(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 101052033 B
(45)授权公告日 2012.04.04

(21)申请号 200610074933.0

(22)申请日 2006.04.05

(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 范絮妍 李超 位继伟

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 章社杲 尚志峰

(51)Int.Cl.
*H04L 29/06*(2006.01)

(56)对比文件
GB 2384406 A,2003.07.23, 全文.
GB 2401013 A,2004.10.27, 全文.
CN 1694570 A,2005.11.09, 全文.
US 2004003287 A1,2004.01.01, 全文.
CN 1564514 A,2005.01.12, 全文.

审查员 李彦欣

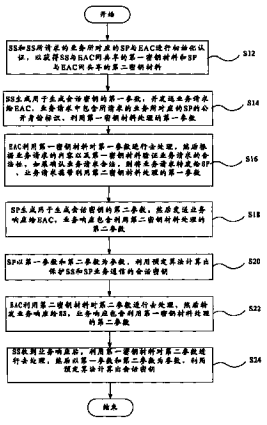
权利要求书 3 页 说明书 10 页 附图 5 页

(54)发明名称

基于TTP的认证与密钥协商方法及其装置

(57)摘要

一种认证与密钥协商方法，用于保护无线网络的通信安全，其包括以下步骤：步骤a，业务签约者生成用于生成会话密钥的第一参数，并发送包含第一参数的业务请求给实体认证中心，；步骤b，实体认证中心根据业务请求的内容将业务请求转发给业务请求所请求的业务所对应的业务提供者；步骤c，业务提供者生成用于生成会话密钥的第二参数，然后发送包含第二参数的业务响应给实体认证中心；步骤d，业务提供者以第一参数和第二参数为参数，利用预定算法计算出会话密钥；步骤e，实体认证中心转发业务响应给业务签约者；以及步骤f，业务签约者收到业务响应后以第一参数和第二参数为参数，利用预定算法计算出会话密钥。还提供了一种认证与密钥协商装置。




CN 101052033 B

1. 一种认证与密钥协商方法，用于保护无线网络的通信安全，其特征在于包括以下步骤：

步骤 a，业务签约者生成用于生成会话密钥的第一参数，并发送包含利用业务签约者与实体认证中心间共享的第一密钥材料处理的第一参数和所请求的业务所对应的业务提供者的公开身份标识的业务请求给实体认证中心；

步骤 b，所述实体认证中心利用所述第一密钥材料对所述第一参数进行去处理，根据所述业务请求的内容以及所述第一密钥材料确认所述业务请求合法，则将所述业务请求转发给所述业务提供者，所述业务请求携带利用业务提供者与实体认证中心间共享的第二密钥材料处理的第一参数；

步骤 c，所述业务提供者生成用于生成会话密钥的第二参数，发送包含利用所述第二密钥材料处理的所述第二参数的业务响应给所述实体认证中心；

步骤 d，所述业务提供者以所述第一参数和所述第二参数为参数，利用预定算法计算出保护所述业务签约者和所述业务提供者业务通信的会话密钥；

步骤 e，所述实体认证中心利用所述第二密钥材料对所述第二参数进行去处理，转发所述业务响应给所述业务签约者，所述业务响应包含利用所述第一密钥材料处理的第二参数；以及

步骤 f，所述业务签约者收到所述业务响应后，利用所述第一密钥材料对所述第二参数进行去处理，以所述第一参数和所述第二参数为参数，利用所述预定算法计算出会话密钥。

2. 根据权利要求 1 所述的认证与密钥协商方法，其特征在于还包括在执行步骤 a 之前执行以下步骤：

步骤 g，所述业务签约者和所述业务提供者与所述实体认证中心进行初始化认证，以获得所述业务签约者与所述实体认证中心间共享的第一密钥材料和所述业务提供者与所述实体认证中心间共享的第二密钥材料。

3. 根据权利要求 2 所述的认证与密钥协商方法，其特征在于，

在所述步骤 a 中，所述业务请求中还包含利用所述第一密钥材料处理的中间业务请求标识；以及

在所述步骤 c 中，所述业务响应还包含利用所述第二密钥材料处理的中间业务查询标识。

4. 根据权利要求 3 所述的认证与密钥协商方法，其特征在于还包括以下步骤：

步骤 h，所述实体认证中心收到所述步骤 a 所发送的所述业务请求后，利用所述第一密钥材料对所述中间业务请求标识进行去处理，并利用所述中间业务请求标识验证所述业务签约者身份的合法性，其中，

所述实体认证中心根据所述中间业务请求标识查找所述第一密钥材料以及所述业务签约者的真实身份，如果查找成功，证明所述业务签约者是合法用户，否则返回错误响应，以及

所述步骤 b 在所述步骤 h 确认所述业务签约者是合法用户后执行。

5. 根据权利要求 4 所述的认证与密钥协商方法，其特征在于，所述步骤 b 还包括以下步骤：

所述实体认证中心根据所述公开身份标识确定所述业务类型，利用所述业务签约者的

真实身份到签约信息数据库中查找所述业务签约者的签约信息确定该所述业务签约者是否签约了所述业务，如果没有则返回错误响应。

6. 根据权利要求 5 所述的认证与密钥协商方法，其特征在于还包括以下步骤：

步骤 i，所述实体认证中心根据所述公开身份标识找到所述第二密钥材料，并且到实体签约信息数据库中查找该所述业务提供者是否与所述无线网络签约提供所述业务，如果成功，则证明所述业务提供者身份合法，而且具有提供所述业务的权限，以及

所述步骤 b 在所述步骤 i 确认所述业务提供者身份合法后执行。

7. 根据权利要求 3 所述的认证与密钥协商方法，其特征在于还包括以下步骤：

步骤 j，所述实体认证中心收到所述步骤 c 发送的业务响应后，利用所述第二密钥材料对所述中间业务查询标识进行去处理，并利用所述中间业务查询标识验证所述业务提供者的真实身份，其中

所述实体认证中心将所述中间业务查询标识匹配所述公开身份标识，如果匹配成功，则证明所述业务提供者身份合法，否则返回错误响应，以及

所述步骤 e 在所述步骤 j 确认所述业务提供者身份合法后执行。

8. 根据权利要求 3 所述的认证与密钥协商方法，其特征在于还包括以下步骤：

步骤 k，所述实体认证中心收到所述步骤 a 发送的所述业务请求消息后，利用第一密钥材料对所述中间业务请求标识去处理，然后比较所去处理的所述中间业务请求标识是否与明文的所述中间业务请求标识一致，若一致，则确认所述第一参数未被篡改，否则返回错误响应，以及

所述步骤 b 在所述步骤 k 确认所述第一参数未被篡改后执行。

9. 根据权利要求 3 所述的认证与密钥协商方法，其特征在于还包括以下步骤：

步骤 l，所述业务提供者收到所述步骤 b 发送的所述业务请求消息后，利用所述第二密钥材料对所述中间业务请求标识进行去处理，然后比较所去处理的所述中间业务请求标识是否与明文的所述中间业务请求标识一致，若一致，则确认所述第一参数未被篡改，否则返回错误响应，以及

