

(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
2018 年 1 月 25 日 (25.01.2018)



(10) 国际公布号
WO 2018/014535 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2017/072253
- (22) 国际申请日: 2017 年 1 月 23 日 (23.01.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610563016.2 2016年7月16日 (16.07.2016) CN
201610633776.6 2016年8月4日 (04.08.2016) CN
201610819335.5 2016年9月9日 (09.09.2016) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 吴荣 (WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong

518129 (CN)。张博 (ZHANG, Bo); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。甘露 (GAN, Lu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD.); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM,

(54) Title: NETWORK VERIFICATION METHOD AND ASSOCIATED APPARATUS AND SYSTEM

(54) 发明名称: 一种网络认证方法、相关设备及系统

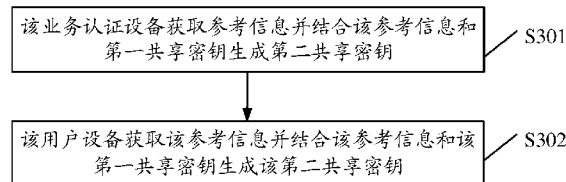


图 3A

S301 SERVICE VERIFICATION APPARATUS OBTAINS REFERENCE INFORMATION, AND COMBINES THE REFERENCE INFORMATION WITH A FIRST PUBLIC KEY TO GENERATE A SECOND PUBLIC KEY

S302 USER EQUIPMENT OBTAINS THE REFERENCE INFORMATION, AND COMBINES THE REFERENCE INFORMATION WITH THE FIRST PUBLIC KEY TO GENERATE THE SECOND PUBLIC KEY

(57) Abstract: Embodiments of the present invention disclose a network verification method, and an associated apparatus and system. The system comprises user equipment, a network verification apparatus and a service verification apparatus. The service verification apparatus obtains reference information, and combines the reference information with a first public key to generate a second public key, wherein the first public key is a pre-configured public key used between the user equipment and the service verification apparatus. The user equipment obtains the reference information, and combines the reference information with the first public key to generate the second public key. The service verification apparatus transmits the second public key to the network verification apparatus. The network verification apparatus receives the second public key, which is used by the user equipment and the network verification equipment to generate a target public key. The target public key or a public key generated based on the target public key is a public key for ensuring secure data transmission and is agreed between the network verification apparatus and the user equipment. The present invention is capable of increasing the security level of a target public key.

ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本发明实施例公开了一种网络认证方法、相关设备及系统, 该系统包括用户设备、网络认证设备和业务认证设备, 业务认证设备用于获取参考信息并结合参考信息和第一共享密钥生成第二共享密钥, 第一共享密钥为用户设备与业务认证设备之间预先配置的共享密钥; 用户设备用于获取参考信息并结合参考信息和第一共享密钥生成第二共享密钥; 业务认证设备用于将第二共享密钥发送给网络认证设备; 网络认证设备用于接收第二共享密钥, 第二共享密钥用于用户设备和网络认证设备生成目标共享密钥, 目标共享密钥或者基于目标共享密钥衍生的共享密钥为网络认证设备与用户设备协商的保护数据安全传输的共享密钥。采用本发明, 能够提高目标共享密钥的安全级别。

一种网络认证方法、相关设备及系统

技术领域

本发明实施例涉及计算机技术领域，尤其涉及一种网络认证方法、相关设备及系统。

背景技术

物联网(英文: Internet of Things, 简称: IoT)是第五代移动通信技术(英文: 5th-Generation, 简称: 5G)的重要应用场景, IoT 中的用户设备接入到 5G 网络需要进行网络认证, 从而生成用于保护网络数据安全传输的共享密钥。用户设备通过网络访问的某项业务时也需要进行业务认证, 从而生成用于保护业务数据安全传输的共享密钥。基于共享密钥来保证数据安全传输的原理如下:

用户 1 (User1) 和用户 2 (User2) 提前共享对称密钥 K, 也称作共享密钥。

方式一: User1 使用共享密钥 K 对消息 m 进行加密, 例如, 可表示为 $ciphertext = En_K(m)$; 然后 User1 并将加密后的消息发送给 USER2。USER2 接收该 User1 发送的消息并利用 K 和 ciphertext 恢复出消息 m, 例如, 可表示为 $m = decrypt(K, ciphertext)$, 该过程保证了消息 m 传输的安全性。基于该共享密钥 K 的加密技术可以为高级加密标准(英文: Advanced Encryption Standard, 缩写: AES), 三重数据加密算法(英文: Triple Data Encryption Algorithm, 简称: 3DES), Blowfish, Serpent, Snow 3G, ZUC, HC-256, Grain 等算法。

方式二: User1 利用共享密钥 K 计算消息 m 的消息认证码(英文: message Authentication code, 简称: MAC), 例如, 可表示为 $MAC1 = MAC_K(m)$, 即利用共享密钥 K 计算出消息 m 对应的消息认证码 MAC1。然后 User1 将消息 m 和消息认证码 MAC1 发送给该 USER2。该 USER2 接收该消息 m 和该消息认证码 MAC1, 并利用 K 和 m 验证 MAC1 的正确性, 若验证正确则表明消息 m 未被篡改, 该过程保证了消息 m 传输的安全性。基于该共享密钥 K 生成消息认证码的技术可以为哈希消息认证码(英文: Hash-based Message Authentication Code, 简称: HMAC), OMAC, CBC-MAC, PMAC, UMAC 和 VMAC 等算法。

如何在海量 IoT 的场景下提高网络认证的效率以及提高网络认证的安全性, 是本领域的技术人员正在探讨的问题。

发明内容

本发明实施例公开了一种网络认证方法、相关设备及系统, 能够提高网络认证的效率以及提高网络认证的安全性。

第一方面, 本发明实施例提供了一种网络认证系统, 所述系统包括用户设备、网络认证设备和业务认证设备, 其中:

所述业务认证设备用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥, 所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥, 所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息;

所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥;

所述业务认证设备用于将所述第二共享密钥发送给所述网络认证设备;

所述网络认证设备用于接收所述第二共享密钥,所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在上述系统中,用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥,然后该业务认证设备将该第二共享密钥发送给该网络认证设备,使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说,生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息,提升了该目标共享密钥的安全级别。

结合第一方面,在第一方面的第一种可能的实现方式中,所述网络认证设备和所述用户设备用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

结合第一方面的第一种可能的实现方式,在第一方面的第二种可能的实现方式中:

所述网络认证设备和所述用户设备用于进行网络认证生成第三共享密钥;

所述网络认证设备和所述用户设备用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥,具体为:

所述网络认证设备和所述用户设备用于根据所述第二共享密钥进行网络认证生成第四共享密钥;

所述网络认证设备和所述用户设备均用于根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

结合第一方面,在第一方面的第三种可能的实现方式中,所述结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥;

所述网络认证设备和所述用户设备用于将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

结合第一方面的第一种可能的实现方式,或者第一方面的第二种可能的实现方式,或者第一方面的第三种可能的实现方式,在第一方面的第四种可能的实现方式中:

所述网络认证设备还用于将所述目标共享密钥发送给所述业务认证设备;

所述业务认证设备用于接收所述目标共享密钥;

所述业务认证设备和所述用户设备用于将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第一方面,在第一方面的第五种可能的实现方式中:

所述网络认证设备和所述用户设备用于进行网络认证生成第三共享密钥;

所述结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证

生成第二共享密钥;

所述网络认证设备和所述用户设备均用于根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥; 或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

结合第一方面, 在第一方面的第六种可能的实现方式中:

所述网络认证设备和所述用户设备均用于根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥; 或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥, 所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

结合第一方面, 在第一方面的第七种可能的实现方式中: 所述参考信息包括所述网络认证设备所在蜂窝网的网络参数; 所述结合所述参考信息和第一共享密钥生成第二共享密钥, 具体为:

根据所述参考信息和所述第一共享密钥进行业务认证生成第二共享密钥;

所述业务认证设备还用于将所述第二共享密钥作为所述目标共享密钥。

结合第一方面, 在第一方面的第八种可能的实现方式中:

所述业务认证设备用于获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥;

所述结合所述参考信息和第一共享密钥生成第二共享密钥, 具体为:

结合所述参考信息、第一共享密钥和所述第五共享密钥进行业务认证生成第二共享密钥;

所述网络认证设备用于将所述第二共享密钥作为所述目标共享密钥。

结合第一方面, 在第一方面的第九种可能的实现方式中:

所述网络认证设备用于向所述业务认证设备获取所述第一共享密钥;

所述网络认证设备用于根据所述第一共享密钥和第五共享密钥生成网络侧信息, 所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥;

所述网络认证设备用于将所述网络侧信息发送给所述业务认证设备;

所述业务认证设备用于接收并向所述用户设备转发所述网络侧信息;

所述结合所述参考信息和第一共享密钥生成第二共享密钥, 具体为:

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥, 所述网络参数包括所述网络侧信息;

所述网络认证设备用于将所述第二共享密钥作为所述目标共享密钥。

结合第一方面, 或者第一方面的第一种可能的实现方式, 或者第一方面的第二种可能的实现方式, 或者第一方面的第三种可能的实现方式, 或者第一方面的第四种可能的实现方式, 或者第一方面的第五种可能的实现方式, 或者第一方面的第六种可能的实现方式, 或者第一方面的第七种可能的实现方式, 或者第一方面的第八种可能的实现方式, 或者第一方面的第九种可能的实现方式, 在第一方面的第十种可能的实现方式中, 所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第一方面的第十种可能的实现方式, 在第一方面的第十一种可能的实现方式中,

所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第二方面，本发明实施例提供一种网络认证系统，其特征在于，所述系统包括用户设备、网络认证设备和业务认证设备，其中：

所述业务认证设备用于将预存的目标业务的业务参数发送给所述网络认证设备和所述用户设备；

所述网络认证设备和所述用户设备用于接收所述业务参数；

所述网络认证设备和所述用户设备均用于结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

在上述系统中，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二方面，在第二方面的第一种可能的实现方式中，所述网络认证设备和所述用户设备均用于结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

所述网络认证设备和所述用户设备均用于根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

所述网络认证设备和所述用户设备均用于根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第二方面，或者第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第三方面，本发明实施例提供一种网络认证系统，所述系统包括用户设备、网络认证设备和业务认证设备，其中：

所述业务认证设备用于获取所述用户设备的身份标识；

所述业务认证设备用于结合自身的业务公钥、业务私钥和所述身份标识生成身份密钥，并将所述身份密钥、所述业务公钥发送给所述网络认证设备；

所述网络认证设备用于接收所述身份密钥和所述业务公钥，并结合所述身份密钥、所述业务公钥和所述网络认证设备所在蜂窝网的网络参数生成认证根密钥；

所述网络认证设备用于将所述认证根密钥写入所述用户设备；

所述网络认证设备和所述用户设备用于根据所述认证根密钥进行网络认证生成目标

共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在上述系统中，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第三方面，在第三方面的第一种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第四方面，本发明实施例提供一种网络认证系统，其特征在于，所述系统包括用户设备、网络认证设备和业务认证设备，其中：

所述业务认证设备和所述用户设备用于进行业务认证生成参考共享密钥，或者所述业务认证设备和所述用户设备用于预先配置参考共享密钥；

所述业务认证设备用于将所述参考共享密钥发送给所述网络认证设备；

所述网络认证设备用于接收所述参考共享密钥；

所述网络认证设备和所述用户设备用于结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在上述网络认证系统中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第四方面，在第四方面的第一种可能的实现方式中，所述网络认证设备用于将所述网络认证设备所在蜂窝网的网络参数发送给所述用户设备；所述网络认证设备和所述用户设备用于结合所述参考共享密钥生成目标共享密钥，具体为：

所述网络认证设备和所述用户设备均用于根据所述网络参数和所述参考共享密钥生成认证共享密钥；

所述网络认证设备和所述用户设备用于根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第四方面的第一种可能的实现方式，在第四方面的第二种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

结合第四方面，或者第四方面的第一种可能的实现方式，或者第四方面的第二种可能的实现方式，在第四方面的第三种可能的实现方式中：

所述网络认证设备还用于将所述目标共享密钥发送给所述业务认证设备;

所述业务认证设备用于接收所述目标共享密钥;

所述业务认证设备和所述用户设备用于将所述目标共享密钥,或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

第五方面,本发明实施例提供一种业务认证设备,该业务认证设备包括:

第一获取单元,用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥,所述第一共享密钥为用户设备与所述业务认证设备之间预先配置的共享密钥,所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥,所述参考信息包括所述用户设备、网络认证设备和所述业务认证设备中至少一项预先关联的信息;

发送单元,用于将所述第二共享密钥发送给所述网络认证设备,所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元,用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥,然后该业务认证设备将该第二共享密钥发送给该网络认证设备,使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说,生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息,提升了该目标共享密钥的安全级别。

结合第五方面,在第五方面的第一种可能的实现方式中,所述第一获取单元结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

结合第五方面,或者第五方面的第一种可能的实现方式,在第五方面的第二种可能的实现方式中,还包括:

第一接收单元,用于接收所述网络认证设备发送的所述目标共享密钥;

生成单元,用于将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第五方面,或者第五方面的第一种可能的实现方式,在第五方面的第三种可能的实现方式中,还包括:

生成单元,用于将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第五方面,在第五方面的第四种可能的实现方式中,还包括:

第二获取单元,用于获取所述用户设备与所述网络认证设备之间预先配置的第二共享密钥;

所述第一获取单元结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

结合所述参考信息、第一共享密钥和所述第二共享密钥进行网络认证生成第二共享密

钥。

结合第五方面，在第五方面的第五种可能的实现方式中，还包括：

第二接收单元，用于接收所述网络认证设备根据所述网络认证设备所在蜂窝网的网络参数生成的网络侧信息，并向所述用户设备转发所述网络侧信息；

所述第一获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

结合第五方面，或者第五方面的第一种可能的实现方式，或者第五方面的第二种可能的实现方式，或者第五方面的第三种可能的实现方式，或者第五方面的第四种可能的实现方式，或者第五方面的第五种可能的实现方式，在第五方面的第六种可能的实现方式中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第五方面的第六种可能的实现方式，在第五方面的第七种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第六方面，本发明实施例提供一种用户设备，该用户设备包括：

获取单元，用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥；所述第一共享密钥为所述用户设备与业务认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥，所述业务认证设备还用于将所述第二共享密钥发送给网络认证设备；

生成单元，用于根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

结合第六方面，在第六方面的第一种可能的实现方式中，所述获取单元根据所述第二共享密钥生成目标共享密钥，具体为：

将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

结合第六方面，在第六方面的第二种可能的实现方式中，所述获取单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的

共享密钥进行网络认证生成目标共享密钥。

结合第六方面的第二种可能的实现方式，在第六方面的第三种可能的实现方式中，该用户设备还包括：

认证单元，用于和所述网络认证设备进行网络认证生成第三共享密钥；

所述获取单元和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥，具体为：

和所述网络认证设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

结合第六方面，在第六方面的第四种可能的实现方式中，所述生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述网络认证设备进行网络认证生成第三共享密钥；

根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

结合第六方面，在第六方面的第五种可能的实现方式中，所述生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的共享密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

结合第六方面，在第六方面的第六种可能的实现方式中，所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述参考信息、第一共享密钥和第五共享密钥与所述业务认证设备进行业务认证生成第二共享密钥；所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述第五共享密钥。

结合第六方面，或者第六方面的第一种可能的实现方式，或者第六方面的第二种可能的实现方式，或者第六方面的第三种可能的实现方式，或者第六方面的第四种可能的实现方式，或者第六方面的第五种可能的实现方式，在第六方面的第七种可能的实现方式中，所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

和业务认证设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

结合第六方面，或者第六方面的第一种可能的实现方式，或者第六方面的第二种可能的实现方式，或者第六方面的第三种可能的实现方式，或者第六方面的第四种可能的实现方式，或者第六方面的第五种可能的实现方式，在第六方面的第八种可能的实现方式中，还包括：

第一接收单元，用于接收所述业务认证设备转发的来自所述网络认证设备的网络侧信息，所述网络侧信息为所述网络认证设备根据第五共享密钥和获取的所述第一共享密钥生成，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥与所述业务认证设备进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

结合第六方面，或者第六方面的第一种可能的实现方式，或者第六方面的第二种可能的实现方式，或者第六方面的第三种可能的实现方式，或者第六方面的第四种可能的实现方式，或者第六方面的第五种可能的实现方式，或者第六方面的第六种可能的实现方式，或者第六方面的第七种可能的实现方式，或者第六方面的第八种可能的实现方式，在第六方面的第九种可能的实现方式中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第六方面的第九种可能的实现方式，在第六方面的第十种可能的实现方式中，当所述参考信息包含所述业务参数时，还包括：

第二接收单元，用于接收所述网络认证设备转发的来自所述业务认证设备的所述业务参数。

结合第六方面的第九种可能的实现方式，或者第六方面的第十种可能的实现方式，在第六方面的第十一种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第七方面，本发明实施例提供一种网络认证设备，该网络认证设备包括：

接收单元，用于接收业务认证设备发送的第二共享密钥，业务认证设备和用户设备均用于结合第一共享密钥和参考信息生成所述第二共享密钥，所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥，所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息；

第一生成单元，用于根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

结合第七方面，在第七方面的第一种可能的实现方式中，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

结合第七方面的第一种可能的实现方式，在第七方面的第二种可能的实现方式中，还包括：

认证单元，用于和所述用户设备进行网络认证生成第三共享密钥；

所述认证单元和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密

钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

和所述用户设备均根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

结合第七方面，在第七方面的第三种可能的实现方式中，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为目标共享密钥。

结合第七方面，在第七方面的第四种可能的实现方式中，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备进行网络认证生成第三共享密钥；

和所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

结合第七方面，在第七方面的第五种可能的实现方式中，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

结合第七方面，或者第七方面的第一种可能的实现方式，或者第七方面的第二种可能的实现方式，或者第七方面的第三种可能的实现方式，或者第七方面的第四种可能的实现方式，或者第七方面的第五种可能的实现方式，在第七方面的第六种可能的实现方式中，还包括：

获取单元，用于向所述业务认证设备获取所述第一共享密钥；

第二生成单元，用于根据所述第一共享密钥和第五共享密钥生成网络侧信息，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述网络认证设备将所述网络侧信息发送给所述业务认证设备，以使所述业务认证设备向所述用户设备转发所述网络侧信息，所述网络参数属于所述参考信息。

结合第七方面，或者第七方面的第一种可能的实现方式，或者第七方面的第二种可能的实现方式，或者第七方面的第三种可能的实现方式，或者第七方面的第四种可能的实现方式，或者第七方面的第五种可能的实现方式，在第七方面的第七种可能的实现方式中，还包括：

发送单元，用于将所述目标共享密钥发送给所述业务认证设备，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥用作所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第七方面，或者第七方面的第一种可能的实现方式，或者第七方面的第二种可能的实现方式，或者第七方面的第三种可能的实现方式，或者第七方面的第四种可能的实现

方式，或者第七方面的第五种可能的实现方式，或者第七方面的第六种可能的实现方式，或者第七方面的第七种可能的实现方式，在第七方面的第八种可能的实现方式中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第七方面的第八种可能的实现方式，在第七方面的第九种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第八方面，本发明实施例提供一种业务认证设备，该业务认证设备包括：

发送单元，用于将预存的目标业务的业务参数发送给网络认证设备和用户设备；以使所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过运行上述单元，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第八方面，在第八方面的第一种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第九方面，本发明实施例提供一种用户设备，该用户设备包括：

接收单元，用于接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给网络认证设备；

生成单元，用于和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过运行上述单元，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第九方面，在第九方面的第一种可能的实现方式中，所述生成单元和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述网络认证设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第九方面，或者第九方面的第一种可能的实现方式，在第九方面的第二种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第十方面，本发明实施例提供一种网络认证设备，该网络认证设备包括：

接收单元，用于接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给用户设备；

生成单元，用于和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过运行上述单元，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

结合第十方面，在第十方面的第一种可能的实现方式中，所述生成单元和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述用户设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第十方面，或者第十方面的第一种可能的实现方式，在第十方面的第二种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第十一方面，本发明实施例提供一种业务认证设备，该业务认证设备包括

获取单元，用于获取用户设备的身份标识；

生成单元，用于结合自身的业务公钥、业务私钥和所述身份标识生成身份密钥，并将所述身份密钥、所述业务公钥发送给所述网络认证设备，所述身份密钥和所述业务公钥用于所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也

即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及
与网络相关的信息，提升了该目标共享密钥的安全级别。

第十二方面，本发明实施例提供一种用户设备，该用户设备包括：

生成单元，用于和网络认证设备根据认证根密钥进行网络认证生成目标共享密钥，所述认证根密钥为所述网络认证设备根据身份密钥、业务认证设备管理的目标业务的业务公钥和所述网络认证设备所在蜂窝网的网络参数生成的并写入到所述用户设备中的密钥，所述身份密钥由所述业务认证设备根据所述业务公钥、所述目标业务的业务私钥和获取的所述用户设备的身份标识生成的，所述业务认证设备用于将所述业务公钥和所述身份私钥发送给所述网络认证设备；所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及
与网络相关的信息，提升了该目标共享密钥的安全级别。

结合第十二方面，在第十二方面的第一种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第十三方面，本发明实施例提供一种网络认证设备，该网络认证设备包括：

接收单元，用于接收身份密钥和业务认证设备管理的目标业务的业务公钥，所述身份密钥为所述业务认证设备根据所述目标业务的业务私钥、所述业务公钥和获取的用户设备的身份标识生成的密钥；

生成单元，用于结合所述身份密钥、所述业务公钥和所述网络认证设备所在蜂窝网的网络参数生成认证根密钥；

写入单元，用于将所述认证根密钥写入所述用户设备；

认证单元，用于和所述用户设备根据所述认证根密钥进行网络认证生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及
与网络相关的信息，提升了该目标共享密钥的安全级别。

结合第十三方面，在第十三方面的第一种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第十四方面，本发明实施例提供一种业务认证设备，该业务认证设备包括：

认证单元，用于和用户设备进行业务认证生成参考共享密钥，或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥；

发送单元，用于将所述参考共享密钥发送给网络认证设备，以使所述网络认证设备和所述用户设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第十四方面，在第十四方面的第一种可能的实现方式中，还包括：

接收单元，用于接收所述网络认证设备发送的所述目标共享密钥；

确定单元，用于将所述目标共享密钥，或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

第十五方面，本发明实施例提供一种用户设备，该用户设备包括：

配置单元，用于和业务认证设备进行业务认证生成参考共享密钥，或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥，所述业务认证设备用于将所述参考共享密钥发送给网络认证设备；

生成单元，用于和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第十五方面，在第十五方面的第一种可能的实现方式中，还包括：

接收单元，用于接收所述网络认证设备发送的所述网络认证设备所在蜂窝网的网络参数；

所述生成单元和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述网络参数和所述参考共享密钥生成认证共享密钥；

和所述网络认证设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第十五方面的第一种可能的实现方式，在第十五方面的第二种可能的实现方式中，

所述网络参数包括运营商标识, 接入网络标识, 服务网络标识, 网络类型标识, 局域网网络标识, 切片标识, 承载标识, 服务质量标识和流标识中的至少一项。

第十六方面, 本发明实施例提供一种网络认证设备, 该网络认证设备包括:

接收单元, 用于接收业务认证设备发送的参考共享密钥, 所述参考共享密钥由所述业务认证设备和用户设备进行业务认证生成的或者预先配置的;

生成单元, 用于和所述用户设备结合所述参考共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元, 该业务认证设备与该用户设备进行业务认证生成参考共享密钥, 然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数; 该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥, 并基于该认证共享密钥进行网络认证生成目标共享密钥。也就是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息, 提升了该目标共享密钥的安全级别。

结合第十六方面, 在第十六方面的第一种可能的实现方式中, 该网络认证设备还包括:

第一发送单元, 用于将所述网络认证设备所在蜂窝网的网络参数发送给所述用户设备;

所述生成单元和所述用户设备结合所述参考共享密钥生成目标共享密钥, 具体为:

和所述用户设备均根据所述网络参数和所述参考共享密钥生成认证共享密钥;

和所述用户设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第十六方面的第一种可能的实现方式, 在第十六方面的第二种可能的实现方式中, 所述网络参数包括运营商标识, 接入网络标识, 服务网络标识, 网络类型标识, 局域网网络标识, 切片标识, 承载标识, 服务质量标识和流标识中的至少一项。

结合第十六方面, 或者第十六方面的第一种可能的实现方式中, 或者第十六方面的第二种可能的实现方式, 在第十六方面的第三种可能的实现方式中, 该网络认证设备还包括:

第二发送单元, 用于将所述目标共享密钥发送给所述业务认证设备, 以使所述业务认证设备将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

第十七方面, 本发明实施例提供一种网络认证方法, 该方法包括:

业务认证设备获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥, 所述第一共享密钥为用户设备与所述业务认证设备之间预先配置的共享密钥, 所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥, 所述参考信息包括所述用户设备、网络认证设备和所述业务认证设备中至少一项预先关联的信息;

所述业务认证设备将所述第二共享密钥发送给所述网络认证设备, 所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全

传输的共享密钥。

通过执行上述步骤，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

结合第十七方面，在第十七方面的第一种可能的实现方式中，所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

结合第十七方面，或者第十七方面的第一种可能的实现方式，在第十七方面的第二种可能的实现方式中，所述业务认证设备将所述第二共享密钥发送给所述网络认证设备之后，所述方法还包括：

所述业务认证设备接收所述网络认证设备发送的所述目标共享密钥；

所述业务认证设备将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第十七方面，或者第十七方面的第一种可能的实现方式，在第十七方面的第三种可能的实现方式中，所述业务认证设备获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥之后，所述方法还包括：

所述业务认证设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第十七方面，在第十七方面的第四种可能的实现方式中，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述业务认证设备获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述参考信息、第一共享密钥和所述第五共享密钥进行网络认证生成第二共享密钥。

结合第十七方面，在第十七方面的第五种可能的实现方式中，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述业务认证设备接收所述网络认证设备根据所述网络认证设备所在蜂窝网的网络参数生成的网络侧信息，并向所述用户设备转发所述网络侧信息；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

结合第十七方面，或者第十七方面的第一种可能的实现方式，或者第十七方面的第一种可能的实现方式，或者第十七方面的第二种可能的实现方式，或者第十七方面的第三种可能的实现方式，或者第十七方面的第四种可能的实现方式，或者第十七方面的第五种可

能的实现方式，在第十七方面的第六种可能的实现方式中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第十七方面的第六种可能的实现方式，在第十七方面的第七种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第十八方面，本发明实施例提供一种网络认证方法，该方法包括：

用户设备获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥；所述第一共享密钥为所述用户设备与业务认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥，所述业务认证设备还用于将所述第二共享密钥发送给网络认证设备；

所述用户设备根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

结合第十八方面，在第十八方面的第一种可能的实现方式中，所述用户设备根据所述第二共享密钥生成目标共享密钥，包括：

所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

结合第十八方面，在第十八方面的第二种可能的实现方式中，所述用户设备根据所述第二共享密钥生成目标共享密钥，包括：

所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥。

结合第十八方面的第二种可能的实现方式，在第十八方面的第三种可能的实现方式中，所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥之前，所述方法还包括：

所述用户设备和所述网络认证设备进行网络认证生成第三共享密钥；

所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥，包括：

所述用户设备和所述网络认证设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

所述用户设备根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

结合第十八方面，在第十八方面的第四种可能的实现方式中，所述用户设备根据所述第二共享密钥生成目标共享密钥，包括：

所述用户设备和所述网络认证设备进行网络认证生成第三共享密钥；

所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

结合第十八方面，在第十八方面的第五种可能的实现方式中，所述用户设备根据所述第二共享密钥生成目标共享密钥，包括：

所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的共享密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

结合第十八方面，在第十八方面的第六种可能的实现方式中，所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述参考信息、第一共享密钥和第五共享密钥与所述业务认证设备进行业务认证生成第二共享密钥；所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述第五共享密钥。

结合第十八方面，或者第十八方面的第一种可能的实现方式，或者第十八方面的第二种可能的实现方式，或者第十八方面的第三种可能的实现方式，或者第十八方面的第四种可能的实现方式，或者第十八方面的第五种可能的实现方式，或者第十八方面的第六种可能的实现方式，在第十八方面的第七种可能的实现方式中，所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

用户设备和业务认证设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

结合第十八方面，或者第十八方面的第一种可能的实现方式，或者第十八方面的第二种可能的实现方式，或者第十八方面的第三种可能的实现方式，或者第十八方面的第四种可能的实现方式，或者第十八方面的第五种可能的实现方式，或者第十八方面的第六种可能的实现方式，在第十八方面的第八种可能的实现方式中，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述用户设备接收所述业务认证设备转发的来自所述网络认证设备的网络侧信息，所述网络侧信息为所述网络认证设备根据第五共享密钥和获取的所述第一共享密钥生成，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述网络参数和第一共享密钥与所述业务认证设备进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

结合第十八方面，或者第十八方面的第一种可能的实现方式，或者第十八方面的第二种可能的实现方式，或者第十八方面的第三种可能的实现方式，或者第十八方面的第四种可能的实现方式，或者第十八方面的第五种可能的实现方式，或者第十八方面的第六种可

能的实现方式，或者第十八方面的第七种可能的实现方式，或者第十八方面的第八种可能的实现方式，在第十八方面的第九种可能的实现方式中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第十八方面的第九种可能的实现方式，在第十八方面的第十种可能的实现方式中，当所述参考信息包含所述业务参数时，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述用户设备接收所述网络认证设备转发的来自所述业务认证设备的所述业务参数。

结合第十八方面的第九种可能的实现方式，或者结合第十八方面的第十种可能的实现方式，在第十八方面的第十一种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第十九方面，本发明实施例提供一种网络认证方法，该方法包括：

网络认证设备接收业务认证设备发送的第二共享密钥，业务认证设备和用户设备均用于结合第一共享密钥和参考信息生成所述第二共享密钥，所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥，所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息；

所述网络认证设备根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

结合第十九方面，在第十九方面的第一种可能的实现方式中，所述网络认证设备根据所述第二共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

结合第十九方面的第一种可能的实现方式，在第十九方面的第二种可能的实现方式中，所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥之前，所述方法还包括：

所述网络认证设备和所述用户设备进行网络认证生成第三共享密钥；

所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述第二共享密钥进行网络认证生成第四共

享密钥;

所述网络认证设备和所述用户设备均根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

结合第十九方面,在第十九方面的第三种可能的实现方式中,所述网络认证设备根据所述第二共享密钥生成目标共享密钥,包括:

所述网络认证设备和所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为目标共享密钥。

结合第十九方面,在第十九方面的第四种可能的实现方式中,所述网络认证设备根据所述第二共享密钥生成目标共享密钥,包括:

所述网络认证设备和所述用户设备进行网络认证生成第三共享密钥;

所述网络认证设备和所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥;或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

结合第十九方面,在第十九方面的第五种可能的实现方式中,所述网络认证设备根据所述第二共享密钥生成目标共享密钥,包括:

所述网络认证设备和所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥;或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥,所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

结合第十九方面,或者第十九方面的第一种可能的实现方式,或者第十九方面的第二种可能的实现方式,或者第十九方面的第三种可能的实现方式,或者第十九方面的第四种可能的实现方式,或者第十九方面的第五种可能的实现方式,在第十九方面的第六种可能的实现方式中,所述方法还包括:

所述网络认证设备向所述业务认证设备获取所述第一共享密钥;

所述网络认证设备根据所述第一共享密钥和第五共享密钥生成网络侧信息,所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥;

所述网络认证设备将所述网络侧信息发送给所述业务认证设备,以使所述业务认证设备向所述用户设备转发所述网络侧信息,所述网络参数属于所述参考信息。

结合第十九方面,或者第十九方面的第一种可能的实现方式,或者第十九方面的第二种可能的实现方式,或者第十九方面的第三种可能的实现方式,或者第十九方面的第四种可能的实现方式,或者第十九方面的第五种可能的实现方式,在第十九方面的第七种可能的实现方式中,所述网络认证设备根据所述第二共享密钥生成目标共享密钥之前,所述方法还包括:

所述网络认证设备将所述目标共享密钥发送给所述业务认证设备,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥用作所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

结合第十九方面,或者第十九方面的第一种可能的实现方式,或者第十九方面的第二

种可能的实现方式，或者第十九方面的第三种可能的实现方式，或者第十九方面的第四种可能的实现方式，或者第十九方面的第五种可能的实现方式，或者第十九方面的第六种可能的实现方式，或者第十九方面的第七种可能的实现方式，在第十九方面的第八种可能的实现方式中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

结合第十九方面的第八种可能的实现方式，在第十九方面的第九种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第二十方面，本发明实施例提供一种网络认证方法，该方法包括：

业务认证设备将预存的目标业务的业务参数发送给网络认证设备和用户设备；以使所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过执行上述步骤，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二十方面，在第二十方面的第一种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第二十一方面，本发明实施例提供一种网络认证方法，该方法包括：

用户设备接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给网络认证设备；

所述用户设备和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过执行上述步骤，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二十一方面，在第二十一方面的第一种可能的实现方式中，所述用户设备和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，包括：

所述用户设备和所述网络认证设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

所述用户设备和所述网络认证设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第二十一方面，或者第二十一方面的第一种可能的实现方式，在第二十一方面的第二种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第二十二方面，本发明实施例提供一种网络认证方法，该方法包括：

网络认证设备接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给用户设备；

所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过执行上述步骤，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二十二方面，在第二十二方面的第一种可能的实现方式中，所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

所述网络认证设备和所述用户设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第二十二方面，或者第二十二方面的第一种可能的实现方式，在第二十二方面的第二种可能的实现方式中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

第二十三方面，本发明实施例提供一种网络认证方法，该方法包括：

业务认证设备获取用户设备的身份标识；

所述业务认证设备结合自身的业务公钥、业务私钥和所述身份标识生成身份密钥，并将所述身份密钥、所述业务公钥发送给所述网络认证设备，所述身份密钥和所述业务公钥用于所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，

该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

第二十四方面，本发明实施例提供一种网络认证方法，该方法包括：

用户设备和网络认证设备根据认证根密钥进行网络认证生成目标共享密钥，所述认证根密钥为所述网络认证设备根据身份密钥、业务认证设备管理的目标业务的业务公钥和所述网络认证设备所在蜂窝网的网络参数生成的并写入到所述用户设备中的密钥，所述身份密钥由所述业务认证设备根据所述业务公钥、所述目标业务的业务私钥和获取的所述用户设备的身份标识生成的，所述业务认证设备用于将所述业务公钥和所述身份私钥发送给所述网络认证设备；所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二十四方面，在第二十四方面的第一种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第二十五方面，本发明实施例提供一种网络认证方法，该方法包括：

网络认证设备接收身份密钥和业务认证设备管理的目标业务的业务公钥，所述身份密钥为所述业务认证设备根据所述目标业务的业务私钥、所述业务公钥和获取的用户设备的身份标识生成的密钥；

所述网络认证设备结合所述身份密钥、所述业务公钥和所述网络认证设备所在蜂窝网的网络参数生成认证根密钥；

所述网络认证设备将所述认证根密钥写入所述用户设备；

所述网络认证设备和所述用户设备根据所述认证根密钥进行网络认证生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二十五方面，在第二十五方面的第一种可能的实现方式中，所述网络参数包括

运营商标识, 接入网络标识, 服务网络标识, 网络类型标识, 局域网网络标识, 切片标识, 承载标识, 服务质量标识和流标识中的至少一项。

第二十六方面, 本发明实施例提供一种网络认证方法, 包括:

业务认证设备和用户设备进行业务认证生成参考共享密钥, 或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥;

所述业务认证设备将所述参考共享密钥发送给网络认证设备, 以使所述网络认证设备和所述用户设备结合所述参考共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤, 该业务认证设备与该用户设备进行业务认证生成参考共享密钥, 然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数; 该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥, 并基于该认证共享密钥进行网络认证生成目标共享密钥。也就是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息, 提升了该目标共享密钥的安全级别。

结合第二十六方面, 在第二十六方面的第一种可能的实现方式中, 所述方法还包括:

所述业务认证设备接收所述网络认证设备发送的所述目标共享密钥;

所述业务认证设备将所述目标共享密钥, 或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

第二十七方面, 本发明实施例提供一种网络认证方法, 该方法包括:

用户设备和业务认证设备进行业务认证生成参考共享密钥, 或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥, 所述业务认证设备用于将所述参考共享密钥发送给网络认证设备;

所述用户设备和所述网络认证设备结合所述参考共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤, 该业务认证设备与该用户设备进行业务认证生成参考共享密钥, 然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数; 该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥, 并基于该认证共享密钥进行网络认证生成目标共享密钥。也就是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息, 提升了该目标共享密钥的安全级别。

结合第二十七方面, 在第二十七方面的第一种可能的实现方式中, 所述用户设备和所述网络认证设备结合所述参考共享密钥生成目标共享密钥之前, 所述方法还包括:

所述用户设备接收所述网络认证设备发送的所述网络认证设备所在蜂窝网的网络参数;

所述用户设备和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，包括：

所述用户设备和所述网络认证设备根据所述网络参数和所述参考共享密钥生成认证共享密钥；

所述用户设备和所述网络认证设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第二十七方面的第一种可能的实现方式，在第二十七方面的第二种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

第二十八方面，本发明实施例提供一种网络认证方法，该方法包括：

网络认证设备接收业务认证设备发送的参考共享密钥，所述参考共享密钥由所述业务认证设备和用户设备进行业务认证生成的或者预先配置的；

所述网络认证设备和所述用户设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述步骤，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

结合第二十八方面，在第二十八方面的第一种可能的实现方式中，所述网络认证设备和所述用户设备结合所述参考共享密钥生成目标共享密钥之前，所述方法还包括：

所述网络认证设备将所述网络认证设备所在蜂窝网的网络参数发送给所述用户设备；

所述网络认证设备和所述用户设备结合所述参考共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备均根据所述网络参数和所述参考共享密钥生成认证共享密钥；

所述网络认证设备和所述用户设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

结合第二十八方面的第一种可能的实现方式，在第二十八方面的第二种可能的实现方式中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

结合第二十八方面，或者第二十八方面的第一种可能的实现方式，或者第二十八方面的第二种可能的实现方式，在第二十八方面的第三种可能的实现方式中，所述方法还包括：

所述网络认证设备将所述目标共享密钥发送给所述业务认证设备，以使所述业务认证设备将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

第二十九方面，本发明实施例提供一种业务认证设备，所述业务认证设备包括处理器

和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第十七方面或者第十七方面的任意实现方式中的全部或部分步骤的功能单元。

第三十方面，本发明实施例提供一种用户设备，所述用户设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第十八方面或者第十八方面的任意实现方式中的全部或部分步骤的功能单元。

