[19] 中华人民共和国国家知识产权局

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

[12] 发明专利说明书

专利号 ZL 200410001029.8

[45] 授权公告日 2007 年 2 月 14 日

[11] 授权公告号 CN 1300976C

[22] 申请日 2004.1.16
[21] 申请号 200410001029.8
[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
[56] 参考文献
CN1458788A 2003.11.26
JP2003－337917A 2003.11.28
CN1280727A 2001.1.17
CN1462536A 2003.12.17
EP1365620A1 2003.11.26
审查员 向 琳

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 张颖玲 王 琦

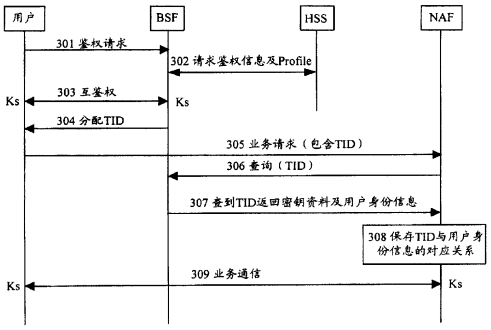
权利要求书 1 页 说明书 6 页 附图 2 页

[54] 发明名称

一种网络应用实体获取用户身份标识信息的方法

[57] 摘要

本发明提供了一种网络应用实体获取用户身份标识信息的方法，应用本发明，使 NAF 从 BSF 上获取了用户的身份标识信息，进而方便了 NAF 对用户的管理，如实现对用户进行计费和或访问控制。当 NAF 作为应用服务器代理时，能够在转发的消息中插入用户身份标识，使接收转发消息的应用服务器能够对用户进行识别。 本发明实现简便，且与现有的相关流程具有很好的兼容性。



1、一种网络应用实体获取用户身份标识信息的方法，其特征在于，该方法包括以下步骤：

a、BSF 预先保存通过鉴权用户的 TID，以及用户所应用的 TID 与该用户身份标识信息的对应关系；

b、当 BSF 接收到来自网络应用实体 NAF 的查询 TID 的消息时，判断本地是否保存有 NAF 所查询的 TID，如果有，则根据步骤 a 所述的对应关系获取该 TID 所对应的用户身份标识信息，并向 NAF 发送至少包含其所需要的 TID 和该 TID 所对应用户身份标识信息的成功的响应消息，由 NAF 将所述成功响应消息中的 TID 信息以及该 TID 所对应用户身份标识信息进行关联保存，否则 BSF 向 NAF 发送失败响应消息，并结束本处理流程。

2、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：预先设定关联保存的时间，当用户与 NAF 断开通信连接后，NAF 继续保存用户所应用的 TID 与该用户身份标识信息的对应关系，在超出预先设定的关联保存时间后，NAF 删除或禁用 TID 及该 TID 所对应的用户身份标识信息。

3、根据权利要求 2 所述的方法，其特征在于，所述预先设定的关联保存时间为 TID 的有效时间。

4、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：NAF 根据用户的身份标识信息，对该用户进行计费和或业务应用层的访问控制。

5、根据权利要求 1 所述的方法，其特征在于，所述用户身份标识信息为完整的 Profile 文件，或与用户身份标识相关的部分 Profile 文件，或为用户身份标识。

6、根据权利要求 5 所述的方法，其特征在于，该方法进一步包括：当 NAF 是应用服务器代理，并向其它应用服务器转发消息时，在转发的消息中插入用户身份标识。

一种网络应用实体获取用户身份标识信息的方法

技术领域

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框架中的网络应用实体获取用户身份标识信息的方法。

背景技术

在第三代无线通信标准中，通用鉴权框架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，应用通用鉴权框架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，例如多个服务和一个代理相连，这个通用鉴权框架把代理也当作一种业务来处理，组织结构可以很灵活，而且，对于以后新开发的业务也同样可以应用通用鉴权框架对应用业务的用户进行检查和验证身份。

图 1 所示为通用鉴权框架的结构示意图。通用鉴权框架通常由用户 101、执行用户身份初始检查验证的实体（BSF）102、用户归属网络服务器（HSS）103 和网络应用实体（NAF）104 组成。BSF 102 用于与用户 101 进行互验证身份，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 还兼有产生鉴权信息的功能。NAF104 可以是一个应用服务器，也可以是应用服务器的代理，当 NAF104 作为应用服务器的代理时，其后将连接应用服务器 105 和应用服务器 106 等多个应用服务器。