所述步骤 c 在所述步骤 l 确认所述第一参数未被篡改后执行。

10. 根据权利要求 1 至 8 中任一项所述的认证与密钥协商方法，其特征在于，

所述第一参数是所述业务签约者生成的第一随机数，或者所述第一随机数的预定函数；以及

所述第二参数是业务提供者生成的第二随机数，或者所述第二随机数的预定函数。

11. 根据权利要求 1 至 8 中任一项所述的认证与密钥协商方法，其特征在于，

所述第一密钥材料包括对称密钥、非对称密钥、密码算法、压缩算法、或安全关联中的至少一种；以及

所述第二密钥材料包括对称密钥、非对称密钥、密码算法、压缩算法、或安全关联中的至少一种。

12. 根据权利要求 1 至 8 中任一项所述的认证与密钥协商方法，其特征在于，还包括以下步骤：

所述业务签约者和所述业务提供者协商基于所述会话密钥的互认证方法。

13. 一种认证与密钥协商装置，用于保护无线网络的通信安全，其特征在于包括：

初始化模块，用于使业务签约者和所述业务签约者所请求的业务所对应的业务提供者与实体认证中心进行初始化认证，以获得所述业务签约者与所述实体认证中心间共享的第一密钥材料和所述业务提供者与所述实体认证中心间共享的第二密钥材料；

业务请求模块，用于使所述业务签约者生成用于生成会话密钥的第一参数，并发送业务请求给所述实体认证中心，所述业务请求中包含所请求的业务所对应的所述业务提供者的公开身份标识、利用所述第一密钥材料处理的所述第一参数；

请求转发模块，用于使所述实体认证中心利用所述第一密钥材料对所述第一参数进行去处理，然后根据所述业务请求的内容以及第一密钥材料验证所述业务请求的合法性，如果确认所述业务请求合法，则将所述业务请求转发给所述业务提供者，所述业务请求携带利用所述第二密钥材料处理的所述第一参数；

业务响应模块，用于使所述业务提供者生成用于生成会话密钥的第二参数，然后发送业务响应给所述实体认证中心，所述业务响应包含利用所述第二密钥材料处理的所述第二参数；

会话密钥第一生成模块，用于使所述业务提供者以所述第一参数和所述第二参数为参数，利用预定算法计算出保护所述业务签约者和所述业务提供者业务通信的会话密钥；

响应转发模块，用于使所述实体认证中心利用所述第二密钥材料对所述第二参数进行去处理，然后转发所述业务响应给所述业务签约者，所述业务响应包含利用所述第一密钥材料处理的所述第二参数；以及

会话密钥第二生成模块，用于使所述业务签约者收到所述业务响应后，利用所述第一密钥材料对所述第二参数进行去处理，然后以所述第一参数和所述第二参数为参数，利用所述预定算法计算出所述会话密钥。

# 基于 TTP 的认证与密钥协商方法及其装置

## 技术领域

[0001] 本发明涉及无线通信领域，更具体而言，涉及一种用于无线网络端到端通信安全的基于 TTP 的认证与密钥协商方法及其装置。

## 背景技术

[0002] 在无线网络业务端到端通信中，为了保护通信内容，人们发展了一种通信认证的方案。下面将参照图 1 来说明相关技术中无线网络业务端到端通信认证的方法。

[0003] 图 1 所示为相关技术的无线移动网络中的一种端到端通信认证框架 100 的示意图，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。涉及到的网络元素除了 3 种业务实体：SS 102(ServiceSubscriber，业务签约者）、SSP 104(Service Subscriber and Provider，既是业务签约者又是业务提供者）、SP 106(Service Provider，业务提供者）以外，在运营商网络中，还应该存在一个 EAC 108(EntityAuthentication Center，实体认证中心）和一个 ESD 110(EntitySubscription Database，实体签约信息数据库）。

[0004] 实体认证中心 (Entity Authentication Center，缩写为 EAC)108，是认证框架中的一个网络元素。其功能是完成认证协商，生成与业务实体间的共享秘密信息，接受认证查询，以及计算衍生密钥等。EAC 还应包括检测证书的功能，Kerberos 服务器的功能等；

[0005] 业务签约者 (Service subscriber，缩写为 SS)102，只能申请服务，一般为普通的移动用户；以及

[0006] 业务提供者 (Service Provider，缩写为 SP)106，是运营商网络的 AS(Application Server，应用服务器）或外部网络的 SP。

[0007] SP 106 在能够向其它实体提供业务，或者 SS 102 向其它实体请求业务之前，应该首先已经与网络存在签约关系，并将签约信息存放于 ESD 110 中。

[0008] 网络中每个 SS 102 与 SP 106 进行通信之前，应该先到 EAC 108 协商认证方式，并完成对身份的认证过程。

[0009] 认证方式的协商过程应该由业务实体发起，并在请求消息携带自身身份标识。EAC 108 根据本地策略情况和实体签约信息，选择一种认证方式，并将相应信息返回给认证请求者。请求者再发确认信息表示协商过程结束。

[0010] 接下来实体与 EAC 108 按照协商的方式进行认证。该认证应该是双向的。认证结束后，认证请求实体和 EAC 108 应该共享一个密钥，并且 EAC 108 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 102(SS 102/SSP 104)，则共享密钥为 Ks，EAC 108 将向其分配一个中间业务请求标识 (ISR-ID)。2) 如果该认证请求实体是 SP 106(SP106/SSP 104)，则共享密钥为 Kp，EAC 108 将向其分配一个中间业务查询标识 IAC-ID。

[0011] 最后 EAC 108 将业务实体的临时身份标识 ISR-ID 或 IAC-ID 以及有效期发送给请求认证的业务实体，此后该业务实体与 EAC 108 之间的通信都可以采用认证过程生成的业

务实体与 EAC 108 间的共享密钥 Ks 进行保护。

[0012] 认证建立的信任关系存在一个有效期。当快要过期或过了有效期时，业务实体需要到 EAC 108 之间进行重认证过程，建立新的信任关系。

[0013] 在 SS 102 向 SP 106 请求业务时，EAC 108 要查询二者的认证情况，确定二者身份是否合法以及是否有请求和提供某项业务的权限，并且帮助二者协商共享的衍生密钥。

[0014] 在相关技术中，提出了一种 Mediation 模型，用于实现相关技术中无线网络业务端到端通信认证。Mediation 模型是一种基于 TTP(Trusted Third Party，可信任第三方）的通信双方认证与密钥协商模型。TTP 是在认证模型中为通信双方所信任的一个权威机构，具有验证通信者的身份，为其分发会话密钥等功能。

[0015] 图 2 示出了相关技术的 Mediation 密钥协商模型 200 的方框图。

[0016] 如图 2 所示，Mediation 密钥协商模型 200 包括可信任第三方 (TTP)202，业务请求者 204，以及业务提供者 206 ；其密钥协商的过程如下 ：

[0017] 在步骤 S102 中，业务请求者 204 向业务提供者 206 请求服务时，首先向可信任第三方 202 发起服务请求，携带业务请求者 204 和业务提供者 206 的身份标识等参数 ；

[0018] 在步骤 S104 中，可信任第三方 202 验证对应业务请求者 204 的身份，认证通过后，向对应的业务提供者 206 转发业务请求 ；

[0019] 在步骤 S106 中，业务提供者 206 响应可信任第三方 202 转发来的业务请求 ；以及

[0020] 在步骤 S108 中，可信任第三方 202 转发业务响应给业务提供者 206，生成业务提供者 206 和业务请求者 204 之间的会话密钥，并分发给业务提供者 206 和业务请求者 204。

[0021] 然而，从以上的描述中可以看到，当将 Mediation 密钥协商模型应用于通信认证时，还存在以下问题 ：

[0022] 在上述的步骤 S108 中，由于可信任第三方在分发密钥前没有完全认证业务请求者和提供者的身份，所以给攻击者留下了空挡，使得攻击者可以冒充其中一方进行攻击。另外，分发密钥时，会话密钥在传输过程中有可能被截获并被破解，导致双方通信受到安全威胁。

