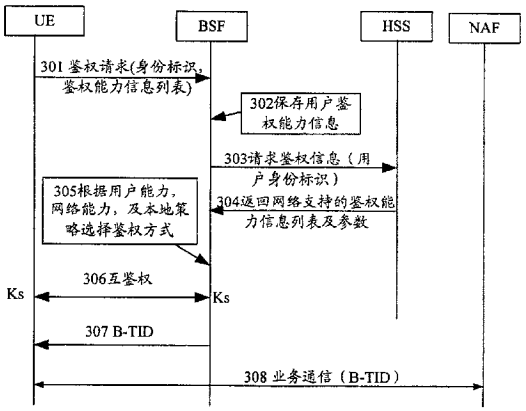
权利要求书 3 页 说明书 8 页 附图 2 页

(54)发明名称

一种通用鉴权网络及一种实现鉴权的方法

(57)摘要

本发明公开了一种通用鉴权网络中实现鉴权的方法，其关键是实体认证中心根据发起鉴权请求的实体提供的其所支持的鉴权方式和当前网络提供的其所支持的鉴权方式，确定当前网络和该发起鉴权请求的实体都支持的所有鉴权方式，从所确定的鉴权方式中选择一种鉴权方式，与发起鉴权请求的实体进行互鉴权。应用本发明提供的方法，在鉴权过程中增加了鉴权方式的选择过程，使通用鉴权网络应用的更为广泛，而且，由于能够使多种鉴权方式共存，为运营商的网络配置和应用提供了更多的选择。本发明还公开了一种通用鉴权网络，其关键是使网络中的应用服务器既能为普通用户提供业务服务，还能向其他服务器请求业务服务，充分地利用了网络中的各种资源。




CN 1835436 B

1. 一种通用鉴权网络中实现鉴权的方法，所述通用鉴权网络中包括用于与发起鉴权请求的实体进行鉴权操作的实体认证中心，其特征在于，该方法包括以下步骤：

实体认证中心接收到来自发起鉴权请求实体的鉴权请求后，获取该发起鉴权请求实体所支持鉴权方式以及当前网络支持的鉴权方式，之后，从所获取的鉴权方式中选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式，并应用该鉴权方式与发起鉴权请求实体实现鉴权。

2. 根据权利要求 1 所述的方法，其特征在于，所述实体认证中心获取发起鉴权请求实体所支持鉴权方式的方法为：

实体认证中心接收到来自发起鉴权请求实体的包含其所支持鉴权方式的鉴权请求后，从该鉴权请求中获取发起鉴权请求实体所支持鉴权方式；或者，

实体认证中心向发起鉴权请求实体发送提供所支持的鉴权方式的请求消息，从发起鉴权请求实体返回的响应消息中获取该发起鉴权请求实体所支持的鉴权方式。

3. 根据权利要求 1 所述的方法，其特征在于，所述实体认证中心获取当前网络支持的鉴权方式的方法为：

实体认证中心向实体签约信息数据库服务器发送包含发起鉴权请求实体身份标识的请求鉴权信息的消息，实体签约信息数据库服务器接收到该消息后，确定当前网络支持的鉴权方式后，将所确定的鉴权方式包含在发送给实体认证中心的请求鉴权信息的响应消息中，实体认证中心从实体签约信息数据库服务器返回的响应消息中获取当前网络支持的鉴权方式；

或者，实体认证中心从自身预先保存的当前网络支持的鉴权方式信息中获取当前网络支持的鉴权方式。

4. 根据权利要求 3 所述的方法，其特征在于，所述实体签约信息数据库服务器确定当前网络支持的鉴权方式的方法为：根据网络侧的预先配置确定当前网络支持的所有鉴权方式，并将所确定的所有鉴权方式作为当前网络支持的鉴权方式。

5. 根据权利要求 3 所述的方法，其特征在于，所述实体签约信息数据库服务器确定当前网络支持的鉴权方式的方法为：从来自实体认证中心的鉴权信息请求消息中获取发起鉴权请求实体身份标识，根据该发起鉴权请求实体身份标识获取该发起鉴权请求实体的签约信息，从该签约信息中获取该发起鉴权请求实体支持的所有鉴权方式，根据网络侧的预先配置，确定当前网络支持的所有鉴权方式，选择当前网络和该发起鉴权请求实体都支持的鉴权方式，并将所选择的所有鉴权方式作为当前网络支持的鉴权方式。

6. 根据权利要求 1 所述的方法，其特征在于，所述实体认证中心选择鉴权方式的方法为：实体认证中心根据已获取的当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，确定当前网络和该发起鉴权请求实体都支持的所有鉴权方式，从所确定的鉴权方式中随机选择一种鉴权方式。

7. 根据权利要求 1 所述的方法，其特征在于，所述实体认证中心所获取的当前网络支持的鉴权方式具有优先级信息；

所述实体认证中心选择鉴权方式的方法为：实体认证中心根据已获取的当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，确定当前网络和该发起鉴权请求实体都支持的所有鉴权方式，从所确定的鉴权方式中选择优先级最高的鉴权方式。