第三十一方面，本发明实施例提供一种网络认证设备，所述网络认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第十九方面或者第十九方面的任意实现方式中的全部或部分步骤的功能单元。

第三十二方面，本发明实施例提供一种业务认证设备，所述业务认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十方面或者第二十方面的任意实现方式中的全部或部分步骤的功能单元。

第三十三方面，本发明实施例提供一种用户设备，所述用户设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十一方面或者第二十一方面的任意实现方式中的全部或部分步骤的功能单元。

第三十四方面，本发明实施例提供一种网络认证设备，所述网络认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十二方面或者第二十二方面的任意实现方式中的全部或部分步骤的功能单元。

第三十五方面，本发明实施例提供一种业务认证设备，所述业务认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十三方面或者第二十三方面的任意实现方式中的全部或部分步骤的功能单元。

第三十六方面，本发明实施例提供一种用户设备，所述用户设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十四方面或者第二十四方面的任意实现方式中的全部或部分步骤的功能单元。

第三十七方面，本发明实施例提供一种网络认证设备，所述网络认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十五方面或者第二十五方面的任意实现方式中的全部或部分步骤的功能单元。

第三十八方面，本发明实施例提供一种业务认证设备，所述业务认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十六方面或者第二十六方面的任意实现方式中的全部或部分步骤的功能单元。

第三十九方面，本发明实施例提供一种用户设备，所述用户设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十七方面或者第二十七方面的任意实现方式中的全部或部分步骤的功能单元。

第四十方面，本发明实施例提供一种网络认证设备，所述网络认证设备包括处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第二十八方面或者第二十八方面的任意实现方式中的全部或部分步骤的功能单元。

在上面的一些可能的实现方式中，所述网络认证设备包括认证功能单元 CP-AU，所述网络认证设备和所述用户设备用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥中，所述网络认证设备和所述用户设

备用于根据所述第二共享密钥进行网络认证生成所述目标共享密钥，具体为：

UE 向 CP-AU 发送请求接入网络的消息，所述请求接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识，所述目标业务为所述 UE 当前执行的业务；

所述 CP-AU 接收所述请求接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；

所述 CP-AU 接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；

所述 CP-AU 将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码，并向所述 UE 发送认证请求消息，所述认证请求消息包含所述业务参考消息认证码；

所述 CP-AU 将通过预设的响应算法对所述第二共享密钥和所述初始期待响应进行计算得到的参考期待响应；

所述 UE 接收所述 CP-AU 发送的所述认证请求消息；

所述 UE 通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码，所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取，或者所述 UE 预先存储了所述第二共享密钥；

所述 UE 判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同；

若相同，则所述 UE 通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应；

所述 UE 将所述参考响应发送给所述 CP-AU；

所述 CP-AU 接收所述参考响应；

所述 CP-AU 判断所述参考期待响应与所述参考响应是否相同；

若相同，则所述 CP-AU 和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。可选的，所述基础密钥为基于所述预置密钥和网络参数生成的密钥。

在上面的一些可能的实现方式中，所述网络认证设备包括 CP-AU；用户设备 UE 执行所述和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥的操作中，和所述网络认证设备根据所述第二共享密钥进行网络认证生成目标共享密钥，具体为：

向 CP-AU 发送请求接入网络的消息，所述请求接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识，所述目标业务为所述 UE 当前执行的业务；所述 CP-AU 用于接收所述请求接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥，以及

向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;所述 CP-AU 还用于接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应;所述 CP-AU 还用于将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包括所述业务参考消息;所述 CP-AU 还用于通过所述预设的响应算法对所述第二共享密钥和所述初始期待响应进行处理得到参考期待响应;

接收所述认证请求消息;

通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同;

若相同,则通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应;

将所述参考响应发送给所述 CP-AU,所述 CP-AU 用于接收所述参考响应并判断所述参考期待响应与所述参考响应是否相同;

在所述 CP-AU 的判断结果为是时,与所述 CP-AU 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

在上面的一些可能的实现方式中,所述网络认证设备包括 CP-AU;所述和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥中,和所述用户设备根据所述第二共享密钥进行网络认证生成所述目标共享密钥,具体为:

接收所述 UE 发送的请求接入网络的消息并根据身份标识和业务标识获取第二共享密钥,以及向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;所述请求接入网络的消息包含所述 UE 的所述身份标识和目标业务的所述业务标识,所述目标业务为所述 UE 当前执行的业务;

接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应;

将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包含所述业务参考消息认证码;所述 UE 用于接收所述认证请求消息并通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的消息认证码算法对所述第二

共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码, 所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取, 或者所述 UE 预先存储了所述第二共享密钥;

所述 UE 还用于判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同; 所述 UE 用于在判断出相同时, 通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应; 所述 UE 还用于将所述参考响应发送给所述 CP-AU;

通过所述预设的响应算法对所述第二共享密钥和所述初始期待响应进行处理得到参考期待响应;

接收所述参考响应;

判断所述参考期待响应与所述参考响应是否相同;

若相同, 则和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。可选的, 所述基础密钥为基于所述预置密钥和网络参数生成的密钥。

在上面的一些可能的实现方式中, 所述网络认证设备包括认证功能单元 CP-AU, 所述网络认证设备和所述用户设备 UE 用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥中, 所述网络认证设备和所述用户设备用于根据所述第二共享密钥进行网络认证生成所述目标共享密钥, 具体为:

UE 向 CP-AU 发送接入网络的消息, 所述接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识, 所述目标业务为所述 UE 当前执行的业务;

所述 CP-AU 接收所述接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥, 以及向签约服务器请求基于预置密钥生成的认证向量, 所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;

所述 CP-AU 接收所述签约服务器发送的所述认证向量, 所述认证向量包含消息认证码和期待响应, 所述认证向量包含的所述消息认证码为网络侧初始消息认证码, 所述认证向量包含的期待响应为初始期待响应;

所述 CP-AU 将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码, 并向 UE 发送认证请求消息, 所述认证请求消息包括所述网络侧附加消息认证码和所述网络侧初始消息认证码;

所述 UE 接收所述 CP-AU 发送的所述认证请求消息;

所述 UE 通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应, 生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应, 并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码, 所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取, 或者所述 UE 预先存储了所述第二共享密钥;

所述 UE 判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同, 且所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同;

若均相同, 则所述 UE 通过预设的第二消息认证码算法对自身的所述第二共享密钥进

行处理得到用户侧响应消息认证码;

所述 UE 将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU;

所述 CP-AU 接收所述参考响应和所述用户侧响应消息认证码;

所述 CP-AU 通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码;

所述 CP-AU 判断所述初始期待响应是否与所述初始响应相同,且所述网络侧响应消息认证码是否与所述用户侧响应消息认证码相同;

若均相同,则所述 CP-AU 和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

在上面的一些可能的实现方式中,所述网络认证设备包括 CP-AU; 用户设备 UE 执行所述和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥的操作中,和所述网络认证设备根据所述第二共享密钥进行网络认证生成目标共享密钥,具体为:

向 CP-AU 发送接入网络的消息,所述接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识,所述目标业务为所述 UE 当前执行的业务; 所述 CP-AU 用于接收所述接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥,以及向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥; 所述 CP-AU 还用于接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应; 所述 CP-AU 还用于将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包含所述网络侧附加消息认证码和所述网络侧初始消息认证码;

接收所述 CP-AU 发送的所述认证请求消息;

通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同,且所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同;

若均相同,则通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码;

将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU; 所述 CP-AU 用于接收所述参考响应和所述用户侧响应消息认证码; 所述 CP-AU 还用于通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码; 所述 CP-AU 还用于判断所述初始期待响应是否与所述初始响应相同,且所述网络侧响应消息

认证码是否与所述用户侧响应消息认证码相同；

在所述 CP-AU 的判断结果为均相同时，和所述 CP-AU 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

在上面的一些可能的实现方式中，所述网络认证设备包括 CP-AU；所述和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥中，和所述用户设备 UE 根据所述第二共享密钥进行网络认证生成所述目标共享密钥，具体为：

接收 UE 发送的接入网络的消息并根据身份标识和业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；所述接入网络的消息包含所述 UE 的所述身份标识和目标业务的所述业务标识，所述目标业务为所述 UE 当前执行的业务；

接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；

将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码，并向 UE 发送认证请求消息，所述认证请求消息包括所述网络侧附加消息认证码和所述网络侧初始消息认证码发送给所述 UE；所述 UE 用于接收所述认证请求消息；所述 UE 用于通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码，所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取，或者所述 UE 预先存储了所述第二共享密钥；所述 UE 用于判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同，且判断所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同；若均相同，则所述 UE 用于通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码；所述 UE 还用于将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU；

接收所述参考响应和所述用户侧响应消息认证码；

通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码；

判断所述初始期待响应是否与所述初始响应相同，且所述网络侧响应消息认证码是否与所述用户侧响应消息认证码相同；

若均相同，则和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

通过实施本发明实施例，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的

安全级别。

附图说明

图 1 是本发明实施例提供的一种网络认证系统的结构示意图；
图 2 是本发明实施例提供的又一种网络认证系统的结构示意图；
图 3A 是本发明实施例提供的一种网络认证方法的流程示意图；
图 3B 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3C 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3D 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3E 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3F 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3G 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3H 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3I 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3J 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3K 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 3L 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 4A 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 5A 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 5B 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6A 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6B 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6C 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6D 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6E 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6F 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6G 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6H 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 6I 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 7 是本发明实施例提供的一种业务认证设备的结构示意图；
图 8 是本发明实施例提供的一种用户设备的结构示意图；
图 9 是本发明实施例提供的一种网络认证设备的结构示意图；
图 10 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 11 是本发明实施例提供的又一种用户设备的结构示意图；
图 12 是本发明实施例提供的又一种网络认证设备的结构示意图；
图 13 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 14 是本发明实施例提供的又一种用户设备的结构示意图；
图 15 是本发明实施例提供的又一种网络认证设备的结构示意图；

图 16 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 17 是本发明实施例提供的又一种用户设备的结构示意图；
图 18 是本发明实施例提供的又一种网络认证设备的结构示意图；
图 19 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 20 是本发明实施例提供的又一种用户设备的结构示意图；
图 21 是本发明实施例提供的又一种网络认证设备的结构示意图；
图 22 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 23 是本发明实施例提供的又一种用户设备的结构示意图；
图 24 是本发明实施例提供的又一种网络认证设备的结构示意图；
图 25 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 26 是本发明实施例提供的又一种用户设备的结构示意图；
图 27 是本发明实施例提供的又一种网络认证设备的结构示意图；
图 28 是本发明实施例提供的又一种业务认证设备的结构示意图；
图 29 是本发明实施例提供的又一种用户设备的结构示意图；
图 30 是本发明实施例提供的又一种网络认证设备的结构示意图；
图 31 是本发明实施例提供的一种网络认证系统的结构示意图；
图 32 是本发明实施例提供的又一种网络认证方法的流程示意图；
图 33 是本发明实施例提供的又一种网络认证方法的流程示意图。

具体实施方式

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描述。

请参见图 1，图 1 是本发明实施例提供的一种网络认证系统 10 的架构示意图；该网络认证系统 10 包括用户设备 101、业务认证设备 103 和运营商提供网络接入的网络认证设备 102。可选的，该业务认证设备 103 均为运营商可控的设备，即该运营商的网络认证设备 102 可以直接调用该业务认证设备 103 中的数据；可选的，该业务认证设备 103 为该运营商不可控的设备，即该运营商的网络认证设备 102 不可以直接调用该业务认证设备 103 中的数据。

该网络认证设备 102 可以为用户设备 101 需要接入蜂窝网时涉及到的至少一个网络侧设备，用户设备 101 在接入该蜂窝网时需要先与该网络认证设备 102 进行网络认证目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该网络认证设备与该用户设备协商的保护数据安全传输的共享密钥。

可选的，该用户设备 101 可以是手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备（英文：mobile internet device，简称：MID）、可穿戴设备（例如智能手表（如 iWatch 等）、智能手环、计步器等）或其可接入运营商网络的终端设备。

可选的，该网络认证设备 102 包括接入网（英文：Access Network，简称：AN）、移动性管理（英文：Mobility Management，简称：MM）设备、会话管理（英文：Session Management，简称：SM）设备、切片选择设备 SSF（英文：Slice Selection Function）、认证功能单元（英文：Control Plane-Authentication Unit，简称：CP-AU）、新配置与网络认

证相关的功能设备（为了方便描述后续可称为网络认证服务器）等中的至少一项，以下以该网络认证设备包括网络认证服务器、CP-AU 和 AN 为例来进行描述以方便理解。当该网络认证设备 102 只包括一个设备时，后续描述到的网络认证设备 102 所执行的操作均由该一个设备完成；当该网络认证设备 102 包括多个设备时，后续描述到的网络认证设备 102 所执行的操作由该多个设备协作完成，即该多个设备中不同设备各执行一些操作，执行操作所产生的数据、参数均可以根据需要在该多个设备之间传输。图 2 为该网络认证系统的一种可选的细化结构示意图。

该业务认证设备 103 至少存在如下两种情况：

一、该业务认证设备 103 是用来管理业务认证的设备，该业务认证设备 103 包括至少一个与业务相关的设备，用户设备 101 要使用某业务时需要与管理该某业务的业务认证设备 103 进行业务认证生成目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该业务认证设备与该用户设备协商的保护数据安全传输的共享密钥。

可选的，业务认证设备 103 可以为用户生成证书或者基于身份的私钥，最终发送给用户设备 101。生成证书时可使用户设备 101 与网络认证设备 102 相互认证时使用基于证书的方法；生成基于身份的私钥时，可以使得用户设备 101、网络相互认证时或者用户设备 101、业务认证设备 103 相互认证时可以使用基于身份的密码机制的方法。

在一种可选的方案中，用来提供业务的具体数据的设备（为了方便描述后续可称为业务服务器）和用来管理该业务的业务认证的设备（为了方便描述后续可称为业务认证服务器）为同一个设备，即该业务认证设备 103；在又一种可选的方案中，该业务认证设备 103 包括业务认证服务器，但是不包括业务管理服务器；在又一种可选的方案中，该业务认证设备 103 包括业务认证服务器和业务服务器，当该业务认证设备 103 包括业务服务器和业务认证服务器时，后续描述到的业务认证设备 103 所执行的操作可能由该业务认证服务器和业务服务器协作完成，该业务认证服务器和该业务服务器在操作过程中产生的数据、参数均可以根据需要进行相互传输。可选的，以上业务可以包括即时通讯业务、新闻资讯业务、水表业务、电表业务、物流业务、工厂自动化等业务。

二、该业务认证设备 103 不是用来提供业务的具体数据的设备，也不是用来管理业务的业务认证的设备，而是一个单纯的提供认证的设备，可以为该网络认证设备 102 和该业务认证设备 103 分担认证流程的设备。在 IoT 场景中，会有海量的用户设备 101 需要与该网络认证设备 102 进行网络认证，导致该网络认证设备 102 的负载较高，因此本发明实施例提供该业务认证设备 103 来分担该网络认证设备 102 的部分或全部流程。

请参见图 3A，图 3A 是本发明实施例提供的一种网络认证方法的流程示意图，该方法可以基于图 1 所示的网络认证系统来实现，该方法包括但不限于如下步骤。

步骤 S301：该业务认证设备获取参考信息并结合该参考信息和第一共享密钥生成第二共享密钥。

具体地，该参考信息包括该用户设备、该网络认证设备和该业务认证设备中至少一项预先关联的信息。

该用户设备预先关联的信息可以为该用户设备的身份标识（UEID），例如，移动设备国际识别码（英文：International Mobile Equipment Identity，简称：IMEI）、移动设备签约

标识（英文：International Mobile Subscriber Identity，简称：IMSI）媒体访问控制（英文：Media Access Control，简称：MAC）地址、互联网协议（英文：Internet Protocol，简称：IP）地址等能够在一定范围内用来与其他终端设备进行区分的信息。

该网络认证设备预先关联的信息可以为该网络认证设备所处蜂窝网的网络参数，例如公共陆地移动网络标识（PLMN ID），运营商标识（Operator ID），接入网络标识（Access Network ID），服务网络标识（Serving Network ID），网络类型标识（Network Type ID），局域网网络标识，切片标识，承载（bearer）ID，服务质量（英文：Quality of Service，简称：QoS）和流（flow）ID 等。所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

该业务认证设备预先关联的信息可以为该业务认证设备的身份标识、该业务特征相关的等信息，当该业务认证设备为管理目标业务的设备时，该业务认证设备预先关联的信息还可以包括目标业务的业务参数，例如，业务序列号 SN、密钥管理中心的标识、会话标识（session ID）、链路标识、应用标识（app ID）、切片标识、服务标识（service ID）、业务标识、业务等级、业务数据速率、时延和所在服务器的服务器标识等，该目标业务具体为什么业务此处暂不做限制，可选的，该目标业务为该用户设备当前需要访问的业务。该目标业务的业务参数可能预先存储在了该业务认证设备中，例如，该业务认证设备是用于管理该目标业务的业务认证流程的设备，那么可以预先将该目标业务的业务参数存储到该业务认证设备。该目标业务的业务参数也可能为其他设备在获得相应的触发操作后即时发送给该业务认证设备的，例如，该业务认证设备用来对用户设备进行业务认证，那么该网络认证设备会触发业务服务器将该目标业务的业务参数发送给该业务认证设备。

可以理解的是，该用户设备、网络认证设备和业务认证设备之间可以预先建立直接或者间接的连接关系，因此相互之间可获取所需要的参考信息。该参考信息也可能是预先配置在该用户设备、网络认证设备和业务认证设备中。

该第一共享密钥为该用户设备与该业务认证设备之间预先配置的共享密钥，包括该用户设备与该业务认证设备基于证书（certificate）、用户名与密码、身份密码机制等方式得到的共享密钥。该业务认证设备结合参考信息和第一共享密钥生成第二共享密钥旨在表明，计算该第二共享密钥用到的参数包含该参考信息和该第一共享密钥，不排除还要用到其他信息。

步骤 S302: 该用户设备获取该参考信息并结合该参考信息和该第一共享密钥生成该第二共享密钥。

具体地，该第二共享密钥用于该用户设备和该网络认证设备生成目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该网络认证设备与该用户设备协商的保护数据安全传输的共享密钥。

在一种可选的方案中，该方法还可以包括：该业务认证设备将该第二共享密钥发送给该网络认证设备；该网络认证设备接收该第二共享密钥；该网络认证设备和该用户设备根据该第二共享密钥或者根据基于该第二共享密钥衍生的共享密钥进行网络认证生成该目标共享密钥。为了方便理解，以下通过图 3B 和 3C 结合不同的几个场景进行具体描述。

请参见图 3B，图 3B 是本发明实施例提供的一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器；该用户设备与该业务认证设备预先共享了第一共享密钥，该方法包括步骤 S401~S410，各个步骤的详细描述如下：

步骤 S401：用户设备向网络认证服务器发送第一请求消息。

步骤 S402：该网络认证服务器接收该第一请求消息，并根据该第一请求消息查找相应的业务认证服务器后，向该业务认证服务器发送第二认证请求。

具体地，该第一请求消息可以包含一些标识信息来表明该用户设备想要请求什么业务；该网络认证服务器根据该第一请求消息获知该用户设备想要请求哪种业务后，向该业务认证服务器发送第二请求消息，该第二请求消息可以包含该用户设备的身份标识（UEID）。

步骤 S403：该业务认证服务器接收该第二请求消息，并根据该第二认证消息获取业务参数，该业务参数即属于上述参考信息；可选的，该业务参数存储在该业务认证服务器的存储空间中，该业务认证服务器通过读取该存储空间来获取该业务参数。可选的，该业务参数存储在该业务服务器上，该业务认证服务器可以向该业务服务器请求该业务参数。

步骤 S404：该业务认证服务器将该业务参数发送给该网络认证服务器；

步骤 S405：该网络认证服务器用于接收并向该用户设备转发该业务参数；

步骤 S406：该业务认证服务器根据第一共享密钥、该用户设备的 UEID、网络参数、业务参数等信息来生成第二共享密钥。

步骤 S407：该用户设备根据第一共享密钥、该用户设备的 UEID 和该业务参数来生成第二共享密钥。

步骤 S408：该业务认证服务器将该第二共享密钥发送给该网络认证服务器。

步骤 S409：该网络认证服务器接收并向该 CP-AU 转发该第二共享密钥。可选的，该业务认证服务器还可能直接将该第二共享密钥发送给该 CP-AU，相应地，该 CP-AU 接收该业务认证服务器发送的该第二共享密钥。

步骤 S410：该 CP-AU 接收该第二共享密钥并基于该第二共享密钥与该用户设备进行网络认证生成目标共享密钥，该网络认证可以通过认证与密钥协商协议（英文：Authentication and Key Agreement，简称：AKA）等认证技术来实现。

可选的，当该网络认证设备包含多个设备时，接收第一请求消息、认证用户设备、查找业务认证服务器、给该业务认证服务器发送第二请求消息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成，例如，可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成，或者该多个网元中的至少两个网元协同完成。

可选的，该网络认证服务器向该用户设备发送网络参数，该用户设备相应地接收该网络参数；该网络认证服务器和该用户设备均基于该第二共享密钥和该网络参数生成新的共享密钥，该网络认证服务器还将该新的共享密钥发送给该 CP-AU；该 CP-AU 与该用户设备基于该新的共享密钥进行网络认证生成目标共享密钥。

可选的，该用户设备每次发送该第一请求消息便执行一次生成目标共享密钥的流程，保证了安全性和随机性。

可选的，网络认证设备与业务认证设备提前协商以获得业务参数，当用户设备发送该

第一请求消息时，网络认证设备才发送业务参数给该用户设备以使用户设备和该业务认证设备可以基于该业务参数生成。

可选的，该用户设备提前获取相关参数(如果业务参数提前获取或写入)，根据该业务参数对应推导出第二共享密钥，网络认证服务器获取该第二共享密钥后，UE 和网络认证服务器可以进一步基于网络参数和第二共享密钥生成该目标共享密钥。

可选的，该 UE 还含有与网络认证设备共享的根密钥，网络认证设备获取第二共享密钥后，UE 与网络认证设备基于与网络认证设备共享的根密钥和第二共享密钥相互认证生成该目标根密钥。

在图 3B 所示的方法中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图 3C，图 3C 是本发明实施例提供的一种网络认证方法的流程示意图，该业务认证设备可以为单纯具备认证功能的第三方，例如，具备认证、授权和计费（英文：Authentication Authorization Accounting，简称：AAA）功能的 AAA 服务器，下面实施例以业务认证设备为 AAA 服务器为例来描述，该用户设备与该业务认证设备预先共享了第一共享密钥，该方法包括步骤 S501~S507，各个步骤的详细描述如下：

步骤 S501：用户设备向 AN 发送第一请求消息，该第一请求消息可以携带该用户设备的身份标识 UEID，可能还有目标业务的业务标识，AAA 服务器标识（如 AAA ID）等。

步骤 S502：该 AN 接收该第一请求消息并根据该第一请求消息查找对应的 AAA 服务器，并向查找到的 AAA 服务器发送第二请求消息，该第二请求消息携带该用户设备的身份标识 UEID，可能还有运营商标识、业务标识、业务参数、AAA 服务器标识等信息。

步骤 S503：该 AAA 服务器接收该第二请求消息，基于 UEID 和第一共享密钥来生成第二共享密钥，生成该第二共享密钥还可能考虑了其他信息，例如，该其他信息可以包括网络参数、业务参数和 UEID 中至少一项，该其他信息属于该参考信息。

步骤 S504：AAA 服务器将该第二共享密钥发送给网络认证服务器。

步骤 S505：该网络认证服务器接收并向 CP-AU 发送该第二共享密钥；可选的，该 AAA 服务器还可能直接将该第二共享密钥发送给该 CP-AU，相应地，该 CP-AU 接收该 AAA 服务器发送的该第二共享密钥。

步骤 S506：该用户设备基于该 UEID 和该第一共享密钥生成该第二共享密钥；当生成该第二共享密钥还需要其他信息时，该用户设备还可以向其他设备获取该其他信息。

步骤 S507：该用户设备与 CP-AU 基于该第二共享密钥进行网络认证生成目标共享密钥。

可选的，该网络认证服务器在接收到该第二共享密钥后，结合该第二共享密钥和相关信息（例如，网络参数）生成新的共享密钥，并将该新的共享密钥发送给该 CP-AU；该用户设备相应地从该网络认证设备获取该相关信息，并结合该第二共享密钥和该相关信息生

成新的共享密钥。相应地，步骤 S507 就调整为通过新的共享密钥进行网络认证。

可选的，当该网络认证设备包含多个设备时，接收第一请求消息、认证用户设备、查找 AAA 服务器、给 AAA 服务器发送第二请求消息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成，例如，可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成，或者该多个网元中的至少两个网元协同完成。

可选的，该网络认证设备中可以预存 AAA 服务器标识、业务参数等信息与该 AAA 服务器的对应关系，因此可以基于 AAA 服务器标识、业务参数等信息查找对应的 AAA 服务器。

可选的，该 UE 还含有与网络认证设备共享的根密钥，网络认证设备获取第二共享密钥后，UE 与网络认证设备基于与网络共享的根密钥和第二共享密钥相互认证生成该目标根密钥。

在图 3C 所示的方法中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥进行网络认证生成目标共享密钥。也就是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

在又一种可选的方案中，所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。该方法还可以包括：所述业务认证设备用于将所述第二共享密钥发送给所述网络认证设备；所述网络认证设备用于接收所述第二共享密钥；所述网络认证设备和所述用户设备用于将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。为了方便理解，以下根据图 3D 结合具体场景进行描述。

请参见图 3D，图 3D 是本发明实施例提供的一种网络认证方法的流程示意图，该业务认证设备可以为单纯具备认证功能的第三方，例如，具备 AAA 功能的 AAA 服务器，下面实施例以业务认证设备为 AAA 服务器为例来描述，该用户设备与该业务认证设备预先共享了第一共享密钥，该方法包括步骤 S601~S607，各个步骤的详细描述如下：

步骤 S601：用户设备向 AN 发送第一请求消息，该第一请求消息可以携带该用户设备的身份标识 UEID，可能还有业务标识，AAA 服务器标识（如 AAA ID）等。

步骤 S602：该 AN 接收该第一请求消息并根据该第一请求消息查找对应的 AAA 服务器的信息，例如，IP 地址信息、MAC 地址信息等，然后将该 AAA 服务器的信息发送给该用户设备。

步骤 S603：该用户设备接收该 AAA 服务器的信息。

步骤 S604：该用户设备根据该 AAA 服务器的信息与该 AAA 服务器进行业务认证生成第二共享密钥，业务认证的过程使用到了该第一共享密钥和参考信息，该参考信息可以包括该用户设备的身份标识 UEID、该网络认证设备发送给该用户设备的网络参数、业务认证设备获取的业务参数等。

步骤 S605：该 AAA 服务器将该第二共享密钥发送给该网络认证服务器。

步骤 S606：该网络认证服务器接收并向 CP-AU 转发该第二共享密钥。

步骤 S607: 该 CP-AU 接收该第二共享密钥并将该第二共享密钥作为目标共享密钥, 该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥; 也即是说, 该用户设备与该 CP-AU 之间可以不再进行网络认证来生成保护数据安全传输的共享密钥; 可选的, 该 SM、MM、SSF、AN 等网元也可以被共享该第二共享密钥。

可选的, 当该网络认证设备包含多个设备时, 接收第一请求消息、认证用户设备、查找 AAA 服务器的信息、向用户设备发送该 AAA 服务器的信息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成, 例如, 可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成, 或者该多个网元中的至少两个网元协同完成。

可选的, 该网络认证服务器接收到该第二共享密钥后, 结合该用户设备的 UEID、该网络参数等信息生成新的共享密钥; 该用户设备相应的接收该网络认证设备发送的网络参数, 然后基于该第二共享密钥、UEID、网络参数等信息生成该新的共享密钥; 该网络认证服务器将该新的共享密钥发送给该 CP-AU, 该 CP-AU 和该用户设备可以将该新的共享密钥作为该目标共享密钥。可选的, 该网络认证设备与该用户设备可以基于该第二共享密钥 (或该新的共享密钥) 进行网络认证生成该目标共享密钥。

可选的, 该 UE 还含有与网络认证设备共享的根密钥, 网络认证设备获取第二共享密钥后, UE 与网络认证设备基于与网络共享的根密钥和第二共享密钥相互认证生成该目标根密钥。

可选的, 该网络认证设备和该用户设备均有了第二共享密钥时, 该网络认证设备可以将网络参数发送给该用户设备, 然后基于该第二共享密钥和该网络参数生成该目标共享密钥。

在图 3D 所示的方法中, 用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥进行相互认证生成第二共享密钥, 然后该业务认证设备将该第二共享密钥发送给该网络认证设备, 使得该网络认证设备和该用户设备将该第二共享密钥作为该目标共享密钥。也即是说, 该业务认证设备和该用户设备生成的第二共享密钥直接作为该网络认证设备的目标共享密钥, 同时该第二共享密钥还可以作为该业务认证设备自身的目标共享密钥, 相当于执行上述流程完成了网络认证和业务认证这两次认证, 提高了认证的效率。

进一步地, 该方法还可以包括: 该网络认证设备和该用户设备进行网络认证生成第三共享密钥; 该网络认证设备和该用户设备根据该第二共享密钥或者根据基于该第二共享密钥衍生的共享密钥进行网络认证生成该目标共享密钥, 具体为: 该网络认证设备和该用户设备结合该第二共享密钥进行网络认证生成第四共享密钥, 根据该第三共享密钥和该第四共享密钥生成该目标共享密钥。为了方便理解, 以下通过图 3E 和 3F 结合具体场景进行描述。

请参见图 3E, 图 3E 是本发明实施例提供的一种网络认证方法的流程示意图, 该业务认证设备可以为单纯具备认证功能的第三方, 例如, 具备 AAA 功能的 AAA 服务器, 下面实施例以业务认证设备为 AAA 服务器为例来描述, 该用户设备与该业务认证设备预先共享

了第一共享密钥，该方法包括步骤 S701~S709，各个步骤的详细描述如下：

步骤 S701：该 CP-AU 与该用户设备进行网络认证生成第三共享密钥。

步骤 S702：用户设备向 AN 发送第一请求消息，该第一请求消息可以携带该用户设备的身份标识 UEID，可能还有业务标识，AAA 服务器信息等。

步骤 S703：该 AN 接收该第一请求消息并根据该第一请求消息查找对应的 AAA 服务器，并向查找到的 AAA 服务器发送第二请求消息，该第二请求消息携带该用户设备的身份标识 UEID，可能还有业务参数、网络参数等信息。

步骤 S704：该 AAA 服务器接收该第二请求消息，基于第一共享密钥来生成第二共享密钥，生成该第二共享密钥还可能考虑了其他信息，例如，UEID、网络参数和业务参数中至少一项，该其他信息均属于该参考信息。

步骤 S705：该 AAA 服务器将该第二共享密钥发送给网络认证服务器。

步骤 S706：该网络认证服务器接收并向该 CP-AU 转发该第二共享密钥。

步骤 S707：该用户设备基于该 UEID 和该第一共享密钥生成该第二共享密钥；当生成该第二共享密钥还需要其他信息时，该用户设备还可以向其他设备获取该其他信息。

步骤 S708：该用户设备与该 CP-AU 基于该第二共享密钥或者基于该第二共享密钥衍生的共享密钥进行网络认证生成第四共享密钥。

步骤 S709：该用户设备与该 CP-AU 均根据该第三共享密钥和该第四共享密钥生成目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥。

可选的，当该网络认证设备包含多个设备时，接收第一请求消息、认证用户设备、查找 AAA 服务器的信息、向该 AAA 服务器发送第二请求消息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成，例如，可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成，或者该多个网元中的至少两个网元协同完成。

可选的，该用户设备与该 CP-AU 还可以不基于该第二共享密钥进行认证，而是各自根据该第二共享密钥和该第三共享密钥生成该目标共享密钥。该第三共享密钥或者基于该第三共享密钥衍生的共享密钥用来保护公共数据的安全传输，该第二共享密钥或者基于该第二共享密钥衍生的共享密钥用来保护特定业务数据的安全传输。

可选的，该用户设备与该 CP-AU 还可以基于该第三共享密钥和该第二共享密钥进行相互认证，或者基于该第三共享密钥和该第二共享密钥衍生的共享密钥进行相互认证。

可选的，该 UE 还含有与网络认证设备共享的根密钥，网络认证设备获取第二共享密钥后，UE 与网络认证设备基于与网络共享的根密钥和第二共享密钥相互认证生成该目标共享密钥。

可选的，该 UE 还含有与网络认证设备共享的根密钥，该用户设备和该 CP-AU 之间的网络认证可以基于该共享根密钥完成以生成第三共享密钥。

进一步地，该方法还可以包括：该网络认证设备还用于将该目标共享密钥发送给该业务认证设备；该业务认证设备用于接收该目标共享密钥；该业务认证设备和该用户设备用于将该目标共享密钥或者基于该目标共享密钥衍生的共享密钥作为该业务认证设备与该用

户设备协商的保护数据安全传输的共享密钥。

在图 3E 所示的方法中，该网络认证设备与该用户设备进行网络认证生成第三共享密钥，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，该网络认证设备与该用户设备进行网络认证生成第四共享密钥；该用户设备和该网络认证设备均根据第一次认证生成的该第三共享密钥和第二次认证生成的第四共享密钥生成目标共享密钥，也就是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图 3F，图 3F 是本发明实施例提供的一种网络认证方法的流程示意图，该业务认证设备可以包括业务认证服务器和业务服务器，例如，该业务认证服务器可以为具备 AAA 功能的 AAA 服务器，下面实施例以业务认证服务器为 AAA 服务器为例来描述，该用户设备与该业务认证设备预先共享了第一共享密钥，该方法包括步骤 S711~S719，各个步骤的详细描述如下：

步骤 S711：该 CP-AU 与该用户设备进行网络认证生成第三共享密钥。

步骤 S712：用户设备向 AN 发送第一请求消息，该第一请求消息可以携带该用户设备的身份标识 UEID，可能还有业务标识等。

步骤 S713：该 AN 接收该第一请求消息并根据该第一请求消息查找对应的 AAA 服务器，并向查找到的 AAA 服务器发送第二请求消息，该第二请求消息携带该用户设备的身份标识 UEID，可能还有业务参数、网络参数等信息。

步骤 S714：该 AAA 服务器接收该第二请求消息，向业务服务器申请获取业务参数，业务服务器返回业务参数，该 AAA 服务器基于第一共享密钥来生成第二共享密钥，生成该第二共享密钥还可能考虑了其他信息，例如，UEID、网络参数和业务参数中至少一项，该其他信息属于该参考信息。

步骤 S715：该 AAA 服务器将该第二共享密钥发送给网络认证服务器。

步骤 S716：该网络认证服务器接收并向该 CP-AU 转发该第二共享密钥。

步骤 S717：该用户设备基于该第一共享密钥生成该第二共享密钥；生成该第二共享密钥还可能考虑了该其他信息，当生成该第二共享密钥还需要其他信息时，该用户设备还可以向其他设备获取该其他信息。

步骤 S718：该用户设备与该 CP-AU 基于该第二共享密钥进行网络认证生成第四共享密钥。

步骤 S719：该用户设备与该 CP-AU 均根据该第三共享密钥和该第四共享密钥生成目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥。

可选的，该用户设备与该 CP-AU 还可以不基于该第二共享密钥进行认证，而是各自根据该第二共享密钥和该第三共享密钥生成该目标共享密钥。

可选的，该第三共享密钥或者基于该第三共享密钥衍生的共享密钥用来保护公共数据的安全传输，该第二共享密钥或者基于该第二共享密钥衍生的共享密钥用来保护特定业务

数据的安全传输。也即是说，将该第二共享密钥或者基于该第二共享密钥衍生的共享密钥作为一种类型的目标共享密钥，将该第三共享密钥或者基于该第三共享密钥衍生的共享密钥作为另一种共享密钥。

可选的，该用户设备与该 CP-AU 还可以基于该第三共享密钥和该第二共享密钥进行相互认证生成目标共享密钥，或者基于该第三共享密钥和该第二共享密钥衍生的共享密钥进行相互认证生成目标共享密钥。

可选的，该 UE 还含有与网络认证设备共享的根密钥，网络认证设备获取第二共享密钥后，UE 与网络认证设备基于与网络共享的根密钥和第二共享密钥相互认证生成该目标根密钥。

可选的，该 UE 还含有与网络认证设备共享的根密钥，该用户设备与网络认证设备基于该根密钥相互认证获取第三共享密钥。

可选的，当该网络认证设备包含多个设备时，接收第一请求消息、查找 AAA 服务器、给 AAA 服务器发送第二请求消息和与用户设备相互认证的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成，例如，可以由 SM、MM、SSF、CP-AU、网络认证服务器等多个网元中的一个网元单独完成，或者该多个网元中的至少两个网元协同完成。

进一步地，该方法还可以包括：该网络认证设备还用于将该目标共享密钥发送给该业务认证设备；该业务认证设备用于接收该目标共享密钥；该业务认证设备和该用户设备用于将该目标共享密钥或者基于该目标共享密钥衍生的共享密钥作为该业务认证设备与该用户设备协商的保护数据安全传输的共享密钥。

在图 3F 所示的方法中，该网络认证设备与该用户设备进行网络认证生成第三共享密钥，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，该网络认证设备与该用户设备进行网络认证生成第四共享密钥；该用户设备和该网络认证设备均根据第一次认证生成的该第三共享密钥和第二次认证生成的第四共享密钥生成目标共享密钥，也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

在又一种可选的方案中，该方法还可以包括：该网络认证设备与该用户设备进行网络认证生成第三共享密钥；所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。该业务认证设备将该第二共享密钥发送给该网络认证设备；该网络认证设备接收该第二共享密钥；该网络认证设备和该用户设备均根据该第二共享密钥和该第三共享密钥生成该目标共享密钥；或者将该第二共享密钥和该第三共享密钥分别作为保护不同类型数据的该目标共享密钥，例如，该第三共享密钥或者基于该第三共享密钥衍生的共享密钥用来保护公共数据的安全传输，该第二共享密钥或者基于该第二共享密钥衍生的共享密钥用来保护特定业务数据的安全传输。为了方便理解，以下根据图 3G 和 3H 结合具体场景进行描述。

请参见图 3G，图 3G 是本发明实施例提供的一种网络认证方法的流程示意图，该业务

认证设备可以为单纯具备认证功能的第三方，例如，具备 AAA 功能的 AAA 服务器，下面实施例以业务认证设备为 AAA 服务器为例来描述，该用户设备与该业务认证设备预先共享了第一共享密钥，该方法包括步骤 S801~S808，各个步骤的详细描述如下：