[0023] 在相关技术中提出了一种 Diffie-Hellman 密钥交换协议，目的是使会话的双方能够安全地交换密钥。Diffie-Hellman 密钥交换协议规定如下 ：

[0024] 假设 p 是一个大素数，a 是 GF(p) 的一个本原元，且 p 和 a 是公开的。共有两个参与协议的主题 A 和 B，协议的目标是使他们能够安全地交换密钥，在协议结束时可以分别获得一个共享的会话密钥 Kab。

[0025] (1)A 随机地选择 Xa，$0 \leqslant Xa \leqslant p-2$ ；

[0026] (2)A 计算 $Ya = a^{Xa} \bmod p$，并发送 Ya 给 B ；

[0027] (3)B 随机地选择 Xb，$0 \leqslant Xb \leqslant p-2$ ；

[0028] (4)B 计算 $Yb = a^{Xb} \bmod p$，并发送 Yb 给 A ；

[0029] (5)A 计算 $Kab = Yb^{Xa} \bmod p = a^{XbXa} \bmod p$ ；

[0030] (6)B 计算 $Kab = Ya^{Xb} \bmod p = a^{XaXb} \bmod p$。

[0031] 然而，从以上的描述中可以看到，Diffie-Hellman 密钥交换协议不能抵抗如下的“中间人 (man-in-the-middle)”攻击 ：

[0032] 假设攻击者是 P ；

[0033] (1)P 随机地选择 Xp,0 ≤ Xp ≤ p-2,并计算 $Yp = a^{Xp} \bmod p$;

[0034] (2)A 计算 $Ya = a^{Xa} \bmod p$,并发送 Ya 给 B;

[0035] (3)P 中途拦截 $Ya = a^{Xa} \bmod p$,并发送 Yp 给 B;

[0036] (4)B 计算 $Yb = a^{Xb} \bmod p$,并发送 Yb 给 A;

[0037] (5)P 中途拦截 $Yb = a^{Xb} \bmod p$,并发送 Yp 给 A。

[0038] 中间人攻击的结果是:A 实际上和攻击者 P 之间建立了秘密密钥 Kap。当 A 加密一个消息发送给 B 时,P 能解密它而 B 不能。

[0039] 因此,人们需要提供一种解决方案,能够解决上述相关技术中的问题。

## 发明内容

[0040] 本发明提出了一种基于 TTP 的认证与密钥协商模型,其基本上克服了由于现有技术的局限和缺陷而造成的一个或多个问题,既能够认证通信双方的身份,又能够安全地获得共享密钥,而且密钥的生成需要通信双方参与,增强了共享密钥的安全性。

[0041] 根据本发明的一个方面,提供了一种认证与密钥协商方法,用于保护无线网络的通信安全,其特征在于包括以下步骤:步骤 a,业务签约者生成用于生成会话密钥的第一参数,并发送包含利用业务签约者与实体认证中心间共享的第一密钥材料处理的第一参数和所请求的业务所对应的业务提供者的公开身份标识的业务请求给实体认证中心;步骤 b,所述实体认证中心利用所述第一密钥材料对所述第一参数进行去处理,根据所述业务请求的内容以及所述第一密钥材料确认所述业务请求合法,则将所述业务请求转发给所述业务提供者,所述业务请求携带利用业务提供者与实体认证中心间共享的第二密钥材料处理的第一参数;步骤 c,业务提供者生成用于生成会话密钥的第二参数,发送包含利用所述第二密钥材料处理的第二参数的业务响应给实体认证中心;步骤 d,业务提供者以第一参数和第二参数为参数,利用预定算法计算出保护所述业务签约者和所述业务提供者业务通信的会话密钥;步骤 e,实体认证中心利用所述第二密钥材料对所述第二参数进行去处理,转发业务响应给业务签约者,所述业务响应包含利用所述第一密钥材料处理的第二参数;以及步骤 f,业务签约者收到业务响应后,利用所述第一密钥材料对所述第二参数进行去处理,以第一参数和第二参数为参数,利用预定算法计算出会话密钥。

[0042] 在上述的认证与密钥协商方法中,还包括以下步骤:步骤 g,业务签约者和业务提供者与实体认证中心进行初始化认证,以获得业务签约者与实体认证中心间共享的第一密钥材料和业务提供者与实体认证中心间共享的第二密钥材料。

[0043] 在上述的认证与密钥协商方法中,在步骤 a 中,业务请求中还包含利用第一密钥材料处理的中间业务请求标识;以及在步骤 c 中,业务响应还包含利用第二密钥材料处理的中间业务查询标识。

[0044] 在上述的认证与密钥协商方法中,还包括以下步骤:步骤 h,实体认证中心收到步骤 a 所发送的业务请求后,利用第一密钥材料对中间业务请求标识进行去处理,并利用中间业务请求标识验证业务签约者身份的合法性,其中,实体认证中心根据中间业务请求标识查找第一密钥材料以及业务签约者的真实身份,如果查找成功,证明业务签约者是合法用户,否则返回错误响应,以及步骤 b 在步骤 h 确认业务签约者是合法用户后执行。

[0045] 在上述的认证与密钥协商方法中,步骤 b 还包括以下步骤:实体认证中心根据公

开身份标识确定业务类型，利用业务签约者的真实身份到签约信息数据库中查找业务签约者的签约信息确定该业务签约者是否签约了业务，如果没有则返回错误响应。

[0046] 在上述的认证与密钥协商方法中，还包括以下步骤：步骤 i，实体认证中心根据公开身份标识找到第二密钥材料，并且到实体签约信息数据库中查找该业务提供者是否与无线网络签约提供业务，如果成功，则证明业务提供者身份合法，而且具有提供业务的权限，以及步骤 b 在步骤 i 确认业务提供者身份合法后执行。

[0047] 在上述的认证与密钥协商方法中，还包括以下步骤：步骤 j，实体认证中心收到步骤 c 发送的业务响应后，利用第二密钥材料对中间业务查询标识进行去处理，并利用中间业务查询标识验证业务提供者的真实身份，其中实体认证中心将中间业务查询标识匹配公开身份标识，如果匹配成功，则证明业务提供者身份合法，否则返回错误响应，以及步骤 e 在步骤 j 确认业务提供者身份合法后执行。

[0048] 在上述的认证与密钥协商方法中，还包括以下步骤：步骤 k，实体认证中心收到步骤 a 发送的业务请求消息后，利用第一密钥材料对中间业务请求标识去处理，然后比较所去处理的中间业务请求标识是否与明文的中间业务请求标识一致，若一致，则确认第一参数未被篡改，否则返回错误响应，以及步骤 b 在步骤 k 确认第一参数未被篡改后执行。

[0049] 在上述的认证与密钥协商方法中，还包括以下步骤：步骤 l，业务提供者收到步骤 b 发送的业务请求消息后，利用第二密钥材料对中间业务请求标识进行去处理，然后比较所去处理的中间业务请求标识是否与明文的中间业务请求标识一致，若一致，则确认第一参数未被篡改，否则返回错误响应，以及步骤 c 在步骤 l 确认第一参数未被篡改后执行。

[0050] 在上述的认证与密钥协商方法中，第一参数是业务签约者生成的第一随机数，或者第一随机数的预定函数；以及第二参数是业务提供者生成的第二随机数，或者第二随机数的预定函数。