8. 根据权利要求 6 或 7 所述的方法，其特征在于，所述实体认证中心确定当前网络和该发起鉴权请求实体都支持的所有鉴权方式后，在从所确定的所有鉴权方式中选择一种鉴权方式之前，进一步包括：所述实体认证中心判断自身是否预先配置有不同鉴权方式的优先级信息，如果有，则按照自身的优先级信息，从所确定的鉴权方式中选择一种优先级最高的鉴权方式，如果没有，则继续后续处理。

9. 根据权利要求 1 ～ 7 任一所述的方法，其特征在于，所述实体签约信息数据库服务器为用户归属网络服务器 HSS，所述发起鉴权请求的实体为用户终端 UE 或应用服务器 (AS，Application Server)。

10. 根据权利要求 9 所述的方法，其特征在于，

所述发起鉴权请求的实体为用户终端时，所述鉴权请求中进一步包括：用户终端的终端能力信息；

实体认证中心从接收到该鉴权请求后，进一步包括：获取并保存用户终端的终端能力信息；

鉴权成功后，该方法进一步包括：实体认证中心根据自身已保存的用户终端的终端能力信息以及终端能力信息和所使用的鉴权方式是否一致，确定是否需要对鉴权成功后产生的密钥进行格式转换。

11. 一种通用鉴权网络，包括：仅使用服务的实体、仅提供服务的实体、实体认证中心和实体签约信息数据库服务器，其特征在于，该通用鉴权网络还包括：既使用服务又提供服务的实体，其中，

仅使用服务的实体，与实体认证中心、仅提供服务的实体和既使用服务又提供服务的实体分别直接相连，向实体认证中心发起鉴权请求，或者，向仅提供服务的实体或既使用服务又提供服务的实体发起业务请求，

实体认证中心，与实体签约信息数据库服务器、仅使用服务的实体、仅提供服务的实体和既使用服务又提供服务的实体分别直接相连，用于接收来自仅使用服务的实体、仅提供服务的实体或既使用服务又提供服务的实体的鉴权请求，获取当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，从所获取的鉴权方式中，选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式，应用所选定的鉴权方式与发起鉴权请求的实体进行互鉴权，或者，根据实体签约信息数据库服务器提供的签约信息为仅提供服务的实体或既使用服务又提供服务的实体提供其所需的鉴权结果信息，

实体签约信息数据库服务器，用于存储仅使用服务实体、仅提供服务实体和既使用服务又提供服务的实体的签约信息，向实体认证中心提供仅使用服务实体或既使用服务又提供服务的实体的鉴权信息，或者，向实体认证中心提供仅提供服务实体或既使用服务又提供服务的实体的签约信息，

仅提供服务的实体，与既使用服务又提供服务的实体直接相连，用于向实体认证中心发起鉴权请求，并用于根据从实体认证中心获取的鉴权结果与仅使用服务的实体或既使用服务又提供服务的实体建立连接，提供业务服务，

所述既使用服务又提供服务的实体，用于向实体认证中心发起鉴权请求，应用实体认证中心选定的鉴权方式，与实体认证中心进行互鉴权，获取用于业务请求的标识和用于认证查询标识，

或者，应用业务请求的标识向仅提供服务的实体发起业务请求，与仅提供服务的实体建立连接，使用其所提供的服务；

或者，用于接收仅使用服务实体的业务请求，应用认证查询标识从实体认证中心获取仅使用服务实体的鉴权结果，与仅使用服务的实体建立连接，为其提供业务服务。

12. 根据权利要求 11 所述的通用鉴权网络，其特征在于，所述仅使用服务的实体为用户终端 UE，所述仅提供服务的实体为业务应用功能实体 NAF 或应用服务器 (AS，Application Server)，所述实体认证中心为执行初始检查验证的功能实体 BSF，所述实体签约信息数据库服务器为用户归属网络服务器 HSS，所述既使用服务又提供服务的实体为应用服务器 (AS，Application Server)，或用户终端 UE。

# 一种通用鉴权网络及一种实现鉴权的方法

## 技术领域

[0001] 本发明涉及第三代无线通信技术领域，特别是指一种通用鉴权网络及在通用鉴权网络中一种实现鉴权的方法。

## 背景技术

[0002] 在第三代无线通信标准中，通用鉴权网络是多种应用业务实体使用的一个用于完成对用户身份进行验证的通用结构，应用通用鉴权网络可实现对应用业务的用户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。

[0003] 图1所示为现有的通用鉴权网络的结构示意图。通用鉴权网络通常由用户终端(UE)101、执行初始检查验证的功能实体(BSF)102、用户归属网络服务器(HSS)103和网络应用功能实体(NAF)104组成。BSF 102用于与用户终端101互验证身份，同时生成BSF 102与用户终端101的共享密钥；HSS 103中存储有用于描述用户信息的描述(Profile)文件，该Profile中包括用户身份标识等所有与用户有关的描述信息，同时HSS 103还兼有产生鉴权矢量信息的功能。