步骤 S801：该 CP-AU 与该用户设备进行网络认证生成第三共享密钥。

步骤 S802：用户设备向 AN 发送第一请求消息，该第一请求消息可以携带该用户设备的身份标识 UEID，可能还有业务标识等。

步骤 S803：该 AN 接收该第一请求消息并根据该第一请求消息查找对应的 AAA 服务器的信息，例如，IP 地址信息、MAC 地址信息等，然后将该 AAA 服务器的信息发送给该用户设备。

步骤 S804：该用户设备根据该 AAA 服务器的信息与该 AAA 服务器进行业务认证生成第二共享密钥，业务认证的过程使用到了该第一共享密钥和参考信息，该参考信息可以包括该用户设备的身份标识 UEID、该 CP-AU 发送给该用户设备的网络参数、业务参数等。

步骤 S805：该 AAA 服务器将该第二共享密钥发送给该网络认证服务器。

步骤 S806：该网络认证服务器用于接收并向该 CP-AU 转发该第二共享密钥。

步骤 S807：该 CP-AU 接收该第二共享密钥。

步骤 S808：该用户设备和该 CP-AU 均根据该第二共享密钥和该第三共享密钥生成目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥。

可选的，该用户设备和该网络认证服务器还有预先配置的共享根密钥时，该用户设备和该 CP-AU 之间的网络认证可以基于该共享根密钥完成以生成第三共享密钥。

可选的，该用户设备含有该 AAA 服务器的信息时，该 AN 无须再将 AAA 服务器信息返回给该用户设备。

可选的，当该网络认证设备包含多个设备时，接收第一请求消息、认证用户设备、查找 AAA 服务器的信息、向用户设备发送该 AAA 服务器的信息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成，例如，可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成，或者该多个网元中的至少两个网元协同完成。可选的，该第三共享密钥或者基于该第三共享密钥衍生的共享密钥用来保护公共数据的安全传输，该第二共享密钥或者基于该第二共享密钥衍生的共享密钥用来保护特定业务数据的安全传输。也即是说，将第二共享密钥或者基于该第二共享密钥衍生的共享密钥作为一种类型的目标共享密钥，将第三共享密钥或者基于该第三共享密钥衍生的共享密钥作为另一种类型的目标共享密钥。

在图 3G 所示的方法中，该网络认证设备与该用户设备进行网络认证生成第三共享密钥，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥进行网络认证生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备；该用户设备和该网络认证设备均根据该第三共享密钥和第二共享密钥生成目标共享密钥，也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图 3H, 图 3H 是本发明实施例提供的一种网络认证方法的流程示意图, 该业务认证设备可以包括业务认证服务器和业务服务器, 例如, 该业务认证服务器可以为具备 AAA 功能的 AAA 服务器, 下面实施例以业务认证服务器为 AAA 服务器为例来描述, 该用户设备与该业务认证设备预先共享了第一共享密钥, 该方法包括步骤 S811~S818, 各个步骤的详细描述如下:

步骤 S811: 该 CP-AU 与该用户设备进行网络认证生成第三共享密钥。

步骤 S812: 用户设备向 AN 发送第一请求消息, 该第一请求消息可以携带该用户设备的身份标识 UEID, 可能还有业务标识等。

步骤 S813: 该 AN 接收该第一请求消息并根据该第一请求消息查找对应的 AAA 服务器的信息, 例如, IP 地址信息、MAC 地址信息等, 然后将该 AAA 服务器的信息发送给该用户设备。

步骤 S814: 该用户设备根据该 AAA 服务器的信息与该 AAA 服务器进行业务认证生成第二共享密钥, 业务认证的过程使用到了该第一共享密钥和参考信息, 该参考信息可以包括该用户设备的身份标识 UEID、该 CP-AU 发送给该用户设备的网络参数、业务参数等。

步骤 S815: 该 AAA 服务器将该第二共享密钥发送给该网络认证服务器。

步骤 S816: 该网络认证服务器用于接收并向该 CP-AU 转发该第二共享密钥。

步骤 S817: 该 CP-AU 接收该第二共享密钥。

步骤 S818: 该用户设备和该 CP-AU 均根据该第二共享密钥和该第三共享密钥生成目标共享密钥, 该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥。

可选的, 该第三共享密钥或者基于该第三共享密钥衍生的共享密钥用来保护公共数据的安全传输, 该第二共享密钥或者基于该第二共享密钥衍生的共享密钥用来保护特定业务数据的安全传输。也即是说, 将第二共享密钥或者基于该第二共享密钥衍生的共享密钥作为一种类型的目标共享密钥, 将第三共享密钥或者基于该第三共享密钥衍生的共享密钥作为另一种类型的目标共享密钥。

可选的, 当该网络认证设备包含多个设备时, 接收第一请求消息、认证用户设备、查找 AAA 服务器的信息、向用户设备发送该 AAA 服务器的信息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成, 例如, 可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成, 或者该多个网元中的至少两个网元协同完成。可选的, 该 UE 还含有与网络认证设备共享的根密钥, 该用户设备与网络认证设备基于该根密钥相互认证获取第三共享密钥。

在图 3H 所示的方法中, 该网络认证设备与该用户设备进行网络认证生成第三共享密钥, 用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥进行网络认证生成第二共享密钥, 然后该业务认证设备将该第二共享密钥发送给该网络认证设备; 该用户设备和该网络认证设备均根据该第三共享密钥和第二共享密钥生成目标共享密钥, 也即是说, 生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息, 提升了该目标共享密钥的安全级别。

在又一种可选的方案中，该方法还可以包括：该参考信息为该网络认证设备所在蜂窝网的网络参数；该结合该参考信息和第一共享密钥生成第二共享密钥，具体为：该业务认证设备与该用户设备根据该参考信息和该第一共享密钥进行业务认证生成第二共享密钥。该业务认证设备将该第二共享密钥发送给该网络认证设备；该网络认证设备接收该第二共享密钥并将该第二共享密钥作为该目标共享密钥。为了方便理解，以下根据图 3I 结合具体场景进行描述。

请参照图 3I，图 3I 为本发明实施例提供的一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器，该业务服务器用于提供业务的访问，业务认证过程中如果需要使用业务参数，那么该业务参数可能存储在该业务认证服务器中，也可能存在该业务服务器中。该用户设备与该业务认证设备预先共享了第一共享密钥，该方法可以包括步骤 SA901~S907，各个步骤的详细描述如下。

步骤 S901：用户设备向网络认证服务器发送第一请求消息，该第一请求消息可以包含该用户设备的身份标识 UEID，还可能包含与目标业务相关的信息。

步骤 S902：该网络认证服务器接收该第一请求消息，并根据该第一请求消息向该业务认证服务器发送第二请求消息。

具体地，该第一请求消息可以包含一些标识信息来表明该用户设备想要请求什么业务；该网络认证设备根据该第一请求消息获知该用户设备想要请求哪种业务后，向该业务认证设备发送第二请求消息，该第二请求消息可以包含该用户设备的身份标识（UEID），该第二请求消息还可能包含该网络认证服务器所在蜂窝网的网络参数。

步骤 S903：该业务认证服务器接收该第二请求消息；该业务认证服务器还可以获取目标业务的业务参数，该业务参数可能存储在该业务认证服务器中，也可能存储在该业务服务器中，当存储在该业务服务器中时该业务认证服务器向该业务服务器发送请求该业务参数的请求消息，该业务服务器相应地返回该业务参数给该业务认证服务器。

步骤 S904：该业务认证服务器与该用户设备基于该第一共享密钥进行业务认证生成第二共享密钥，该业务认证过程中还可能用到了业务参数、网络参数、UEID 等信息，用到的除该第一共享密钥的信息均可属于该参考信息，用户设备用到的业务参数和网络参数可以由该网络认证服务器发送。

步骤 S905：该业务认证服务器将该第二共享密钥发送给该网络认证服务器。

步骤 S906：该网络认证服务器接收并转发该第二共享密钥给该 CP-AU。

步骤 S907：该 CP-AU 接收该第二共享密钥，此时该用户设备与该 CP-AU 均具有该第二共享密钥，因此可以将该第二共享密钥直接确定为目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥，可以省去该用户设备再与该 CP-AU 进行网络认证的过程。

可选的，当该网络认证设备包含多个设备时，接收第一请求消息、向业务认证服务器发送第二请求消息和接收第二共享密钥的动作可能由该多个设备中任一设备完成或者相关功能设备协同完成，例如，可以由 SM、MM、SSF、CP-AU 等多个网元中的一个网元单独完成，或者该多个网元中的至少两个网元协同完成。

可选的，该业务认证服务器和该用户设备均可以根据该第一共享密钥，再结合一些其

他信息（例如，网络参数，业务参数、UEID 等）来生成新的共享密钥。这样一来，在步骤 S904 中，该业务认证服务器与该用户设备具体结合该新的共享密钥进行网络认证生成第二共享密钥。

可选的，用户设备与该业务服务器在进行业务认证的过程时，交互的信息可以由该网络认证设备转发，也可以不经过该网络认证设备转发，例如，通过有线网络直接发送。

在图 3I 所示的方法中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥进行业务认证生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备将该第二共享密钥作为目标共享密钥。也即是说，该业务认证设备和该用户设备生成的第二共享密钥直接作为该网络的目标共享密钥，同时该第二共享密钥还可以作为该业务自身的目标共享密钥，相当于执行上述流程完成了网络认证和业务认证这两次认证，提高了认证的效率。

请参照图 3J，图 3J 为本发明实施例提供的一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务和业务服务器，该业务服务器用于提供业务的访问，业务认证过程中如果需要使用业务参数，那么该业务参数可能存储在该业务认证服务器中，也可能存在该业务服务器中。该用户设备与该业务认证设备预先共享了第一共享密钥，该方法可以包括步骤 S1001~S1007，各个步骤的详细描述如下。

步骤 S1001：该用户设备向该业务服务器发送第一请求消息。

步骤 S1002：该业务服务器接收该第一请求消息，并根据该第一请求消息向该 CP-AU 发送第二请求消息，该第二请求消息用于请求该 CP-AU 反馈该 CP-AU 所在网络的网络参数给该业务认证服务器。

步骤 S1003：该 CP-AU 向该业务认证服务器发送该网络参数。

步骤 S1004：该业务认证服务器接收该网络参数，并将该网络参数和目标业务的业务参数发送给该用户设备。

步骤 S1005：该用户设备接收该网络参数和该业务参数。

步骤 S1006：该业务认证服务器与该用户设备根据该第一共享密钥、该网络参数和该业务参数进行业务认证生成第二共享密钥，生成该第二共享密钥用到的信息中，除该第一共享密钥外均可以属于该参考信息。

步骤 S1007：该业务认证服务器将该第二共享密钥发送给该 CP-AU，该 CP-AU 可能还要将该第二共享密钥发送给该网络认证服务器存储备用。由于该 CP-AU 和该用户设备均具有该第二共享密钥，因此该将该第二共享密钥作为目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥，可以省去该用户设备再与该 CP-AU 进行网络认证。

可选的，接收和发送该第一请求消息、第二请求消息的设备可以为该业务服务器，也可以为该业务认证服务器，或者该业务认证设备包括的其他设备；

可选的，网络认证设备中用于接收该第二请求消息的设备可以为该 CP-AU，也可以为该网络认证设备中的其他设备，如，网络认证服务器、CP-AU、MM、SM、AN 等。

可选的，该用户设备用到的业务参数除了由该业务认证服务器发送外，还可以是预置

在该用户设备中的。

可选的，该 CP-AU 和该用户设备还可以基于该第二共享密钥进一步生成新的共享密钥，然后基于该新的共享密钥、网络参数、业务参数来生成该目标共享密钥。

可选的，该 CP-AU 与该用户设备还可以进一步基于该第二共享密钥进行网络认证生成该目标共享密钥。

可选的，该业务认证设备不发送第二共享密钥给网络认证设备，该网络认证设备只需要知道该用户设备认证成功即可。

在图 3J 所示的方法中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥进行业务认证生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备将该第二共享密钥作为目标共享密钥。也即是说，该业务认证设备和该用户设备生成的第二共享密钥直接作为该网络认证设备的目标共享密钥，同时该第二共享密钥还可以作为该业务认证设备自身的目标共享密钥，相当于执行上述流程完成了网络认证和业务认证这两次认证，提高了认证的效率。

在又一种可选的方案中，该方法还可以包括：该业务认证设备获取该用户设备与该网络认证设备之间预先配置的第五共享密钥；该结合该参考信息和第一共享密钥生成第二共享密钥，具体为：结合该参考信息、第一共享密钥和该第五共享密钥进行业务认证生成第二共享密钥。该业务认证设备将该第二共享密钥发送给该网络认证设备；该网络认证设备接收该第二共享密钥并将该第二共享密钥作为该目标共享密钥。为了方便理解，以下根据图 3K 结合具体场景进行描述。

请参见图 3K，图 3K 是本发明实施例提供的一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器。该用户设备与该业务认证设备预先共享了第一共享密钥，该用户设备与该网络认证设备预先共享了第五共享密钥；该方法可以包括步骤 S1101~S1106，各个步骤的详细描述如下。

步骤 S1101：该用户设备向该业务认证服务器发送第一请求消息。

步骤 S1102：该业务认证服务器接收该第一请求消息，并根据该第一请求消息向该 CP-AU 发送第二请求消息，该第二请求消息用于请求该 CP-AU 向该业务认证服务器发送该第五共享密钥。

步骤 S1103：该 CP-AU 接收该第二请求消息，并向该业务认证服务器发送该第五共享密钥（或者由该第五共享密钥衍生的密钥）。

步骤 S1104：该业务认证服务器接收该第五共享密钥，还可能接收了该 CP-AU 发送的网络参数。

步骤 S1105：该业务认证服务器与该用户设备根据该第一共享密钥和该第五共享密钥进行业务认证生成第二共享密钥，或者根据该第一共享密钥和基于该第五共享密钥衍生的密钥进行业务认证生成第二共享密钥；该第二共享密钥或者基于该第二共享密钥衍生的共享密钥为该业务认证服务器与该用户设备协商的保护数据安全传输的共享密钥。

步骤 S1106：该业务认证服务器将该第二共享密钥发送给该 CP-AU，该 CP-AU 可能还要将该第二共享密钥发送给该网络认证服务器存储备用。由于该 CP-AU 和该用户设备均

具有该第二共享密钥，因此该网络认证设备和该用户设备将该第二共享密钥作为目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥，可以省去该用户设备再与该 CP-AU 进行网络认证的流程。

可选的，网络认证设备中用于接收该第二请求消息的设备可以为该 CP-AU，也可以为其他设备，如，网络认证服务器、MM、SM、AN 等。

可选的，该用户设备用到的业务参数除了由该业务认证服务器发送外，还可以是预置在该用户设备中的。

可选的，该 CP-AU 和该用户设备还可以基于该第二共享密钥进一步生成新的共享密钥，然后基于该新的共享密钥、网络参数、业务参数来生成该目标共享密钥。

可选的，该 CP-AU 与该用户设备还可以进一步基于该第二共享密钥进行网络认证生成该目标共享密钥。

可选的，该业务认证设备不发送第二共享密钥给网络认证设备，该网络认证设备只需要知道该用户设备认证成功即可。

在又一种可选的方案中，该方法还包括：所述业务认证设备将所述第二共享密钥发送给所述网络认证设备；所述网络认证设备接收所述第二共享密钥；所述网络认证设备和所述用户设备均根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第五共享密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

在图 3K 所示的方法中，用户设备与业务认证设备根据第一共享密钥和第五共享密钥进行业务认证生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备将该第二共享密钥作为目标共享密钥。也即是说，该业务认证设备和该用户设备生成的第二共享密钥直接作为该网络认证设备的目标共享密钥，同时该第二共享密钥还可以作为该业务认证设备自身的目标共享密钥，相当于执行上述流程完成了网络认证和业务认证这两次认证，提高了认证的效率。

在又一种可选的方案中，该方法还可以包括：该网络认证设备根据自身所在的蜂窝网的网络参数生成网络侧信息；该网络认证设备将该网络侧信息发送给该业务认证设备；该业务认证设备接收并向该用户设备转发该网络侧信息；该结合该参考信息和第一共享密钥生成第二共享密钥，具体为：结合该网络参数和第一共享密钥进行业务认证生成第二共享密钥，该网络参数包括该网络侧信息。该业务认证设备将该第二共享密钥发送给该网络认证设备；该网络认证设备用于接收该第二共享密钥并将该第二共享密钥作为该目标共享密钥。为了方便理解，以下根据图 3L 结合具体场景进行描述。

请参见图 3L，图 3L 是本发明实施例提供的一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器。该用户设备与该业务认证设备预先共享了第一共享密钥，用户设备与该网络认证设备预先共享了第五共享密钥；该方法可以包括步骤 S1201~S1207，各个步骤的详细描述如下。

步骤 S1201：该用户设备向该业务认证服务器发送第一请求消息。

步骤 S1202: 该业务认证服务器接收该第一请求消息, 并根据该第一请求消息向该 CP-AU 发送第二请求消息, 该第二请求消息包含该第一共享密钥和目标业务的业务参数。

步骤 S1203: 该 CP-AU 接收该第二请求消息, 并向该业务认证服务器发送该网络参数, 以及基于网络参数、业务参数、该第一共享密钥、该第五共享密钥生成的网络侧信息。

步骤 S1204: 该业务认证服务器接收该网络侧信息和网络参数, 并向该用户设备发送该网络参数和该业务参数。

步骤 S1205: 该用户设备接收该网络参数和该业务参数, 并基于该第一共享密钥、第五共享密钥、该网络参数和该业务参数生成该网络侧信息 (如, Kcombination), 该网络侧信息属于该参考信息。

步骤 S1206: 该业务认证服务器与该用户设备根据该网络侧信息进行业务认证生成第二共享密钥。

步骤 S1207: 该业务认证服务器将该第二共享密钥发送给该 CP-AU, 该 CP-AU 可能还要将该第二共享密钥发送给该网络认证服务器存储备用。由于该 CP-AU 和该用户设备均具有该第二共享密钥, 因此该 CP-AU 和该用户设备将该第二共享密钥作为目标共享密钥, 该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该 CP-AU 与该用户设备协商的保护数据安全传输的共享密钥, 可以省去该用户设备再与该 CP-AU 进行网络认证。

可选的, 网络认证设备中用于接收该第二请求消息的设备可以为该 CP-AU, 也可以为其他设备, 如, 网络认证服务器、MM、SM、AN 等。

可选的, 该用户设备用到的业务参数除了由该业务认证服务器发送外, 还可以是预置在该用户设备中的。

可选的, 该 CP-AU 和该用户设备还可以基于该第二共享密钥进一步生成新的共享密钥, 然后基于该新的共享密钥、网络参数、业务参数来生成该目标共享密钥。

可选的, 该 CP-AU 与该用户设备还可以进一步基于该第二共享密钥进行网络认证生成该目标共享密钥。

可选的, 该业务认证设备不发送第二共享密钥给网络认证设备, 该网络认证设备只需要知道该用户设备认证成功即可。

在图 3L 所示的方法中, 用户设备与业务认证设备根据获取的网络侧信息和预先共享的第一共享密钥进行业务认证生成第二共享密钥, 然后该业务认证设备将该第二共享密钥发送给该网络认证设备, 使得该网络认证设备将该第二共享密钥作为目标共享密钥。也就是说, 该业务认证设备和该用户设备生成的第二共享密钥直接作为该网络认证设备的目标共享密钥, 同时该第二共享密钥还可以作为该业务认证设备自身的目标共享密钥, 相当于执行上述流程完成了网络认证和业务认证这两次认证, 提高了认证的效率。

请参见图 4A, 图 4A 是本发明实施例提供的又一种网络认证方法的流程示意图, 该方法可以基于图 1 所示的网络认证系统来实现, 该方法包括但不限于如下步骤。

步骤 S1401: 该业务认证设备将预存的目标业务的业务参数发送给该网络认证设备和该用户设备。

具体地, 该业务认证设备中预存了该目标业务的业务参数, 该目标业务及其业务参数

的具体情况可以参照图 3A 所示的方法实施例的描述，此处不赘述。

在一种可选的方案中，该用户设备未通过除蜂窝网以外的网络与该业务认证设备连接；该业务认证设备可以在接收到该用户设备发送的并经过该网络认证设备转发的第一请求消息后再发送该业务参数，由于该第一请求消息由该用户设备经该网络认证设备转发给该业务认证设备，因此可通过相反路径将该业务参数发送给该网络认证设备，进而由该网络认证设备转发给该用户设备。可选的，该第一请求消息中携带了该用户设备的身份标识，并在发送到该网络认证设备时经过该网络认证设备添加了该网络认证设备所在蜂窝网的相关信息（如，网络标识），因此该业务认证设备可以基于该用户设备的身份标识以及该蜂窝网的相关信息将该业务参数依次发送给该网络认证设备和该用户设备。

在又一种可选的方案中，该用户设备未通过除蜂窝网以外的网络与该业务认证设备连接，该业务认证设备可以在接收到该网络认证设备发送第二请求消息后再发送该业务参数，该业务认证设备接收到该网络认证设备发送的第二请求消息即向该网络认证设备反馈该业务参数，该网络认证设备接收到该业务参数后在将该业务参数发送给该用户设备。

在又一种可选的方案中，该用户设备通过除蜂窝网以外的网络与该业务认证设备建立了通信连接，该业务认证设备可以在接收到该网络认证设备发送的第二请求消息后再发送该业务参数，该第二请求消息中可以携带该网络认证设备的相关信息（如，网络标识），这样一来，该业务认证设备就可以根据该相关信息向该网络认证设备发送该业务参数，并根据接收该第一请求消息的路径向该用户设备返回该业务参数。

步骤 S1402：该网络认证设备和该用户设备接收该业务参数。

步骤 S1403：该网络认证设备和该用户设备结合该业务参数和原始共享密钥进行网络认证生成目标共享密钥，该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该网络认证设备与该用户设备协商的保护数据安全传输的共享密钥。需要说明的是，此处的原始目标共享密钥相当于上面描述的第五共享密钥，即该原始共享密钥为该网络认证设备与该用户设备预先共享的共享密钥。

在一种可选的方案中，该方法还包括：该网络认证设备和该用户设备结合该业务参数和原始共享密钥进行网络认证生成目标共享密钥，具体为：网络认证设备和该用户设备结合该业务参数和原始共享密钥生成认证共享密钥。该网络认证设备和该用户设备根据该认证共享密钥进行网络认证生成目标共享密钥。

在图 4A 所示的方法中，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 5A，图 5A 是本发明实施例提供的又一种网络认证方法的流程示意图，该方法可以基于图 1 所示的网络认证系统来实现，该方法包括但不限于如下步骤。

步骤 S1701：该业务认证设备获取该用户设备的身份标识。

步骤 S1702：该业务认证设备结合自身的业务公钥、业务私钥和该身份标识生成身份密钥，并将该身份密钥、该业务公钥发送给该网络认证设备。

步骤 S1703: 该网络认证设备接收该身份密钥, 并结合该身份密钥、该业务公钥和网络参数生成认证根密钥, 该网络参数为与该网络认证设备所处蜂窝网相关的参数, 以上有对该网络参数的描述, 此处不赘述。结合该身份密钥、该业务公钥和网络参数生成认证根密钥, 具体指: 生成该认证根密钥需要用到的信息包括但不限于该身份密钥、该业务公钥和网络参数。

步骤 S1704: 该网络认证设备将该认证根密钥写入该用户设备; 例如, 该网络认证设备可以将该认证根密钥写入到全球用户识别卡(英文: Universal Subscriber Identity Module, 简称: USIM), 而该 USIM 卡是用来配置到用户设备的, 因此可以看做该网络认证设备将该认证根密钥写入到该用户设备。另外, 该网络认证设备将该认证根密钥写入到该用户设备包括该网络认证设备直接写入该用户设备, 也包括该网络认证设备通过其他设备写入该用户设备, 还包括其他设备通过调用该网络认证设备中的认证根密钥并写入该用户设备。

步骤 S1705: 该网络认证设备与该用户设备用于通过该认证根密钥进行网络认证生成目标共享密钥, 该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该网络认证设备与该用户设备协商的保护数据安全传输的共享密钥。为了便于理解, 以下根据图 5B 结合具体场景进行描述。

请参见图 5B, 图 5B 是本发明实施例提供的又一种网络认证方法的流程示意图; 该业务认证设备可以包括业务认证服务器和业务服务器。该用户设备与该网络认证设备预先共享了第一共享密钥; 该方法可以包括步骤 S1801~S1806, 各个步骤的详细描述如下。

步骤 S1801: 用户设备向业务认证服务器发送第一请求消息, 该第一请求消息包含该用户设备的身份标识, 上面实施例有对该用户设备的身份标识的描述, 此处不再赘述。业务公钥可理解为基于 IBS 的全局公钥; 业务私钥可理解为基于 IBS 的全局私钥。

步骤 S1802: 该业务认证服务器接收该第一请求消息, 并根据自身的业务私钥(英文: Secret Key, 简称: SK)、业务公钥(英文: public key, 简称: PK)和该用户设备的身份标识生成身份密钥。

步骤 S1803: 该业务认证服务器将身份密钥、该业务公钥和该用户设备的身份标识发送给该 CP-AU。

步骤 S1804: 该 CP-AU 接收该身份密钥、该业务公钥和该用户设备的身份标识, 并结合该身份密钥、该业务公钥和该用户设备的身份标识生成认证根密钥。

步骤 S1805: 该 CP-AU 将该认证根密钥写入到该用户设备中。可选的, 可以将身份密钥和业务公钥写入该用户设备, 如果是写入的是身份密钥和业务公钥, 则后续跟用户设备与网络认证设备可以基于 IBS 根据该身份密钥和业务公钥相互认证。

步骤 S1806: 该 CP-AU 和该用户设备基于该认证根密钥进行网络认证生成目标共享密钥。

可选的, 该 CP-AU 将生成的目标共享密钥发送给该业务认证服务器, 以便该业务认证服务器和该用户设备将该目标共享密钥, 或者基于该目标共享密钥衍生的共享密钥作为该业务认证服务器与该用户设备协商的保护数据安全传输的共享密钥。

可选的, CP-AU 可以向网络认证服务器获取认证向量来与该用户设备进行网络认证。

在图 5B 所示的方法中, 该业务认证设备将业务公钥、身份密钥发送给该网络认证设

备,该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥,该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说,生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息,提升了该目标共享密钥的安全级别。

请参见图 6A,图 6A 是本发明实施例提供的又一种网络认证方法的流程示意图,该方法可以基于图 1 所示的网络认证系统来实现,该方法包括但不限于如下步骤。

步骤 S1901:该业务认证设备与该用户设备进行业务认证生成参考共享密钥。可选的,该用户设备通过蜂窝网以外的网络与该业务认证设备建立了通信连接,该用户设备与该业务认证设备可以基于证书、用户名密码、基于身份密码机制以及预置共享密钥来进行业务认证。该认证共享密钥可以具体基于该用户设备的身份标识 UEID、该业务认证设备管理的目标业务的业务参数等信息来生成。以 UEID 为例,该用户设备可以向该业务认证设备发送请求消息来,该请求消息中携带了该 UEID。

步骤 S1902:该业务认证设备将该参考共享密钥发送给该网络认证设备;该业务认证设备发送的信息还可以包括该用户设备的相关信息,例如,UEID、IP 地址、MAC 地址等,这样一来该业务认证设备就可以知道后续需要与哪个用户设备基于该参考共享密钥生成目标共享密钥。

步骤 S1903:该网络认证设备接收该参考共享密钥。

步骤 S1904:该网络认证设备和该用户设备结合该参考共享密钥生成目标共享密钥,该目标共享密钥或者基于该目标共享密钥衍生的共享密钥为该网络认证设备与该用户设备协商的保护数据安全传输的共享密钥。该用户设备与该网络认证设备生成目标共享密钥需要参考的信息至少包括该参考共享密钥。

在一种可选的方案中,该方法还可以包括:该网络认证设备将该网络认证设备所在蜂窝网的网络参数发送给该用户设备;该网络认证设备和该用户设备结合该参考共享密钥生成目标共享密钥,具体为:该网络认证设备和该用户设备均根据该网络参数和该参考共享密钥生成认证共享密钥;该网络认证设备和该用户设备根据该认证共享密钥进行网络认证生成目标共享密钥。为了方便理解,以下根据图 6B 结合具体场景进行描述。

请参见图 6B,图 6B 是本发明实施例提供的又一种网络认证方法的流程示意图;该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2001~S2009,各个步骤的详细描述如下。

步骤 S2001:该用户设备与该业务认证服务器进行业务认证生成参考共享密钥,或者该业务认证设备和该用户设备直接预先配置参考共享密钥,该参考共享密钥即为该用户设备与该业务认证设备之间的预先共享的根密钥。

步骤 S2002:该业务认证服务器将该参考共享密钥发送给该网络认证服务器。

步骤 S2003:该网络认证服务器接收该参考共享密钥并向该业务认证服务器发送网络参数。

步骤 S2004:该业务认证服务器接收该网络参数并将该网络参数转发给该用户设备;可选的,该网络认证服务器还可以直接将该网络参数发送给该用户设备。

步骤 S2005: 该网络认证服务器根据该参考共享密钥和该网络参数生成认证共享密钥。

步骤 S2006: 该网络认证服务器将该认证共享密钥发送给该 CP-AU。

步骤 S2007: 该 CP-AU 接收该认证共享密钥。

步骤 S2008: 该用户设备根据该参考共享密钥和该网络参数生成该认证共享密钥。

步骤 S2009: 该 CP-AU 和该用户设备用于根据该认证共享密钥进行网络认证生成目标共享密钥。

可选的, 该网络认证设备和该用户设备之间还可以预先共享第五共享密钥, 这样一来, 该网络认证设备和该用户设备就可以基于该第五共享密钥和该参考共享密钥相互认证生成该目标根密钥。

在又一种可选的方案中, 该方法还可以包括: 该网络认证设备将该目标共享密钥发送给该业务认证设备; 该业务认证设备接收该目标共享密钥; 该业务认证设备和该用户设备将该目标共享密钥, 或者基于该目标共享密钥衍生的共享密钥作为该业务认证设备与用户设备协商的保护数据安全传输的共享密钥。也即是说, 该网络认证设备与该用户设备进行网络认证之后, 该网络认证设备将该网络认证的结果发送给该业务认证设备, 该业务认证设备可以直接使用该网络认证的结果, 而不需要再与该用户设备进行业务认证来生成加密传输数据的共享密钥。

在图 6B 所示的方法中, 该业务认证设备与该用户设备进行业务认证生成参考共享密钥, 然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数; 该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥, 并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及网络相关的信息, 提升了该目标共享密钥的安全级别。

请参见图 6C, 图 6C 是本发明实施例提供的又一种网络认证方法的流程示意图, 该方法可以基于图 1 所示的网络认证系统来实现, 该方法包括但不限于如下步骤。

步骤 S2101: 网络认证设备生成经过初始共享密钥加密的访问令牌, 所述初始共享密钥为所述网络认证设备与业务认证设备预先共享的密钥;

步骤 S2102: 所述网络认证设备将所述访问令牌发送给所述用户设备;

步骤 S2103: 所述用户设备接收所述访问令牌并将所述访问令牌发送给所述业务认证设备;

步骤 S2104: 所述业务认证设备接收所述访问令牌并通过所述初始共享密钥验证所述访问令牌的正确性;

步骤 S2105: 所述业务认证设备在验证出所述访问令牌正确时向所述用户设备发送验证成功消息, 以通知与所述用户设备之间成功完成业务认证。

在一种可选的方案中, 所述访问令牌中包含目标共享密钥, 所述用户设备和所述业务认证设备用于在所述用户设备与所述业务认证设备之间成功完成业务认证时, 将所述访问令牌中的所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥, 作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。可选的, 该目标共享密钥为

该网络认证设备与该用户设备进行网络认证得到的共享密钥。

在又一种可选的方案中，所述访问令牌包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项。可选的，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

进一步地，该访问令牌还可以包括通过初始共享密钥生成的针对网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项的消息认证码。当包含该消息认证码时，在步骤 S2104 中还需要基于该初始共享密钥验证该消息认证码的正确性，步骤 S2105 中所述业务认证设备在验证出所述访问令牌正确时向所述用户设备发送验证成功消息，具体为：所述业务认证设备在验证出所述访问令牌正确以及验证出所述消息认证码正确时时向所述用户设备发送验证成功消息。

为了方便理解，以下分别结合图 6D 和图 6E 的具体场景进行描述。

请参见图 6D，图 6D 是本发明实施例提供的又一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2201~S2207，各个步骤的详细描述如下。

步骤 S2201：用户设备 UE 与网络认证设备进行网络认证，网络认证生成的共享密钥为网络共享密钥 K1；该 UE 可以在网络认证之前或者之后或者网络认证的过程中向该网络认证设备发送业务认证设备的相关信息，以表明该 UE 需要与该业务认证设备认证。

步骤 S2202：网络认证设备根据该业务认证设备的相关信息确定该网络认证设备预先与该业务认证设备共享的初始共享密钥 K0；基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token。可选的， $\text{token} = \text{Enc_K0_}(\text{K2, 基础信息, MAC})$ ，也即是说，该访问令牌 token 为采用初始共享密钥 K0 对 K2、基础信息和 MAC 进行的加密；其中，K2 为该网络认证设备确定的，可能用作用户设备与业务认证设备之间保护数据传输的共享密钥，基础信息包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项， $\text{MAC} = \text{MAC_K0_}(\text{新鲜参数和/或基础信息})$ ，即 MAC 为该基础信息的信息认证码，或者该新鲜参数的消息认证码（此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同），或者该基础信息和该新鲜参数的消息认证码；该消息认证码 MAC 的生成采用初始共享密钥 K0。

需要说明的是，若上述推导公式中用到新鲜参数 nonce，则网络认证设备还需要将用到的新鲜参数发送至 UE，并由 UE 发送至业务认证设备，后续该业务认证设备可以通过该新鲜参数验证 token 的新鲜性。

进一步地，共享密钥 K2 可以为配置的随机的参数，也可以为网络共享密钥 K1，还可以为基于网络共享密钥 K1 推导出来的共享密钥，例如， $\text{K2} = \text{KDF}(\text{K1, 基础信息})$ ，即通过预设的算法对该网络共享密钥 K1 和基础信息进行计算来得到该共享密钥 K2。

进一步地，业务认证设备的相关信息为能够在一定范围内区分该业务认证设备与其他设备的信息，例如，可以为该业务认证设备的 IP 地址，或者业务 ID。步骤 S2203：该网络

认证设备向 UE 发送 K2 和 token，还可能发送网络认证设备的相关信息，该网络认证设备的相关信息可以包括网络参数。

步骤 S2204：UE 接收 K2 和 token 并向业务认证设备发送该 token 和该网络认证设备的相关信息。UE 可以自己生成该网络认证设备的相关信息，也可以在与该网络认证设备进行网络认证之时，或者之前，或者之后接收该网络认证设备发送的该网络认证设备的相关信息，优选的，UE 在步骤 S2203 中接收该网络认证设备发送的网络认证设备的相关信息。

步骤 S2205：业务认证设备接收该 token 和该网络认证设备的相关信息，根据该网络认证设备的相关信息来确定预先与该网络认证设备共享的初始共享密钥 K0，并使用 K0 解密 token 得到该共享密钥 K2、该基础信息和消息认证码 MAC；然后根据 K0 验证 MAC 的正确性，验证 MAC 成功后则表明该业务认证设备验证 token 成功。因此，该业务认证设备将该 K2 作为与该 UE 之间用于保护数据传输的共享密钥。

步骤 S2206：该业务认证设备向该 UE 发送消息以通知验证 token 成功，相应地，该 UE 接收消息。

步骤 S2207：该业务认证设备和该 UE 将该共享密钥 K2 作为该 UE 与该业务认证设备之间用户保护数据安全传输的共享密钥。

可选的，UE 与业务认证设备根据 K2 进一步推导出共享密钥 K3，例如， $K3 = KDF(K2, \text{基础信息})$ ，即通过预设算法对该 K2 和基础信息进行计算得到 K3，K3 用于该 UE 与该业务认证设备之间保护数据的安全传输。

可选的，当该共享密钥 K2 为网络共享密钥 K1 时，该 UE 和该业务认证设备均可以基于该 K1 衍生出的共享密钥 K3。

可选的，加密 token 的共享密钥为 K1 而不是 K0，业务认证设备接收到 token 后根据网络认证设备的相关信息向该网络认证设备转发该 token 和该 UE 的相关信息；该网络认证设备根据该 UE 的相关信息确定与该 UE 认证生成的共享密钥 K1，再根据 K1 来解密 token，并验证该 token 中 MAC 的正确性，验证成功即表明该 UE 与该业务认证设备认证成功，因此将 K2 发送给该业务认证设备，以便该 UE 和该业务认证设备将该 K2 作为保护数据安全传输的共享密钥。可选的，该 UE 的相关信息可以由该 UE 发送给业务认证设备，再由该业务认证设备发送给该网络认证设备，该 UE 的相关信息可以为该 UE 的身份标识。

请参见图 6E，图 6E 是本发明实施例提供的又一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2301~S2305，各个步骤的详细描述如下。

步骤 S2301：用户设备 UE 与网络认证设备进行网络认证，网络认证生成的共享密钥为网络共享密钥 K1；该 UE 可以在网络认证之前或者之后或者网络认证的过程中向该网络认证设备发送业务认证设备的相关信息，以表明该 UE 需要与该业务认证设备认证。

步骤 S2302：网络认证设备根据该业务认证设备的相关信息确定该网络认证设备预先与该业务认证设备共享的初始共享密钥 K0；基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token，并通过该初始共享密钥 K0 加密该访问令牌 token。可选的，token 可以为消息认证码，消息认证码 $MAC = MAC_K_(\text{新})$

鲜参数和/或基础信息), 即 MAC 为该基础信息的信息认证码, 或者该新鲜参数的消息认证码 (此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同), 或者该基础信息和该新鲜参数的消息认证码; 该基础信息包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项; 该消息认证码 MAC 还经过了该初始共享密钥 K0 加密。

需要说明的是, 若上述推导公式中用到新鲜参数 nonce, 则网络认证设备还需要将用到的新鲜参数发送至 UE, 并由 UE 发送至业务认证设备, 后续该业务认证设备可以通过该新鲜参数验证 token 的新鲜性。

步骤 S2303: 该网络认证设备向 UE 发送 token, 还可能发送该网络认证设备的相关信息, 所述网络认证设备的相关信息可以包括该网络参数。

步骤 S2304: UE 接收 token 并向业务认证设备发送该 token 和该网络认证设备的相关信息。

步骤 S2305: 业务认证设备接收该 token 和该网络认证设备的相关信息, 根据该网络认证设备的相关信息来确定预先与该网络认证设备共享的初始共享密钥 K0, 然后根据 K0 验证 MAC 的正确性, 验证 MAC 成功后则表明该业务认证设备验证 token 成功。至此, 该 UE 与该业务认证设备之间成功完成了认证。