[0051] 在上述的认证与密钥协商方法中，第一密钥材料包括对称密钥、非对称密钥、密码算法、压缩算法、或安全关联中的至少一种；以及第二密钥材料包括对称密钥、非对称密钥、密码算法、压缩算法、或安全关联中的至少一种。

[0052] 在上述的认证与密钥协商方法中，还包括以下步骤：业务签约者和业务提供者协商基于会话密钥的互认证方法。

[0053] 根据本发明的另一方面，提供了一种认证与密钥协商装置，用于保护无线网络的通信安全，其特征在于包括：初始化模块，用于使业务签约者和业务签约者所请求的业务所对应的业务提供者与实体认证中心进行初始化认证，以获得业务签约者与实体认证中心间共享的第一密钥材料和业务提供者与实体认证中心间共享的第二密钥材料；业务请求模块，用于使业务签约者生成用于生成会话密钥的第一参数，并发送业务请求给实体认证中心，业务请求中包含所请求的业务所对应的业务提供者的公开身份标识、利用第一密钥材料处理的第一参数；请求转发模块，用于使实体认证中心利用第一密钥材料对第一参数进行去处理，然后根据业务请求的内容以及第一密钥材料验证业务请求的合法性，如果确认业务请求合法，则将业务请求转发给业务提供者，业务请求携带利用第二密钥材料处理的第一参数；业务响应模块，用于使业务提供者生成用于生成会话密钥的第二参数，然后发送业务响应给实体认证中心，业务响应包含利用第二密钥材料处理的第二参数；会话密钥第一生成模块，用于使业务提供者以第一参数和第二参数为参数，利用预定算法计算出保护

业务签约者和业务提供者业务通信的会话密钥；响应转发模块，用于使实体认证中心利用第二密钥材料对第二参数进行去处理，然后转发业务响应给业务签约者，业务响应包含利用第一密钥材料处理的第二参数；以及会话密钥第二生成模块，用于使业务签约者收到业务响应后，利用第一密钥材料对第二参数进行去处理，然后以第一参数和第二参数为参数，利用预定算法计算出会话密钥。

[0054] 通过上述技术方案，本发明实现了如下技术效果：

[0055] 本发明提出了一种基于 TTP 的认证与密钥协商方法，通信双方通过可信任的第三方交换密钥材料生成共享密钥。本发明使得共享密钥直接由通信双方产生无需传输，从而有效防止了密钥的中途拦截以及泄漏；另外，本发明中加入了 TTP 来认证通信双方的身份，从而有效地防止了中间人攻击。

[0056] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

## 附图说明

[0057] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0058] 图 1 示出了相关技术的无线移动网络中的一种端到端通信认证框架的示意图；

[0059] 图 2 示出了相关技术的 Mediation 的密钥协商模型的方框图；

[0060] 图 3 示出了根据本发明的无线网络端到端通信认证方法的流程图；

[0061] 图 4 示出了根据本发明的无线网络端到端通信认证装置的方框图；

[0062] 图 5 示出了根据本发明的另一个实施例的无线网络端到端通信认证方法的流程图；以及

[0063] 图 6 示出了根据本发明的另一个实施例的 Diffie-Hellman 密钥交换实施例的流程图。

## 具体实施方式

[0064] 下面将参考附图详细说明本发明。

[0065] 下面图 3 和图 4 说明本发明的原理。

[0066] 从以上相关技术的描述中可以看出，基于 TTP 的认证与协商模型，通过加入了 TTP 来认证通信双方的身份，可以有效地防止 Diffie-Hellman 密钥交换协议中发生的中间人攻击的问题。另外，从以上相关技术的描述中可以看出，借鉴 Diffie-Hellman 密钥交换协议的思想，可以有效地解决基于 TTP 的认证与协商模型中分发密钥时，会话密钥在传输过程中有可能被截获并被破解的缺陷。

[0067] 因此，本发明提出了一种解决方案：在基于 TTP 的认证与协商模型中采用 Diffie-Hellman 密钥交换协议的思想，使得共享密钥直接由通信双方本地产生而无需传输，从而解决了上述相关技术中的一个或多个问题。

[0068] 图 3 示出了根据本发明的无线网络端到端通信认证方法的流程图；以及图 4 示出了根据本发明的无线网络端到端通信认证装置的方框图。

[0069] 具体来说，如图 3 所示，在图 1 所示的无线移动网络端到端通信认证框架中，根据本发明的原理的无线网络端到端通信认证方法包括以下步骤：

[0070] 在步骤 S12 中，SS 和 SS 所请求的业务所对应的 SP 与 EAC 进行初始化认证，以获得 SS 与 EAC 间共享的第一密钥材料和 SP 与 EAC 间共享的第二密钥材料；

[0071] 在步骤 S14 中，SS 生成用于生成会话密钥的第一参数，并发送业务请求给 EAC，业务请求中包含所请求的业务所对应的 SP 的公开身份标识、利用第一密钥材料处理的第一参数；

[0072] 在步骤 S16 中，EAC 利用第一密钥材料对第一参数进行去处理，然后根据业务请求的内容以及第一密钥材料验证业务请求的合法性，如果确认业务请求合法，则将业务请求转发给 SP，业务请求携带利用第二密钥材料处理的第一参数；

[0073] 在步骤 S18 中，SP 生成用于生成会话密钥的第二参数，然后发送业务响应给 EAC，业务响应包含利用第二密钥材料处理的第二参数；

[0074] 在步骤 S20 中，SP 以第一参数和第二参数为参数，利用预定算法计算出保护 SS 和 SP 业务通信的会话密钥；

[0075] 在步骤 S22 中，EAC 利用第二密钥材料对第二参数进行去处理，然后转发业务响应给 SS，业务响应包含利用第一密钥材料处理的第二参数；以及

[0076] 在步骤 S24 中，SS 收到业务响应后，利用第一密钥材料对第二参数进行去处理，然后以第一参数和第二参数为参数，利用预定算法计算出会话密钥。

[0077] 所述的利用第一密钥材料处理的第一参数，以及利用第二密钥材料处理的第二参数，是指运用某种密码算法保护第一参数和第二参数的机密性以及完整性、不可否认性等。

[0078] 密钥材料可以是对称密钥、非对称密钥、密码算法、压缩算法、或安全关联等。

[0079] 可选地，SS 和 SP 在业务通信前协商基于所述会话密钥的互认证方法，并在认证过程中生成进一步的针对本次业务通信的会话密钥。

[0080] 具体来说，如图 4 所示，在图 1 所示的无线移动网络端到端通信认证框架中，根据本发明的原理的无线网络端到端通信认证装置 300 包括：

[0081] 初始化模块 302，用于使 SS 和 SS 所请求的业务所对应的 SP 与 EAC 进行初始化认证，以获得 SS 与 EAC 间共享的第一密钥材料和 SP 与 EAC 间共享的第二密钥材料；

[0082] 业务请求模块 304，用于使 SS 生成用于生成会话密钥的第一参数，并发送业务请求给 EAC，业务请求中包含所请求的业务所对应的 SP 的公开身份标识、利用第一密钥材料处理的第一参数；

[0083] 请求转发模块 306，用于使 EAC 利用第一密钥材料对第一参数进行去处理，然后根据业务请求的内容以及第一密钥材料验证业务请求的合法性，如果确认业务请求合法，则将业务请求转发给 SP，业务请求携带利用第二密钥材料处理的第一参数；