[0004] 用户需要使用某种业务时，如果其知道需要到BSF进行互鉴权，则直接与BSF交互以进行互鉴权，否则，用户会首先和该业务对应的NAF联系，如果该NAF应用通用鉴权网络且需要用户到BSF进行身份验证，则通知用户应用通用鉴权网络进行身份验证，否则进行其它相应处理。

[0005] 用户终端与BSF之间的互认证过程是：用户向BSF发出鉴权请求，该鉴权请求消息中包括用户的永久身份标识，BSF接到来自用户的鉴权请求后，向HSS请求该用户的鉴权信息，该请求消息中也包含了该用户终端的永久身份标识，HSS根据该用户终端的永久身份标识查找到该用户的profile文件并且生成鉴权信息返回给BSF。BSF根据所获取的鉴权信息与用户之间执行鉴权和密钥协商协议(AKA)进行互鉴权。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Ks，BSF为这个密钥Ks定义有效期限，以便Ks进行更新。之后，BSF分配一个会话事务标识(B-TID)给UE，在将B-TID和密钥Ks发送给UE的同时包含了Ks的有效期限，该B-TID是与Ks相关联的。共享密钥Ks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Ks衍生出的密钥作为通信保护。

[0006] 当用户发现Ks即将过期，或NAF要求用户重新到BSF进行鉴权时，用户就会重复上述的步骤重新到BSF进行鉴权，以得到新的Ks及B-TID。

[0007] 在现有的鉴权过程中，UE与BSF之间通过Http AKA协议进行鉴权，该鉴权过程是一种基于3G的鉴权过程，而且，UE和BSF之间只有这一种鉴权方式。但是，随着技术的发展，将来在UE和BSF之间很可能通过其他方式实现鉴权，例如基于公私钥算法(DH，Diffie-Hellman)鉴权方式等。另外，通用鉴权网络也有可能为2G的用户提供服务，而2G用户的鉴权方式与3G用户的鉴权方式又是不相同的。在增加了这么许多鉴权方式后用户

和网络侧之间需要能够协商它们采用那种鉴权方法来完成互鉴权过程，而在现有技术中根本不存在协商的过程。

[0008] 再有，在现有的通用鉴权网络中，请求业务应用的只能是最普通的用户终端，即使其有能力为其他用户提供一些简单的业务，比如用户自己建立了一个简单的网站，其也不能通过通用鉴权网络体系来提供服务，因为在现有的通用鉴权网络体系中，应用服务器(AS)是不能作为一个用户来请求业务服务的，相应地，应用功能服务器只能为用户提供业务服务，而不能请求向其他服务器请求业务服务。由此看出，现有的通用鉴权网络并不能充分利用网络中的各种资源。

## 发明内容

[0009] 有鉴于此，本发明的一个目的在于提供一种通用鉴权网络中实现鉴权的方法，在用户使用通用鉴权网络进行鉴权时，能够和网络协商所使用的鉴权方式，应用该协商出的鉴权方式实现鉴权。本发明的另一目的是提供一种通用鉴权网络，使网络中的各种资源能够被充分利用。

[0010] 为达到上述目的，本发明的技术方案是这样实现的：

[0011] 一种通用鉴权网络中实现鉴权的方法，所述通用鉴权网络中包括用于与发起鉴权请求的实体进行鉴权操作的实体认证中心，该方法包括以下步骤：

[0012] 实体认证中心接收到来自发起鉴权请求实体的鉴权请求后，获取该发起鉴权请求实体所支持鉴权方式以及当前网络支持的鉴权方式，之后，从所获取的鉴权方式中选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式，并应用该鉴权方式与发起鉴权请求实体实现鉴权。

[0013] 较佳地，所述实体认证中心获取发起鉴权请求实体所支持鉴权方式的方法为：

[0014] 实体认证中心接收到来自发起鉴权请求实体的包含其所支持鉴权方式的鉴权请求后，从该鉴权请求中获取发起鉴权请求实体所支持鉴权方式；或者，

[0015] 实体认证中心向发起鉴权请求实体发送提供所支持的鉴权方式的请求消息，从发起鉴权请求实体返回的响应消息中获取该发起鉴权请求实体所支持的鉴权方式。

[0016] 较佳地，所述实体认证中心获取当前网络支持的鉴权方式的方法为：

[0017] 实体认证中心向实体签约信息数据库服务器发送包含发起鉴权请求实体身份标识的请求鉴权信息的消息，实体签约信息数据库服务器接收到该消息后，确定当前网络支持的鉴权方式后，将所确定的鉴权方式包含在发送给实体认证中心的请求鉴权信息的响应消息中，实体认证中心从实体签约信息数据库服务器返回的响应消息中获取当前网络支持的鉴权方式；

[0018] 或者，实体认证中心从自身预先保存的当前网络支持的鉴权方式信息中获取当前网络支持的鉴权方式。

[0019] 较佳地，所述实体签约信息数据库服务器确定当前网络支持的鉴权方式的方法为：根据网络侧的预先配置确定当前网络支持的所有鉴权方式，并将所确定的所有鉴权方式作为当前网络支持的鉴权方式。