可选的, 生成 token 的共享密钥为 K1 而不是 K0, 业务认证设备接收到 token 后根据网络认证设备的相关信息向该网络认证设备转发该 token 和该 UE 的相关信息; 该网络认证设备根据该 UE 的相关信息确定与该 UE 认证生成的共享密钥 K1, 然后验证该 token 中 MAC 的正确性, 验证成功即表明该 UE 与该业务认证设备认证成功, 因此想该 UE 和该业务认证设备发送通知消息以通知该 UE 与该业务认证设备之间认证成功。

请参见图 6F, 图 6F 是本发明实施例提供的又一种网络认证方法的流程示意图; 该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2401~S2408, 各个步骤的详细描述如下。

步骤 S2401: 用户设备 UE 与网络认证设备进行网络认证。

步骤 S2402: 网络认证设备在网络认证通过后生成认证令牌 token 和该 token 的过期信息, 该过期信息用于表征该 token 什么时候过期; 还可以生成范围信息, 该范围信息用于表征该 token 可以被哪些业务认证设备使用; 或者该范围信息用于表征该 token 可以被哪些用户设备使用。

步骤 S2403: 网络认证设备向该 UE 发送该 token; 还可以发送该网络认证设备相关的信息, 该网络认证设备相关的信息用于表明该 token 来自于该网络认证设备。

步骤 S2404: 该用户设备向该业务认证设备发送该 token 和该网络认证设备的相关信息;

步骤 S2405: 该业务认证设备接收该 token 和该网络认证设备的相关信息, 并根据该网络认证设备的相关信息向该网络认证设备发送该 token; 发送的消息可能还包括 UE ID 和业务认证设备的相关信息中的至少一项。

步骤 S2406: 该网络认证设备接收该 token, 判断该 token 是否为自身生成的 token, 如果该 token 为自身生成的 token 则进一步他根据该过期信息判断该 token 是否过期, 若没

过期则表明验证 token 成功。可选的, 当该网络认证设备生成了范围信息时, 该网络认证设备还需要根据该范围信息判断发送该 token 的业务认证设备是否为该范围信息中允许的业务认证设备, 若为允许的业务认证设备且该 token 未过期则表明验证 token 成功。可选的, 该范围信息用于表征该 token 可以被哪个用户设备使用时, 该网络认证设备还需要根据该范围信息判断该用户设备是否为该范围信息中允许的用户设备, 若该用户设备为允许的用户设备且该业务认证设备为允许的业务认证设备, 并且该 token 未过期则表明验证 token 成功。

可选的, 步骤 S2405 中不包含业务认证设备的相关信息, 该网络认证设备也可以根据接收的 token 的来源确定业务认证设备的相关信息。

可选的, 判断该用户设备是否为该范围信息中允许的用户设备时用到的该用户设备的相关信息, 可以为该用户设备将该用户设备自身的相关信息发送至业务认证设备, 再由业务认证设备在步骤 S2405 中一同发送至该网络认证设备。

步骤 S2407: 若验证 token 成功, 则该网络认证设备向该业务认证设备发送消息通知 token 验证成功;

步骤 S2408: 该业务认证设备向该 UE 发送消息通知 token 验证成功。业务认证设备和 UE 双方都获知了 token 验证成功, 即表明该业务认证设备与该 UE 之间认证成功。

请参见图 6G, 图 6G 是本发明实施例提供的又一种网络认证方法的流程示意图; 该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2501~S2508, 各个步骤的详细描述如下。

步骤 S2501: 用户设备 UE 与网络认证设备进行网络认证, 网络认证生成的共享密钥为网络共享密钥 K1。

步骤 S2502: UE 基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token, 并通过该网络共享密钥 K1 加密该访问令牌 token。可选的, $\text{token} = \text{Enc_K1_}(\text{K2}, \text{基础信息}, \text{MAC})$, 也即是说, 该访问令牌 token 为采用 K1 对 K2、基础信息和 MAC 加密生成; 其中, K2 为该 UE 确定的后续可能用作用户设备与业务认证设备之间保护数据传输的共享密钥, 基础信息包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项, 可选的, 该用户设备可以预先向该网络认证设备和该业务认证设备获取需要用到信息; $\text{MAC} = \text{MAC_K1_}(\text{新鲜参数和/或基础信息})$, 即 MAC 为该基础信息的信息认证码, 或者该新鲜参数的消息认证码 (此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同), 或者该基础信息和该新鲜参数的消息认证码; 该消息认证码 MAC 由该网络共享密钥 K1 生成。

需要说明的是, 若上述推衍公式中用到新鲜参数 nonce, 则 UE 还需要将用到的新鲜参数发送至业务认证设备, 由该业务认证设备将该新鲜参数转发给该网络认证设备, 后续该网络认证设备可以通过该新鲜参数验证 token 的新鲜性。

进一步地, 共享密钥 K2 可以为配置的随机的参数, 也可以为网络共享密钥 K1, 还可以为基于网络共享密钥 K1 推衍出来的共享密钥, 例如, $\text{K2} = \text{KDF}(\text{K1}, \text{基础信息})$, 即通过预设的算法对该网络共享密钥 K1 和基础信息进行计算来得到该共享密钥 K2。

步骤 S2503: UE 向业务认证设备发送该 token。

步骤 S2504: 业务认证设备接收该 UE 发送的该 token 并将该 token 转发给该网络认证设备, 该业务认证设备还可能向该网络认证设备发送该 UE 的相关信息 (包括但不限于 UE ID), 该相关信息可能由该 UE 发送至该业务认证设备的, 该相关信息可以在一定范围内区分该 UE 与其他设备。

步骤 S2505: 该网络认证设备接收该 token 和该 UE 的相关信息; 根据该 UE 的相关信息并找到与该 UE 网络认证生成的网络共享密钥 K1, 并使用 K1 解密 token 得到该共享密钥 K2、该基础信息和消息认证码 MAC; 然后根据 K1 验证 MAC 的正确性, 若验证 MAC 正确则表明验证 token 成功。

步骤 S2506: 若验证 token 成功, 则该网络认证设备向该业务认证设备发送消息通知 token 验证成功, 该通知消息中还包括从 token 中获得的共享密钥 K2;

步骤 S2507: 该业务认证设备向该 UE 发送消息通知 token 验证成功。业务认证设备和 UE 双方都获知了 token 验证成功, 即表明该业务认证设备与该 UE 之间认证成功。

步骤 S2508: 该 UE 和该业务认证设备将该 K2 作为该 UE 与该业务认证设备之间用于保护数据安全传输的共享密钥。

可选的, UE 与业务认证设备根据 K2 进一步推导出共享密钥 K3, 例如, $K3 = KDF(K2, \text{基础信息})$, 即通过预设算法对该 K2 和基础信息进行计算得到 K3, K3 用于该 UE 与该业务认证设备之间保护数据的安全传输。

请参见图 6H, 图 6H 是本发明实施例提供的又一种网络认证方法的流程示意图; 该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2601~S2607, 各个步骤的详细描述如下。

步骤 S2601: 用户设备 UE 与网络认证设备进行网络认证, 网络认证生成的共享密钥为网络共享密钥 K1。

步骤 S2602: UE 基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token, 可选的, 该 token 为消息认证码 MAC, $MAC = MAC_K1_(\text{新鲜参数和/或基础信息})$, 即 MAC 为该基础信息的消息认证码, 或者该新鲜参数的消息认证码 (此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同), 或者该基础信息和该新鲜参数的消息认证码; 该消息认证码 MAC 由该网络共享密钥 K1 生成。

需要说明的是, 若上述推导公式中用到新鲜参数 nonce, 则 UE 还需要将用到的新鲜参数发送至业务认证设备, 由该业务认证设备将该新鲜参数发送给该网络认证设备, 后续该网络认证设备可以通过该新鲜参数验证 token 的新鲜性。

步骤 S2603: UE 向业务认证设备发送该 token。

步骤 S2604: 业务认证设备接收该 UE 发送的该 token 并将该 token 转发给该网络认证设备, 该业务认证设备还可能向该网络认证设备发送该 UE 的相关信息, 该相关信息可能由该 UE 发送该业务认证设备的, 该相关信息可以在一定范围内区分该 UE 与其他设备, 例如, 该用户设备的相关信息可以为该用户设备的身份标识 (UEID)。

步骤 S2605: 该网络认证设备接收该 token 和该 UE 的相关信息; 根据该 UE 的相关信

息并找到与该 UE 网络认证生成的网络共享密钥 K1，并根据 K1 验证 MAC 的正确性，若验证 MAC 正确则表明验证 token 成功。

步骤 S2606：若验证 token 成功，则该网络认证设备向该业务认证设备发送消息通知 token 验证成功；

步骤 S2607：该业务认证设备向该 UE 发送消息通知 token 验证成功。业务认证设备和 UE 双方都获知了 token 验证成功，即表明该业务认证设备与该 UE 之间认证成功。

需要说明的是，还可以基于上述方案显而易见地推导出以下方案，即 UE 首先与业务认证设备建立双向认证，由 UE 或者业务认证设备生成 token；之后 UE 发送 token 至网络认证设备，网络认证设备可以自己验证 token 的正确性，也可能将 token 发送至业务认证设备，由业务认证设备验证 token 的正确性，并将验证结果发送至网络认证设备。相当于将 6C-6H 中涉及到的业务认证设备与网络认证设备进行了调换。另外，token 包含但不限于如下两种情况：情况一 $\text{token} = \text{Enc_K0_}(\text{K2}, \text{基础信息}, \text{MAC_K0_}(\text{基础信息和/或 nonce}))$ ，情况二： $\text{token} = \text{MAC_K0_}(\text{基础信息和/或 nonce})$ 。这两种情况的理解可以参照以上描述，此处不再赘述。

为了便于理解，以下以 token 由业务认证设备生成为例来进行描述，token 由 UE 生成的情况可以参照图 6D~6I 的描述。

请参见图 6I，图 6I 是本发明实施例提供的又一种网络认证方法的流程示意图；该业务认证设备可以包括业务认证服务器和业务服务器。该方法可以包括步骤 S2708~S2707，各个步骤的详细描述如下。

步骤 S2701：用户设备 UE 与业务认证设备进行业务认证，生成的共享密钥为业务共享密钥 K1；该 UE 可以在业务认证之前或者之后或者业务认证的过程中向该业务认证设备发送网络认证设备的相关信息，以表明该 UE 需要与该网络认证设备认证。

步骤 S2702：业务认证设备根据该网络认证设备的相关信息确定该网络认证设备预先与该业务认证设备共享的初始共享密钥 K0；基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token。可选的， $\text{token} = \text{Enc_K0_}(\text{K2}, \text{基础信息}, \text{MAC})$ ，也即是说，该访问令牌 token 为采用初始共享密钥 K0 对 K2、基础信息和 MAC 进行的加密；其中，K2 为该业务认证设备确定的，可能用作用户设备与网络认证设备之间保护数据传输的共享密钥，基础信息包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项， $\text{MAC} = \text{MAC_K0_}(\text{新鲜参数和/或基础信息})$ ，即 MAC 为该基础信息的信息认证码，或者该新鲜参数的信息认证码（此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同），或者该基础信息和该新鲜参数的信息认证码；该信息认证码 MAC 的生成采用初始共享密钥 K0。

需要说明的是，若上述推衍公式中用到新鲜参数 nonce，则业务认证设备还需要将用到的新鲜参数发送至 UE，并由 UE 发送至网络认证设备，后续该网络认证设备可以通过该新鲜参数验证 token 的新鲜性。

进一步地，共享密钥 K2 可以为配置的随机的参数，也可以为业务共享密钥 K1，还可以为基于业务共享密钥 K1 推衍出来的共享密钥，例如， $\text{K2} = \text{KDF}(\text{K1}, \text{基础信息})$ ，即通过预设的算法对该业务共享密钥 K1 和基础信息进行计算来得到该共享密钥 K2。

进一步地,网络认证设备的相关信息为能够在一定范围内区分该网络认证设备与其他设备的信息,例如,可以为该网络认证设备的 IP 地址。

步骤 S2703: 该业务认证设备向 UE 发送 K2 和 token,还可能发送业务认证设备的相关信息,所述业务认证设备的相关信息可以包括业务参数。

步骤 S2704: UE 接收 K2 和 token 并向网络认证设备发送该 token 和该业务认证设备的相关信息。UE 可以自己生成该业务认证设备的相关信息,也可以在与该业务认证设备进行业务认证之时,或者之前,或者之后接收该业务认证设备发送的该业务认证设备的相关信息,优选的,在 E 在步骤 S2703 中接收该业务认证设备发送的业务认证设备的相关信息

步骤 S2705: 网络认证设备接收该 token 和该业务认证设备的相关信息,根据该业务认证设备的相关信息来确定预先与该业务认证设备共享的初始共享密钥 K0,并使用 K0 解密 token 得到该共享密钥 K2、该基础信息和消息认证码 MAC; 然后根据 K0 验证 MAC 的正确性,验证 MAC 成功后则表明该网络认证设备验证 token 成功。因此,该网络认证设备将该 K2 作为与该 UE 之间用于保护数据传输的共享密钥。

步骤 S2706: 该网络认证设备向该 UE 发送消息以通知验证 token 成功,相应地,该 UE 接收消息。

步骤 S2707: 该网络认证设备和该 UE 将该共享密钥 K2 作为该 UE 与该网络认证设备之间用户保护数据安全传输的共享密钥。

可选的,UE 与网络认证设备根据 K2 进一步推导出共享密钥 K3,例如, $K3 = KDF(K2, \text{基础信息})$,即通过预设算法对该 K2 和基础信息进行计算得到 K3, K3 用于该 UE 与该网络认证设备之间保护数据的安全传输。

可选的,加密 token 的共享密钥为 K1 而不是 K0,网络认证设备接收到 token 后根据业务认证设备的相关信息向该业务认证设备转发该 token 和该 UE 的相关信息;该业务认证设备根据该 UE 的相关信息确定与该 UE 认证生成的共享密钥 K1,再根据 K1 来解密 token,并验证该 token 中 MAC 的正确性,验证成功即表明该 UE 与该网络认证设备认证成功,因此将 K2 发送给该网络认证设备,以便该 UE 和该网络认证设备将该 K2 作为保护数据安全传输的共享密钥。可选的,该 UE 的相关信息可以由该 UE 发送给业务认证设备,该 UE 的相关信息可以为该 UE 的身份标识。

需要说明的是,还可以对图 6C~6I 所示实施例进行相应拓展,拓展的思路如下:

K1 为 UE 与网络认证设备之间的共享密钥,包括但不限于 Kasme,加密密钥(英文: cipher key,简称: CK)和完整性保护密钥(英文: integrity key,简称: IK)中的至少一项。

另外,也可能采用非对称密码的形式计算 token,例如 $\text{token} = \text{Enc_PK_业务_}(K2, (\text{nonce1}, \text{基本信息}), \text{signature} = \text{MAC_SK_网络_}(\text{nonce2}, \text{基本信息}))$ 。PK_业务表示该业务认证设备提供的业务的公钥参数,SK_网络表示该网络认证设备所在的运营商网络的私钥参数。此时业务认证设备可以根据自己的私钥 SK_业务解密打开 token;并且利用网络认证设备所在运营商网络的公钥 PK_网络,验证 token 中签名的正确性。此时 token 的验证更加灵活,不需要与网络认证设备进行网络认证交互即可完成验证。另外,此处加密和签名的算法可以为基于公钥基础设施(英文: Public key infrastructure,简称: PKI)等非对称

密码技术，也可以为基于身份的密码技术。

需要说明的是，以上各个实施例中列出的步骤的先后顺序此处不做限制，有些步骤先执行还是后执行对实施例的实施不会产生实质的影响，因此在以上列出的步骤的先后顺序的基础上，对步骤执行的先后顺序进行调整所形成的方案依然落入本发明的保护范围。

上述详细阐述了本发明实施例的方法，为了便于更好地实施本发明实施例的上述方案，相应地，下面提供了本发明实施例的装置。

请参见图 7，图 7 是本发明实施例提供的一种业务认证设备 70 的结构示意图，该业务认证设备 70 可以包括第一获取单元 701 和发送单元 702，其中，各个单元的详细描述如下。

第一获取单元 701 用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥，所述第一共享密钥为用户设备与所述业务认证设备之间预先配置的共享密钥，所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥，所述参考信息包括所述用户设备、网络认证设备和所述业务认证设备中至少一项预先关联的信息；

发送单元 702 用于将所述第二共享密钥发送给所述网络认证设备，所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述第一获取单元 701 结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

在又一种可选的方案中，还包括：

第一接收单元，用于接收所述网络认证设备发送的所述目标共享密钥；

生成单元，用于将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在又一种可选的方案中，还包括：

生成单元，用于将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在又一种可选的方案中，还包括：

第二获取单元，用于获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥；

所述第一获取单元 701 结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述参考信息、第一共享密钥和所述第五共享密钥进行网络认证生成第二共享密

钥。

在又一种可选的方案中，还包括：

第二接收单元，用于接收所述网络认证设备根据所述网络认证设备所在蜂窝网的网络参数生成的网络侧信息，并向所述用户设备转发所述网络侧信息；

所述第一获取单元 701 结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

在又一种可选的方案中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 7 所示的业务认证设备中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图 8，图 8 是本发明实施例提供的一种用户设备 80 的结构示意图，用户设备 80 可以包括获取单元 801 和生成单元 802，其中，各个单元的详细描述如下。

获取单元 801 用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥；所述第一共享密钥为所述用户设备与业务认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥，所述业务认证设备还用于将所述第二共享密钥发送给网络认证设备；

生成单元 802 用于根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述获取单元根据所述第二共享密钥生成目标共享密钥，具体为：

将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享

密钥。

在又一种可选的方案中，所述获取单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，还包括：

认证单元，用于和所述网络认证设备进行网络认证生成第三共享密钥；

所述获取单元和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥，具体为：

和所述网络认证设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

在又一种可选的方案中，所述生成单元 802 根据所述第二共享密钥生成目标共享密钥，具体为：

和所述网络认证设备进行网络认证生成第三共享密钥；

根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

在又一种可选的方案中，所述生成单元 802 根据所述第二共享密钥生成目标共享密钥，具体为：

根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的共享密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

在又一种可选的方案中，所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述参考信息、第一共享密钥和第五共享密钥与所述业务认证设备进行业务认证生成第二共享密钥；所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述第五共享密钥。

在又一种可选的方案中，所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

和业务认证设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

在又一种可选的方案中，还包括：

第一接收单元，用于接收所述业务认证设备转发的来自所述网络认证设备的网络侧信息，所述网络侧信息为所述网络认证设备根据第五共享密钥和获取的所述第一共享密钥生成，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥与所述业务认证设备进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

在又一种可选的方案中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

在又一种可选的方案中，当所述参考信息包含所述业务参数时，还包括：

第二接收单元，用于接收所述网络认证设备转发的来自所述业务认证设备的所述业务参数。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照方法实施例的相应描述。

在图8所示的用户设备中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图9，图9是本发明实施例提供的一种网络认证设备90的结构示意图，网络认证设备90可以包括接收单元901和第一生成单元902，其中，各个单元的详细描述如下。

接收单元901用于接收业务认证设备发送的第二共享密钥，业务认证设备和用户设备均用于结合第一共享密钥和参考信息生成所述第二共享密钥，所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥，所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息；

第一生成单元902用于根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述第一生成单元902根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

在又一种可选的实现方案中，还包括：

认证单元，用于和所述用户设备进行网络认证生成第三共享密钥；

所述认证单元和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

和所述用户设备均根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

在又一种可选的方案中，所述第一生成单元 902 根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为目标共享密钥。

在又一种可选的方案中，所述第一生成单元 902 根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备进行网络认证生成第三共享密钥；

和所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

在又一种可选的方案中，所述第一生成单元 902 根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

在又一种可选的方案中，还包括：

获取单元，用于向所述业务认证设备获取所述第一共享密钥；

第二生成单元，用于根据所述第一共享密钥和第五共享密钥生成网络侧信息，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述网络认证设备将所述网络侧信息发送给所述业务认证设备，以使所述业务认证设备向所述用户设备转发所述网络侧信息，所述网络参数属于所述参考信息。

在又一种可选的方案中，还包括：

发送单元，用于将所述目标共享密钥发送给所述业务认证设备，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥用作所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在又一种可选的方案中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 9 所示的网络认证设备中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给

该网络认证设备,使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说,生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息,提升了该目标共享密钥的安全级别。

请参见图 10,图 10 是本发明实施例提供的一种业务认证设备 100 的结构示意图,业务认证设备 100 可以包括发送单元 1001。

发送单元 1001 用于将预存的目标业务的业务参数发送给网络认证设备和用户设备;以使所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥,所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过运行上述单元,该业务认证设备将业务参数发送给该网络认证设备,该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说,生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息,提升了该目标共享密钥的安全级别。

在一种可选的方案中,所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

在本发明实施例中,各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 10 所示的业务认证设备 100 中,该业务认证设备将业务参数发送给该网络认证设备,该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说,生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息,提升了该目标共享密钥的安全级别。

请参见图 11,图 11 是本发明实施例提供的一种用户设备 110 的结构示意图,用户设备 110 可以包括接收单元 1101 和生成单元 1102,其中,各个单元的详细描述如下。

接收单元 1101 用于接收业务认证设备发送的预存的目标业务的业务参数,所述业务认证设备还用于将所述业务参数发送给网络认证设备;

生成单元 1102 用于和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥,所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过运行上述单元,该业务认证设备将业务参数发送给该网络认证设备,该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说,生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息,提升了该目标共享密钥的安全级别。

在一种可选的方案中,所述生成单元 1102 和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥,具体为:

和所述网络认证设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述网络认证设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 11 所示的用户设备 110 中，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 12，图 12 是本发明实施例提供的一种网络认证设备 120 的结构示意图，网络认证设备 120 可以包括接收单元 1201 和生成单元 1202，其中，各个单元的详细描述如下。

接收单元 1201 用于接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给用户设备；

生成单元 1202 用于和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过运行上述单元，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述生成单元 1202 和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述用户设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 12 所示的网络认证设备中，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共

享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 13，图 13 是本发明实施例提供的一种业务认证设备 130 的结构示意图，业务认证设备 130 可以包括获取单元 1301 和生成单元 1302，其中，各个单元的详细描述如下。

获取单元 1301 用于获取用户设备的身份标识；

生成单元 1302 用于结合自身的业务公钥、业务私钥和所述身份标识生成身份密钥，并将所述身份密钥、所述业务公钥发送给所述网络认证设备，所述身份密钥和所述业务公钥用于所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 13 所示的业务认证设备中，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 14，图 14 是本发明实施例提供的一种用户设备 140 的结构示意图，用户设备 140 可以包括生成单元 1401。

生成单元 1401 用于和网络认证设备根据认证根密钥进行网络认证生成目标共享密钥，所述认证根密钥为所述网络认证设备根据身份密钥、业务认证设备管理的目标业务的业务公钥和所述网络认证设备所在蜂窝网的网络参数生成的并写入到所述用户设备中的密钥，所述身份密钥由所述业务认证设备根据所述业务公钥、所述目标业务的业务私钥和获取的所述用户设备的身份标识生成的，所述业务认证设备用于将所述业务公钥和所述身份私钥发送给所述网络认证设备；所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 14 所示的用户设备中，该业务认证设备将业务公钥、身份密钥发送给该网络认

证设备, 该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥, 该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息, 提升了该目标共享密钥的安全级别。

请参见图 15, 图 15 是本发明实施例提供的一种网络认证设备 150 的结构示意图, 网络认证设备 150 可以包括接收单元 1501、生成单元 1502、写入单元 1503 和认证单元 1504, 其中, 各个单元的详细描述如下。

接收单元 1501 用于接收身份密钥和业务认证设备管理的目标业务的业务公钥, 所述身份密钥为所述业务认证设备根据所述目标业务的业务私钥、所述业务公钥和获取的用户设备的身份标识生成的密钥;

生成单元 1502 用于结合所述身份密钥、所述业务公钥和所述网络认证设备所在蜂窝网的网络参数生成认证根密钥;

写入单元 1503 用于将所述认证根密钥写入所述用户设备;

认证单元 1504 用于和所述用户设备根据所述认证根密钥进行网络认证生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元, 该业务认证设备将业务公钥、身份密钥发送给该网络认证设备, 该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥, 该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息, 提升了该目标共享密钥的安全级别。

在一种可选的方案中, 所述网络参数包括运营商标识, 接入网络标识, 服务网络标识, 网络类型标识, 局域网网络标识, 切片标识, 承载标识, 服务质量标识和流标识中的至少一项。

在本发明实施例中, 各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 15 所示的网络认证设备中, 该业务认证设备将业务公钥、身份密钥发送给该网络认证设备, 该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥, 该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息, 提升了该目标共享密钥的安全级别。

请参见图 16, 图 16 是本发明实施例提供的一种业务认证设备 160 的结构示意图, 业务认证设备 160 可以包括认证单元 1601 和发送单元 1602, 其中, 各个单元的详细描述如下。

认证单元 1601 用于和用户设备进行业务认证生成参考共享密钥, 或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥;

发送单元 1602 用于将所述参考共享密钥发送给网络认证设备, 以使所述网络认证设

备和所述用户设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，还包括：

接收单元，用于接收所述网络认证设备发送的所述目标共享密钥；

确定单元，用于将所述目标共享密钥，或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 16 所示的业务认证设备中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 17，图 17 是本发明实施例提供的一种用户设备 170 的结构示意图，用户设备 170 可以包括配置单元 1701 和生成单元 1702，其中，各个单元的详细描述如下。

配置单元 1701 用于和业务认证设备进行业务认证生成参考共享密钥，或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥，所述业务认证设备用于将所述参考共享密钥发送给网络认证设备；

生成单元 1702 用于和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，还包括：

接收单元，用于接收所述网络认证设备发送的所述网络认证设备所在蜂窝网的网络参数；

所述生成单元和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，具体为：
和所述网络认证设备根据所述网络参数和所述参考共享密钥生成认证共享密钥；
和所述网络认证设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 17 所示的用户设备中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 18，图 18 是本发明实施例提供的一种网络认证设备 180 的结构示意图，网络认证设备 180 可以包括接收单元 1801 和生成单元 1802，其中，各个单元的详细描述如下。

接收单元 1801 用于接收业务认证设备发送的参考共享密钥，所述参考共享密钥由所述业务认证设备和用户设备进行业务认证生成的或者预先配置的；

生成单元 1802 用于和所述用户设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过运行上述单元，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，还包括：

第一发送单元，用于将所述网络认证设备所在蜂窝网的网络参数发送给所述用户设备；
所述生成单元和所述用户设备结合所述参考共享密钥生成目标共享密钥，具体为：
和所述用户设备均根据所述网络参数和所述参考共享密钥生成认证共享密钥；
和所述用户设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在又一种可选的方案中，还包括：

第二发送单元，用于将所述目标共享密钥发送给所述业务认证设备，以使所述业务认

证设备将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

在本发明实施例中，各个单元的具体实现还可以对应参照上述方法实施例的相应描述。

在图 18 所示的网络认证设备中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 19，图 19 是本发明实施例提供的一种业务认证设备 190，该业务认证设备 190 包括处理器 1901 和存储器 1902，所述处理器 1901 和存储器 1902 通过总线相互连接。

存储器 1902 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 1902 用于相关指令及数据。

处理器 1901 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 1901 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

所述业务认证设备 190 中的处理器 1901 读取所述存储器 1902 中存储的程序代码，用于执行以下操作：

获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥，所述第一共享密钥为用户设备与所述业务认证设备之间预先配置的共享密钥，所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥，所述参考信息包括所述用户设备、网络认证设备和所述业务认证设备中至少一项预先关联的信息；

将所述第二共享密钥发送给所述网络认证设备，所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述操作，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述处理器 1901 结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

在又一种可选的方案中，所述处理器 1901 将所述第二共享密钥发送给所述网络认证设备之后，还用于：

接收所述网络认证设备发送的所述目标共享密钥；

将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证

设备与所述用户设备协商的保护数据安全传输的共享密钥。

在又一种可选的方案中，所述处理器 1901 获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥之后，还用于：

将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在又一种可选的方案中，所述处理器 1901 结合所述参考信息和第一共享密钥生成第二共享密钥之前，还包括：

所获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥；

所述处理器 1901 结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述参考信息、第一共享密钥和所述第五共享密钥进行网络认证生成第二共享密钥。

在又一种可选的方案中，所述处理器 1901 结合所述参考信息和第一共享密钥生成第二共享密钥之前，还包括：

接收所述网络认证设备根据所述网络认证设备所在蜂窝网的网络参数生成的网络侧信息，并向所述用户设备转发所述网络侧信息；

所述处理器 1901 结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

在又一种可选的方案中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，业务认证设备的具体实现还可以对应参照上述方法实施例的相应描述，此处不再赘述。

在图 19 所示的业务认证设备中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图 20，图 20 是本发明实施例提供的一种用户设备 200，该用户设备 200 包括处理器 2001 和存储器 2002，所述处理器 2001 和存储器 2002 通过总线相互连接。

存储器 2002 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 2002 用于相关指令及数据。

处理器 2001 可以是一个或多个中央处理器(英文: Central Processing Unit, 简称: CPU), 在处理器 2001 是一个 CPU 的情况下, 该 CPU 可以是单核 CPU, 也可以是多核 CPU。

所述用户设备 200 中的处理器 2001 读取所述存储器 2002 中存储的程序代码, 用于执行以下操作:

获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥; 所述第一共享密钥为所述用户设备与业务认证设备之间预先配置的共享密钥, 所述业务认证设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥, 所述业务认证设备还用于将所述第二共享密钥发送给网络认证设备;

根据所述第二共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述操作, 用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥, 然后该业务认证设备将该第二共享密钥发送给该网络认证设备, 使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说, 生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息, 提升了该目标共享密钥的安全级别。

在一种可选的方案中, 所述处理器 2001 根据所述第二共享密钥生成目标共享密钥, 具体为:

将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

在又一种可选的方案中, 所述处理器 2001 根据所述第二共享密钥生成目标共享密钥, 具体为:

和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中, 所述处理器 2001 和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥之前, 还用于:

和所述网络认证设备进行网络认证生成第三共享密钥;

和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥, 包括:

和所述网络认证设备根据所述第二共享密钥进行网络认证生成第四共享密钥;

备根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

在又一种可选的方案中, 所述处理器 2001 根据所述第二共享密钥生成目标共享密钥, 具体为:

和所述网络认证设备进行网络认证生成第三共享密钥;

根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥; 或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

在又一种可选的方案中, 所述处理器 2001 根据所述第二共享密钥生成目标共享密钥,

具体为:

根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥;或者将所述第二共享密钥和基于所述第五共享密钥衍生的共享密钥分别作为保护不同类型数据的所述目标共享密钥,所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

在又一种可选的方案中,所述处理器 2001 结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

结合所述参考信息、第一共享密钥和第五共享密钥与所述业务认证设备进行业务认证生成第二共享密钥;所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥,所述业务认证设备用于获取所述第五共享密钥。

在又一种可选的方案中,所述处理器 2001 结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

和业务认证设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

在又一种可选的方案中,所述处理器 2001 结合所述参考信息和第一共享密钥生成第二共享密钥之前,还用于:

接收所述业务认证设备转发的来自所述网络认证设备的网络侧信息,所述网络侧信息为所述网络认证设备根据第五共享密钥和获取的所述第一共享密钥生成,所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥;

所述处理器 2001 结合所述参考信息和第一共享密钥生成第二共享密钥,具体为:

结合所述网络参数和第一共享密钥与所述业务认证设备进行业务认证生成第二共享密钥,所述网络参数包括所述网络侧信息。

在又一种可选的方案中,所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

在又一种可选的方案中,当所述参考信息包含所述业务参数时,所述处理器 2001 结合所述参考信息和第一共享密钥生成第二共享密钥之前,还用于:

接收所述网络认证设备转发的来自所述业务认证设备的所述业务参数。

在又一种可选的方案中,所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项;所述网络参数包括运营商标识,接入网络标识,服务网络标识,网络类型标识,局域网网络标识,切片标识,承载标识,服务质量标识和流标识中的至少一项。

在本发明实施例中,用户设备的具体实现可以对应参照上述方法实施例的相应描述。

在图 20 所示的用户设备中,用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥,然后该业务认证设备将该第二共享密钥发送给该网络认证设备,使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说,生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息,提升了该目标共享密钥的安全级别。

请参见图 21,图 21 是本发明实施例提供的一种网络认证设备 210,该网络认证设备

210 包括处理器 2101 和存储器 2102, 所述处理器 2101 和存储器 2102 通过总线相互连接。

存储器 2102 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM), 该存储器 2102 用于相关指令及数据。

处理器 2101 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU), 在处理器 2101 是一个 CPU 的情况下, 该 CPU 可以是单核 CPU, 也可以是多核 CPU。

所述网络认证设备 210 中的处理器 2101 读取所述存储器 2102 中存储的程序代码, 用于执行以下操作:

接收业务认证设备发送的第二共享密钥, 业务认证设备和用户设备均用于结合第一共享密钥和参考信息生成所述第二共享密钥, 所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥, 所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息;

根据所述第二共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

通过执行上述操作, 用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥, 然后该业务认证设备将该第二共享密钥发送给该网络认证设备, 使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说, 生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息, 提升了该目标共享密钥的安全级别。

在一种可选的方案中, 所述处理器 2101 根据所述第二共享密钥生成目标共享密钥, 具体为:

和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

在又一种可选的方案中, 所述处理器 2101 和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥之前, 还用于:

和所述用户设备进行网络认证生成第三共享密钥;

备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥, 包括:

和所述用户设备根据所述第二共享密钥进行网络认证生成第四共享密钥;

和所述用户设备均根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

在又一种可选的方案中, 所述处理器 2101 根据所述第二共享密钥生成目标共享密钥, 具体为:

和所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为目标共享密钥。

在又一种可选的方案中, 所述处理器 2101 根据所述第二共享密钥生成目标共享密钥,

具体为：

和所述用户设备进行网络认证生成第三共享密钥；

和所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

在又一种可选的方案中，所述处理器 2101 根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

在又一种可选的方案中，所述处理器 2101 还用于：

向所述业务认证设备获取所述第一共享密钥；

根据所述第一共享密钥和第五共享密钥生成网络侧信息，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

将所述网络侧信息发送给所述业务认证设备，以使所述业务认证设备向所述用户设备转发所述网络侧信息，所述网络参数属于所述参考信息。

在又一种可选的方案中，所述处理器 2101 根据所述第二共享密钥生成目标共享密钥之前，还用于：

将所述目标共享密钥发送给所述业务认证设备，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥用作所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在又一种可选的方案中，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，网络认证设备 210 的具体实现还可以参照上述方法实施例的相应描述。

在图 21 所述的网络认证设备 210 中，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也就是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

请参见图 22，图 22 是本发明实施例提供的一种业务认证设备 220，该业务认证设备

220 包括处理器 2201 和存储器 2202, 所述处理器 2201 和存储器 2202 通过总线相互连接。

存储器 2202 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器(EPROM 或者快闪存储器)、或便携式只读存储器(CD-ROM), 该存储器 2202 用于相关指令及数据。

处理器 2201 可以是一个或多个中央处理器(英文: Central Processing Unit, 简称: CPU), 在处理器 2201 是一个 CPU 的情况下, 该 CPU 可以是单核 CPU, 也可以是多核 CPU。

所述业务认证设备 220 中的处理器 2201 读取所述存储器 2202 中存储的程序代码, 用于执行以下操作:

将预存的目标业务的业务参数发送给网络认证设备和用户设备; 以使所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥, 所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过执行上述操作, 该业务认证设备将业务参数发送给该网络认证设备, 该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息, 提升了该目标共享密钥的安全级别。

在一种可选的方案中, 所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

在本发明实施例中, 业务认证设备 220 的具体实现还可以对应参照上述方法实施例的相应描述。

在图 22 所示的业务认证设备 220 中, 该业务认证设备将业务参数发送给该网络认证设备, 该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息, 提升了该目标共享密钥的安全级别。

请参见图 23, 图 23 是本发明实施例提供的一种用户设备 230, 该用户设备 230 包括处理器 2301 和存储器 2302, 所述处理器 2301 和存储器 2302 通过总线相互连接。

存储器 2302 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器(EPROM 或者快闪存储器)、或便携式只读存储器(CD-ROM), 该存储器 2302 用于相关指令及数据。

处理器 2301 可以是一个或多个中央处理器(英文: Central Processing Unit, 简称: CPU), 在处理器 2301 是一个 CPU 的情况下, 该 CPU 可以是单核 CPU, 也可以是多核 CPU。

所述用户设备 230 中的处理器 2301 读取所述存储器 2302 中存储的程序代码, 用于执行以下操作:

接收业务认证设备发送的预存的目标业务的业务参数, 所述业务认证设备还用于将所述业务参数发送给网络认证设备;

和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过执行上述操作，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述处理器 2301 和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述网络认证设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

在本发明实施例中，用户设备 230 的具体实现还可以参照上述方法实施例的相应描述。

在图 23 所示的用户设备 230 中，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及和网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 24，图 24 是本发明实施例提供的一种网络认证设备 240，该网络认证设备 240 包括处理器 2401 和存储器 2402，所述处理器 2401 和存储器 2402 通过总线相互连接。

存储器 2402 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 2402 用于相关指令及数据。

处理器 2401 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 2401 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

网络认证设备 240 中的处理器 2401 读取所述存储器 2402 中存储的程序代码，用于执行以下操作：

接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给用户设备；

和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

通过执行上述操作，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

在一种可选的方案中，所述处理器 2401 和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述用户设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

在本发明实施例中，网络认证设备 240 的具体实现还可以参照上述方法实施例的相应描述。

在图 24 所示的网络认证设备 240 中，该业务认证设备将业务参数发送给该网络认证设备，该网络认证设备根据自身预先与该用户设备共享的原始共享密钥和该业务参数生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 25，图 25 是本发明实施例提供的一种业务认证设备 250，该业务认证设备 250 包括处理器 2501 和存储器 2502，所述处理器 2501 和存储器 2502 通过总线相互连接。

存储器 2502 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 2502 用于相关指令及数据。

处理器 2501 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 2501 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

业务认证设备 250 中的处理器 2501 读取所述存储器 2502 中存储的程序代码，用于执行以下操作：

获取用户设备的身份标识；

结合自身的业务公钥、业务私钥和所述身份标识生成身份密钥，并将所述身份密钥、所述业务公钥发送给所述网络认证设备，所述身份密钥和所述业务公钥用于所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在本发明实施例中，业务认证设备 250 的具体实现还可以参照上述方法实施例的相应描述。