[0084] 业务响应模块 308，用于使 SP 生成用于生成会话密钥的第二参数，然后发送业务响应给 EAC，业务响应包含利用第二密钥材料处理的第二参数；

[0085] 会话密钥第一生成模块 310，用于使 SP 以第一参数和第二参数为参数，利用预定算法计算出保护 SS 和 SP 业务通信的会话密钥；

[0086] 响应转发模块 312，用于使 EAC 利用第二密钥材料对第二参数进行去处理，然后转发业务响应给 SS，业务响应包含利用第一密钥材料处理的第二参数；以及

[0087] 会话密钥第二生成模块 314，用于使 SS 收到业务响应后，利用第一密钥材料对第二参数进行去处理，然后以第一参数和第二参数为参数，利用预定算法计算出会话密钥。

[0088] 下面参照图 5 来说明本发明的一个实施例，图 5 示出了根据本发明的另一个实施例的无线网络端到端通信认证方法的流程图。

[0089] 具体来说，如图 5 所示，在图 1 所示的无线移动网络端到端通信认证框架中，根据本发明的一个实施例的无线网络端到端通信认证方法包括以下步骤：

[0090] 在步骤 S202 中，SS 和 SP 作为业务签约者和业务提供者需要首先和 EAC 进行初始化认证，认证成功后获得其与 EAC 共享的密钥 Ks(SS 和 EAC 间的共享密钥）或 Kp(SP 和 EAC 间的共享密钥），其中，Ks 和 Kp 用于保护会话密钥资料的传输，以及二者的身份信息，如果 SS 需要某个 SP 的服务，则 SS 需要通过 EAC 与该 SP 建立联系，以确认双方身份的合法性，并彼此交换会话密钥的生成参数；

[0091] 在步骤 S204 中，首先，SS 生成一个随机数 Ns，并发送业务请求给 EAC，消息中携带 SS 的 ISR-ID，提供业务的 SP 的 UID(PublicIdentity，公开身份标识），以及由 Ks 加密的随机数 Ns（或经过某种运算后的 Ns’ = f(Ns)）和 ISR-ID，其中 Ns 用于将来生成会话密钥；

[0092] 在步骤 S206 中，EAC 收到业务请求消息后根据 ISR-ID 查找有效的共享密钥 Ks 以及 SS 的真实身份（如 IMSI(International MobileSubscriber Identity，国际移动用户标识)），如果查找成功，证明该 SS 已通过身份认证是合法用户，否则返回错误响应；

[0093] 在步骤 S208 中，EAC 根据 UID 确定业务类型，利用 SS 的真实身份到 ESD 中查找 SS 的签约信息确定该 SS 是否签约了此项业务，如果没有则返回错误响应；

[0094] 在步骤 S210 中，上述查找成功后，EAC 利用 Ks 解密随机数 Ns 或 Ns’以及 ISR-ID，若该 ISR-ID 与明文的 ISR-ID 一致证明随机数未被篡改，否则返回错误响应；

[0095] 在步骤 S212 中，EAC 根据 UID 找到 SP 与 EAC 有效的共享密钥 Kp，并且到 ESD 中查找该 SP 是否与网络签约提供此项业务，如果成功，证明该 SP 已通过了 EAC 的身份认证，身份合法，而且具有提供此项业务的权限；

[0096] 在步骤 S214 中，然后，EAC 将 SS 的业务请求转发给 SP，其中的随机数 Ns 或 Ns’以及 ISR-ID 由 Kp 加密，否则返回错误响应；

[0097] 在步骤 S216 中，SP 收到业务请求消息后，用 Kp 解密 Ns，Ns’，以及 ISR-ID，与明文 ISR-ID 比对一致证明无篡改，否则返回业务请求失败响应；

[0098] 在步骤 S218 中，SP 产生随机数 Np，发送业务响应给 EAC，消息携带 IAC-ID 以及由 Kp 加密的 Np（或经过某种运算后的 Np’ = f(Np)）以及 UID，其中 Np（或者 Np’）用于将来生成会话密钥；

[0099] 在步骤 S220 中，SP 以 Ns 和 Np（或 Ns’和 Np’）为参数，利用某种算法计算出保护 SS 和 SP 业务通信的会话密钥 Ksp；

[0100] 在步骤 S222 中，EAC 收到业务响应后，匹配 IAC-ID 和 UID 如果他们都代表同一 SP，则转发响应给 SS，并将 Np 或 Np’以及 UID 由 Ks 加密；

[0101] 在步骤 S224 中，SS 收到响应后，解密获得随机数 Np 或 Np’并验证 UID 的一致性，成功后，利用与 SP 相同的算法和参数生成会话密钥 Ksp。

[0102] 这样 SS 和 SP 就共享了会话密钥 Ksp。他们可以利用 Ksp 进行进一步的认证或加密通信。

[0103] 另外，在上述的过程中，通过步骤S206和步骤S212实现了EAC对SS和SP的身份认证，从而解决了相关技术中可信任第三方在分发密钥前没有完全认证业务请求者和提供者的身份的问题。

[0104] 下面参照图6来说明本发明的一个实施例。

[0105] 图6示出了根据本发明的一个实施例的Diffie-Hellman密钥交换实施例的流程图。

[0106] 本实施例是一个改进的Diffie-Hellman密钥交换实施例，假设p是一个大素数，a是GF(p)的一个本原元，且p和a是公开的。共有两个参与协议的主体除了业务签约者SS和业务请求者SP之外，还有充当可信任第三方TTP功能的EAC(实体认证中心)

[0107] 如图6所示，其过程如下：

[0108] 在步骤S302中，首先，业务签约者SS随机地选择一个随机数Ns，$0 \leqslant Ns \leqslant p-2$，计算$Ns' = a^{Ns} \bmod p$，并发送业务请求给EAC，消息中携带SS的ISR-ID，提供业务的SP的UID，以及由Ks加密的Ns'和ISR-ID；

[0109] 在步骤S304中，EAC收到业务请求消息后根据ISR-ID查找有效的共享密钥Ks以及SS的真实身份(如IMSI)，如果查找成功，证明该SS已通过身份认证是合法用户，否则返回错误响应。EAC根据UID确定业务类型，利用SS的真实身份到ESD(实体签约信息数据库)中查找SS的签约信息确定该SS是否签约了此项业务，如果没有则返回错误响应。

[0110] 上述查找成功后，EAC利用Ks解密Ns'以及ISR-ID，若该ISR-ID与明文的ISR-ID一致证明随机数未被篡改，否则返回错误响应。

[0111] EAC根据UID找到SP与EAC有效的共享密钥Kp，并且到ESD中查找该SP是否与网络签约提供此项业务；如果成功，证明该SP已通过了EAC的身份认证，身份合法，而且具有提供此项业务的权限。

[0112] 在步骤S306中，如果上述验证成功，则EAC将SS的业务请求转发给SP，其中Ns'以及ISR-ID由Kp加密。否则EAC向SS返回请求失败响应。

[0113] 在步骤S308中，SP收到业务请求消息后，用Kp解密Ns'，以及ISR-ID，与明文ISR-ID比对一致证明无篡改，否则返回业务请求失败响应。

[0114] SP产生随机数Np，$0 \leqslant Np \leqslant p-2$，计算$Np' = a^{Np} \bmod p$，SP计算$Ksp = Ns'^{Np} \bmod p = a^{NsNp} \bmod p$，将Ksp作为保护SS和SP业务通信的会话密钥Ksp。