[0020] 较佳地，所述实体签约信息数据库服务器确定当前网络支持的鉴权方式的方法为：从来自实体认证中心的鉴权信息请求消息中获取发起鉴权请求实体身份标识，根据该

发起鉴权请求实体身份标识获取该发起鉴权请求实体的签约消息，从该签约信息中获取该发起鉴权请求实体支持的所有鉴权方式，根据网络侧的预先配置，确定当前网络支持的所有鉴权方式，选择当前网络和该发起鉴权请求的实体都支持的鉴权方式，并将所选择的所有鉴权方式作为当前网络支持的鉴权方式。

[0021] 较佳地，所述实体认证中心选择鉴权方式的方法为：实体认证中心根据已获取的当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，确定当前网络和该发起鉴权请求实体都支持的所有鉴权方式，从所确定的鉴权方式中随机选择一种鉴权方式。

[0022] 较佳地，所述所获取的当前网络支持的鉴权方式具有优先级信息；

[0023] 所述实体认证中心选择鉴权方式的方法为：实体认证中心根据已获取的当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，确定当前网络和该发起鉴权请求实体都支持的所有鉴权方式，从所确定的鉴权方式中选择优先级最高的鉴权方式。

[0024] 较佳地，所述实体认证中心确定当前网络和该发起鉴权请求实体都支持的所有鉴权方式后，在从所确定的所有鉴权方式中选择一种鉴权方式之前，进一步包括：判断自身内是否预先配置有不同鉴权方式的优先级信息，如果有，则按照自身的优先级信息，从所确定的鉴权方式中选择一种优先级最高的鉴权方式，如果没有，则继续后续处理。

[0025] 较佳地，所述实体签约信息数据库服务器为用户归属网络服务器 HSS，所述发起鉴权请求的实体为用户终端 UE 或应用服务器 AS。

[0026] 较佳地，所述发起鉴权请求的实体为用户终端时，所述鉴权请求中进一步包括：用户终端的终端能力信息；

[0027] 实体认证中心从接收到该鉴权请求后，进一步包括：获取并保存用户终端的终端能力信息；

[0028] 鉴权成功后，该方法进一步包括：实体认证中心根据自身已保存的用户终端的终端能力信息以及终端能力信息和所使用的鉴权方式是否一致，确定是否需要对鉴权成功后产生的密钥进行格式转换。

[0029] 一种通用鉴权网络，包括：仅使用服务的实体、仅提供服务的实体、实体认证中心和实体签约信息数据库服务器，该通用鉴权网路还包括：既使用服务又提供服务的实体，其中，

[0030] 仅使用服务的实体，与实体认证中心、仅提供服务的实体和既使用服务又提供服务的实体分别直接相连，向实体认证中心发起鉴权请求，或者，向仅提供服务的实体或既使用服务又提供服务的实体发起业务请求，

[0031] 实体认证中心，与实体签约信息数据库服务器、仅使用服务的实体、仅提供服务的实体和既使用服务又提供服务的实体分别直接相连，用于接收来自仅使用服务的实体、仅提供服务的实体或既使用服务又提供服务的实体的鉴权请求，获取当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，从所获取的鉴权方式中，选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式，应用所选定的鉴权方式与发起鉴权请求的实体进行互鉴权，或者，根据实体签约信息数据库服务器提供的签约信息为仅提供服务的实体或既使用服务又提供服务的实体提供其所需的鉴权结果信息，

[0032] 实体签约信息数据库服务器，用于存储仅使用服务实体、仅提供服务实体和既使用服务又提供服务的实体的签约信息，向实体认证中心提供仅使用服务实体或既使用服务

又提供服务的实体的鉴权信息，或者，向实体认证中心提供仅提供服务实体或既使用服务又提供服务的实体的签约信息，

[0033] 仅提供服务的实体，与既使用服务又提供服务的实体直接相连，用于向实体认证中心发起鉴权请求，并用于根据从实体认证中心获取的鉴权结果与仅使用服务的实体或既使用服务又提供服务的实体建立连接，提供业务服务，

[0034] 所述既使用服务又提供服务的实体，用于向实体认证中心发起鉴权请求，应用实体认证中心选定的鉴权方式，与实体认证中心进行互鉴权，获取用于业务请求的标识和用于认证查询标识，

[0035] 或者，应用业务请求的标识向仅提供服务的实体发起业务请求，与仅提供服务的实体建立连接，使用其所提供的服务；

[0036] 或者，用于接收仅使用服务实体的业务请求，应用认证查询标识从实体认证中心获取仅使用服务实体的鉴权结果，与仅使用服务的实体建立连接，为其提供业务服务。

[0037] 较佳地，所述仅使用服务的实体为用户终端 UE，所述仅提供服务的实体为业务应用功能实体 NAF 或应用服务器 (AS，Application Server)，所述实体认证中心为执行初始检查验证的功能实体 BSF，所述实体签约信息数据库服务器为用户归属网络服务器 HSS，所述既使用服务又提供服务的实体为应用服务器 (AS，Application Server)，或用户终端 UE。