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，用户会首先和某个业务对应的 NAF

联系，如果该 NAF 应用通用鉴权框架需要用户到 BSF 进行身份验证，则通知用户应用通用鉴权框架进行身份验证，否则进行其它相应处理。

图 2 所示为现有技术的应用通用鉴权框架进行用户身份认证的流程图。

步骤 201，用户向 BSF 发送初始鉴权认证请求消息；

步骤 202，BSF 接收到用户的鉴权请求消息后，向 HSS 查询该用户的鉴权信息以及 Profile；

步骤 203，BSF 得到 HSS 发送的包含其所查信息的响应消息后，应用所查到的信息与用户执行鉴权和密钥协商协议（AKA）进行互鉴权，当 BSF 与用户完成 AKA 互鉴权，即相互认证了身份后，BSF 与用户之间就拥有了共享密钥 Ks；

步骤 204，BSF 给用户分配会话事务标识（TID），该 TID 对于每个用户是唯一的，且与共享密钥 Ks 相关联；

步骤 205，用户收到 BSF 分配的 TID 后，重新向 NAF 发送业务应用请求消息，该请求消息中包含 TID 信息；

步骤 206，NAF 接收到用户发送的包含 TID 信息的业务应用请求消息时，首先在 NAF 本地进行查询，如查询到，则直接执行步骤 208，否则，向 BSF 发送查询 TID 的消息；

步骤 207，BSF 接收到来自 NAF 的查询消息后，如查询到 NAF 所需的 TID，则向 NAF 发送成功的响应消息，NAF 将该消息中的内容保存后，执行步骤 208，否则 BSF 向 NAF 发送响应失败的查询消息，通知 NAF 没有该用户的信息，由 NAF 通知用户到 BSF 进行鉴权，并结束本处理流程；

该成功的响应消息中包括查到的 TID 以及该 TID 对应用户应用的共享密钥 Ks，或根据该 NAF 的安全级别由共享密钥 Ks 生成的衍生密钥，同时 NAF 和用户也共享了密钥 Ks 或其衍生密钥；

步骤 208，NAF 与用户进行正常的通信，并应用共享密钥 Ks 或由该共享密钥 Ks 衍生的密钥对以后的通信进行保护。

上述方案的缺陷在于：当 NAF 向 BSF 查询 TID 信息时，如果 BSF 能够查询到，则只是返回 TID 以及该 TID 对应用户应用的共享密钥 Ks，由共享密钥 Ks 生成的衍生密钥。而作为应用服务器或应用服务器代理的 NAF，没有获取用户身份标识信息的过程，因此，NAF 也就不能实现对用户计费信息的收集和或对业务层的访问进行控制。

发明内容

有鉴于此，本发明的目的在于提供一种网络应用实体获取用户身份标识信息的方法，使 NAF 能够获取用户的身份标识信息。

为达到上述目的，本发明的技术方案是这样实现的：

一种网络应用实体获取用户身份标识信息的方法，该方法包括以下步骤：

a、BSF 预先保存通过鉴权用户的 TID，以及用户所应用的 TID 与该用户身份标识信息的对应关系；

b、当 BSF 接收到来自网络应用实体 NAF 的查询 TID 的消息时，判断本地是否保存有 NAF 所查询的 TID，如果有，则根据步骤 a 所述的对应关系获取该 TID 所对应的用户身份标识信息，并向 NAF 发送至少包含其所需要的 TID 和该 TID 所对应用户身份标识信息的成功的响应消息，由 NAF 将所述成功响应消息中的 TID 信息以及该 TID 所对应用户身份标识信息进行关联保存，否则 BSF 向 NAF 发送失败响应消息，并结束本处理流程。

较佳地，该方法进一步包括：预先设定关联保存的时间，当用户与 NAF 断开通信连接后，NAF 继续保存用户所应用的 TID 与该用户身份标识信息的对应关系，在超出预先设定的关联保存时间后，NAF 删除或禁用 TID 及该 TID 所对应的用户身份标识信息。