[0115] 在步骤S310中，SP发送业务响应给EAC，消息携带IAC-ID以及由Kp加密的Np'以及UID。

[0116] 在步骤S312中，EAC收到业务响应后，解密获得Np'和UID，并匹配IAC-ID和UID，判断他们是否代表同一SP。

[0117] 在步骤S314中，如果匹配成功，则EAC转发业务响应给SS，并将Np'以及UID由Ks加密；否则向SP返回错误指示；

[0118] 在步骤S316中，SS收到响应后，解密获得Np'并验证UID的一致性，成功后，计算$Ksp = Np' \bmod Ns = a^{NpNs} \bmod p$。

[0119] 这样SS和SP就共享了会话密钥Ksp。他们可以利用Ksp进行进一步的认证或加密通信。

[0120] 因此，本发明实现了如下技术效果：

[0121] 本发明提出了一种基于 TTP 的认证与密钥协商方法，通信双方通过可信任的第三方交换密钥材料生成共享密钥。本发明使得共享密钥直接由通信双方产生无需传输，从而有效防止了密钥的中途拦截以及泄漏；另外，本发明中加入了 TTP 来认证通信双方的身份，从而有效地防止了中间人攻击。

[0122] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。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。

[0123] 缩略语和关键术语定义

[0124] EAC Entity Authentication Center（实体认证中心）

[0125] ESD Entity Subscription Database（实体签约数据库）

[0126] ISR-ID Interim Service Request Identifier（中间业务请求标识）

[0127] IAC-ID Interim Authentication Check Identifier（中间业务查询标识）

[0128] PID Private Identity（私有身份标识）

[0129] UID Public Identity（公开身份标识）

[0130] SP Service Provider（业务提供者）

[0131] SS Service Subscriber（业务签约者）

[0132] SSP Service Subscriber and Provider（既是业务签约者又是业务提供者）

[0133] TTP Trusted Third Party（可信任第三方）

[0134] 密钥：在信息加密或解密的过程中必须使用的一种数据。

[0135] 共享密钥 Ks：由业务实体到 EAC 完成认证和密钥协商过程生成，是业务实体与 EAC 之间的共享密钥。

[0136] 实体衍生密钥：在端到端业务通信中，为了保护业务签约者和业务提供者间的业务通信而生成的一种共享密钥，是由业务签约者与 EAC 的共享密钥 Ks 以及实体的身份信息等导出的。

[0137] 实体认证中心 (EAC)：是认证框架中的一个网络元素。其功能是完成认证协商，生成与业务实体间的共享秘密信息，接受认证查询，以及计算衍生密钥等。EAC 还应包括检测证书的功能，Kerberos 服务器的功能等。

[0138] 实体签约信息数据库 (ESD)：包括该实体签约的服务，或该实体提供的服务，或该实体既签约服务又能提供的服务等等，以及该实体支持的认证方式及认证资料等。实体的签约信息应该与实体的私有身份标识一起保存。

[0139] 业务签约者 (SS)：他只能申请服务。一般为普通的移动用户。

[0140] 既是业务签约者又是业务提供者 (SSP)：可以是普通的移动用户，也可以是第三方的 AS(Application Server)

[0141] 业务提供者 (SP)：运营商网络的 AS 或外部网络的 SP。

[0142] 业务实体：业务提供者与业务签约者的统称，包括 SS、SSP、SP 三种类型。

[0143] 中间业务请求标识 (ISR-ID)：实体认证中心为用户 (SS/SSP) 分配的临时身份标识，该标识是在用户向其它实体请求业务时使用。

[0144] 中间业务查询标识 (IAC-ID)：实体认证中心为业务提供者 (SP/SSP) 分配的临时身份标识，该标识是实体需要向 EAC 查询业务签约者的认证情况时使用。

[0145] 私有身份标识 (PID) :业务实体的真实身份标识,该标识信息属于实体私密信息,只有 EAC 和 ESD 有权获得。

[0146] 公开身份标识 (UID) :业务实体的公开身份,该标识信息是与其它实体联系的身份标识。同一业务实体提供不同的业务应该对应不同的 UID( 即 UID 能够区分出不同的业务 )。

[0147] 可信任第三方 (TTP) :在认证模型中为通信双方所信任的一个权威机构,具有验证通信者的身份,为其分发会话密钥等功能。

[0148] Mediation 模型 :一种基于 TTP 的通信双方认证与密钥协商模型。

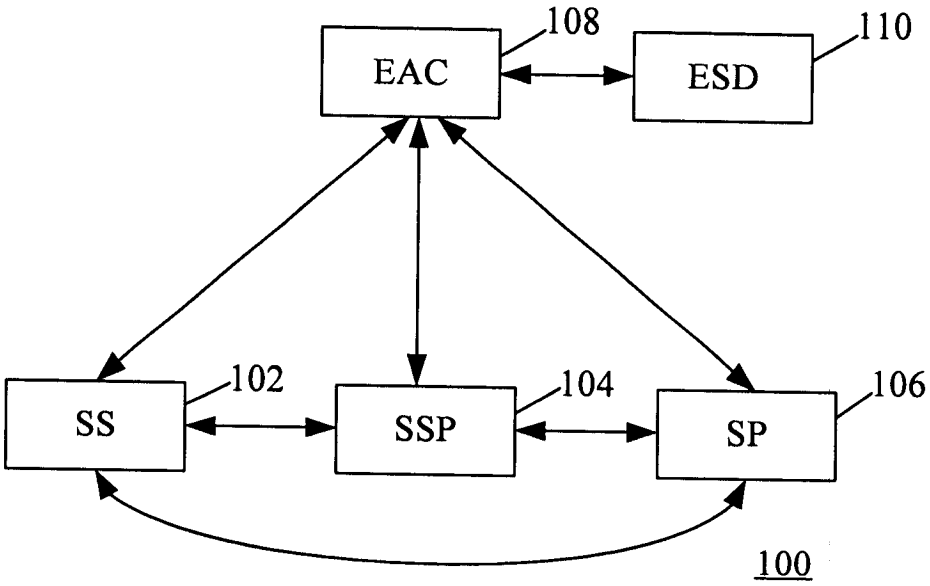

EAC
108
ESD
110
SS
102
SSP
104
SP
106
100

图 1

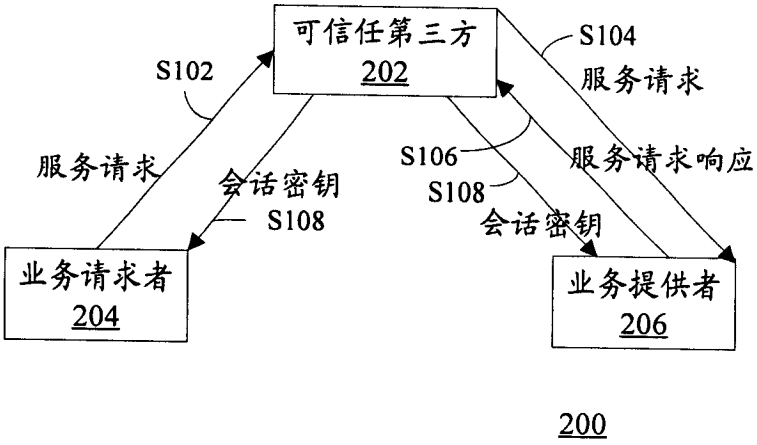

可信任第三方
202
S102
服务请求
S104
服务请求
S106
S108
会话密钥
会话密钥
S108
服务请求响应
业务请求者
204
业务提供者
206
200