[0038] 本发明提供的实现鉴权的方法，关键是实体认证中心根据发起鉴权请求的实体提供的其所支持的鉴权方式和当前网络提供的其所支持的鉴权方式，确定当前网络和该发起鉴权请求的实体都支持的所有鉴权方式，从所确定的鉴权方式中选择一种鉴权方式，与发起鉴权请求的实体进行互鉴权。应用本发明提供的方法，在鉴权过程中增加了鉴权方式的选择过程，使通用鉴权网络应用的更为广泛，而且，由于能够使多种鉴权方式共存，为运营商的网络配置和应用提供了更多的选择。

[0039] 应用本发明提供的通用鉴权网络，使网络中的应用服务器既能为普通用户提供业务服务，还能向其他服务器请求业务服务，充分地利用了网络中的各种资源，同时还能提供选择鉴权方式的操作，为运营商的网络配置和应用提供了更多的选择。

## 附图说明

[0040] 图 1 所示为现有的通用鉴权网络的结构示意图；

[0041] 图 2 所示为本发明的通用鉴权网络结构示意图；

[0042] 图 3 所示为应用本发明一实施例的实现鉴权的流程示意图。

## 具体实施方式

[0043] 下面结合附图，具体说明本发明的技术方案。

[0044] 图 2 所示为本发明的通用鉴权网络结构示意图。在本发明的通用鉴权网络中不仅包括：仅使用服务的实体 201、仅提供服务的实体 204、实体认证中心 (EAC，Entity Authentication Center)202 和实体签约信息数据库服务器 (ESD，Entity Subscription Database)203，还包括既使用服务又提供服务的实体 205。

[0045] 仅使用服务的实体 201，与实体认证中心 202、仅提供服务的实体 204 和既使用服务又提供服务的实体 205 分别直接相连，向实体认证中心 202 发起鉴权请求，或者，向仅提

供服务的实体 204 或既使用服务又提供服务的实体 205 发起业务请求，

[0046] 实体认证中心 202，与实体签约信息数据库服务器 203、仅提供服务的实体 204 和既使用服务又提供服务的实体 205 分别直接相连，用于接收来自仅提供服务实体 204 或既使用服务又提供服务实体 205 的鉴权请求，获取当前网络支持的鉴权方式和发起鉴权请求实体所支持的鉴权方式，从所获取的鉴权方式中，选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式，应用所选定的鉴权方式与发起鉴权请求的实体进行互鉴权，或者，根据实体签约信息数据库服务器 203 提供的签约信息为仅提供服务的实体 204 或既使用服务又提供服务实体 205 提供其所需的鉴权结果信息，

[0047] 实体签约信息数据库服务器 203，既包括用于存储仅使用服务实体 201 和仅提供服务实体 204 的签约信息，还包括既使用服务又提供服务实体 205 的签约信息，向实体认证中心 202 提供签约实体的鉴权信息，即向实体认证中心 202 提供仅使用服务实体 201 和既使用服务又提供服务实体 205 的鉴权信息，或者，向实体认证中心 202 提供仅提供服务实体 204 或既使用服务又提供服务实体 205 的签约信息，

[0048] 仅提供服务的实体 204，与既使用服务又提供服务的实体 205 直接相连，根据从实体认证中心 202 获取的鉴权结果与仅使用服务的实体 201 或既使用服务又提供服务的实体 205 建立连接，提供业务服务，

[0049] 既使用服务又提供服务的实体 205，向实体认证中心 202 发起鉴权请求，应用实体认证中心 202 选定的鉴权方式，与其进行互鉴权，获取用于业务请求的标识和用于认证查询标识，或者，应用业务请求的标识向仅提供服务的实体 204 发起业务请求，与仅提供服务的实体 204 建立连接，使用其所提供的服务，或者，用于接收仅使用服务实体 201 的业务请求，应用认证查询标识从实体认证中心 202 获取仅使用服务实体 201 的鉴权结果，与仅使用服务实体 201 建立连接，为其提供业务服务。

[0050] 上述实体 205 之所以能够既使用服务又提供服务，是因为，在该实体与实体认证中心 202 进行互鉴权成功后，该实体认证中心 202 已从实体签约信息数据库服务器 203 获取该实体 205 的属性，即确认了该请求鉴权实体既签约了订购服务又签约了提供服务的信息，之后，实体认证中心 202 会为该实体 205 分配一个用于业务请求的标识和一个用于认证查询标识。这样，当该实体 205 需要应用其他服务器上的业务时，其会应用业务请求的标识，当实体 205 为用户终端提供业务服务器时，其将应用认证查询标识，从而使得实体 205 既能够使用服务又提供服务。

[0051] 通常，所述仅使用服务的实体 201 为用户终端 UE，所述仅提供服务的实体 205 为业务应用功能实体 NAF 或应用服务器 (AS，Application Server)，所述实体认证中心 202 为执行初始检查验证的功能实体 BSF，所述实体签约信息数据库服务器 203 为用户归属网络服务器 HSS，所述既使用服务又提供服务实体 205 为应用服务器 (AS) 或用户终端 UE。既使用服务又提供服务实体 205 所拥有的用于业务请求的标识和用于认证查询标识具体的应用过程分别与现有的 B-TID 和 NAF 的标识的应用过程相同，在此不再详细描述。当然，随着的技术的发展，图 2 中各个实体的具体载体的名称可能会发生变化，在此，并不对各个具体载体的名称加以限制，只要其实现的功能与图 2 所示各个模块的功能相同，即包含在本发明的范围之内。