较佳地，所述预先设定的关联保存时间为 TID 的有效时间。

较佳地，该方法进一步包括：NAF 根据用户的身份标识信息，对该用户进行计费和或业务应用层的访问控制。

较佳地，所述用户身份标识信息为完整的 Profile 文件，或与用户身份

标识相关的部分 Profile 文件，或为用户身份标识。

较佳地，该方法进一步包括：当 NAF 是应用服务器代理，并向其它应用服务器转发消息时，在转发的消息中插入用户身份标识。

应用本发明，使 NAF 从 BSF 上获取了用户的身份标识信息，进而方便了 NAF 对用户的管理，如实现对用户进行计费和或访问控制。当 NAF 作为应用服务器代理时，能够在转发的消息中插入用户身份标识信息，方便了接收转发消息的应用服务器对用户的识别，另外通过访问控制相应地减少了网络负荷，优化了网络资源。本发明实现简便，且与现有的相关流程具有很好的兼容性。

附图说明

图 1 所示为通用鉴权框架的结构示意图；

图 2 所示为现有技术的应用通用鉴权框架进行用户身份认证的流程图；

图 3 所示为本发明的应用通用鉴权框架进行用户身份认证的流程图。

具体实施方式

为使本发明的技术方案更加清楚，下面结合附图对本发明再做进一步的详细说明。

本发明的思路是：BSF 预先保存通过鉴权用户的 TID，以及用户所应用的 TID 与该用身份标识信息的对应关系；当 BSF 接收到来自 NAF 的查询 TID 的消息时，判断本地是否保存有 NAF 所查询的 TID，如果有，则根据上对应关系获取该 TID 所对应的用户身份标识信息，并向 NAF 发送至少包含其所需要的 TID 和该 TID 所对应用户身份标识信息的成功的响应消息，由 NAF 将所述成功响应消息中的 TID 信息以及该 TID 所对应用户身份标识信息进行关联保存，否则 BSF 向 NAF 发送失败响应消息，并结束本处理流程。

图 3 所示为应用本发明的应用通用鉴权框架进行用户身份认证的流程

图。

步骤 301，用户向 BSF 发送初始鉴权认证请求消息；

步骤 302，BSF 接收到用户的鉴权请求消息后，向 HSS 查询该用户的鉴权信息以及 Profile；

步骤 303，BSF 得到 HSS 发送的包含其所查信息的响应消息后，应用所查到的信息与用户进行 AKA 互鉴权，当 BSF 与用户完成 AKA 互鉴权，即相互认证了身份后，BSF 与用户之间就拥有了共享密钥 Ks；

步骤 304，BSF 给用户分配 TID，该 TID 对于每个用户是唯一的，且与共享密钥 Ks 相关联；

此时，BSF 保存了通过鉴权用户所应用的 TID，以及用户所应用的 TID 与该用户身份标识信息的对应关系，该用户身份标识信息是用户完整的 profile 文件，或与用户身份标识信息有关的部分 profile 文件，或仅为用户身份标识；

步骤 305，用户收到 BSF 分配的 TID 后，重新向 NAF 发送业务应用请求消息，该请求消息中包含 TID 信息；

步骤 306，NAF 接收到用户发送的包含 TID 信息的业务应用请求消息时，首先在 NAF 本地进行查询，如查询到，则直接执行步骤 309，否则，向 BSF 发送查询 TID 的消息，并执行步骤 307；

步骤 307，BSF 接收到来自 NAF 的查询消息后，如查询到 NAF 所需的 TID，则向 NAF 发送成功的响应消息，并执行步骤 308，否则 BSF 向 NAF 发送失败的响应消息，通知 NAF 没有该用户的信息，由 NAF 通知用户到 BSF 上进行鉴权，并结束本处理流程；

该成功的响应消息中不但包括查到的 TID 以及该 TID 对应用户应用的共享密钥 Ks，或根据该 NAF 的安全级别由共享密钥 Ks 生成的衍生密钥，而且还包括根据步骤 304 所述对应关系获取的该 TID 所对应的用户身份标识信息，同时 NAF 和用户也共享了密钥 Ks 或其衍生密钥；