图 2

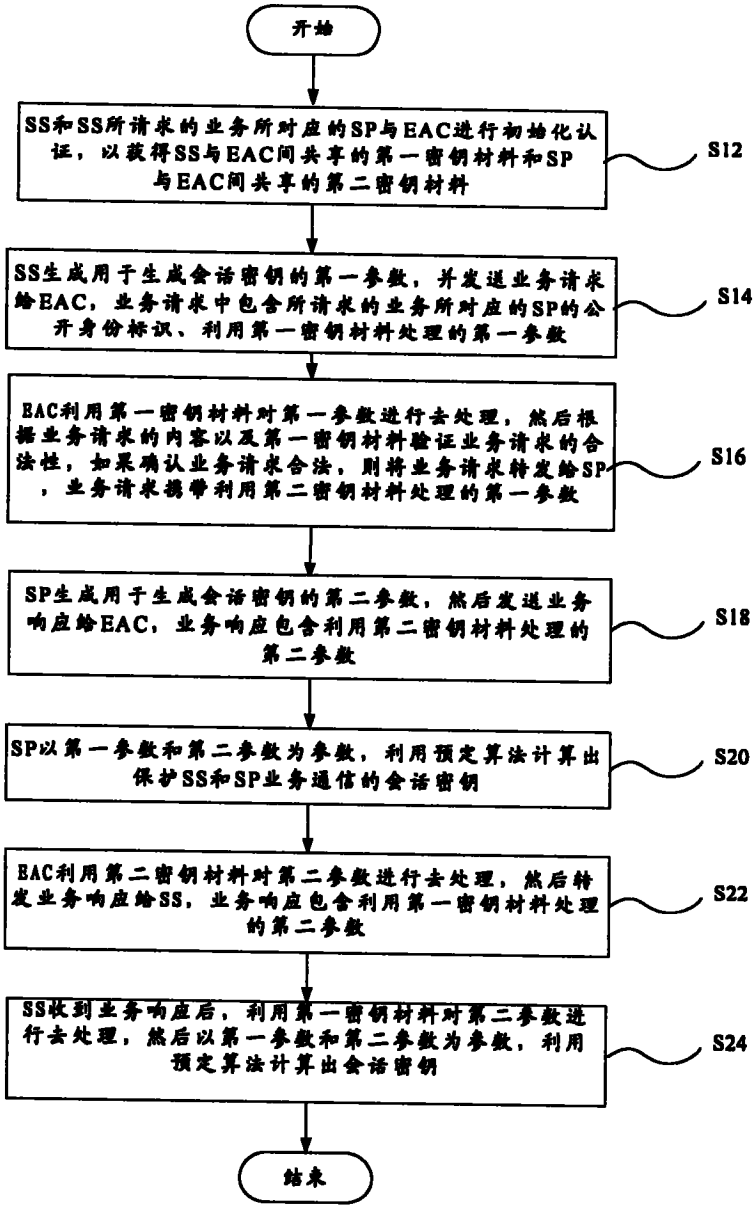

开始
SS和SS所请求的业务所对应的SP与EAC进行初始化认证，以获得SS与EAC间共享的第一密钥材料和SP与EAC间共享的第二密钥材料
S12
SS生成用于生成会话密钥的第一参数，并发送业务请求给EAC，业务请求中包含所请求的业务所对应的SP的公开身份标识、利用第一密钥材料处理的第一参数
S14
EAC利用第一密钥材料对第一参数进行去处理，然后根据业务请求的内容以及第一密钥材料验证业务请求的合法性，如果确认业务请求合法，则将业务请求转发给SP，业务请求携带利用第二密钥材料处理的第一参数
S16
SP生成用于生成会话密钥的第二参数，然后发送业务响应给EAC，业务响应包含利用第二密钥材料处理的第二参数
S18
SP以第一参数和第二参数为参数，利用预定算法计算出保护SS和SP业务通信的会话密钥
S20
EAC利用第二密钥材料对第二参数进行去处理，然后转发业务响应给SS，业务响应包含利用第一密钥材料处理的第二参数
S22
SS收到业务响应后，利用第一密钥材料对第二参数进行去处理，然后以第一参数和第二参数为参数，利用预定算法计算出会话密钥
S24
结束

图 3

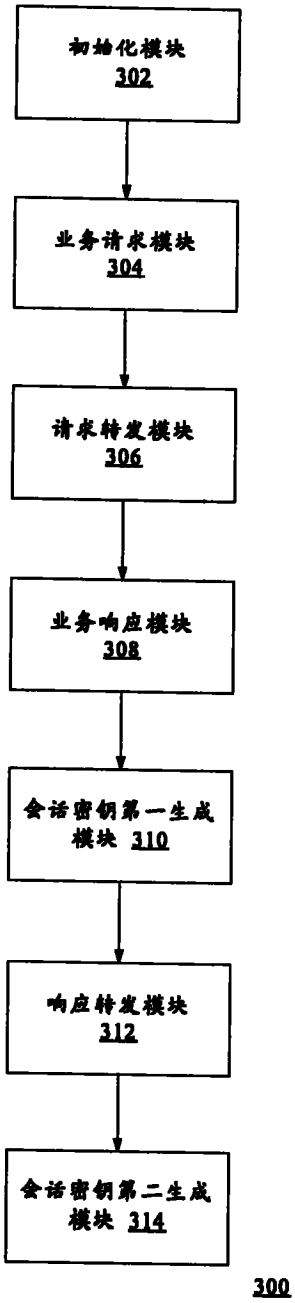

初始化模块
302
业务请求模块
304
请求转发模块
306
业务响应模块
308
会话密钥第一生成模块 310
响应转发模块
312
会话密钥第二生成模块 314
300