[0052] 在下面的方法流程中具体说明上述实体认证中心 202 获取当前网络支持的鉴权

方式和发起鉴权请求实体所支持的鉴权方式，从所获取的鉴权方式中，选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式的方法。

[0053] 图 3 所示为应用本发明一实施例的实现鉴权的流程示意图。在本实施例中发起鉴权请求的实体是用户终端 UE，实体认证中心为 BSF，由 NAF 为 UE 提供服务，由 HSS 作为实体签约信息数据库服务器。

[0054] 步骤 301，UE 向 BSF 发送鉴权请求，该请求中包含用户终端的身份标识、用户终端的能力信息和预设的鉴权能力信息列表。

[0055] 其中，用户终端的能力信息用于表示该用户终端是 3G 的设备还是 2G 的设备；鉴权能力信息用于表示该 UE 能够支持的鉴权方式，在实际应用中可以通过一个简单的字段来标识，例如用一个 4bit 的字段来标识，并设置 0001 表示 AKA 鉴权，0010 表示基于 SIM 的鉴权，0011 标识 SIM 与 TLS 相结合的鉴权，0100 表示基于公私钥的 DH 鉴权，如果用户支持 AKA 鉴权和 DH 鉴权，那么在鉴权能力信息列表中就有 0001 和 0100 这两项。

[0056] 步骤 302，BSF 接收到该鉴权请求后，获取并保存用户终端的能力信息以及鉴权能力信息列表。

[0057] 如果 UE 向 BSF 发送的鉴权请求消息中未包含鉴权能力信息，BSF 可以发送要求 UE 提供其所支持的鉴权方式的请求消息，并从 UE 返回的响应消息中获取该 UE 所支持鉴权方式。

[0058] 步骤 303，BSF 向 HSS 发送请求鉴权信息的消息，该请求消息中包含用户终端的身份标识；

[0059] 步骤 304，HSS 获取当前网络支持的鉴权方式，并根据所获取的鉴权方式以及 UE 的身份标识产生该 UE 的鉴权信息，之后，向 BSF 返回包含访问端鉴权信息和当前网络支持的鉴权方式；

[0060] HSS 获取当前网络支持的鉴权方式的方法为：根据已获取的 UE 身份标识，从其签约信息中获取该 UE 能够支持的所有的鉴权方式，根据网络侧的预先配置，确定当前网络支持的所有鉴权方式，选择当前网络和该 UE 都支持的鉴权方式，并将所选择的鉴权方式作为当前网络支持的鉴权方式；或者，HSS 获取当前网络支持的鉴权方式的方法为：根据网络侧的预先配置确定当前网络支持的所有鉴权方式，并将所确定的鉴权方式作为当前网络支持的鉴权方式。

[0061] 在本实施例中，HSS 向 BSF 返回的当前网络支持的鉴权方式是已列表的形式存在的，该列表中每种鉴权方式后包含该鉴权方式所需的参数即鉴权信息；同时该列表中还包含优先级信息，即优先级高的鉴权方式位于优先级低的鉴权方式之前。当然，BSF 向 HSS 返回的当前网络支持的鉴权方式也可以以其他的形式存在，也可以不包含任何优先级信息。

[0062] 步骤 305，BSF 根据当前网络支持的鉴权方式和已保存的 UE 所支持的鉴权方式，选择一种当前网络和该发起鉴权请求实体都支持的鉴权方式。

[0063] 如果 HSS 返回的当前网络支持的鉴权方式中不包含优先级信息，则 BSF 根据当前网络支持的鉴权方式和已保存的 UE 所支持的鉴权方式，确定当前网络和该 UE 都支持的所有鉴权方式，从所确定的鉴权方式中随机选择一种鉴权方式；

[0064] 如果 HSS 返回的当前网络支持的鉴权方式中包含优先级信息，则 BSF 根据当前网络支持的鉴权方式和已保存的 UE 所支持的鉴权方式，确定当前网络和该 UE 都支持的所有

鉴权方式，从所确定的鉴权方式中选择最高优先级的鉴权方式，即选择位于当前网络支持的鉴权方式列表中最前面的鉴权方式；

[0065] 如果 BSF 内预先配置有不同鉴权方式的优先级信息，则 BSF 根据当前网络支持的鉴权方式和已保存的 UE 所支持的鉴权方式，确定当前网络和该 UE 都支持的所有鉴权方式后，则按照自身的优先级信息，从所确定的鉴权方式中选择一种优先级最高的鉴权方式。如果 BSF 内没有预先配置有不同鉴权方式的优先级信息，则 BSF 再根据 HSS 返回的当前网络支持的鉴权方式中包含优先级信息确定鉴权方式，如果 HSS 返回的当前网络支持的鉴权方式中也未包含优先级信息，BSF 再随机选择鉴权方式。