在图 25 所示的业务认证设备 250 中，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生

成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 26，图 26 是本发明实施例提供的一种用户设备 260，该用户设备 260 包括处理器 2601 和存储器 2602，所述处理器 2601 和存储器 2602 通过总线相互连接。

存储器 2602 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 2602 用于相关指令及数据。

处理器 2601 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 2601 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

用户设备 260 中的处理器 2601 读取所述存储器 2602 中存储的程序代码，用于执行以下操作：

和网络认证设备根据认证根密钥进行网络认证生成目标共享密钥，所述认证根密钥为所述网络认证设备根据身份密钥、业务认证设备管理的目标业务的业务公钥和所述网络认证设备所在蜂窝网的网络参数生成的并写入到所述用户设备中的密钥，所述身份密钥由所述业务认证设备根据所述业务公钥、所述目标业务的业务私钥和获取的所述用户设备的身份标识生成的，所述业务认证设备用于将所述业务公钥和所述身份私钥发送给所述网络认证设备；所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在一种可选的方案中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，用户设备 260 的具体实现还可以参照上述方法实施例的相应描述。

在图 26 所示的用户设备 260 中，该业务认证设备将业务公钥、身份密钥发送给该网络认证设备，该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥，该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 27，图 27 是本发明实施例提供的一种网络认证设备 270，该网络认证设备 270 包括处理器 2701 和存储器 2702，所述处理器 2701 和存储器 2702 通过总线相互连接。

存储器 2702 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 2702 用于相关指令及数据。

处理器 2701 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 2701 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

网络认证设备 270 中的处理器 2701 读取所述存储器 2702 中存储的程序代码，用于执

行以下操作:

接收身份密钥和业务认证设备管理的目标业务的业务公钥, 所述身份密钥为所述业务认证设备根据所述目标业务的业务私钥、所述业务公钥和获取的用户设备的身份标识生成的密钥;

备结合所述身份密钥、所述业务公钥和所述网络认证设备所在蜂窝网的网络参数生成认证根密钥;

将所述认证根密钥写入所述用户设备;

和所述用户设备根据所述认证根密钥进行网络认证生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在一种可选的方案中, 所述网络参数包括运营商标识, 接入网络标识, 服务网络标识, 网络类型标识, 局域网网络标识, 切片标识, 承载标识, 服务质量标识和流标识中的至少一项。

在本发明实施例中, 网络认证设备 270 的具体实现还可以参照上述方法实施例的相应描述。

在图 27 所示的网络认证设备 270 中, 该业务认证设备将业务公钥、身份密钥发送给该网络认证设备, 该网络认证设备根据自身所在网络的信息、该身份密钥和该业务公钥生成认证根密钥, 该网络认证设备与该用户设备进一步基于该认证根密钥进行网络认证生成目标共享密钥。也即是说, 生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息, 提升了该目标共享密钥的安全级别。

请参见图 28, 图 28 是本发明实施例提供的一种业务认证设备 280, 该业务认证设备 280 包括处理器 2801 和存储器 2802, 所述处理器 2801 和存储器 2802 通过总线相互连接。

存储器 2802 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM), 该存储器 2802 用于相关指令及数据。

处理器 2801 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU), 在处理器 2801 是一个 CPU 的情况下, 该 CPU 可以是单核 CPU, 也可以是多核 CPU。

业务认证设备 280 中的处理器 2801 读取所述存储器 2802 中存储的程序代码, 用于执行以下操作:

和用户设备进行业务认证生成参考共享密钥, 或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥;

将所述参考共享密钥发送给网络认证设备, 以使所述网络认证设备和所述用户设备结合所述参考共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在一种可选的方案中, 所述处理器 2801 还用于:

接收所述网络认证设备发送的所述目标共享密钥;

将所述目标共享密钥, 或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证

设备与用户设备协商的保护数据安全传输的共享密钥。

在本发明实施例中，业务认证设备 280 的具体实现还可以参照上述方法实施例的相应描述。

在图 28 所示的业务认证设备 280 中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 29，图 29 是本发明实施例提供的一种用户设备 290，该用户设备 290 包括处理器 2901 和存储器 2902，所述处理器 2901 和存储器 2902 通过总线相互连接。

存储器 2902 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 2902 用于相关指令及数据。

处理器 2901 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 2901 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

用户设备 290 中的处理器 2901 读取所述存储器 2902 中存储的程序代码，用于执行以下操作：

和业务认证设备进行业务认证生成参考共享密钥，或者所述业务认证设备和所述用户设备预先配置所述参考共享密钥，所述业务认证设备用于将所述参考共享密钥发送给网络认证设备；

和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在一种可选的方案中，所述处理器 2901 和所述网络认证设备结合所述参考共享密钥生成目标共享密钥之前，还用于：

接收所述网络认证设备发送的所述网络认证设备所在蜂窝网的网络参数；

和所述网络认证设备结合所述参考共享密钥生成目标共享密钥，包括：

和所述网络认证设备根据所述网络参数和所述参考共享密钥生成认证共享密钥；

和所述网络认证设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

在一种可选的方案中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在本发明实施例中，用户设备 290 的具体实现还可以参照上述方法实施例的相应描述。

在图 29 所示的用户设备 290 中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共

享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

请参见图 30，图 30 是本发明实施例提供的一种网络认证设备 300，该网络认证设备 300 包括处理器 3001 和存储器 3002，所述处理器 3001 和存储器 3002 通过总线相互连接。

存储器 3002 包括但不限于是随机存取存储器 (RAM)、只读存储器 (ROM)、可擦除可编程只读存储器 (EPROM 或者快闪存储器)、或便携式只读存储器 (CD-ROM)，该存储器 3002 用于相关指令及数据。

处理器 3001 可以是一个或多个中央处理器 (英文: Central Processing Unit, 简称: CPU)，在处理器 3001 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

网络认证设备 300 中的处理器 3001 读取所述存储器 3002 中存储的程序代码，用于执行以下操作：

接收业务认证设备发送的参考共享密钥，所述参考共享密钥由所述业务认证设备和用户设备进行业务认证生成的或者预先配置的；

和所述用户设备结合所述参考共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

在一种可选的方案中，所述处理器 3001 和所述用户设备结合所述参考共享密钥生成目标共享密钥之前，还用于：

将所述网络认证设备所在蜂窝网的网络参数发送给所述用户设备；

和所述用户设备结合所述参考共享密钥生成目标共享密钥，包括：

和所述用户设备均根据所述网络参数和所述参考共享密钥生成认证共享密钥；

和所述用户设备根据所述认证共享密钥进行网络认证生成目标共享密钥。

在又一种可选的方案中，所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

在又一种可选的方案中，所述处理器 3001 还用于：

所述网络认证设备将所述目标共享密钥发送给所述业务认证设备，以使所述业务认证设备将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与用户设备协商的保护数据安全传输的共享密钥。

在本发明实施例中，网络认证设备 300 的具体实现还可以参照上述方法实施例的相应描述。

在图 30 所示的网络认证设备 300 中，该业务认证设备与该用户设备进行业务认证生成参考共享密钥，然后该网络认证设备将该参考共享密钥发送给该网络认证设备以及向该用户设备转发来自该网络认证设备的网络参数；该网络认证设备和该用户设备均根据该参考共享密钥和该网络参数生成认证共享密钥，并基于该认证共享密钥进行网络认证生成目标共享密钥。也即是说，生成该目标共享密钥涉及到了与业务相关的信息、与该用户设备

相关的信息以及与网络相关的信息，提升了该目标共享密钥的安全级别。

上述详细阐述了本发明实施例的方法和装置，为了便于更好地实施本发明实施例的上述方案，相应地，下面提供了本发明实施例的相关系统。

请参见图 31，图 31 是本发明实施例提供的一种业务认证系统 310 的结构示意图，该系统包括业务认证设备 3101、用户设备 3102 和网络认证设备 3103。

在一种可选的方案中，该业务认证设备 3101 为图 7 所示的业务认证设备 70 或者图 19 所示的业务认证设备 190；该用户设备 3102 为图 8 所示的用户设备 80 或者图 20 所示的用户设备 200；该网络认证设备 3103 为图 9 所示的网络认证设备 90 或者图 21 所示的网络认证设备 210。

在又一种可选的方案中，该业务认证设备 3101 为图 10 所示的业务认证设备 100 或者图 22 所示的业务认证设备 220；该用户设备 3102 为图 11 所示的用户设备 110 或者图 23 所示的用户设备 230；该网络认证设备 3103 为图 12 所示的网络认证设备 120 或者图 24 所示的网络认证设备 240。

在又一种可选的方案中，该业务认证设备 3101 为图 13 所示的业务认证设备 130 或者图 25 所示的业务认证设备 250；该用户设备 3102 为图 14 所示的用户设备 140 或者图 26 所示的用户设备 260；该网络认证设备 3103 为图 15 所示的网络认证设备 150 或者图 27 所示的网络认证设备 270。

在又一种可选的方案中，该业务认证设备 3101 为图 16 所示的业务认证设备 160 或者图 28 所示的业务认证设备 280；该用户设备 3102 为图 17 所示的用户设备 170 或者图 29 所示的用户设备 290；该网络认证设备 3103 为图 18 所示的网络认证设备 180 或者图 30 所示的网络认证设备 300。

图 1 所示的网络认证系统中包括网络认证设备、业务认证设备和用户设备，在一种可选的方案中，各个设备相互协作来执行如下步骤。

步骤 S3101：网络认证设备生成经过初始共享密钥加密的访问令牌，所述初始共享密钥为所述网络认证设备与业务认证设备预先共享的密钥；该网络认证设备包括生成单元，该网络认证设备具体通过该生成单元来执行步骤 S3101，该生成单元可以基于该网络认证设备的处理器来实现步骤 S3101。

步骤 S3102：所述网络认证设备将所述访问令牌发送给所述用户设备；该网络认证设备包括发送单元，该网络认证设备具体通过该发送单元来执行步骤 S3102，该发送单元可以基于该网络认证设备的收发器来实现步骤 S3102。

步骤 S3103：所述用户设备接收所述访问令牌并将所述访问令牌发送给所述业务认证设备；该用户设备包括收发单元，该用户设备具体通过该收发单元来执行步骤 S3103，该收发单元可以基于该用户设备的收发器来实现步骤 S3103。

步骤 S3104：所述业务认证设备接收所述访问令牌并通过所述初始共享密钥验证所述访问令牌的正确性；该业务认证设备包括接收单元，该业务认证设备具体通过该接收单元来执行步骤 S3104，该接收单元可以基于该业务认证设备的收发器来实现步骤 S3104。

步骤 S3105: 所述业务认证设备在验证出所述访问令牌正确时向所述用户设备发送验证成功消息, 以通知与所述用户设备之间成功完成业务认证。该业务认证设备包括发送单元, 该业务认证设备具体通过该发送单元来执行步骤 S3105, 该发送单元可以基于该业务认证设备的收发器来实现步骤 S3105。

在一种可选的方案中, 所述访问令牌中包含目标共享密钥, 所述用户设备和所述业务认证设备用于在所述用户设备与所述业务认证设备之间成功完成业务认证时, 将所述访问令牌中的所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥, 作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。可选的, 该目标共享密钥为该网络认证设备与该用户设备进行网络认证得到的共享密钥。

在又一种可选的方案中, 所述访问令牌包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项。可选的, 所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项; 所述网络参数包括运营商标识, 接入网络标识, 服务网络标识, 网络类型标识, 局域网网络标识, 切片标识, 承载标识, 服务质量标识和流标识中的至少一项。

进一步地, 该访问令牌还可以包括通过初始共享密钥生成的针对网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项的消息认证码。当包含该消息认证码时, 在步骤 S3104 中还需要基于该初始共享密钥验证该消息认证码的正确性, 步骤 S3105 中所述业务认证设备在验证出所述访问令牌正确时向所述用户设备发送验证成功消息, 具体为: 所述业务认证设备在验证出所述访问令牌正确以及验证出所述消息认证码正确时时向所述用户设备发送验证成功消息。此处描述的网络认证系统还可以参照图 6D 和图 6E 所对应实施例的相应描述。

图 1 所示的网络认证系统中包括网络认证设备、业务认证设备和用户设备, 在一种可选的方案中, 各个设备相互协作来执行如下步骤。

步骤 S3201: 用户设备 UE 与网络认证设备进行网络认证。该用户设备和该网络认证设备均包括认证单元, 该用户设备和该网络认证设备具体通过该认证单元来执行步骤 S3201, 该认证单元可以基于该用户设备和该网络认证设备的处理器来实现步骤 S3201。

步骤 S3202: 网络认证设备在网络认证通过后生成认证令牌 token 和该 token 的过期信息, 该过期信息用于表征该 token 什么时候过期; 还可以生成范围信息, 该范围信息用于表征该 token 可以被哪些业务认证设备使用; 或者该范围信息用于表征该 token 可以被哪些用户设备使用。该网络认证设备包括生成单元, 该网络认证设备具体通过该生成单元来执行步骤 S3202, 该生成单元可以基于该网络认证设备的处理器来实现步骤 S3202。

步骤 S3203: 网络认证设备向该 UE 发送该 token; 还可以发送该网络认证设备相关的信息, 该网络认证设备相关的信息用于表明该 token 来自于该网络认证设备。该网络认证设备包括发送单元, 该网络认证设备具体通过该发送单元来执行步骤 S3203, 该发送单元可以基于该网络认证设备的收发器来实现步骤 S3203。

步骤 S3204: 该用户设备向该业务认证设备发送该 token 和该网络认证设备的相关信

息；该用户设备设备包括发送单元，该用户设备具体通过该发送单元来执行步骤 S3204，该发送单元可以基于该用户设备的收发器来实现步骤 S3204。

步骤 S3205：该业务认证设备接收该 token 和该网络认证设备的相关信息，并根据该网络认证设备的相关信息向该网络认证设备发送该 token；发送的消息可能还包括 UE ID 和业务认证设备的相关信息中的至少一项。该业务认证设备包括接收单元，该业务认证设备具体通过该接收单元来执行步骤 S3205，该接收单元可以基于该业务认证设备的收发器来实现步骤 S3205。

步骤 S3206：该网络认证设备接收该 token，判断该 token 是否为自身生成的 token，如果该 token 为自身生成的 token 则进一步他根据该过期信息判断该 token 是否过期，若没过期则表明验证 token 成功。可选的，当该网络认证设备生成了范围信息时，该网络认证设备还需要根据该范围信息判断发送该 token 的业务认证设备是否为该范围信息中允许的业务认证设备，若为允许的业务认证设备且该 token 未过期则表明验证 token 成功。可选的，该范围信息用于表征该 token 可以被哪个用户设备使用时，该网络认证设备还需要根据该范围信息判断该用户设备是否为该范围信息中允许的用户设备，若该用户设备为允许的用户设备且该业务认证设备为允许的业务认证设备，并且该 token 未过期则表明验证 token 成功。该网络认证设备包括判断单元，该网络认证设备具体通过该判断单元来执行步骤 S3206，该判断单元可以基于该网络认证设备的处理器来实现步骤 S3206。

可选的，步骤 S3205 中不包含业务认证设备的相关信息，该网络认证设备也可以根据接收的 token 的来源确定业务认证设备的相关信息。

可选的，判断该用户设备是否为该范围信息中允许的用户设备时用到的该用户设备的相关信息，可以为该用户设备将该用户设备自身的相关信息发送至业务认证设备，再由业务认证设备在步骤 S3205 中一同发送至该网络认证设备。

步骤 S3207：若验证 token 成功，则该网络认证设备向该业务认证设备发送消息通知 token 验证成功；该网络认证设备包括发送单元，该网络认证设备具体通过该发送单元来执行步骤 S3207，该发送单元可以基于该网络认证设备的收发器来实现步骤 S3207。

步骤 S3208：该业务认证设备向该 UE 发送消息通知 token 验证成功。业务认证设备和 UE 双方都获知了 token 验证成功，即表明该业务认证设备与该 UE 之间认证成功。该业务认证设备包括发送单元，该业务认证设备具体通过该发送单元来执行步骤 S3208，该发送单元可以基于该业务认证设备的收发器来实现步骤 S3208。

图 1 所示的网络认证系统中包括网络认证设备、业务认证设备和用户设备，在一种可选的方案中，各个设备相互协作来执行如下步骤。

步骤 S3301：用户设备 UE 与网络认证设备进行网络认证，网络认证生成的共享密钥为网络共享密钥 K1。该用户设备和该网络认证设备均包括认证单元，该用户设备和该网络认证设备具体通过该认证单元来执行步骤 S3301，该认证单元可以基于该网络认证设备和该用户设备的处理器来实现步骤 S3301。

步骤 S3302：UE 基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token，并通过该网络共享密钥 K1 加密该访问令牌 token。可

选的, $\text{token} = \text{Enc_K1_}(\text{K2}, \text{基础信息}, \text{MAC})$, 也即是说, 该访问令牌 token 为采用 K1 对 K2、基础信息和 MAC 加密生成; 其中, K2 为该 UE 确定的后续可能用作用户设备与业务认证设备之间保护数据传输的共享密钥, 基础信息包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项, 可选的, 该用户设备可以预先向该网络认证设备和该业务认证设备获取需要用到信息; $\text{MAC} = \text{MAC_K1_}(\text{新鲜参数和/或基础信息})$, 即 MAC 为该基础信息的信息认证码, 或者该新鲜参数的信息认证码 (此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同), 或者该基础信息和该新鲜参数的信息认证码; 该信息认证码 MAC 由该网络共享密钥 K1 生成。该用户设备包括生成单元, 该用户设备具体通过该生成单元来执行步骤 S3302, 该生成单元可以基于该用户设备的处理器来实现步骤 S3302。

需要说明的是, 若上述推导公式中用到新鲜参数 nonce, 则 UE 还需要将用到的新鲜参数发送至业务认证设备, 由该业务认证设备将该新鲜参数转发给该网络认证设备, 后续该网络认证设备可以通过该新鲜参数验证 token 的新鲜性。

进一步地, 共享密钥 K2 可以为配置的随机的参数, 也可以为网络共享密钥 K1, 还可以为基于网络共享密钥 K1 推导出来的共享密钥, 例如, $\text{K2} = \text{KDF}(\text{K1}, \text{基础信息})$, 即通过预设的算法对该网络共享密钥 K1 和基础信息进行计算来得到该共享密钥 K2。

步骤 S3303: UE 向业务认证设备发送该 token。该用户设备包括发送单元, 该用户设备具体通过该发送单元来执行步骤 S3303, 该发送单元可以基于该用户设备的收发器来实现步骤 S3303。

步骤 S3304: 业务认证设备接收该 UE 发送的该 token 并将该 token 转发给该网络认证设备, 该业务认证设备还可能向该网络认证设备发送该 UE 的相关信息 (包括但不限于 UE ID), 该相关信息可能由该 UE 发送至该业务认证设备的, 该相关信息可以在一定范围内区分该 UE 与其他设备。该业务认证设备包括接收单元, 该业务认证设备具体通过该接收单元来执行步骤 S3304, 该接收单元可以基于该业务认证设备的收发器来实现步骤 S3304。

步骤 S3305: 该网络认证设备接收该 token 和该 UE 的相关信息; 根据该 UE 的相关信息并找到与该 UE 网络认证生成的网络共享密钥 K1, 并使用 K1 解密 token 得到该共享密钥 K2、该基础信息和信息认证码 MAC; 然后根据 K1 验证 MAC 的正确性, 若验证 MAC 正确则表明验证 token 成功。该网络认证设备包括接收单元, 该网络认证设备具体通过该接收单元来执行步骤 S3305, 该接收单元可以基于该网络认证设备的收发器来实现步骤 S3305。

步骤 S3306: 若验证 token 成功, 则该网络认证设备向该业务认证设备发送消息通知 token 验证成功, 该通知消息中还包括从 token 中获得的共享密钥 K2; 该网络认证设备包括发送单元, 该网络认证设备具体通过该发送单元来执行步骤 S3306, 该发送单元可以基于该网络认证设备的收发器来实现步骤 S3306。

步骤 S3307: 该业务认证设备向该 UE 发送消息通知 token 验证成功。业务认证设备和 UE 双方都获知了 token 验证成功, 即表明该业务认证设备与该 UE 之间认证成功。该业务认证设备包括发送单元, 该业务认证设备具体通过该发送单元来执行步骤 S3307, 该发送单元可以基于该业务认证设备的收发器来实现步骤 S3307。

步骤 S3308: 该 UE 和该业务认证设备将该 K2 作为该 UE 与该业务认证设备之间用于保护数据安全传输的共享密钥。该用户设备和该业务认证设备均包括共享单元, 该用户设备和该业务认证设备具体通过该共享单元来执行步骤 S3308, 该共享单元可以基于该用户设备的处理器和该业务认证设备的处理器来实现步骤 S3308。

可选的, UE 与业务认证设备根据 K2 进一步推导出共享密钥 K3, 例如, $K3 = KDF(K2, \text{基础信息})$, 即通过预设算法对该 K2 和基础信息进行计算得到 K3, K3 用于该 UE 与该业务认证设备之间保护数据的安全传输。

图 1 所示的网络认证系统中包括网络认证设备、业务认证设备和用户设备, 在一种可选的方案中, 各个设备相互协作来执行如下步骤。

步骤 S3401: 用户设备 UE 与网络认证设备进行网络认证, 网络认证生成的共享密钥为网络共享密钥 K1。该网络认证设备和该用户设备均包括认证单元, 该网络认证设备和该用户设备具体通过该认证单元来执行步骤 S3401, 该认证单元可以基于该网络认证设备的处理器和该用户设备的处理器来实现步骤 S3401。

步骤 S3402: UE 基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token, 可选的, 该 token 为消息认证码 MAC, $MAC = MAC_K1_(\text{新鲜参数和/或基础信息})$, 即 MAC 为该基础信息的消息认证码, 或者该新鲜参数的消息认证码 (此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同), 或者该基础信息和该新鲜参数的消息认证码; 该消息认证码 MAC 由该网络共享密钥 K1 生成。该用户设备包括生成单元, 该用户设备具体通过该生成单元来执行步骤 S3402, 该生成单元可以基于该用户设备的处理器来实现步骤 S3402。

需要说明的是, 若上述推导公式中用到新鲜参数 nonce, 则 UE 还需要将用到的新鲜参数发送至业务认证设备, 由该业务认证设备将该新鲜参数发送给该网络认证设备, 后续该网络认证设备可以通过该新鲜参数验证 token 的新鲜性。

步骤 S3403: UE 向业务认证设备发送该 token。该用户设备包括发送单元, 该用户设备具体通过该发送单元来执行步骤 S3403, 该发送单元可以基于该用户设备的收发器来实现步骤 S3403。

步骤 S3404: 业务认证设备接收该 UE 发送的该 token 并将该 token 转发给该网络认证设备, 该业务认证设备还可能向该网络认证设备发送该 UE 的相关信息, 该相关信息可能由该 UE 发送该业务认证设备的, 该相关信息可以在一定范围内区分该 UE 与其他设备, 例如, 该用户设备的相关信息可以为该用户设备的身份标识 (UEID)。该业务认证设备包括收发单元, 该业务认证设备具体通过该收发单元来执行步骤 S3404, 该收发单元可以基于该业务认证设备的收发器来实现步骤 S3404。

步骤 S3405: 该网络认证设备接收该 token 和该 UE 的相关信息; 根据该 UE 的相关信息并找到与该 UE 网络认证生成的网络共享密钥 K1, 并根据 K1 验证 MAC 的正确性, 若验证 MAC 正确则表明验证 token 成功。该网络认证设备包括接收单元, 该网络认证设备具体通过该接收单元来执行步骤 S3405, 该接收单元可以基于该网络认证设备的收发器来实现步骤 S3405。

步骤 S3406: 若验证 token 成功, 则该网络认证设备向该业务认证设备发送消息通知 token 验证成功; 该网络认证设备包括发送单元, 该网络认证设备具体通过该发送单元来执行步骤 S3406, 该发送单元可以基于该网络认证设备的收发器来实现步骤 S3405。

步骤 S3407: 该业务认证设备向该 UE 发送消息通知 token 验证成功。业务认证设备和 UE 双方都获知了 token 验证成功, 即表明该业务认证设备与该 UE 之间认证成功。该业务认证设备包括收发单元, 该业务认证设备具体通过该收发单元来执行步骤 S3407, 该收发单元可以基于该业务认证设备的收发器来实现步骤 S3407。

需要说明的是, 还可以基于上述方案显而易见地推导出以下方案, 即 UE 首先与业务认证设备建立双向认证, 由 UE 或者业务认证设备生成 token; 之后 UE 发送 token 至网络认证设备, 网络认证设备可以自己验证 token 的正确性, 也可能将 token 发送至业务认证设备, 由业务认证设备验证 token 的正确性, 并将验证结果发送至网络认证设备。相当于将 6C-6H 中涉及到的业务认证设备与网络认证设备进行了调换。另外, token 包含但不限于如下两种情况: 情况一 $\text{token} = \text{Enc_K0_}(\text{K2}, \text{基础信息}, \text{MAC_K0_}(\text{基础信息和/或 nonce}))$, 情况二: $\text{token} = \text{MAC_K0_}(\text{基础信息和/或 nonce})$ 。这两种情况的理解可以参照以上描述, 此处不再赘述。

为了便于理解, 以下以 token 由业务认证设备生成为例来进行描述, token 由 UE 生成的情况可以类比。

图 1 所示的网络认证系统中包括网络认证设备、业务认证设备和用户设备, 在一种可选的方案中, 各个设备相互协作来执行如下步骤。

步骤 S3501: 用户设备 UE 与业务认证设备进行业务认证, 生成的共享密钥为业务共享密钥 K1; 该 UE 可以在业务认证之前或者之后或者业务认证的过程中向该业务认证设备发送网络认证设备的相关信息, 以表明该 UE 需要与该网络认证设备认证。该用户设备和该业务认证设备均包括认证单元, 该用户设备和该业务认证设备具体通过该认证单元来执行步骤 S3501, 该认证单元可以基于该用户设备的处理器和该业务认证设备的处理器来实现步骤 S3501。

步骤 S3502: 业务认证设备根据该网络认证设备的相关信息确定该网络认证设备预先与该业务认证设备共享的初始共享密钥 K0; 基于网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项来生成访问令牌 token。可选的, $\text{token} = \text{Enc_K0_}(\text{K2}, \text{基础信息}, \text{MAC})$, 也即是说, 该访问令牌 token 为采用初始共享密钥 K0 对 K2、基础信息和 MAC 进行的加密; 其中, K2 为该业务认证设备确定的, 可能用作用户设备与网络认证设备之间保护数据传输的共享密钥, 基础信息包括网络参数、业务参数、所述用户设备的身份标识和新鲜参数 nonce 中的至少一项, $\text{MAC} = \text{MAC_K0_}(\text{新鲜参数和/或基础信息})$, 即 MAC 为该基础信息的信息认证码, 或者该新鲜参数的消息认证码 (此处的新鲜参数可以与该基础信息中的新鲜参数相同也可以不同), 或者该基础信息和该新鲜参数的消息认证码; 该消息认证码 MAC 的生成采用初始共享密钥 K0。该业务认证设备包括确定单元, 该业务认证设备具体通过该确定单元来执行步骤 S3502, 该确定单元可以基于该业务认证设备的处理器来实现步骤 S3502。

需要说明的是,若上述推衍公式中用到新鲜参数 nonce,则业务认证设备还需要将用到的新鲜参数发送至 UE,并由 UE 发送至网络认证设备,后续该网络认证设备可以通过该新鲜参数验证 token 的新鲜性。

进一步地,共享密钥 K2 可以为配置的随机的参数,也可以为业务共享密钥 K1,还可以为基于业务共享密钥 K1 推衍出来的共享密钥,例如, $K2 = KDF(K1, \text{基础信息})$,即通过预设的算法对该业务共享密钥 K1 和基础信息进行计算来得到该共享密钥 K2。

进一步地,网络认证设备的相关信息为能够在一定范围内区分该网络认证设备与其他设备的信息,例如,可以为该网络认证设备的 IP 地址。

步骤 S3503: 该业务认证设备向 UE 发送 K2 和 token,还可能发送业务认证设备的相关信息,所述业务认证设备的相关信息可以包括业务参数。该业务认证设备包括发送单元,该业务认证设备具体通过该发送单元来执行步骤 S3503,该发送单元可以基于该业务认证设备的收发器来实现步骤 S3503。

步骤 S3504: UE 接收 K2 和 token 并向网络认证设备发送该 token 和该业务认证设备的相关信息。UE 可以自己生成该业务认证设备的相关信息,也可以在与该业务认证设备进行业务认证之时,或者之前,或者之后接收该业务认证设备发送的该业务认证设备的相关信息,优选的,在 E 在步骤 S3503 中接收该业务认证设备发送的业务认证设备的相关信息。该用户设备包括收发单元,该用户设备具体通过该收发单元来执行步骤 S3504,该收发器单元可以基于该用户设备的收发器来实现步骤 S3504。

步骤 S3505: 网络认证设备接收该 token 和该业务认证设备的相关信息,根据该业务认证设备的相关信息来确定预先与该业务认证设备共享的初始共享密钥 K0,并使用 K0 解密 token 得到该共享密钥 K2、该基础信息和消息认证码 MAC;然后根据 K0 验证 MAC 的正确性,验证 MAC 成功后则表明该网络认证设备验证 token 成功。因此,该网络认证设备将该 K2 作为与该 UE 之间用于保护数据传输的共享密钥。该网络认证设备包括接收单元,该网络认证设备具体通过该接收单元来执行步骤 S3505,该接收单元可以基于该网络认证设备的收发器来实现步骤 S3505。

步骤 S3506: 该网络认证设备向该 UE 发送消息以通知验证 token 成功,相应地,该 UE 接收消息。该网络认证设备包括发送单元,该网络认证设备具体通过该发送单元来执行步骤 S3506,该发送单元可以基于该网络认证设备的收发器来实现步骤 S3506。

步骤 S3507: 该网络认证设备和该 UE 将该共享密钥 K2 作为该 UE 与该网络认证设备之间用户保护数据安全传输的共享密钥。该网络认证设备和该用户设备均包括共享单元,该网络认证设备和该用户设备具体通过该共享单元来执行步骤 S3507,该共享单元可以基于该网络认证设备的处理器和该用户设备的的处理器来实现步骤 S3507。

可选的,UE 与网络认证设备根据 K2 进一步推衍出共享密钥 K3,例如, $K3 = KDF(K2, \text{基础信息})$,即通过预设算法对该 K2 和基础信息进行计算得到 K3, K3 用于该 UE 与该网络认证设备之间保护数据的安全传输。

可选的,加密 token 的共享密钥为 K1 而不是 K0,网络认证设备接收到 token 后根据业务认证设备的相关信息向该业务认证设备转发该 token 和该 UE 的相关信息;该业务认证设备根据该 UE 的相关信息确定与该 UE 认证生成的共享密钥 K1,再根据 K1 来解密 token,

并验证该 token 中 MAC 的正确性, 验证成功即表明该 UE 与该网络认证设备认证成功, 因此将 K2 发送给该网络认证设备, 以便该 UE 和该网络认证设备将该 K2 作为保护数据安全传输的共享密钥。可选的, 该 UE 的相关信息可以由该 UE 发送给业务认证设备, 该 UE 的相关信息可以为该 UE 的身份标识。

需要说明的是, 还可以对以上网络认证系统进行相应拓展得到新的网络认证系统, 拓展的思路如下:

K1 为 UE 与网络认证设备之间的共享密钥, 包括但不限于 K_{asme}, 加密密钥 (英文: cipher key, 简称: CK) 和完整性保护密钥 (英文: integrity key, 简称: IK) 中的至少一项。

另外, 也可能采用非对称密码的形式计算 token, 例如 $\text{token} = \text{Enc_PK_业务_}(K2, (\text{nonce1}, \text{基本信息}), \text{signature} = \text{MAC_SK_网络_}(\text{nonce2}, \text{基本信息}))$ 。PK_业务表示该业务认证设备提供的业务的公钥参数, SK_网络表示该网络认证设备所在的运营商网络的私钥参数。此时业务认证设备可以根据自己的私钥 SK_业务解密打开 token; 并且利用网络认证设备所在运营商网络的公钥 PK_网络, 验证 token 中签名的正确性。此时 token 的验证更加灵活, 不需要与网络认证设备进行网络认证交互即可完成验证。另外, 此处加密和签名的算法可以为基于公钥基础设施 (英文: Public key infrastructure, 简称: PKI) 等非对称密码技术, 也可以为基于身份的密码技术。

在本发明实施例中, 所述网络认证设备和所述用户设备根据所述第二共享密钥进行网络认证生成所述目标共享密钥的方式有多种。

在一种可选的方案中, 该网络认证设备可以包括的 CP-AU, 所述网络认证设备和所述用户设备根据所述第二共享密钥进行网络认证生成所述目标共享密钥, 具体为:

步骤 S4201: UE 向 CP-AU 发送请求接入网络的消息, 该请求接入网络的消息包含该 UE 的身份标识 UEID 和该 UE 与目标业务相关的业务标识, 该请求接入网络的消息可以触发网络认证流程, 该目标业务为该 UE 当前执行的业务。

步骤 S4202: 该 CP-AU 接收该请求接入网络的消息并通过预设的规则或者算法对该 UEID 和该业务标识进行处理或者与其他网元进行协商交互得到第二共享密钥 K_{ser}, 以及向签约服务器 (Subscriber Repository) 发送请求签约数据的消息, 该签约服务器中存储了该 UE 的签约信息, 例如, 存储了该 UE 的 SIM 卡号码。

步骤 S4203: 该签约服务器接收该请求签约数据的消息并根据该 UEID 确定与该 UE 预先共享的预置密钥 K (可选的, 该 K 为该 SIM 卡号码), 然后根据该预置密钥 K 计算认证向量 AV, 该认证向量包括随机数 RAND、网络侧认证令牌 (英文: Authentication Token, 简称: AUTN), 期待响应 (英文: Expected Response, 简称: XRES) 和基础密钥 K_{NG} (例如, 该 K_{NG} 接入安全管理密钥 (英文: Key Access Security Management Entity, 简称: K_{ASME})) 等信息, 该 K_{NG} 是基于预置密钥 K 和相关的网络参数来生成的; 为了便于区分可以称该 AV 中的期待响应为初始期待响应, 该网络侧认证令牌中包含消息认证码, 可以称该消息认证码为网络侧初始消息认证码 MAC。

步骤 S4204: 该签约服务器将该认证向量发送给该 CP-AU。

步骤 S4205: 该 CP-AU 接收该签约服务器发送的该认证向量, 并通过预设的消息认证码算法对该第二共享密钥 Kser 和该网络侧初始消息认证码 MAC 进行计算得到业务参考消息认证码 MAC', 例如, 该业务参考消息认证码 $MAC' = MAC(Kser, MAC, (nonce1, RAND, SQN, NAS\ COUNT, UE\ ID\ 的\ 至少\ 一项))$, 即生成该 MAC' 需要考虑 Kser 和 MAC 这两个因素, 除此之外还可以考虑新鲜参数 nonce1、RAND、序列号(英文: Sequence Number, 简称: SQN)、NAS COUNT、UEID 等参数, 若 MAC' 的生成包括 CP-AU 选择的新鲜参数 nonce1, 则 nonce1 可以由 CP-AU 发送给 UE。该消息认证码算法可为 HMACsha-256 等。

步骤 S4206: 该 CP-AU 向该 UE 发送认证请求消息, 该认证请求消息包括该随机数 RAND、K_{NG} 的密钥索引 KSI_{NG}、新的网络侧认证令牌 AUTN', 此处的 $AUTN' = SQN\ xor(异或)\ AK\ ||\ AMF\ ||\ MAC'$, 而上面 $AUTN = SQN\ xor(异或)\ AK\ ||\ AMF\ ||\ MAC$, 也即是说, 该 CP-AU 将签约服务器发送的 AUTN 中的 MAC 替换为了业务参考消息认证码 MAC', 然后就替换后形成的新的网络侧认证令牌 AUTN' 发送给了 UE。该 CP-AU 还要通过该预设的响应算法对该 XRES 和 Kser 进行计算得到参考期待响应 XRES', 该 CP-AU 计算该参考期待响应 XRES' 的时机此处不做限定, 例如, 可以在步骤 S4206 之后以及步骤 S4207 之前; 再如, 在步骤 S4210 之后以及步骤 S4211 之前; 还可以存在其他可能性, 此处不再一一举例。

步骤 S4207: 该 UE 接收该认证请求消息(也可以称“用户认证请求”), 然后通过认证与密钥协商协议(英文: Authentication and Key Agreement, 简称: AKA)的密钥推演算法对该认证请求消息中的信息进行计算, 得到用户侧认证令牌 AUTN_{UE} 和响应(英文: Response, 简称: RES)等信息, 该用户侧认证令牌中的消息认证码可以称为用户侧初始消息认证码, 该用户侧的响应可以称为初始响应。

步骤 S4208: 该 UE 通过上述预设的消息认证码算法对该第二共享密钥 Kser 和该用户侧初始消息认证码 MAC 进行计算得到用户侧参考消息认证码 MAC'', 然后判断业务参考消息认证码 MAC' 与该用户侧参考消息认证码 MAC'' 是否相同, 若相同, 则该 UE 已对该 CP-AU 的认证通过, 由于认证的过程中使用到的信息与业务相关且与网络相关, 因此可以看作该 UE 对该网络 and 该目标业务的认证通过。需要说明的是, 该 UE 预先基于自身已有的 UEID 和业务标识计算出了该第二共享密钥 Kser, 或者该 UE 预先存储了该第二共享密钥 Kser。

步骤 S4209: 若该 UE 对该 CP-AU 的认证通过, 则该 UE 通过预设的响应算法对该 RES 和该 Kser 进行计算得到参考响应 RES', 例如, $RES' = MAC(Kser, RES, (nonce1, nonce2, RAND, SQN, NAS\ COUNT, UE\ ID\ 的\ 至少\ 一项))$, 即计算该 RES' 需要考虑 Kser 和 RES, 除此之外还可能考虑 nonce1、nonce2、RAND、SQN、NAS COUNT、UE ID 等信息; 然后, 该 UE 将该 RES' 发送给该 CP-AU。若 RES' 的生成包括 UE 选择的新鲜参数 nonce2, 则 nonce2 可以由该 UE 发送给该 CP-AU。

步骤 S4210: 该 CP-AU 接收该 RES'。

步骤 S4211: 该 CP-AU 判断自身计算出参考期待响应 XRES' 与该 UE 发送的参考响应 RES' 是否相同, 若相同, 则该 CP-AU 对该 UE 的认证通过, 即网络和业务对 UE 的认证通过, 可选的, 若不相同, 则该 CP-AU 对 UE 的业务认证未通过, 这时, 该 CP-AU 可能向