步骤 308，NAF 将上述成功响应消息中的用户身份标识信息与该用户的 TID 信息进行关联保存；

步骤 309，NAF 与用户进行正常的通信，并应用共享密钥 Ks 或由该共享密钥 Ks 衍生的密钥对以后的通信进行保护，同时，根据用户的身份标识信息，对该用户进行计费和或业务应用层的访问控制。

当 NAF 作为应用服务器代理向其它应用服务器转发消息时，在其转发的消息中插入用户身份标识，以便收到转发消息的应用服务器能够识别用户。

另外，当用户要访问 NAF 后面的某个应用服务器时，NAF 可以根据自身保存的该用户的 profile 信息判断该用户是否已经定购其待访问业务，如果该用户未定购该业务，则 NAF 直接通知用户无权使用，而不需要将消息转发到后面的应用服务器，这样有效地优化了网络资源。

当用户和 NAF 断开通信连接后，NAF 继续保存该用户所应用的 TID 与该用户身份标识的对应关系，保存的时间通常为该 TID 的有效时间。因为在 TID 的有效时间内，用户可以继续使用该 TID 与 NAF 进行通信。当 TID 超时后，该用户的身份标识随着与其相对应的 TID 的删除而删除，或者，随着与其相对应的 TID 的禁用而被禁用。

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，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