图 4

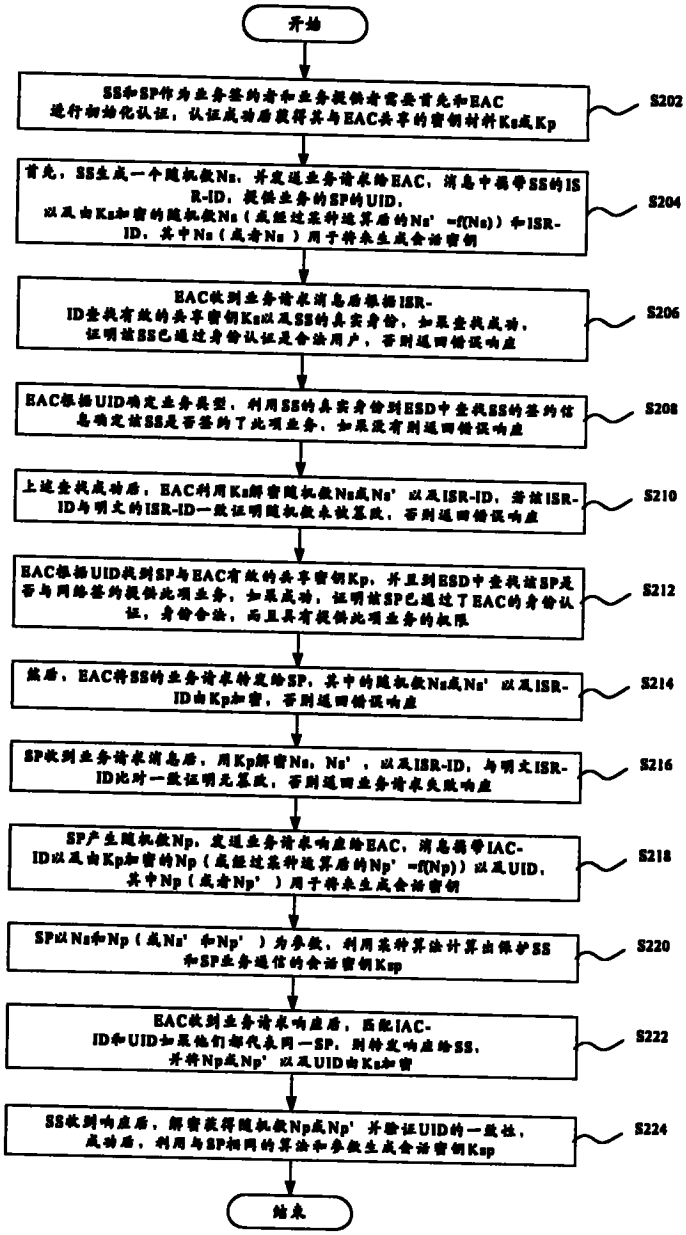

开始
SS和SP作为业务签约者和业务提供者需要首先和EAC进行初始化认证，认证成功后获得其与EAC共享的密钥材料Ks或Kp
S202
首先，SS生成一个随机数Ns，并发送业务请求给EAC，消息中携带SS的ISR-ID，提供业务的SP的UID，以及由Ks加密的随机数Ns（或经过某种运算后的Ns' =f(Ns)）和ISR-ID，其中Ns（或者Ns'）用于将来生成会话密钥
S204
EAC收到业务请求消息后根据ISR-ID查找有效的共享密钥Ks以及SS的真实身份，如果查找成功，证明该SS已通过身份认证是合法用户，否则返回错误响应
S206
EAC根据UID确定业务类型，利用SS的真实身份到ESD中查找SS的签约信息确定该SS是否签约了此项业务，如果没有则返回错误响应
S208
上述查找成功后，EAC利用Ks解密随机数Ns或Ns'以及ISR-ID，若该ISR-ID与明文的ISR-ID一致证明随机数未被篡改，否则返回错误响应
S210
EAC根据UID找到SP与EAC有效的共享密钥Kp，并且到ESD中查找该SP是否与网络签约提供此项业务，如果成功，证明该SP已通过了EAC的身份认证，身份合法，而且具有提供此项业务的权限
S212
然后，EAC将SS的业务请求转发给SP，其中的随机数Ns或Ns'以及ISR-ID由Kp加密，否则返回错误响应
S214
SP收到业务请求消息后，用Kp解密Ns，Ns'，以及ISR-ID，与明文ISR-ID比对一致证明无篡改，否则返回业务请求失败响应
S216
SP产生随机数Np，发送业务请求响应给EAC，消息携带IAC-ID以及由Kp加密的Np（或经过某种运算后的Np' =f(Np)）以及UID，其中Np（或者Np'）用于将来生成会话密钥
S218
SP以Ns和Np（或Ns'和Np'）为参数，利用某种算法计算出保护SS和SP业务通信的会话密钥Ksp
S220
EAC收到业务请求响应后，匹配IAC-ID和UID如果他们都代表同一SP，则转发响应给SS，并将Np或Np'以及UID由Ks加密
S222
SS收到响应后，解密获得随机数Np或Np'并验证UID的一致性，成功后，利用与SP相同的算法和参数生成会话密钥Ksp
S224
结束

图 5

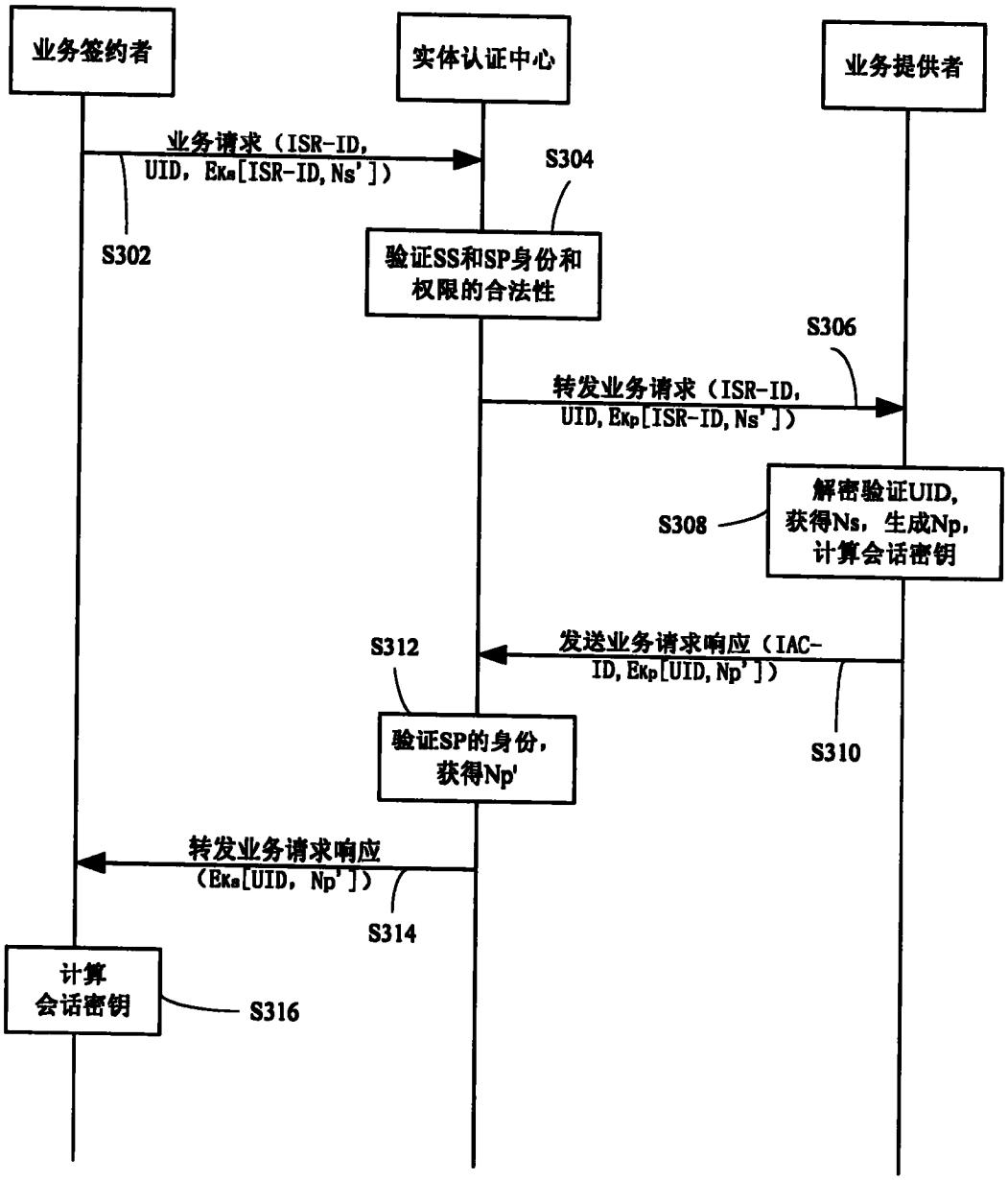

业务签约者
实体认证中心
业务提供者
业务请求（ISR-ID，
UID，EKs[ISR-ID，Ns']）
S304
S302
验证SS和SP身份和
权限的合法性
S306
转发业务请求（ISR-ID，
UID，EKp[ISR-ID，Ns']）
解密验证UID，
获得Ns，生成Np，
计算会话密钥
S308
S312
发送业务请求响应（IAC-
ID，EKp[UID，Np']）
S310
验证SP的身份，
获得Np'
转发业务请求响应
（EKs[UID，Np']）
S314
计算
会话密钥
S316

图 6