该 UE 发送认证拒绝消息，该认证拒绝消息表明业务认证未通过。

步骤 S4212: 当该 UE 对该 CP-AU 的认证通过，以及该 CP-AU 对该 UE 的认证通过后，该 UE 和该 CP-AU 通过相同的密钥生成算法对该 K_{NG} 和 K_{ser} 进行计算生成密钥，生成的密钥即为该 UE 与该 CP-AU 之间双向认证生成的目标共享密钥。该 UE 和 CP-AU 使用的哪种密钥生成算法此处暂不作限定。可以理解的是，该 UE 可以通过 K_{NG} 的索引 KSI_{NG} 获取到该 K_{NG} 。另外，UE 可以在通过了对 CP-AU 的认证后就生成该目标共享密钥，而 CP-AU 可以在通过该 UE 的认证后再生成该目标共享密钥。

请参见图 32，图 32 是本发明实施例提供的又一种网络认证方法的流程示意图，该流程是步骤 S4201~S4212 的一种可能的表现形式，在该可能的表现形式中，UE 与 CP-AU 的之间的交互的信息可以经过无线接入网（英文：Radio Access Network，简称：RAN），该 CP-AU 可以进一步划分为更小的多个网元，由以上描述可知，该 CP-AU 承担的功能包括向签约服务器获取认证向量、根据签约服务器反馈的认证向量生成 MAC' 和 XRES'、向 UE 反馈认证请求消息、验证 RES' 和 XRES' 等操作，这些操作可以由该 CP-AU 中划分的多个网元来分别承担，例如，该 CP-AU 可以划分为安全锚点（英文：Security Anchor Function，简称：SEAF）、（英文：Authentication Server Function，简称：AUSF）等，其中，向签约服务器获取认证向量、根据签约服务器反馈的认证向量生成 MAC' 和 XRES' 由 AUSF 承担，向 UE 反馈认证请求消息、验证 RES' 和 XRES' 由 SEAF 承担，SEAF 和 AUSF 在承担各自的操作的过程中，SEAF 和 AUSF 之间还可能需要进行一些协商；另外，该签约服务器可以为认证信任状存储和处理单元（英文：Authentication Credential Repository and Processing Function，简称：ARPF）。

在又一种可选的方案中，该网络认证设备可以包括的 CP-AU，所述网络认证设备和所述用户设备根据所述第二共享密钥进行网络认证生成所述目标共享密钥，具体为：

步骤 S4301: UE 向 CP-AU 发送请求接入网络的消息，该请求接入网络的消息包含该 UE 的身份标识 UEID 和目标业务的业务标识，该目标业务为该 UE 当前执行的业务。

步骤 S4302: 该 CP-AU 接收请求接入网络的消息并根据对该 UEID 和该业务标识获取第二共享密钥 K_{ser} ，以及向签约服务器（Subscriber Repository）发送请求签约数据的消息，该签约服务器中存储了该 UE 的签约信息，例如，存储了该 UE 的 SIM 卡号码。

步骤 S4303: 该签约服务器接收该请求签约数据的消息并根据该 UEID 确定与该 UE 预先共享的预置密钥 K（可选的，该 K 为该 SIM 卡号码），然后根据该预置密钥 K 计算认证向量 AV，该认证向量包括随机数 RAND、网络侧认证令牌（英文：Authentication Token，简称：AUTN），期待响应（英文：Expected Response，简称：XRES）和基础密钥 K_{NG} （例如，接入安全管理密钥（英文：Key Access Security Management Entity，简称： K_{ASME} ））等信息，该 K_{NG} 是基于预置密钥 K 和相关的网络参数来生成的；为了便于区分可以称该 AV 中的期待响应为初始期待响应，该网络侧认证令牌中包含消息认证码，可以称该消息认证码为网络侧初始消息认证码 MAC。

步骤 S4304: 该签约服务器将该认证向量发送给该 CP-AU。

步骤 S4305: 该 CP-AU 接收该签约服务器发送的该认证向量，并通过预设的第一消息认证码算法对 RAND、该第二共享密钥 K_{ser} 等信息进行计算得到网络侧附加消息认证码

MAC1, 例如, 该网络侧附加消息认证码 $MAC1 = MAC(K_{ser}, RAND, (nonce1, \text{该 } MACSQN, NAS \text{ COUNT}, UE \text{ ID 的至少一项}))$, 即生成该 MAC1 需要考虑 K_{ser} 和 $RAND$, 除此之外还可以考虑该网络侧初始消息认证码新鲜参数 $nonce1$ 、 MAC 、序列号(英文: Sequence Number, 简称: SQN)、 $NAS \text{ COUNT}$ 、 $UEID$ 等参数, 若 $MAC1$ 的生成包括 $CP-AU$ 选择的新鲜参数 $nonce1$, 则 $nonce1$ 可以由 $CP-AU$ 发送给 UE 。该消息认证码算法可为 $HMACsha-256$ 等。

步骤 S4306: 该 $CP-AU$ 向该 UE 发送认证请求消息 (或者称为 “用户认证请求”), 该认证请求消息包括该随机数 $RAND$ 、 K_{NG} 的密钥索引 KSI_{NG} 、网络侧初始消息认证码 MAC 、网络侧附加消息认证码 $MAC1$ 等信息, 该 MAC 和该 $MAC1$ 可以存在于网络侧认证令牌 $AUTN$ 中, 该 MAC 和该 $MAC1$ 存在于网络侧认证令牌 $AUTN$ 中时, $AUTN = SQN \text{ xor}(\text{异或}) AK \parallel AMF \parallel MAC \parallel MAC1$ 。该 $MAC1$ 也可能不存储在该 $AUTN$ 中。

步骤 S4307: 该 UE 接收该认证请求消息, 然后通过认证与密钥协商协议 (英文: Authentication and Key Agreement, 简称: AKA) 的密钥推演算法对该认证请求消息中的信息进行计算, 得到用户侧认证令牌 $AUTN_{UE}$ 和响应 (英文: Response, 简称: RES) 等信息, 该用户侧认证令牌中的消息认证码可以称为用户侧初始消息认证码, 该用户侧认证令牌中的响应可以称为初始响应。

步骤 S4308: 该 UE 同样通过上述预设的第一消息认证码算法对该 $RAND$ 、该第二共享密钥 K_{ser} 和 MAC 进行计算得到用户侧附加消息认证码 $MAC1'$, 然后判断网络侧附加消息认证码 $MAC1$ 是否与该用户侧附加消息认证码 $MAC1'$ 相同, 以及用户侧初始消息认证码与网络侧初始消息认证码是否相同; 若均相同则该 UE 对该 $CP-AU$ 的认证通过。需要说明的是, 该 UE 预先基于自身已有的 $UEID$ 和业务标识计算出了该第二共享密钥 K_{ser} 。由于认证的过程中使用到的信息与业务相关且与网络相关, 因此可以看作该 UE 对该网络和目标业务的认证通过。可以理解的是, 当生成该网络侧附加消息认证码时, 该 UE 需要先判断该网络侧初始消息认证码与该用户侧初始消息认证码是否相同, 若相同再判断该网络侧附加消息认证码与该用户侧附加消息认证码是否相同。

步骤 S4309: 若该 UE 对该 $CP-AU$ 的认证通过, 则该 UE 通过预设的第二消息认证码算法对该 K_{ser} 和 $RAND$ 进行计算得到用户侧响应消息认证码 $MAC2$, 例如, $MAC2 = MAC(K_{ser}, (RES, (nonce1, nonce2, SQN, NAS \text{ COUNT}, UE \text{ ID 的至少一项})))$, 即计算该 $MAC2$ 需要考虑 K_{ser} 和 $RAND$, 除此之外还可能考虑 RES 、 $nonce1$ 、 $nonce2$ 、 SQN 、 $NAS \text{ COUNT}$ 、 $UE \text{ ID}$ 等参数; 然后, 该 UE 将该初始响应 RES 和该用户侧响应消息认证码 $MAC2$ 发送给该 $CP-AU$ 。若 $MAC2$ 的生成包括 UE 选择的新鲜参数 $nonce2$, 则 $nonce2$ 可以由该 UE 发送给该 $CP-AU$ 。

步骤 S4310: 该 $CP-AU$ 接收该 RES 和该 $MAC2$, 然后同样通过该预设的第二消息认证码算法对该 K_{ser} 进行计算得到网络侧响应消息认证码 $MAC2'$ 。

步骤 S4311: 该 $CP-AU$ 判断初始期待响应 $XRES$ 是否与该 UE 发送的初始响应 RES 相同, 且该网络侧响应消息认证码 $MAC2'$ 是否与该用户侧响应消息认证码 $MAC2$ 相同; 若均相同则该 $CP-AU$ 对该 UE 的认证通过, 即该网络对该 UE 的认证通过, 可选的, 若至少有一项不同, 则该 $CP-AU$ 对 UE 的认证未通过, 这时, 该 $CP-AU$ 可以向该 UE 发送认证拒绝消息, 该认证拒绝消息用于对应的表明网络或者业务对 UE 的认证不成功。可以理解的

是，当计算该用户侧响应消息认证码用到了初始响应 RES 时，该 CP-AU 需要先判断该初始响应 RES 与该初始期待响应是否相同，若相同再判断该网络侧响应消息认证码与该用户侧响应消息认证码是否相同。

步骤 S4312：当该 UE 对该 CP-AU 的认证通过，以及该 CP-AU 对该 UE 的认证通过后，该 UE 和该 CP-AU 通过相同的密钥生成算法对该 K_{ASME} 和 K_{ser} 进行计算生成密钥，生成的密钥即为该 UE 与该 CP-AU 之间双向认证生成的目标共享密钥。该 UE 和 CP-AU 使用的哪种密钥生成算法此处暂不作限定。可以理解的是，该 UE 可以通过 K_{NG} 的索引 KSI_{NG} 获取到该 K_{NG} 。另外，UE 可以在通过了对 CP-AU 的认证后就生成该目标共享密钥，而 CP-AU 可以在通过该 UE 的认证后再生成该目标共享密钥。

请参见图 33，图 33 是本发明实施例提供的又一种网络认证方法的流程示意图，该流程是步骤 S4301~S4312 的一种可能的表现形式，在该可能的表现形式中，UE 与 CP-AU 的之间的交互的信息可以经过 RAN，该 CP-AU 可以进一步划分为更小的多个网元，由以上描述可知，该 CP-AU 承担的功能包括向签约服务器获取认证向量、根据签约服务器反馈的认证向量生成 MAC1、向 UE 反馈认证请求消息、生成 MAC2'、验证 MAC2 和 MAC2' 等操作，这些操作可以由该 CP-AU 中划分的多个网元来分别承担，例如，该 CP-AU 可以划分为 SEAF、AUSF 等，其中，向签约服务器获取认证向量、根据签约服务器反馈的认证向量生成 MAC1 由 AUSF 承担，向 UE 反馈认证请求消息、生成 MAC2'、验证 MAC2' 和 MAC2 由 SEAF 承担，SEAF 和 AUSF 在承担各自的操作的过程中，SEAF 和 AUSF 之间还可能需要进行一些协商；另外，该签约服务器可以为 ARPF。

需要说明的是，以上各个实施例中列出的步骤的先后顺序此处不做限制，有些步骤先执行还是后执行对实施例的实施不会产生实质的影响，因此在以上列出的步骤的先后顺序的基础上，对步骤执行的先后顺序进行调整所形成的方案依然落入本发明的保护范围。

综上所述，通过实施本发明实施例，用户设备与业务认证设备根据获取的参考参数以及预先共享的第一共享密钥生成第二共享密钥，然后该业务认证设备将该第二共享密钥发送给该网络认证设备，使得该网络认证设备基于该第二共享密钥得到目标共享密钥。也即是说，生成该目标共享密钥考虑到了业务的相关信息以及网络的相关信息，提升了该目标共享密钥的安全级别。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，可通过计算机程序来指令相关的硬件来完成，该的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可存储程序代码的介质。

权利要求

1、一种网络认证系统，其特征在于，所述系统包括用户设备、网络认证设备和业务认证设备，其中：

所述业务认证设备用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥，所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥，所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息；

所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥；

所述业务认证设备用于将所述第二共享密钥发送给所述网络认证设备；

所述网络认证设备用于接收所述第二共享密钥，所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

2、根据权利要求1所述的系统，其特征在于：

所述网络认证设备和所述用户设备用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

3、根据权利要求2所述的系统，其特征在于：

所述网络认证设备和所述用户设备用于进行网络认证生成第三共享密钥；

所述网络认证设备和所述用户设备用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

所述网络认证设备和所述用户设备用于根据所述第二共享密钥进行网络认证生成第四共享密钥；

所述网络认证设备和所述用户设备均用于根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

4、根据权利要求1所述的系统，其特征在于，所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥；

所述网络认证设备和所述用户设备用于将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

5、根据权利要求2~4任一项所述的系统，其特征在于：

所述网络认证设备还用于将所述目标共享密钥发送给所述业务认证设备；

所述业务认证设备用于接收所述目标共享密钥；

所述业务认证设备和所述用户设备用于将所述目标共享密钥或者基于所述目标共享密

钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

6、根据权利要求 1 所述的系统，其特征在于：

所述网络认证设备和所述用户设备用于进行网络认证生成第三共享密钥；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥；

所述网络认证设备和所述用户设备均用于根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

7、根据权利要求 1 所述系统，其特征在于：

所述网络认证设备和所述用户设备均用于根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

8、根据权利要求 1 所述的系统，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数；所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

根据所述参考信息和所述第一共享密钥进行业务认证生成第二共享密钥；

所述业务认证设备还用于将所述第二共享密钥作为所述目标共享密钥。

9、根据权利要求 1 所述的系统，其特征在于，所述业务认证设备用于获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述参考信息、第一共享密钥和所述第五共享密钥进行业务认证生成第二共享密钥；

所述网络认证设备用于将所述第二共享密钥作为所述目标共享密钥。

10、根据权利要求 1 所述的系统，其特征在于：

所述网络认证设备用于向所述业务认证设备获取所述第一共享密钥；

所述网络认证设备用于根据所述第一共享密钥和第五共享密钥生成网络侧信息，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述网络认证设备用于将所述网络侧信息发送给所述业务认证设备；

所述业务认证设备用于接收并向所述用户设备转发所述网络侧信息；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包

括所述网络侧信息;

所述网络认证设备用于将所述第二共享密钥作为所述目标共享密钥。

11、根据权利要求 1~10 任一项所述的系统，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

12、根据权利要求 11 所述的系统，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

13、根据权利要求 2 所述的系统，其特征在于，所述网络认证设备包括认证功能单元 CP-AU，所述网络认证设备和所述用户设备 UE 用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

UE 向 CP-AU 发送请求接入网络的消息，所述请求接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识，所述目标业务为所述 UE 当前执行的业务；

所述 CP-AU 接收所述请求接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；

所述 CP-AU 接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；

所述 CP-AU 将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码，并向所述 UE 发送认证请求消息，所述认证请求消息包含所述业务参考消息认证码；

所述 CP-AU 将通过预设的响应算法对所述第二共享密钥和所述初始期待响应进行计算得到的参考期待响应；

所述 UE 接收所述 CP-AU 发送的所述认证请求消息；

所述 UE 通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码，所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取，或者所述 UE 预先存储了所述第二共享密钥；

所述 UE 判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同；

若相同，则所述 UE 通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应；

所述 UE 将所述参考响应发送给所述 CP-AU；

所述 CP-AU 接收所述参考响应；

所述 CP-AU 判断所述参考期待响应与所述参考响应是否相同；

若相同，则所述 CP-AU 和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

14、根据权利要求 2 所述的系统，其特征在于，所述网络认证设备包括认证功能单元 CP-AU，所述网络认证设备和所述用户设备 UE 用于根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

UE 向 CP-AU 发送接入网络的消息，所述接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识，所述目标业务为所述 UE 当前执行的业务；

所述 CP-AU 接收所述接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；

所述 CP-AU 接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；

所述 CP-AU 将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码，并向 UE 发送认证请求消息，所述认证请求消息包括所述网络侧附加消息认证码和所述网络侧初始消息认证码；

所述 UE 接收所述 CP-AU 发送的所述认证请求消息；

所述 UE 通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码，所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取，或者所述 UE 预先存储了所述第二共享密钥；

所述 UE 判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同，且所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同；

若均相同，则所述 UE 通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码；

所述 UE 将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU；

所述 CP-AU 接收所述参考响应和所述用户侧响应消息认证码；

所述 CP-AU 通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码；

所述 CP-AU 判断所述初始期待响应是否与所述初始响应相同，且所述网络侧响应消息认证码是否与所述用户侧响应消息认证码相同；

若均相同，则所述 CP-AU 和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

15、一种网络认证系统，其特征在于，所述系统包括用户设备、网络认证设备和业务认证设备，其中：

所述业务认证设备用于将预存的目标业务的业务参数发送给所述网络认证设备和所述用户设备；

所述网络认证设备和所述用户设备用于接收所述业务参数；

所述网络认证设备和所述用户设备均用于结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

16、根据权利要求 15 所述的系统，其特征在于，所述网络认证设备和所述用户设备均用于结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

所述网络认证设备和所述用户设备均用于根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

所述网络认证设备和所述用户设备均用于根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

17、根据权利要求 15 或 16 所述的系统，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

18、一种网络认证设备，其特征在于，包括：

接收单元，用于接收业务认证设备发送的第二共享密钥，业务认证设备和用户设备均用于结合第一共享密钥和参考信息生成所述第二共享密钥，所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥，所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息；

第一生成单元，用于根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

19、根据权利要求 18 所述的网络认证设备，其特征在于，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

20、根据权利要求 19 所述的网络认证设备，其特征在于，还包括：

认证单元，用于和所述用户设备进行网络认证生成第三共享密钥；

所述认证单元和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

和所述用户设备均根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

21、根据权利要求 18 所述的网络认证设备，其特征在于，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为目标共享密钥。

22、根据权利要求 18 所述的网络认证设备，其特征在于，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备进行网络认证生成第三共享密钥；

和所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

23、根据权利要求 18 所述网络认证设备，其特征在于，所述第一生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

24、根据权利要求 18~23 任一项所述的网络认证设备，其特征在于，还包括：

获取单元，用于向所述业务认证设备获取所述第一共享密钥；

第二生成单元，用于根据所述第一共享密钥和第五共享密钥生成网络侧信息，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述网络认证设备将所述网络侧信息发送给所述业务认证设备，以使所述业务认证设备向所述用户设备转发所述网络侧信息，所述网络参数属于所述参考信息。

25、根据权利要求 18~23 任一项所述的网络认证设备，其特征在于，还包括：

发送单元，用于将所述目标共享密钥发送给所述业务认证设备，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥用作所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

26、根据权利要求 18~25 任一项所述的网络认证设备，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

27、根据权利要求 26 所述的网络认证设备，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

28、根据权利要求 19 所述的网络认证设备，其特征在于，所述网络认证设备包括 CP-AU；所述第一生成单元和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

接收所述 UE 发送的请求接入网络的消息并根据身份标识和业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；所述请求接入网络的消息包含所述 UE 的所述身份标识和目标业务的所述业务标识，所述目标业务为所述 UE 当前执行的业务；

接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；

将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码，并向所述 UE 发送认证请求消息，所述认证请求消息包含所述业务参考消息认证码；所述 UE 用于接收所述认证请求消息并通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码，所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取，或者所述 UE 预先存储了所述第二共享密钥；

所述 UE 还用于判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同；所述 UE 用于在判断出相同时，通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应；所述 UE 还用于将所述参考响应发送给所述 CP-AU；

通过所述预设的响应算法对所述第二共享密钥和所述初始期待响应进行处理得到参考期待响应；

接收所述参考响应；

判断所述参考期待响应与所述参考响应是否相同；

若相同，则和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

29、根据权利要求 19 所述的网络认证设备，其特征在于，所述网络认证设备包括 CP-AU；所述第一生成单元和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，具体为：

接收 UE 发送的接入网络的消息并根据身份标识和业务标识获取第二共享密钥, 以及向签约服务器请求基于预置密钥生成的认证向量, 所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥; 所述接入网络的消息包含所述 UE 的所述身份标识和目标业务的所述业务标识, 所述目标业务为所述 UE 当前执行的业务;

接收所述签约服务器发送的所述认证向量, 所述认证向量包含消息认证码和期待响应, 所述认证向量包含的所述消息认证码为网络侧初始消息认证码, 所述认证向量包含的期待响应为初始期待响应;

将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码, 并向 UE 发送认证请求消息, 所述认证请求消息包括所述网络侧附加消息认证码和所述网络侧初始消息认证码发送给所述 UE; 所述 UE 用于接收所述认证请求消息; 所述 UE 用于通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应, 生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应, 并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码, 所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取, 或者所述 UE 预先存储了所述第二共享密钥; 所述 UE 用于判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同, 且判断所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同; 若均相同, 则所述 UE 用于通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码; 所述 UE 还用于将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU;

接收所述参考响应和所述用户侧响应消息认证码;

通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码;

判断所述初始期待响应是否与所述初始响应相同, 且所述网络侧响应消息认证码是否与所述用户侧响应消息认证码相同;

若均相同, 则和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

30、一种用户设备, 其特征在于, 包括:

获取单元, 用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥; 所述第一共享密钥为所述用户设备与业务认证设备之间预先配置的共享密钥, 所述业务认证设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥, 所述业务认证设备还用于将所述第二共享密钥发送给网络认证设备;

生成单元, 用于根据所述第二共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

31、根据权利要求 30 所述用户设备, 其特征在于, 所述获取单元根据所述第二共享密钥生成目标共享密钥, 具体为:

将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

32、根据权利要求 30 所述的用户设备，其特征在于，所述获取单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥。

33、根据权利要求 32 所述的用户设备，其特征在于，还包括：

认证单元，用于和所述网络认证设备进行网络认证生成第三共享密钥；

所述获取单元和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥，具体为：

和所述网络认证设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

34、根据权利要求 30 所述的用户设备，其特征在于，所述生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

和所述网络认证设备进行网络认证生成第三共享密钥；

根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

35、根据权利要求 30 所述的用户设备，其特征在于，所述生成单元根据所述第二共享密钥生成目标共享密钥，具体为：

根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的共享密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

36、根据权利要求 30 所述的用户设备，其特征在于，所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述参考信息、第一共享密钥和第五共享密钥与所述业务认证设备进行业务认证生成第二共享密钥；所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述第五共享密钥。

37、根据权利要求 30~36 任一项所述的用户设备，其特征在于，所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

和业务认证设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

38、根据权利要求 30~36 任一项所述的用户设备，其特征在于，还包括：

第一接收单元，用于接收所述业务认证设备转发的来自所述网络认证设备的网络侧信息，所述网络侧信息为所述网络认证设备根据第五共享密钥和获取的所述第一共享密钥生成，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥与所述业务认证设备进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

39、根据权利要求 30~38 任一项所述的用户设备，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

40、根据权利要求 39 所述的用户设备，其特征在于，当所述参考信息包含所述业务参数时，还包括：

第二接收单元，用于接收所述网络认证设备转发的来自所述业务认证设备的所述业务参数。

41、根据权利要求 39 或 40 所述的用户设备，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

42、根据权利要求 32 所述的用户设备，其特征在于，所述网络认证设备包括 CP-AU；所述获取单元和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥，具体为：

向 CP-AU 发送请求接入网络的消息，所述请求接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识，所述目标业务为所述 UE 当前执行的业务；所述 CP-AU 用于接收所述请求接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；所述 CP-AU 还用于接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；所述 CP-AU 还用于将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码，并向所述 UE 发送认证请求消息，所述认证请求消息包括所述业务参考消息；所述 CP-AU 还用于通过所述预设的响应算法对所述第二共享密钥和所述初始期待响应进行处理得到参考期待响应；

接收所述认证请求消息；

通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的

消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同;

若相同,则通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应;

将所述参考响应发送给所述 CP-AU,所述 CP-AU 用于接收所述参考响应并判断所述参考期待响应与所述参考响应是否相同;

在所述 CP-AU 的判断结果为是时,与所述 CP-AU 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

43、根据权利要求 32 所述的用户设备,其特征在于,所述网络认证设备包括 CP-AU;所述获取单元和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥,具体为:

向 CP-AU 发送接入网络的消息,所述接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识,所述目标业务为所述 UE 当前执行的业务;所述 CP-AU 用于接收所述接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥,以及向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;所述 CP-AU 还用于接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应;所述 CP-AU 还用于将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包含所述网络侧附加消息认证码和所述网络侧初始消息认证码;

接收所述 CP-AU 发送的所述认证请求消息;

通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同,且所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同;

若均相同,则通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码;

将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU;所述 CP-AU 用于接收所述参考响应和所述用户侧响应消息认证码;所述 CP-AU 还用于通过所述预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码;所述 CP-AU 还用于判断所述初始期待响应是否与所述初始响应相同,且所述网络侧响应消息

认证码是否与所述用户侧响应消息认证码相同;

在所述 CP-AU 的判断结果为均相同时, 和所述 CP-AU 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

44、一种业务认证设备, 其特征在于, 包括:

第一获取单元, 用于获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥, 所述第一共享密钥为用户设备与所述业务认证设备之间预先配置的共享密钥, 所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥, 所述参考信息包括所述用户设备、网络认证设备和所述业务认证设备中至少一项预先关联的信息;

发送单元, 用于将所述第二共享密钥发送给所述网络认证设备, 所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

45、根据权利要求 44 所述的业务认证设备, 其特征在于, 所述第一获取单元结合所述参考信息和第一共享密钥生成第二共享密钥, 具体为:

和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

46、根据权利要求 44 或 45 所述的业务认证设备, 其特征在于, 还包括:

第一接收单元, 用于接收所述网络认证设备发送的所述目标共享密钥;

生成单元, 用于将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

47、根据权利要求 44 或 45 所述的业务认证设备, 其特征在于, 还包括:

生成单元, 用于将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

48、根据权利要求 44 所述的业务认证设备, 其特征在于, 还包括:

第二获取单元, 用于获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥;

所述第一获取单元结合所述参考信息和第一共享密钥生成第二共享密钥, 具体为:

结合所述参考信息、第一共享密钥和所述第五共享密钥进行网络认证生成第二共享密钥。

49、根据权利要求 44 所述的业务认证设备, 其特征在于, 还包括:

第二接收单元, 用于接收所述网络认证设备根据所述网络认证设备所在蜂窝网的网络参数生成的网络侧信息, 并向所述用户设备转发所述网络侧信息;

所述第一获取单元结合所述参考信息和第一共享密钥生成第二共享密钥，具体为：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

50、根据权利要求 44~49 任一项所述的业务认证设备，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

51、根据权利要求 50 所述的业务认证设备，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

52、一种网络认证设备，其特征在于，包括：

接收单元，用于接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给用户设备；

生成单元，用于和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

53、根据权利要求 52 所述的网络认证设备，其特征在于，所述生成单元和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述用户设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述用户设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

54、根据权利要求 52 或 53 所述的网络认证设备，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

55、一种用户设备，其特征在于，包括：

接收单元，用于接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给网络认证设备；

生成单元，用于和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备

与所述网络认证设备之间预先配置的共享密钥。

56、根据权利要 55 所述的用户设备，其特征在于，所述生成单元和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，具体为：

和所述网络认证设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

和所述网络认证设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

57、根据权利要求 55 或 56 所述的用户设备，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

58、一种业务认证设备，其特征在于，包括：

发送单元，用于将预存的目标业务的业务参数发送给网络认证设备和用户设备；以使所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

59、根据权利要求 58 所述的业务认证设备，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

60、一种网络认证方法，其特征在于，包括：

网络认证设备接收业务认证设备发送的第二共享密钥，业务认证设备和用户设备均用于结合第一共享密钥和参考信息生成所述第二共享密钥，所述第一共享密钥为所述用户设备与所述业务认证设备之间预先配置的共享密钥，所述参考信息包括所述用户设备、所述网络认证设备和所述业务认证设备中至少一项预先关联的信息；

所述网络认证设备根据所述第二共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

61、根据权利要求 60 所述的方法，其特征在于，所述网络认证设备根据所述第二共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥。

62、根据权利要求 61 所述的方法，其特征在于，所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥之前，所述方法还包括：

所述网络认证设备和所述用户设备进行网络认证生成第三共享密钥；

所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述第二共享密钥进行网络认证生成第四共享密钥；

所述网络认证设备和所述用户设备均根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

63、根据权利要求 60 所述的方法，其特征在于，所述网络认证设备根据所述第二共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为目标共享密钥。

64、根据权利要求 60 所述的方法，其特征在于，所述网络认证设备根据所述第二共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备进行网络认证生成第三共享密钥；

所述网络认证设备和所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

65、根据权利要求 60 所述方法，其特征在于，所述网络认证设备根据所述第二共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥；或者将所述第二共享密钥和基于所述第五共享密钥衍生的密钥分别作为保护不同类型数据的所述目标共享密钥，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

66、根据权利要求 60~65 任一项所述的方法，其特征在于，所述方法还包括：

所述网络认证设备向所述业务认证设备获取所述第一共享密钥；

所述网络认证设备根据所述第一共享密钥和第五共享密钥生成网络侧信息，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述网络认证设备将所述网络侧信息发送给所述业务认证设备，以使所述业务认证设备向所述用户设备转发所述网络侧信息，所述网络参数属于所述参考信息。

67、根据权利要求 60~65 任一项所述的方法，其特征在于，所述网络认证设备根据所

述第二共享密钥生成目标共享密钥之前,所述方法还包括:

所述网络认证设备将所述目标共享密钥发送给所述业务认证设备,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥用作所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

68、根据权利要求 60~67 任一项所述的方法,其特征在于,所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

69、根据权利要求 68 所述的方法,其特征在于,所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项;所述网络参数包括运营商标识,接入网络标识,服务网络标识,网络类型标识,局域网网络标识,切片标识,承载标识,服务质量标识和流标识中的至少一项。

70、根据权利要求 61 所述的网络认证方法,其特征在于,所述网络认证设备包括 CP-AU;所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥,包括:

接收所述 UE 发送的请求接入网络的消息并根据身份标识和业务标识获取第二共享密钥,以及向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;所述请求接入网络的消息包含所述 UE 的所述身份标识和目标业务的所述业务标识,所述目标业务为所述 UE 当前执行的业务;

接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应;

将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包含所述业务参考消息认证码;所述 UE 用于接收所述认证请求消息并通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

所述 UE 还用于判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同;所述 UE 用于在判断出相同时,通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应;所述 UE 还用于将所述参考响应发送给所述 CP-AU;

通过所述预设的响应算法对所述第二共享密钥和所述初始期待响应进行处理得到参考期待响应;

接收所述参考响应;

判断所述参考期待响应与所述参考响应是否相同；

若相同，则和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

71、根据权利要求 61 所述的网络认证方法，其特征在于，所述网络认证设备包括 CP-AU；所述网络认证设备和所述用户设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成所述目标共享密钥，包括：

接收 UE 发送的接入网络的消息并根据身份标识和业务标识获取第二共享密钥，以及向签约服务器请求基于预置密钥生成的认证向量，所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥；所述接入网络的消息包含所述 UE 的所述身份标识和目标业务的所述业务标识，所述目标业务为所述 UE 当前执行的业务；

接收所述签约服务器发送的所述认证向量，所述认证向量包含消息认证码和期待响应，所述认证向量包含的所述消息认证码为网络侧初始消息认证码，所述认证向量包含的期待响应为初始期待响应；

将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码，并向 UE 发送认证请求消息，所述认证请求消息包括所述网络侧附加消息认证码和所述网络侧初始消息认证码发送给所述 UE；所述 UE 用于接收所述认证请求消息；所述 UE 用于通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应，生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应，并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码，所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取，或者所述 UE 预先存储了所述第二共享密钥；所述 UE 用于判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同，且判断所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同；若均相同，则所述 UE 用于通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码；所述 UE 还用于将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU；

接收所述参考响应和所述用户侧响应消息认证码；

通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码；

判断所述初始期待响应是否与所述初始响应相同，且所述网络侧响应消息认证码是否与所述用户侧响应消息认证码相同；

若均相同，则和所述 UE 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

72、一种网络认证方法，其特征在于，包括：

用户设备获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥；所述第一共享密钥为所述用户设备与业务认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥，

所述业务认证设备还用于将所述第二共享密钥发送给网络认证设备;

所述用户设备根据所述第二共享密钥生成目标共享密钥, 所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

73、根据权利要求 72 所述方法, 其特征在于, 所述用户设备根据所述第二共享密钥生成目标共享密钥, 包括:

所述用户设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述目标共享密钥。

74、根据权利要求 72 所述的方法, 其特征在于, 所述用户设备根据所述第二共享密钥生成目标共享密钥, 包括:

所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥。

75、根据权利要求 74 所述的方法, 其特征在于, 所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥之前, 所述方法还包括:

所述用户设备和所述网络认证设备进行网络认证生成第三共享密钥;

所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥, 包括:

所述用户设备和所述网络认证设备根据所述第二共享密钥进行网络认证生成第四共享密钥;

所述用户设备根据所述第三共享密钥和所述第四共享密钥生成所述目标共享密钥。

76、根据权利要求 72 所述的方法, 其特征在于, 所述用户设备根据所述第二共享密钥生成目标共享密钥, 包括:

所述用户设备和所述网络认证设备进行网络认证生成第三共享密钥;

所述用户设备根据所述第二共享密钥和所述第三共享密钥生成所述目标共享密钥; 或者将所述第二共享密钥和所述第三共享密钥分别作为保护不同类型数据的所述目标共享密钥。

77、根据权利要求 72 所述的方法, 其特征在于, 所述用户设备根据所述第二共享密钥生成目标共享密钥, 包括:

所述用户设备根据所述第二共享密钥和第五共享密钥生成所述目标共享密钥; 或者将所述第二共享密钥和基于所述第五共享密钥衍生的共享密钥分别作为保护不同类型数据的所述目标共享密钥, 所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

78、根据权利要求 72 所述的方法，其特征在于，所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述参考信息、第一共享密钥和第五共享密钥与所述业务认证设备进行业务认证生成第二共享密钥；所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥，所述业务认证设备用于获取所述第五共享密钥。

79、根据权利要求 72~78 任一项所述的方法，其特征在于，所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

用户设备和业务认证设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

80、根据权利要求 72~78 任一项所述的方法，其特征在于，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述用户设备接收所述业务认证设备转发的来自所述网络认证设备的网络侧信息，所述网络侧信息为所述网络认证设备根据第五共享密钥和获取的所述第一共享密钥生成，所述第五共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述网络参数和第一共享密钥与所述业务认证设备进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

81、根据权利要求 72~80 任一项所述的方法，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

82、根据权利要求 81 所述的方法，其特征在于，当所述参考信息包含所述业务参数时，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述用户设备接收所述网络认证设备转发的来自所述业务认证设备的所述业务参数。

83、根据权利要求 81 或 82 所述的方法，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

84、根据权利要求 74 所述的网络认证方法，其特征在于，所述网络认证设备包括 CP-AU；所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥，包括：

向 CP-AU 发送请求接入网络的消息，所述请求接入网络的消息包含所述 UE 的身份标

识和目标业务的业务标识,所述目标业务为所述 UE 当前执行的业务;所述 CP-AU 用于接收所述请求接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥,以及向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;所述 CP-AU 还用于接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应;所述 CP-AU 还用于将通过预设的消息认证码算法对所述第二共享密钥和所述网络侧初始消息认证码进行计算得到业务参考消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包括所述业务参考消息;所述 CP-AU 还用于通过所述预设的响应算法对所述第二共享密钥和所述初始期待响应进行处理得到参考期待响应;

接收所述认证请求消息;

通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的消息认证码算法对所述第二共享密钥和所述用户侧初始消息认证码进行计算得到用户侧参考消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

判断所述用户侧参考消息认证码与所述业务参考消息认证码是否相同;

若相同,则通过预设的响应算法对所述第二共享密钥和所述初始响应进行处理得到参考响应;

将所述参考响应发送给所述 CP-AU,所述 CP-AU 用于接收所述参考响应并判断所述参考期待响应与所述参考响应是否相同;

在所述 CP-AU 的判断结果为是时,与所述 CP-AU 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

85、根据权利要求 74 所述的网络认证方法,其特征在于,所述网络认证设备包括 CP-AU;所述用户设备和所述网络认证设备根据所述第二共享密钥或者根据基于所述第二共享密钥衍生的共享密钥进行网络认证生成目标共享密钥,包括:

向 CP-AU 发送接入网络的消息,所述接入网络的消息包含所述 UE 的身份标识和目标业务的业务标识,所述目标业务为所述 UE 当前执行的业务;所述 CP-AU 用于接收所述接入网络的消息并根据所述身份标识和所述业务标识获取第二共享密钥,以及向签约服务器请求基于预置密钥生成的认证向量,所述预置密钥为所述 UE 与所述签约服务器预先共享的密钥;所述 CP-AU 还用于接收所述签约服务器发送的所述认证向量,所述认证向量包含消息认证码和期待响应,所述认证向量包含的所述消息认证码为网络侧初始消息认证码,所述认证向量包含的期待响应为初始期待响应;所述 CP-AU 还用于将通过预设的第一消息认证码算法对所述第二共享密钥进行计算得到网络侧附加消息认证码,并向所述 UE 发送认证请求消息,所述认证请求消息包含所述网络侧附加消息认证码和所述网络侧初始消息认证码;

接收所述 CP-AU 发送的所述认证请求消息;

通过认证与密钥协商协议 AKA 根据所述预置密钥生成消息认证码和响应,生成的所述消息认证码为用户侧初始消息认证码以及生成的所述响应为初始响应,并通过所述预设的第一消息认证码算法对所述第二共享密钥进行计算得到用户侧附加消息认证码,所述 UE 使用的第二共享密钥为所述 UE 根据自身的身份标识和所述业务标识获取,或者所述 UE 预先存储了所述第二共享密钥;

判断所述用户侧附加消息认证码是否与所述网络侧附加消息认证码相同,且所述用户侧初始消息认证码是否与所述网络侧初始消息认证码相同;

若均相同,则通过预设的第二消息认证码算法对自身的所述第二共享密钥进行处理得到用户侧响应消息认证码;

将所述参考响应和所述用户侧响应消息认证码发送给所述 CP-AU;所述 CP-AU 用于接收所述参考响应和所述用户侧响应消息认证码;所述 CP-AU 还用于通过所述预设的所述第二消息认证码算法对自身的所述第二共享密钥进行处理得到网络侧响应消息认证码;所述 CP-AU 还用于判断所述初始期待响应是否与所述初始响应相同,且所述网络侧响应消息认证码是否与所述用户侧响应消息认证码相同;

在所述 CP-AU 的判断结果为均相同时,和所述 CP-AU 使用相同的密钥生成算法对预设的基础密钥和所述第二共享密钥进行处理得到目标共享密钥。

86、一种网络认证方法,其特征在于,包括:

业务认证设备获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥,所述第一共享密钥为用户设备与所述业务认证设备之间预先配置的共享密钥,所述用户设备用于获取所述参考信息并结合所述参考信息和所述第一共享密钥生成所述第二共享密钥,所述参考信息包括所述用户设备、网络认证设备和所述业务认证设备中至少一项预先关联的信息;

所述业务认证设备将所述第二共享密钥发送给所述网络认证设备,所述第二共享密钥用于所述用户设备和所述网络认证设备生成目标共享密钥,所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

87、根据权利要求 86 所述的方法,其特征在于,所述结合所述参考信息和第一共享密钥生成第二共享密钥,包括:

所述业务认证设备和所述用户设备结合所述参考信息和第一共享密钥进行业务认证生成第二共享密钥。

88、根据权利要求 86 或 87 所述的方法,其特征在于,所述业务认证设备将所述第二共享密钥发送给所述网络认证设备之后,所述方法还包括:

所述业务认证设备接收所述网络认证设备发送的所述目标共享密钥;

所述业务认证设备将所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

89、根据权利要求 86 或 87 所述的方法，其特征在于，所述业务认证设备获取参考信息并结合所述参考信息和第一共享密钥生成第二共享密钥之后，所述方法还包括：

所述业务认证设备将所述第二共享密钥或者基于所述第二共享密钥衍生的共享密钥作为所述业务认证设备与所述用户设备协商的保护数据安全传输的共享密钥。

90、根据权利要求 86 所述的方法，其特征在于，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述业务认证设备获取所述用户设备与所述网络认证设备之间预先配置的第五共享密钥；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述参考信息、第一共享密钥和所述第五共享密钥进行网络认证生成第二共享密钥。

91、根据权利要求 86 所述的方法，其特征在于，所述结合所述参考信息和第一共享密钥生成第二共享密钥之前，所述方法还包括：

所述业务认证设备接收所述网络认证设备根据所述网络认证设备所在蜂窝网的网络参数生成的网络侧信息，并向所述用户设备转发所述网络侧信息；

所述结合所述参考信息和第一共享密钥生成第二共享密钥，包括：

结合所述网络参数和第一共享密钥进行业务认证生成第二共享密钥，所述网络参数包括所述网络侧信息。

92、根据权利要求 86~91 任一项所述的方法，其特征在于，所述参考信息包括所述网络认证设备所在蜂窝网的网络参数和目标业务的业务参数中至少一项。

93、根据权利要求 92 所述的方法，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项；所述网络参数包括运营商标识，接入网络标识，服务网络标识，网络类型标识，局域网网络标识，切片标识，承载标识，服务质量标识和流标识中的至少一项。

94、一种网络认证方法，其特征在于，包括：

网络认证设备接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给用户设备；

所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

95、根据权利要求 94 所述的方法，其特征在于，所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，包括：

所述网络认证设备和所述用户设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

所述网络认证设备和所述用户设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

96、根据权利要求 94 或 95 所述的方法，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

97、一种网络认证方法，其特征在于，包括：

用户设备接收业务认证设备发送的预存的目标业务的业务参数，所述业务认证设备还用于将所述业务参数发送给网络认证设备；

所述用户设备和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

98、根据权利要求 97 所述的方法，其特征在于，所述用户设备和所述网络认证设备结合所述业务参数和原始共享密钥生成目标共享密钥，包括：

所述用户设备和所述网络认证设备根据所述业务参数和原始共享密钥进行网络认证生成目标共享密钥；或者，

所述用户设备和所述网络认证设备根据所述业务参数和原始共享密钥生成认证共享密钥，并根据所述认证共享密钥进行网络认证生成目标共享密钥。

99、根据权利要求 97 或 98 所述的方法，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

100、一种网络认证方法，其特征在于，包括：

业务认证设备将预存的目标业务的业务参数发送给网络认证设备和用户设备；以使所述网络认证设备和所述用户设备结合所述业务参数和原始共享密钥生成目标共享密钥，所述目标共享密钥或者基于所述目标共享密钥衍生的共享密钥为所述网络认证设备与所述用户设备协商的保护数据安全传输的共享密钥，所述原始共享密钥为所述用户设备与所述网络认证设备之间预先配置的共享密钥。

101、根据权利要求 100 所述的方法，其特征在于，所述业务参数包括所述目标业务的业务序列号、密钥管理中心的标识、会话标识、链路标识、应用标识、业务标识、业务等级、业务数据速率、时延和业务服务器标识中的至少一项。