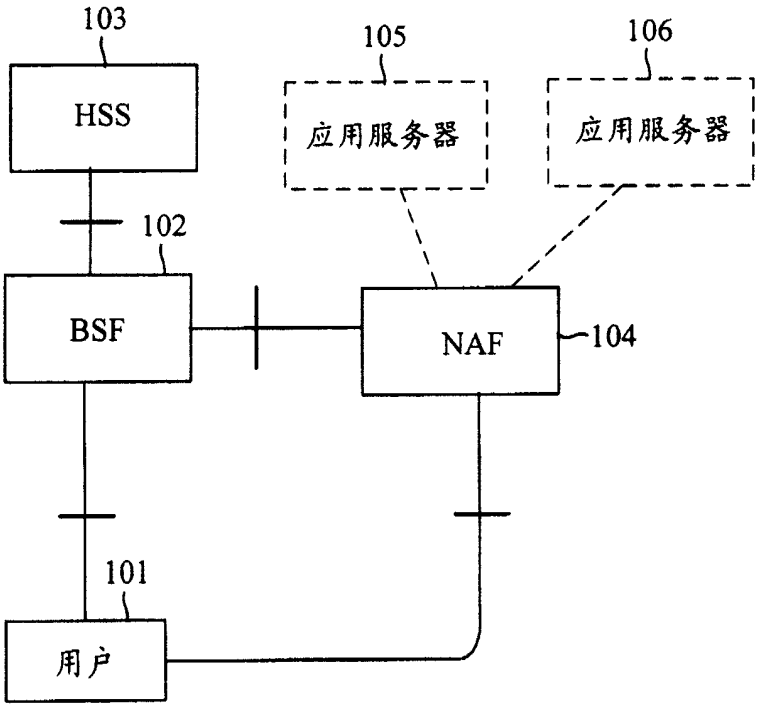


图 1

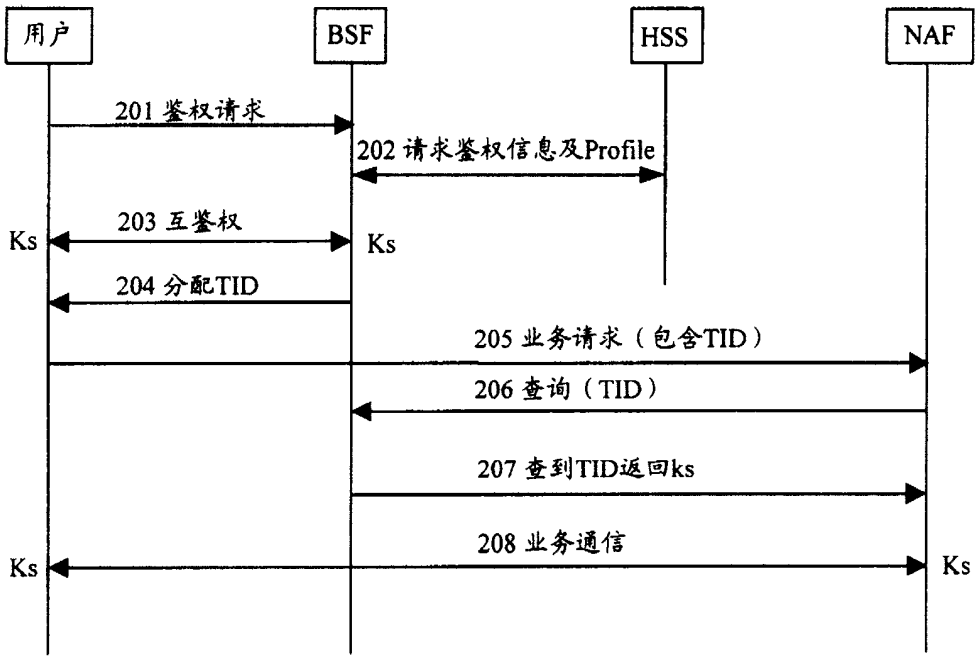

用户
BSF
HSS
NAF
201 鉴权请求
202 请求鉴权信息及Profile
Ks
203 互鉴权
Ks
204 分配TID
205 业务请求（包含TID）
206 查询（TID）
207 查到TID返回ks
208 业务通信
Ks
Ks

图 2

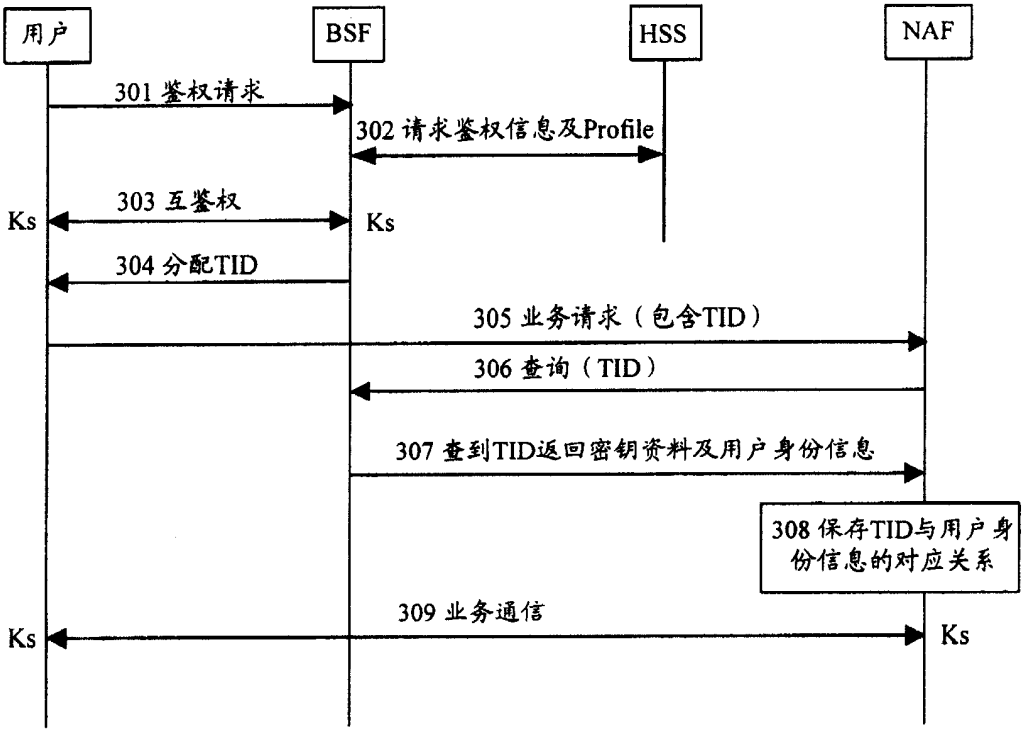

用户
BSF
HSS
NAF
301 鉴权请求
302 请求鉴权信息及Profile
Ks
303 互鉴权
Ks
304 分配TID
305 业务请求（包含TID）
306 查询（TID）
307 查到TID返回密钥资料及用户身份信息
308 保存TID与用户身份信息的对应关系
309 业务通信
Ks
Ks

图 3