[0066] 例如，BSF 已确定当前网络和该 UE 都支持的所有鉴权方式是 0001 和 0100，如果 BSF 没有配置鉴权方式优先级信息，且 BSF 知道 HSS 提供的鉴权方式列表中包含优先级信息，那么 BSF 就按照网络提供的鉴权能力列表中排在前面的鉴权方式进行选择，如果网络侧将 0001 排在了前面，那么 BSF 就选择 0001 作为最后确定的鉴权方式，如果 BSF 已配置鉴权方式 0100 为首选的鉴权方式，则 BSF 将选择 0100 作为最后选定的鉴权方式。

[0067] 步骤 306，UE 与 BSF 应用选定的鉴权方式，及鉴权信息与 UE 实现鉴权，鉴权成功后，BSF 根据自身已保存的 UE 的终端能力信息以及终端能力信息和所使用的鉴权方式是否一致，确定是否需要对密钥的格式进行转换，即 BSF 具有与用户终端相同的密钥转换能力。

[0068] 例如，如果 UE 是不同能力的用户卡手机的组合，那么 BSF 需要对鉴权后产生的密钥进行格式的转换。例如用户卡是 2G 的用户卡而手机是 3G 的手机终端，其采用编号为 0010 的鉴权方式鉴权后，产生的密钥是一个 64bit 的密钥，那么 3G 的手机终端在收到 64bit 的密钥后会将其主动的转换为 3G 需要使用的各自 128bit 的加密密钥 CK 和完整性 IK，这时 BSF 也需要将鉴权产生的 64bit 密钥转换为 128bit 密钥，这样才能与 UE 实现共享密钥。具体的转换方法与 3G 的手机终端转换方法相同，不再详细描述。

[0069] 如果 BSF 与 UE 执行的是 0010 的鉴权方式，且 BSF 根据该用户终端的终端能力信息，确定其用户设备即手机是 3G 的手机，那么 BSF 同样需要执行密钥转换的功能，将 64bits 的密钥转换为 128bits 密钥，即转换为加密密钥 CK 和完整性 IK 的形式。

[0070] 其它方式的用户卡和手机终端的组合，以及手机终端与鉴权方式的组合与此类似。总之，BSF 具有与用户终端相同的密钥转换能力，也就是说，BSF 判断是否需要转换以及具体的转换方法都与用户终端相同。

[0071] 步骤 307，BSF 给 UE 分配 B-TID。

[0072] 步骤 308，UE 使用 B-TID 与 NAF 进行通信。

[0073] 以上所述仅为一实施例，在实际应用中发起鉴权请求的实体是也可以是 AS。如果发起鉴权请求的实体是 AS，那么在步骤 306 中，就不存在密钥格式转换的步骤，在鉴权成功后，BSF 将直接为该 AS 分配一个用于业务请求的标识和一个用于认证查询标识，以便其后续应用。用于业务请求的标识和用于认证查询标识具体的应用过程分别与 B-TID 和 NAF 的标识的应用过程相同，在此不再详细描述。

[0074] 再有，BSF 自身也可以预先保存的当前网络支持的鉴权方式列表，并定期与 HSS 交互以更新该列表，这样，HSS 不需每次提供鉴权信息时都提供当前网络支持的鉴权方式列表，BSF 可以从自身预先保存的信息中获取当前网络支持的鉴权方式，从而避免在网络中经常重复传送大量相同的信息。

[0075] 总之，以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

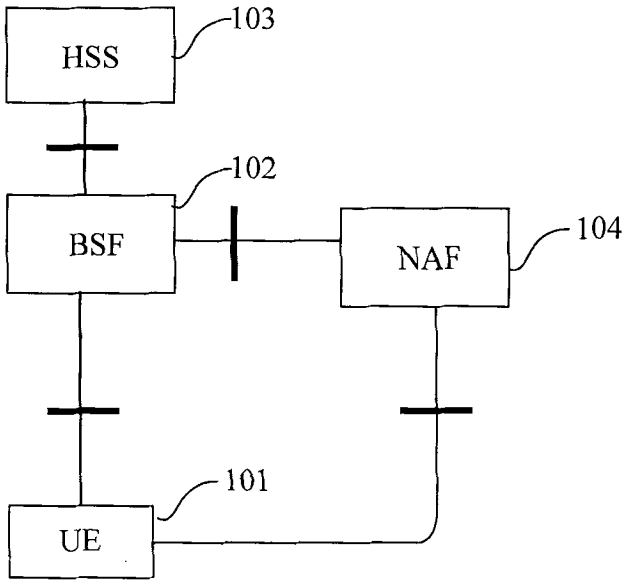

HSS
103
BSF
102
NAF
104
UE
101

图 1

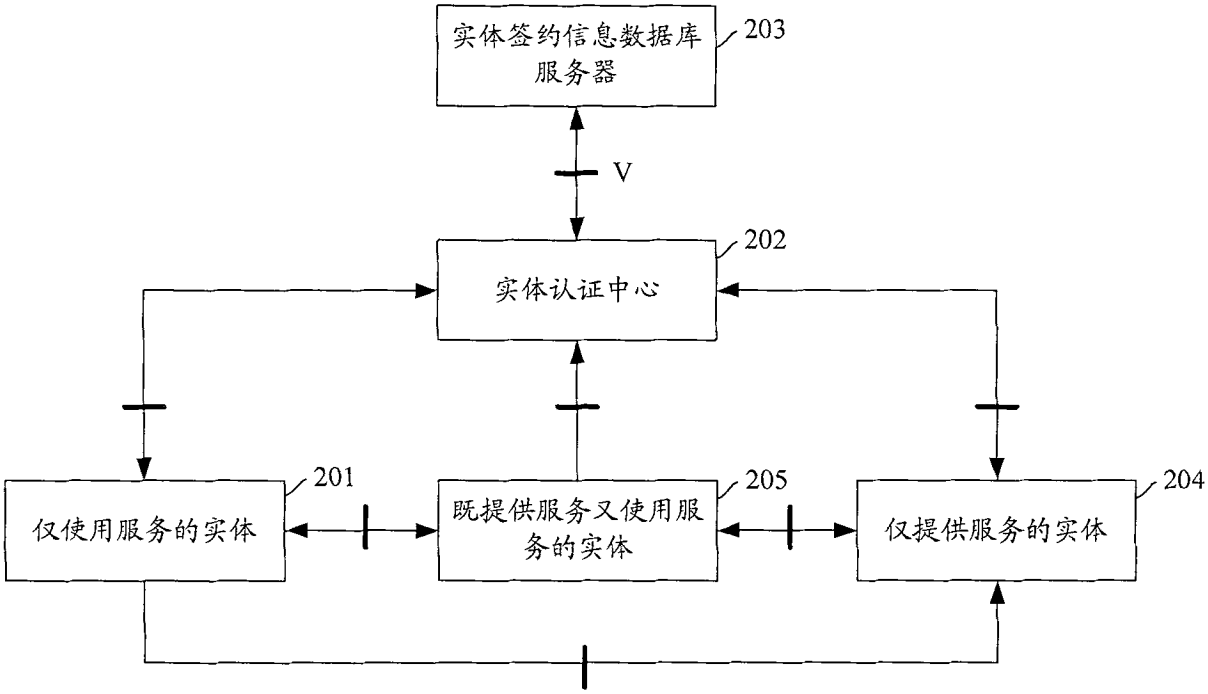

实体签约信息数据库
服务器
203
V
实体认证中心
202
仅使用服务的实体
201
既提供服务又使用服务的实体
205
仅提供服务的实体
204

图 2

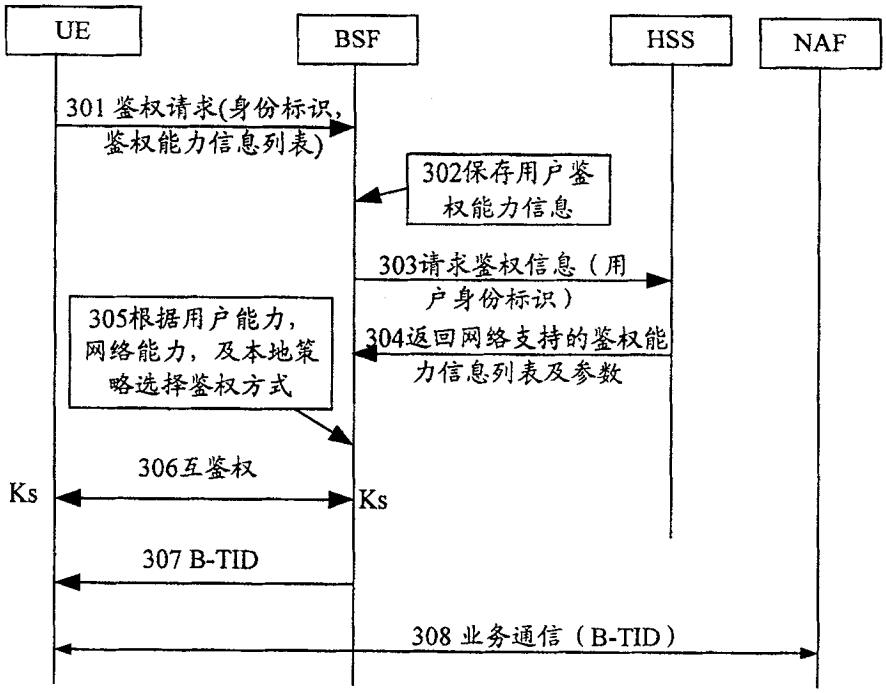

UE
BSF
HSS
NAF
301 鉴权请求(身份标识，鉴权能力信息列表)
302保存用户鉴权能力信息
303请求鉴权信息（用户身份标识）
304返回网络支持的鉴权能力信息列表及参数
305根据用户能力，网络能力，及本地策略选择鉴权方式
306互鉴权
Ks
Ks
307 B-TID
308 业务通信（B-TID）

图 3