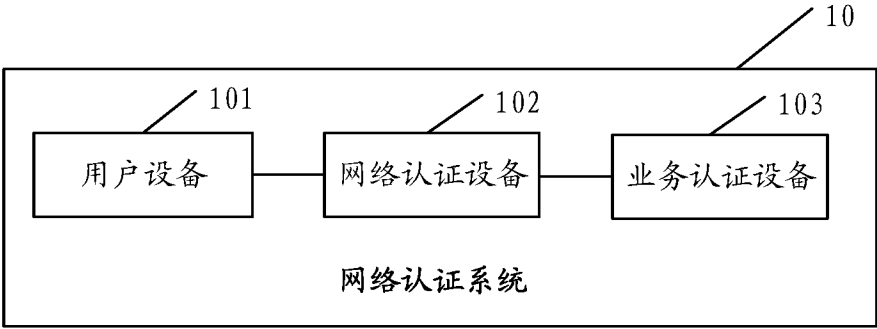


图 1

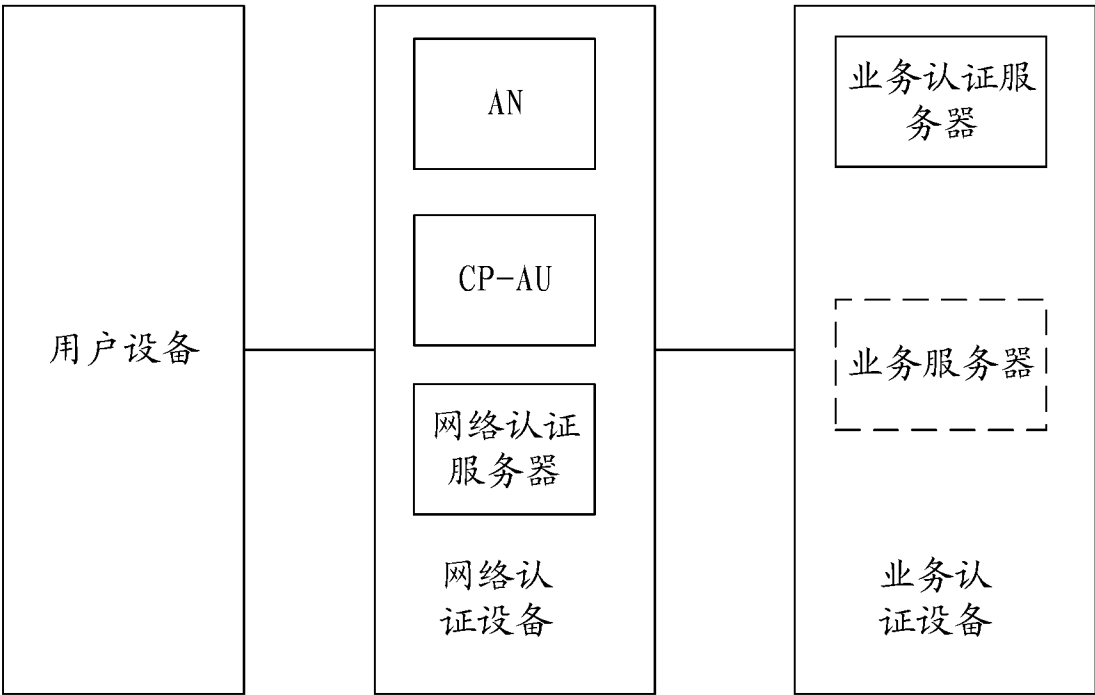


图 2

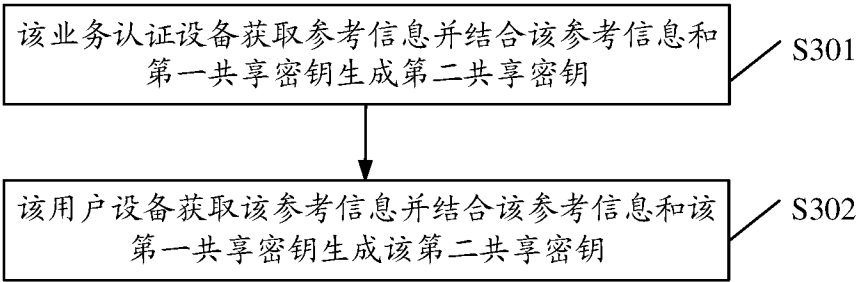


图 3A

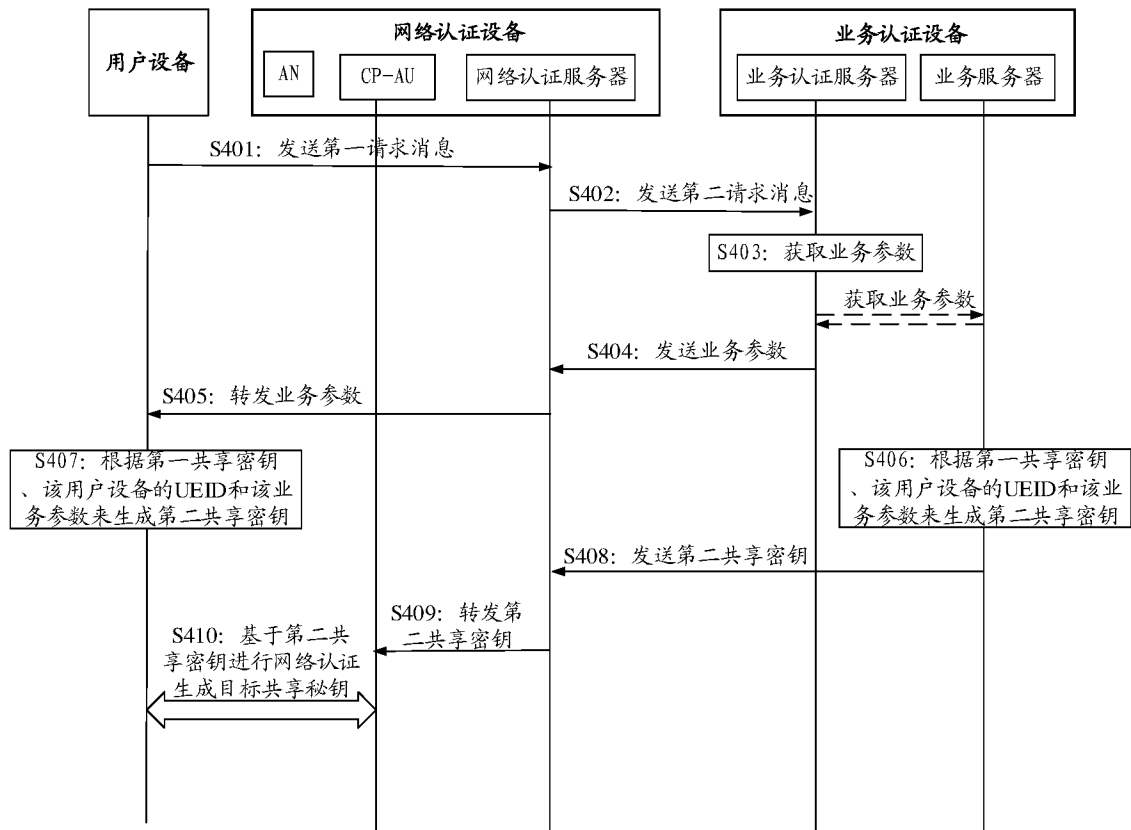


图 3B

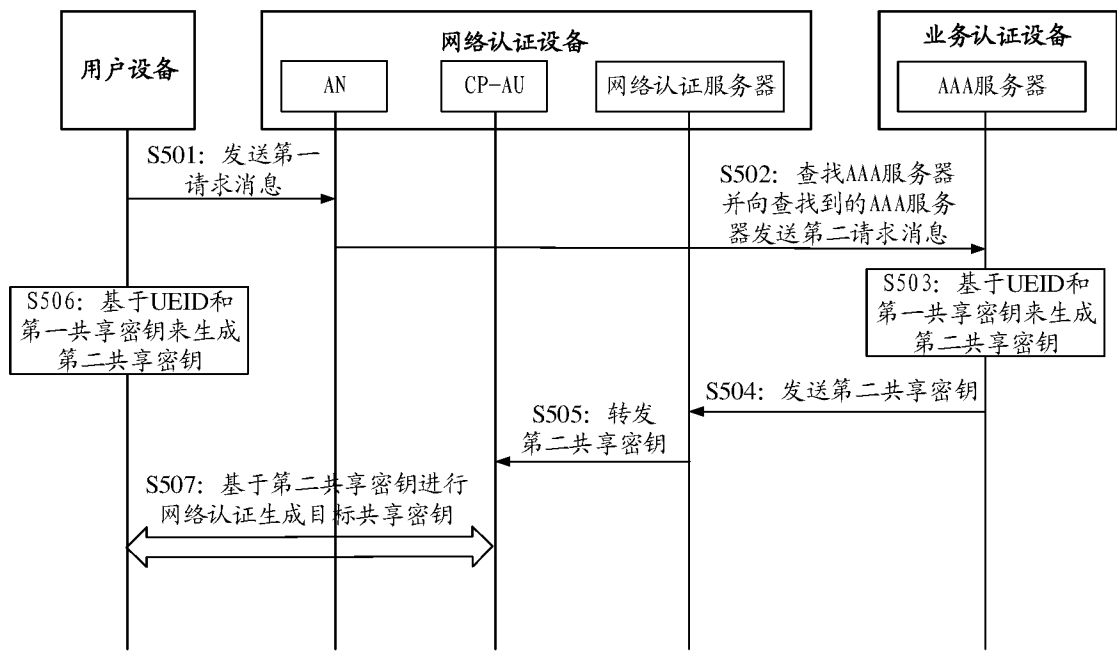


图 3C

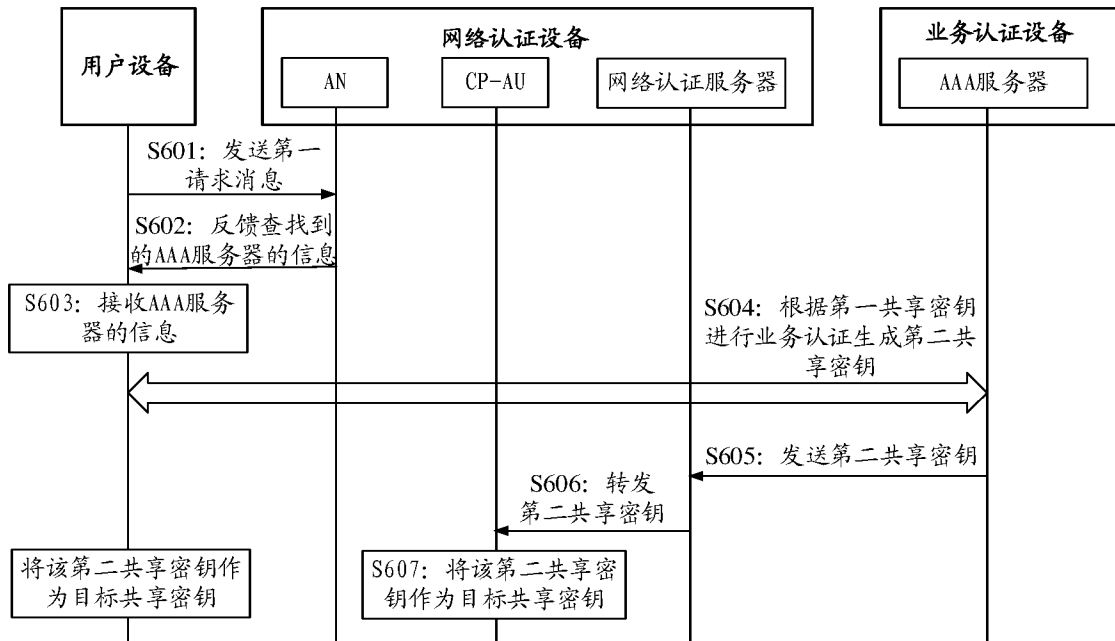


图 3D

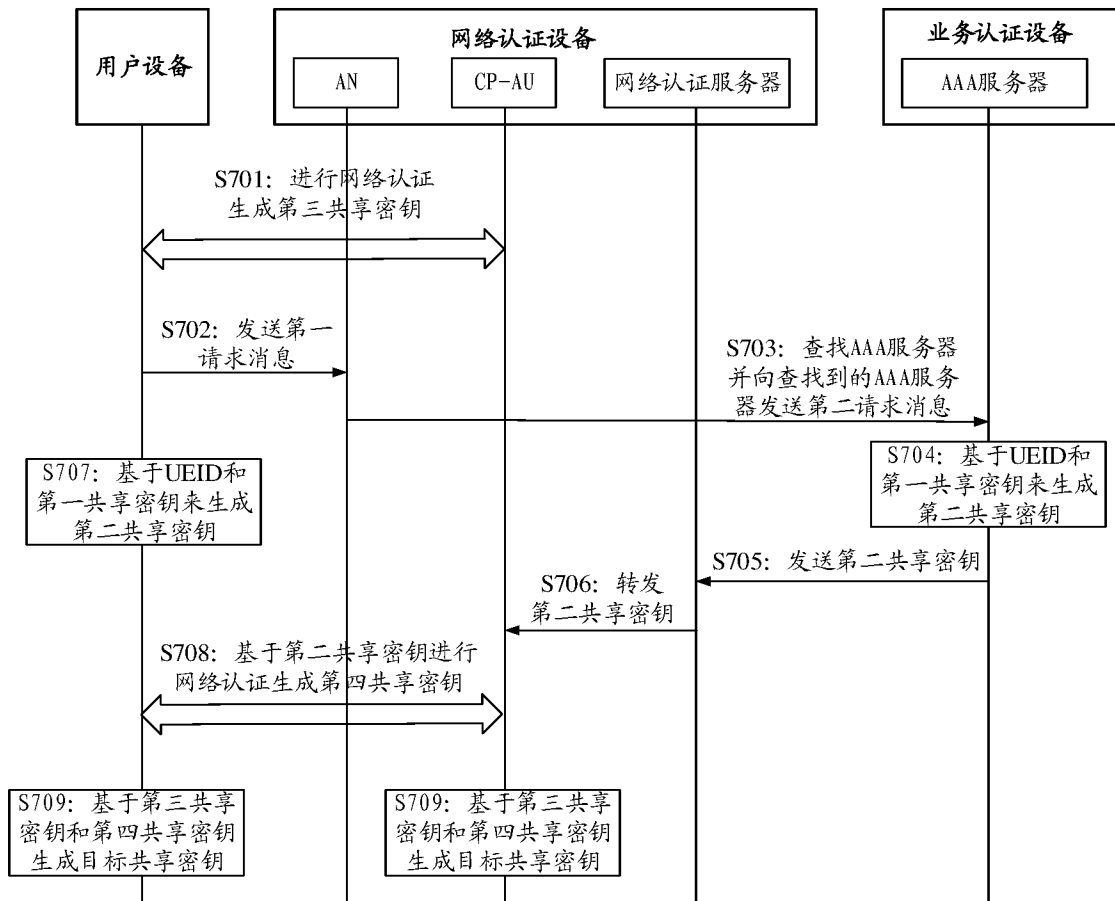


图 3E

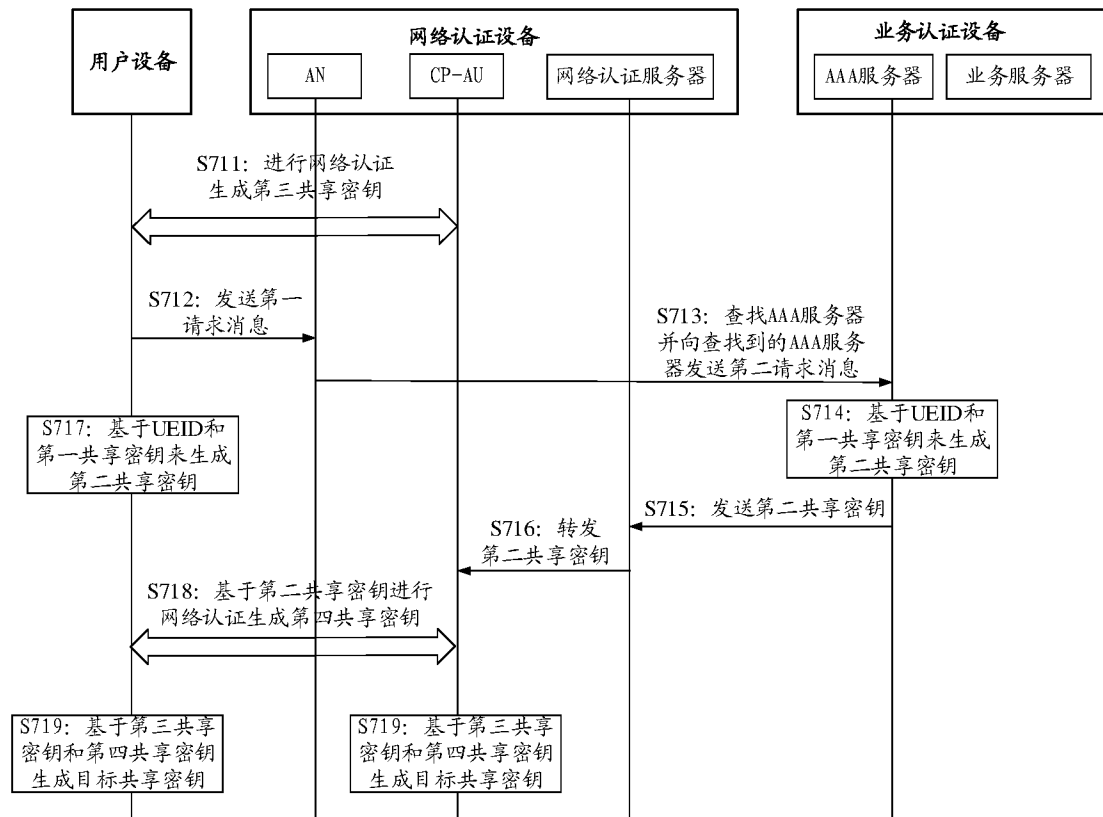


图 3F

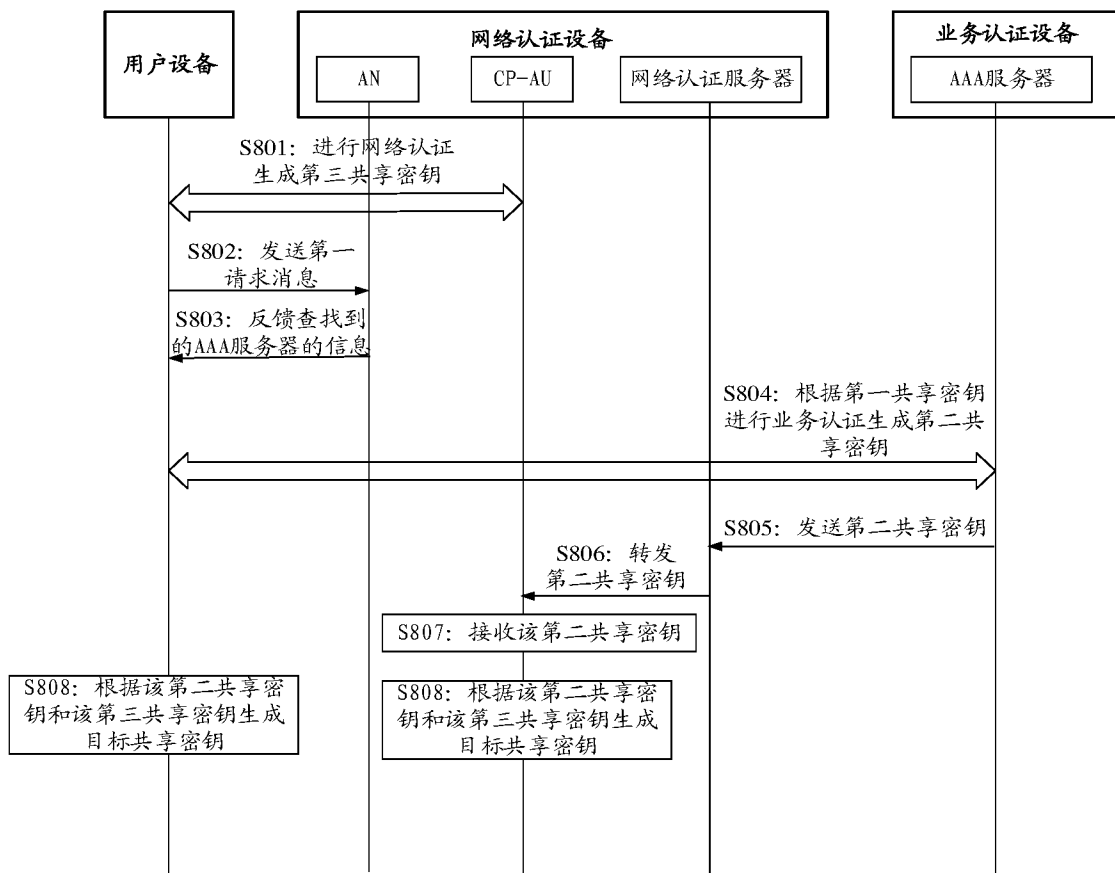


图 3G

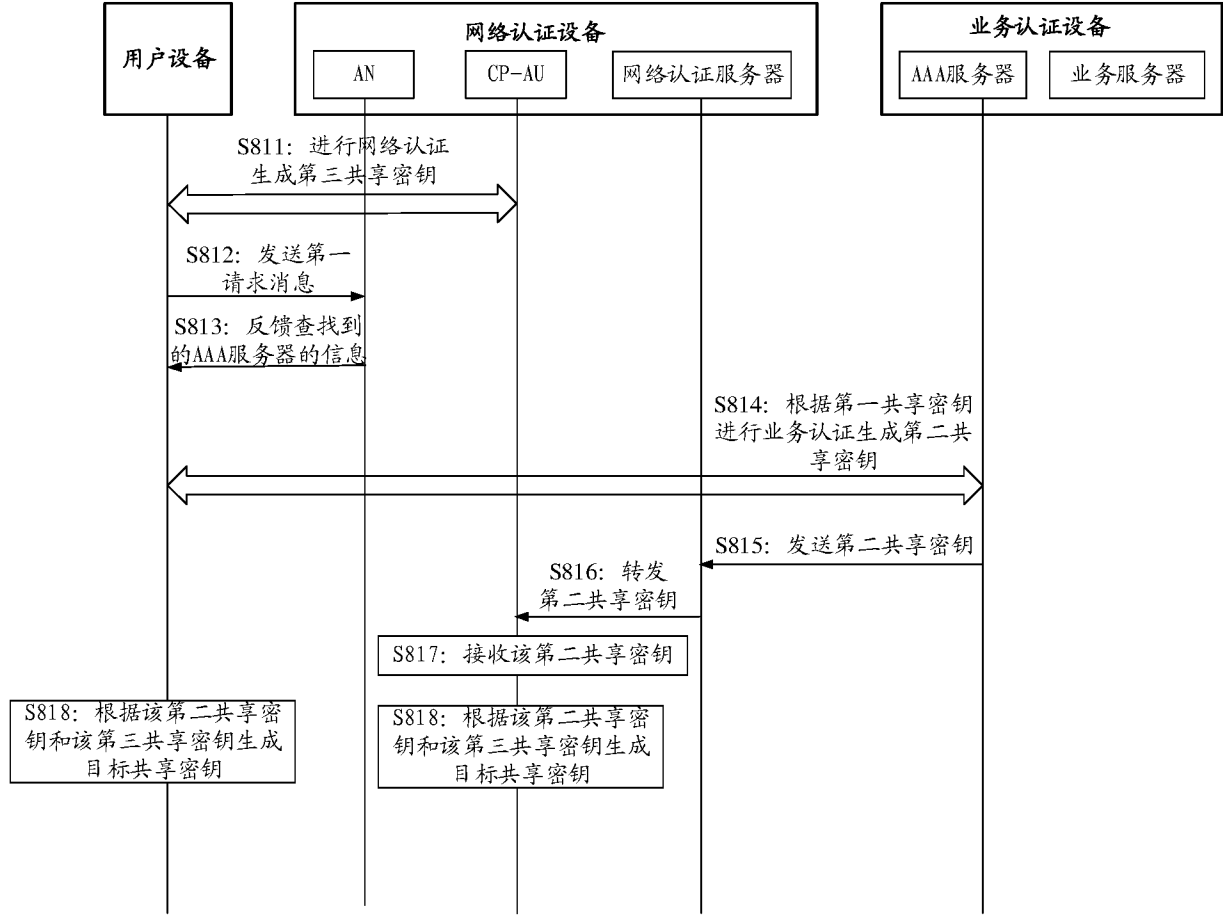


图 3H

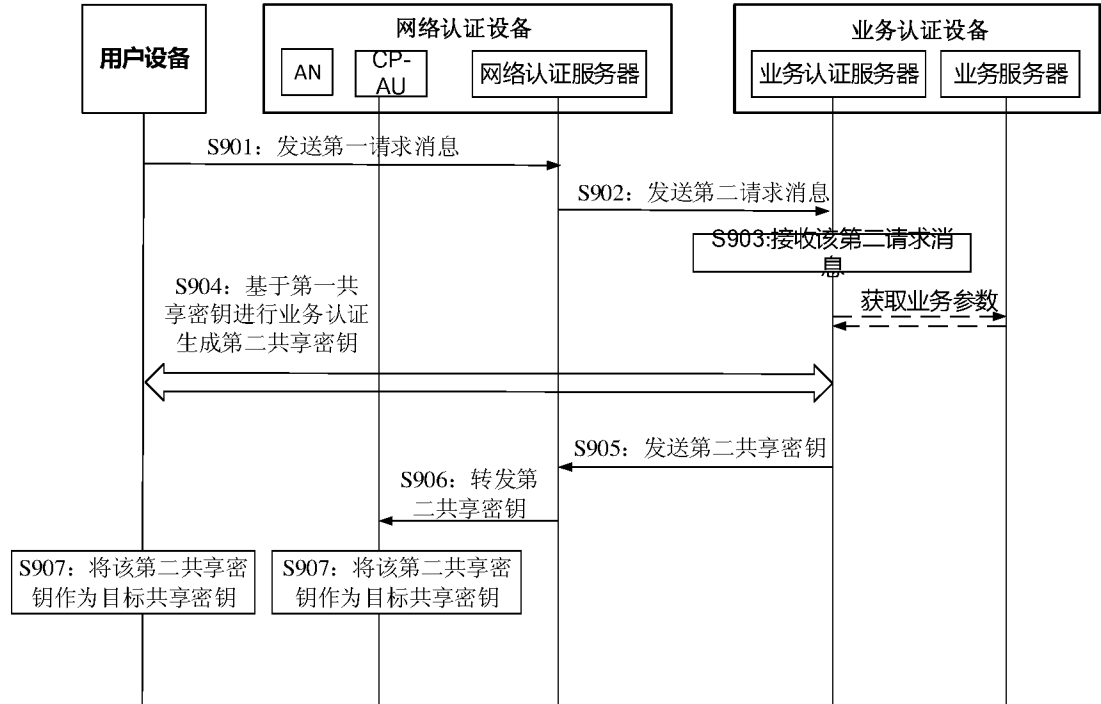


图 3I

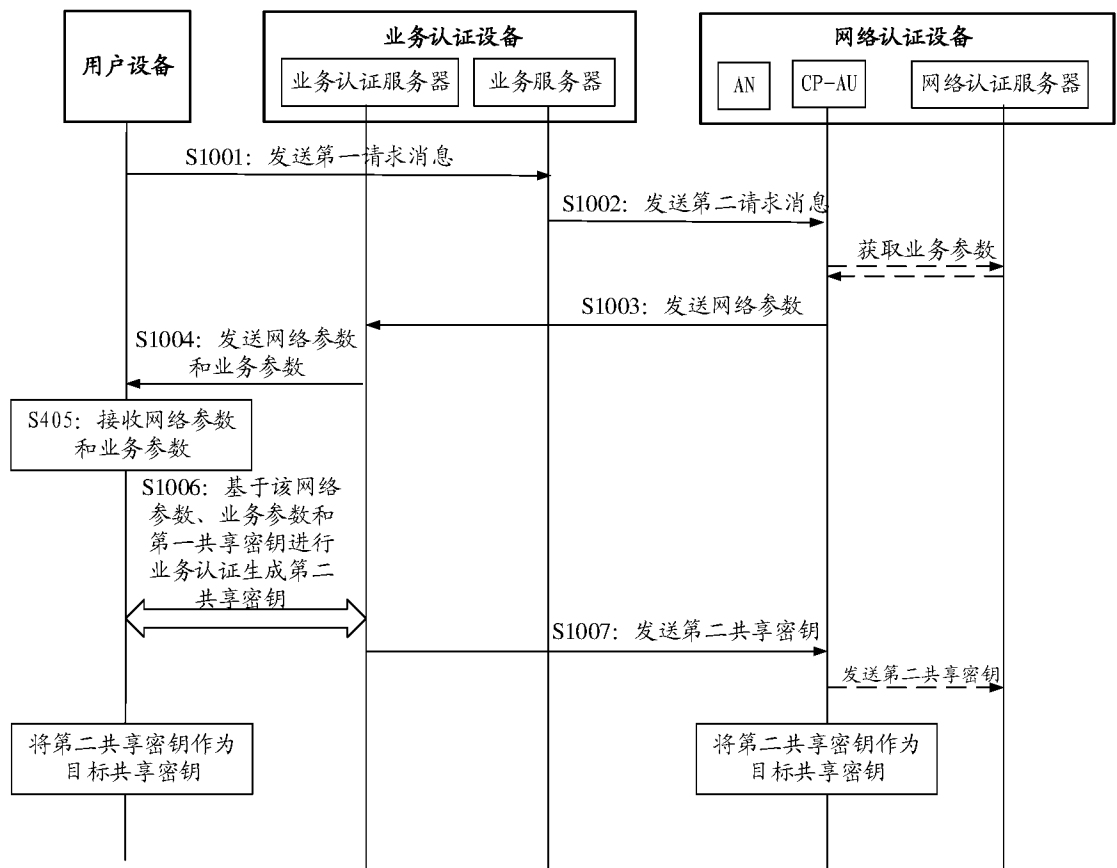


图 3J

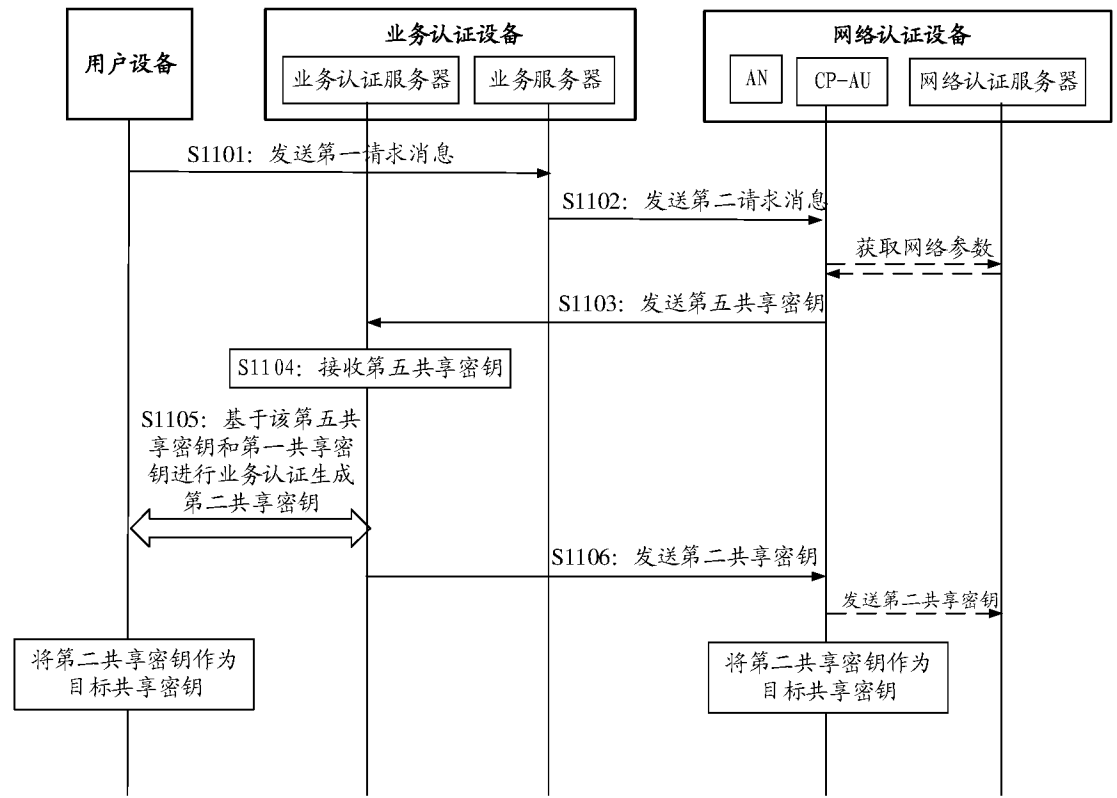


图 3K

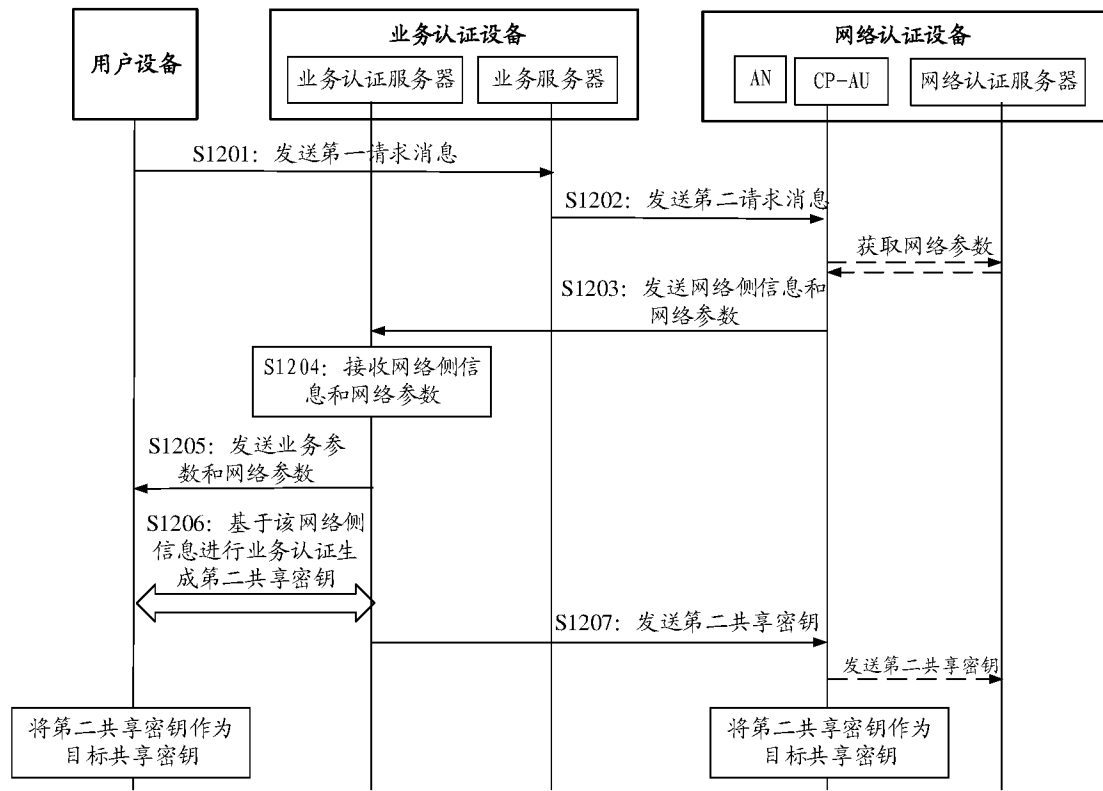


图 3L

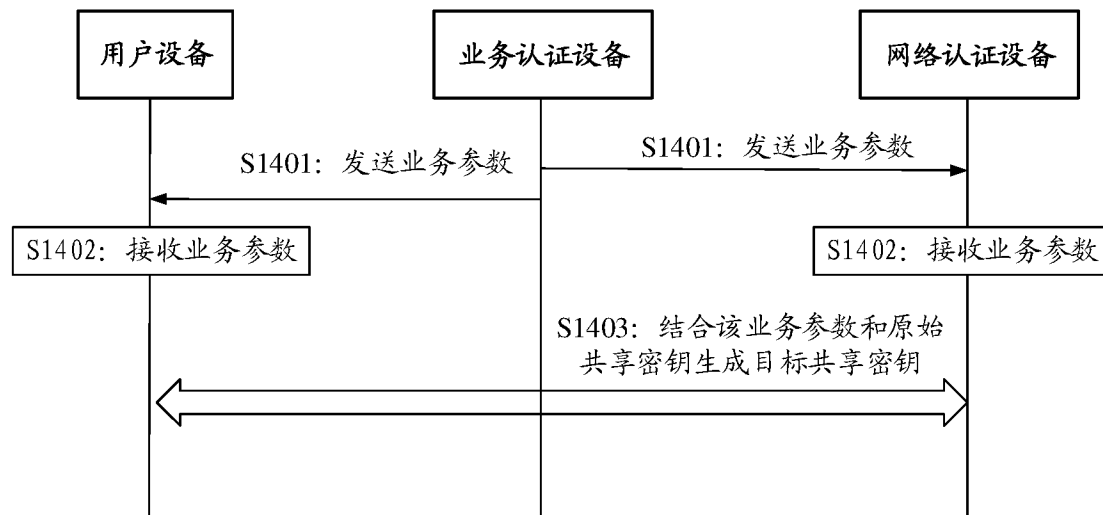


图 4A

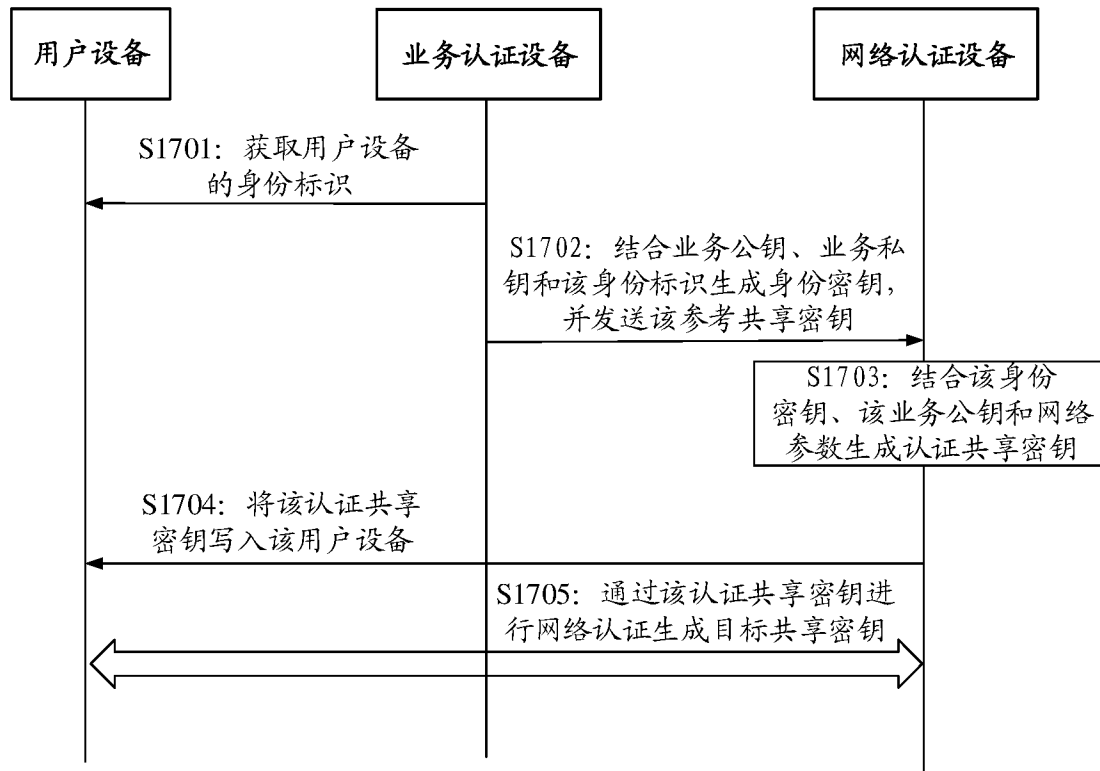


图 5A

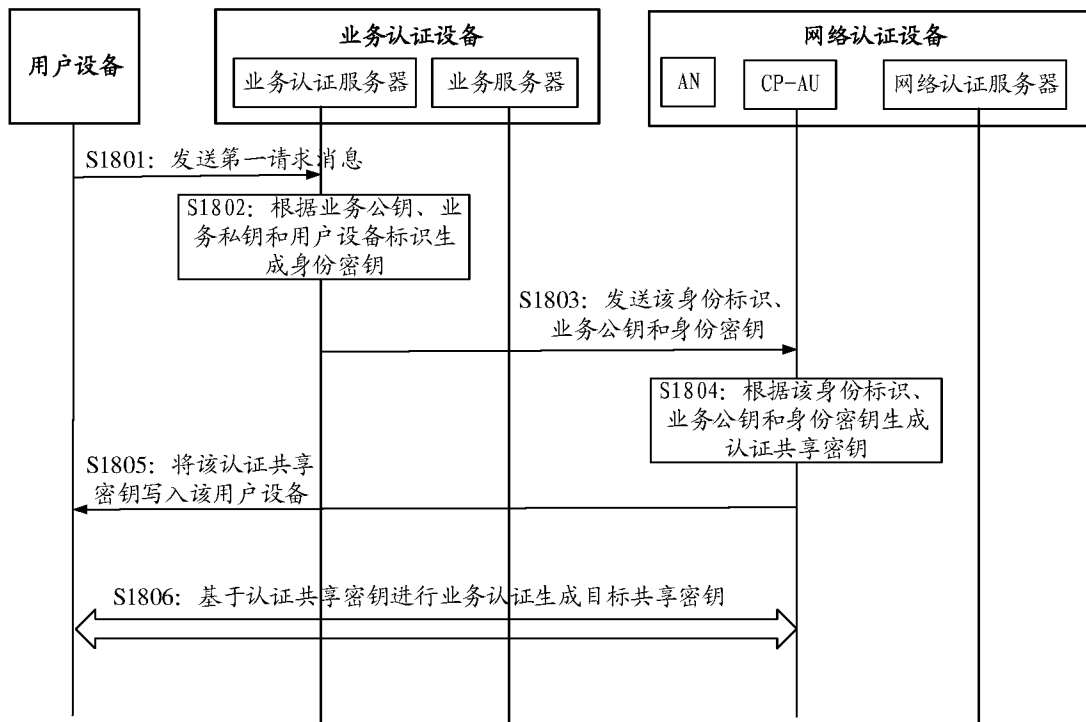


图 5B

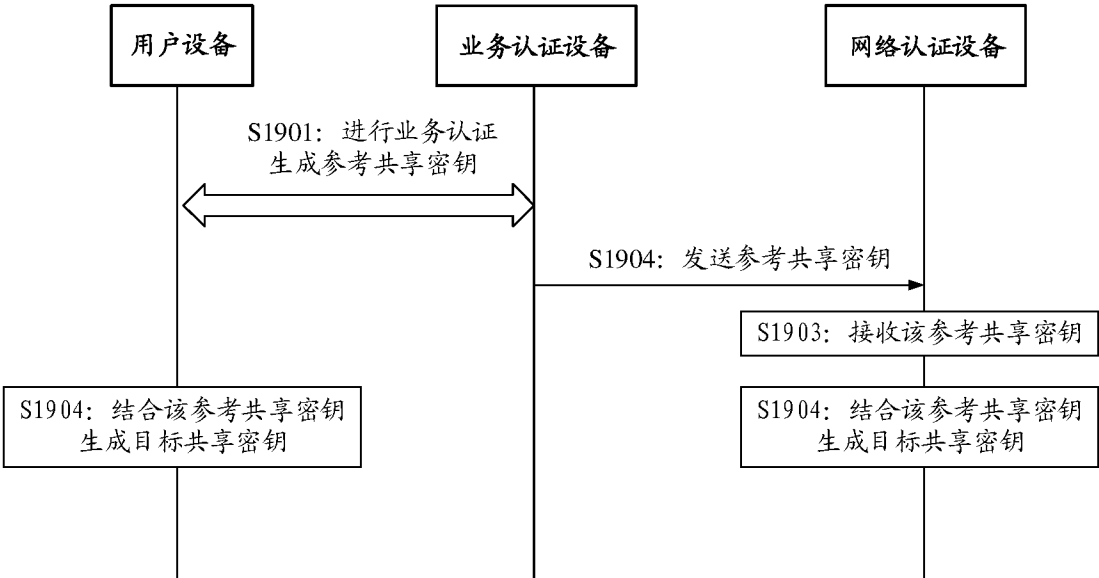


图 6A

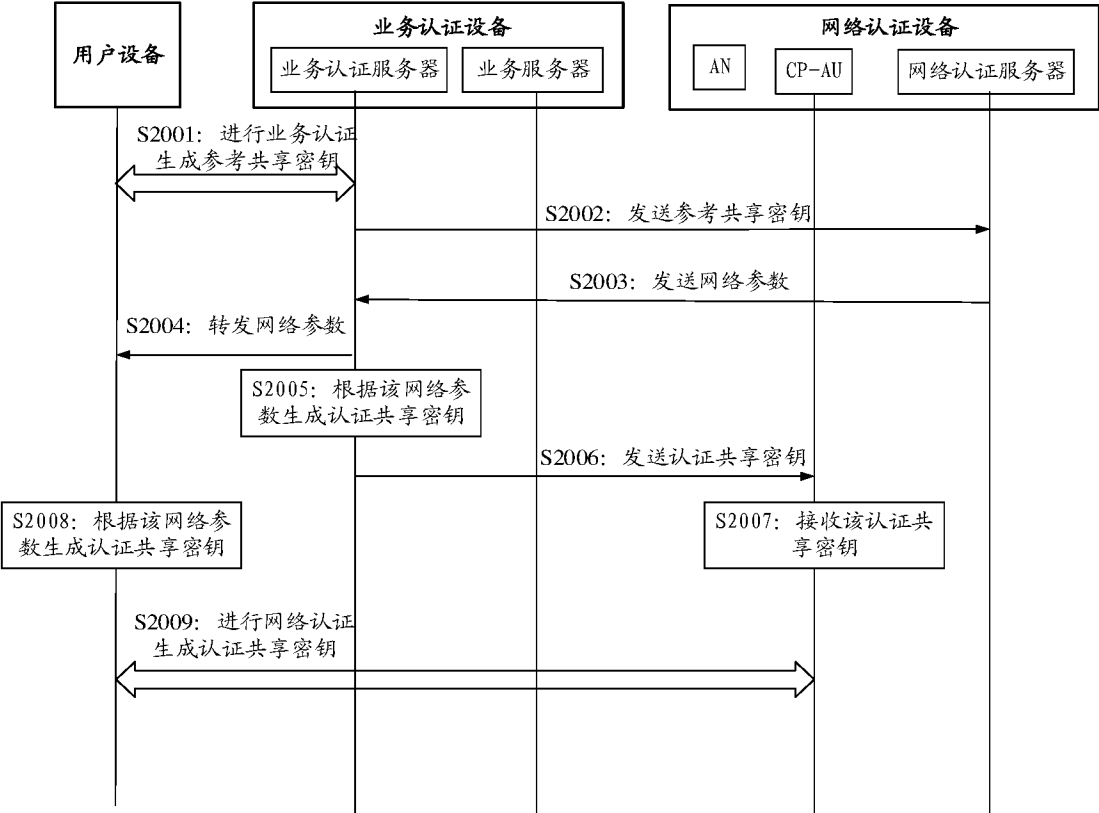


图 6B

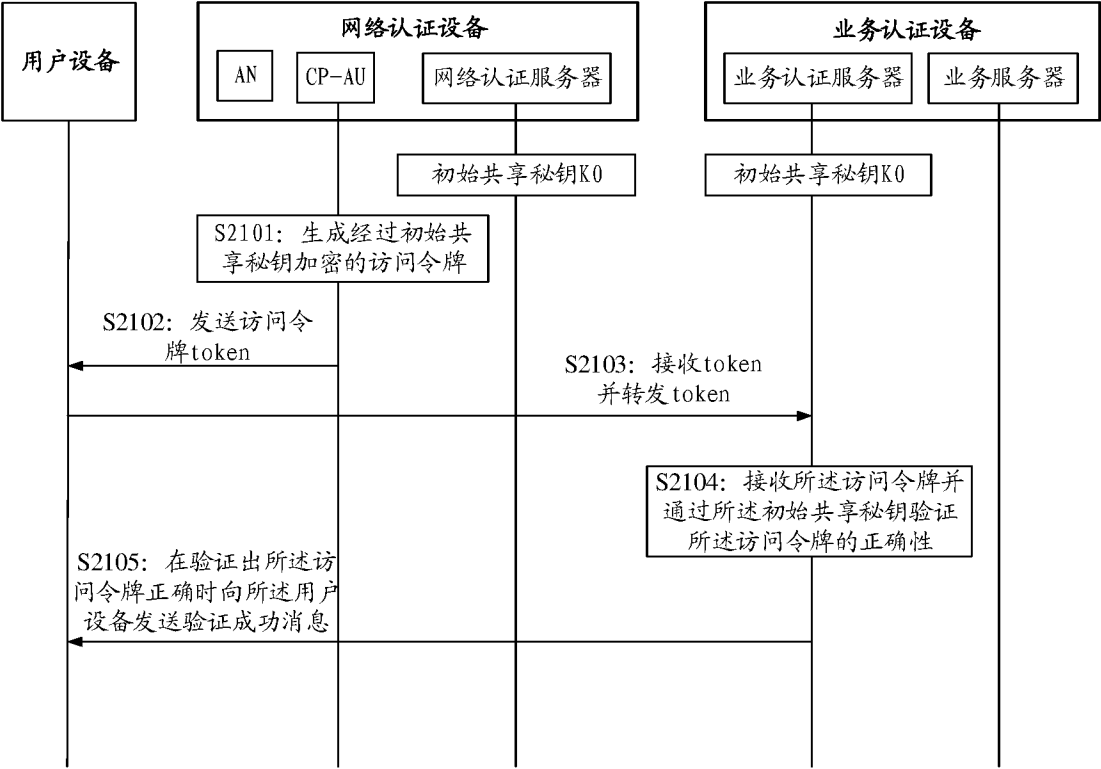


图 6C

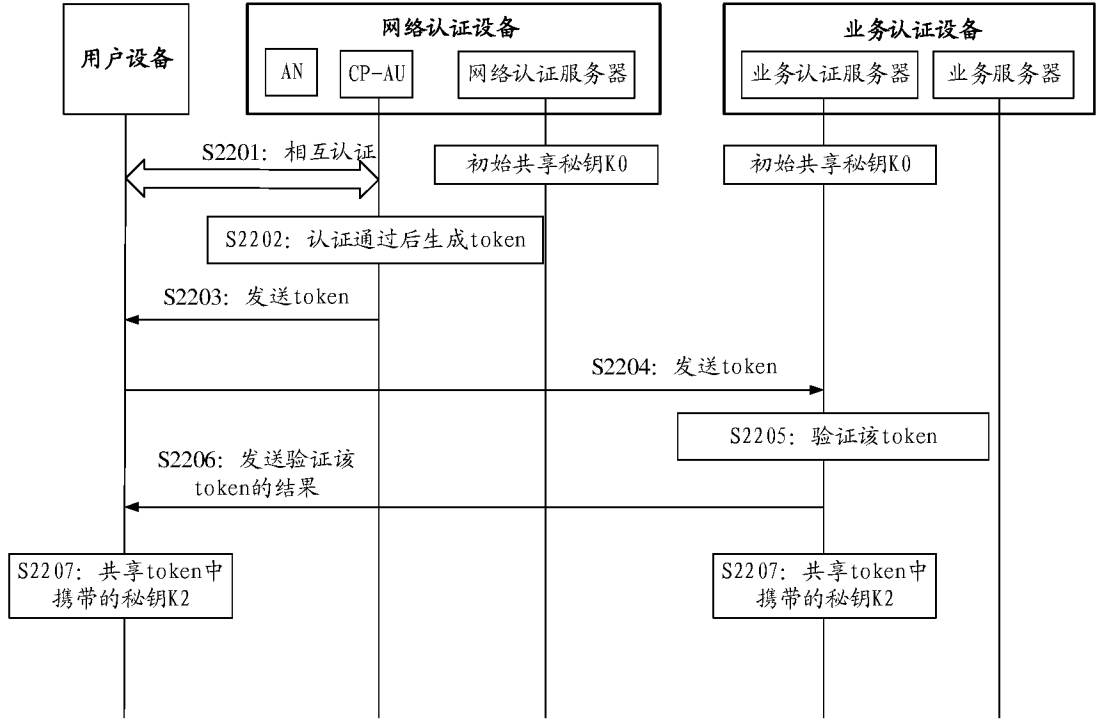


图 6D

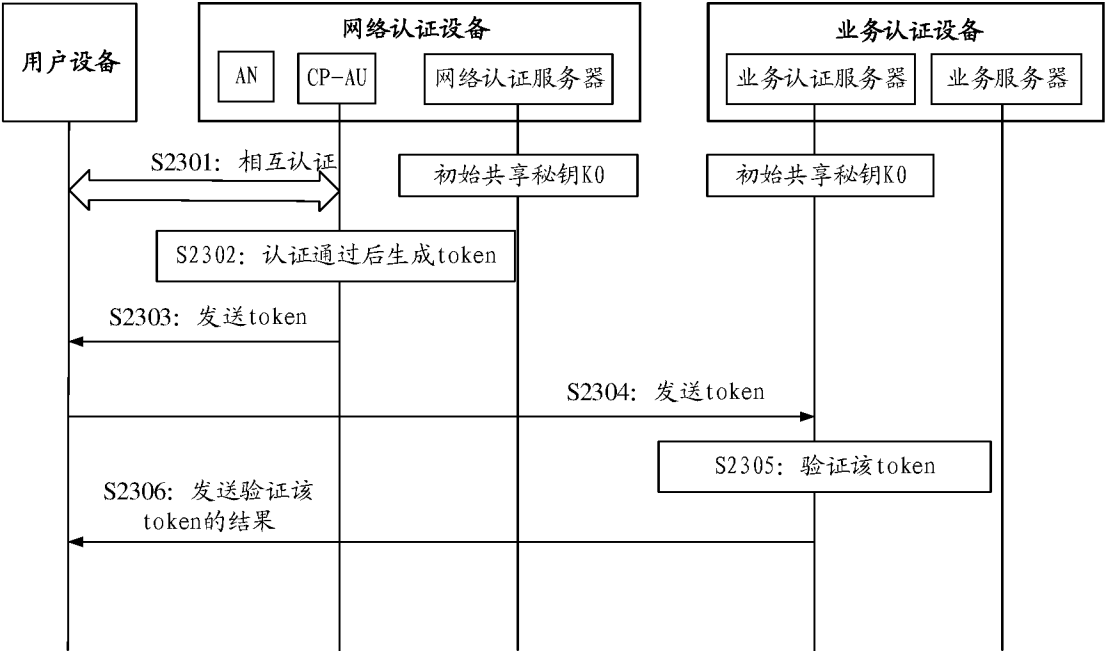


图 6E

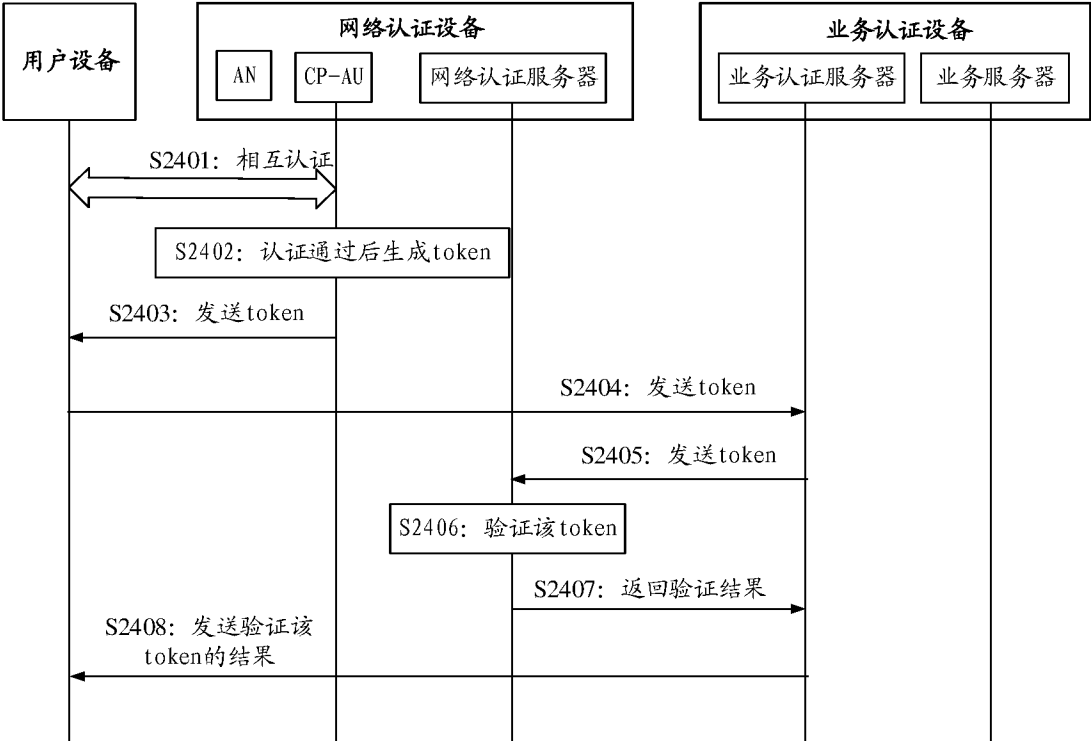


图 6F

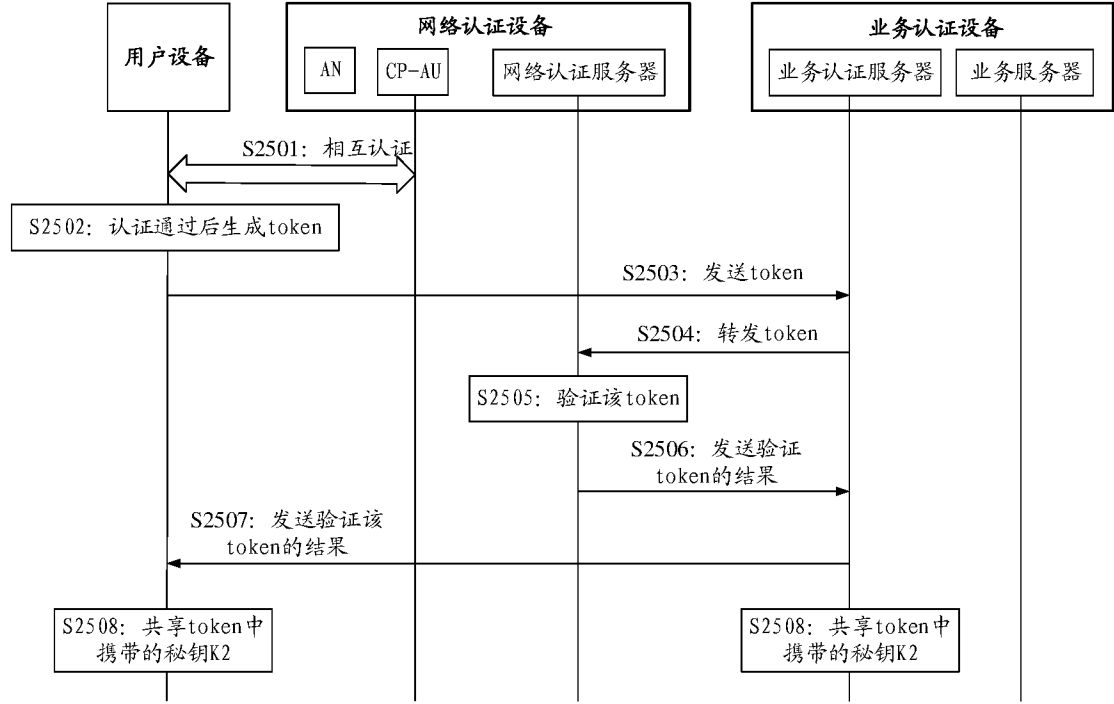


图 6G

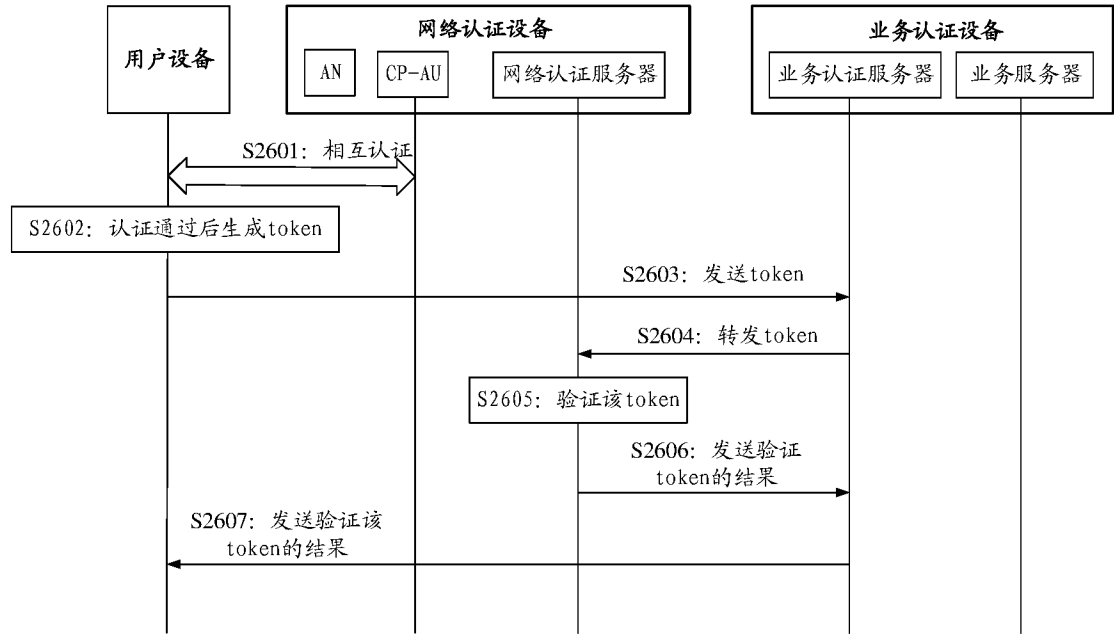


图 6H

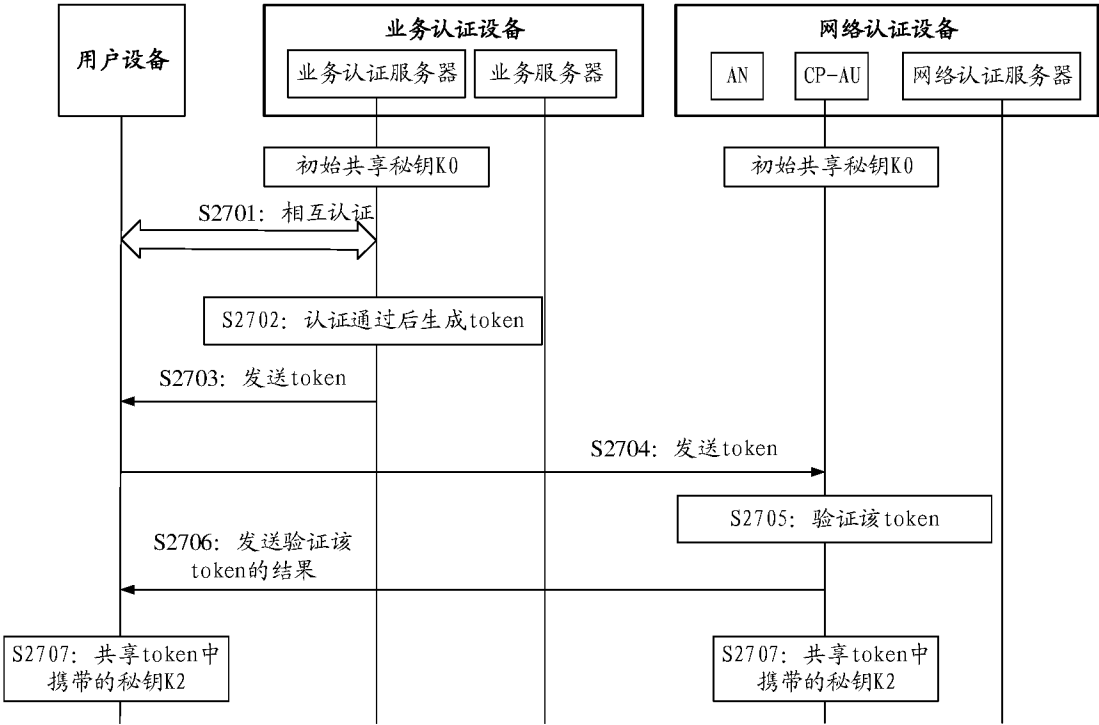


图 6I

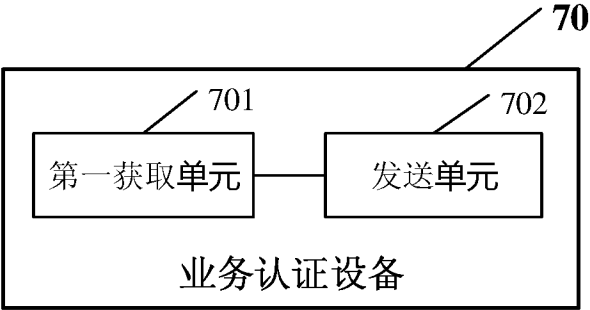


图 7

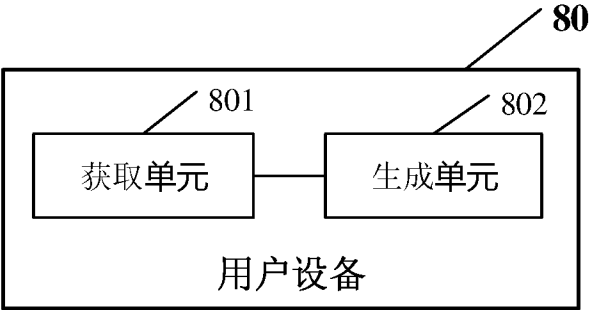


图 8

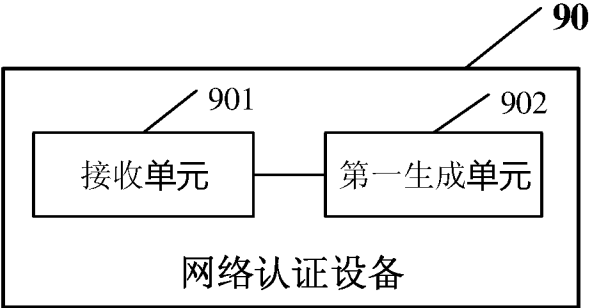


图 9

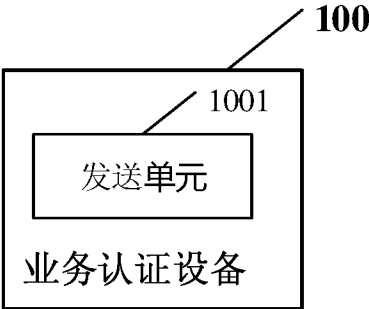


图 10

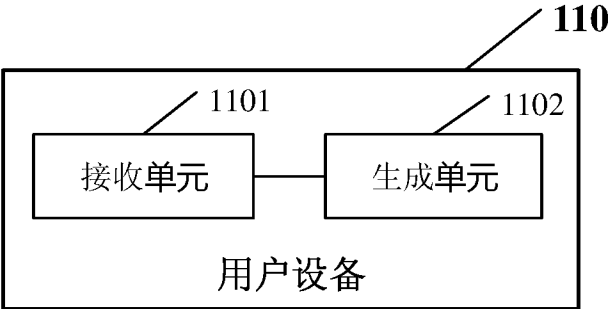


图 11

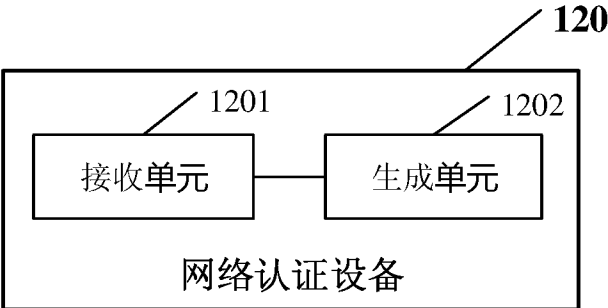


图 12

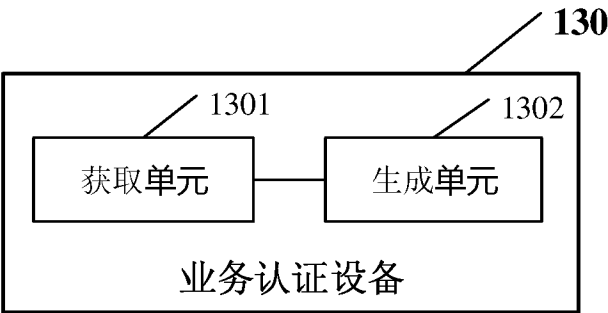


图 13

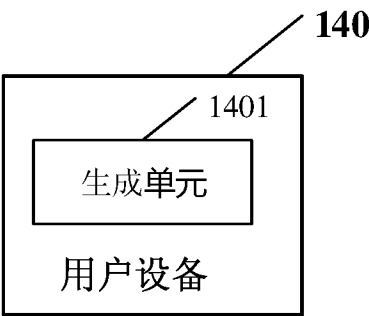


图 14

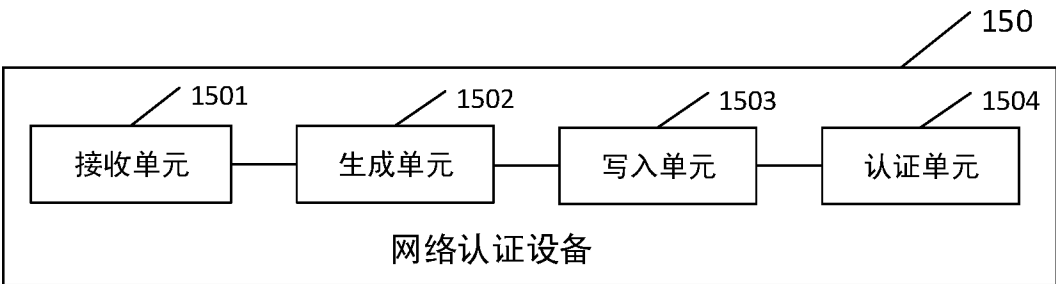


图 15

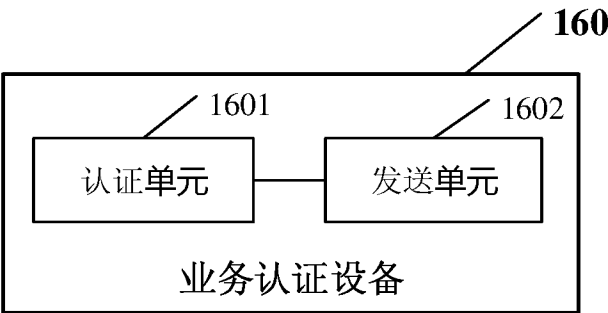


图 16

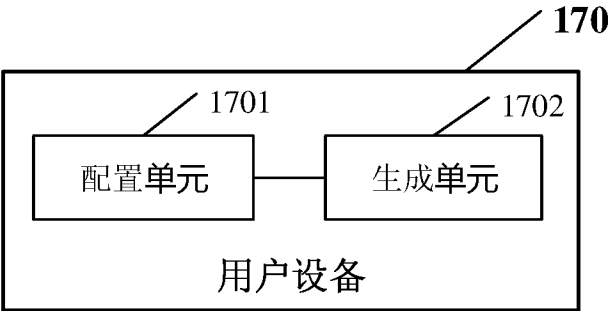


图 17

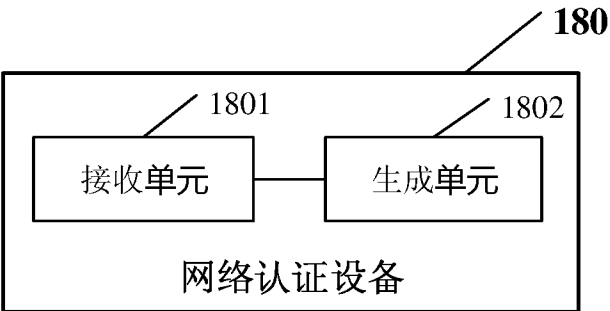


图 18

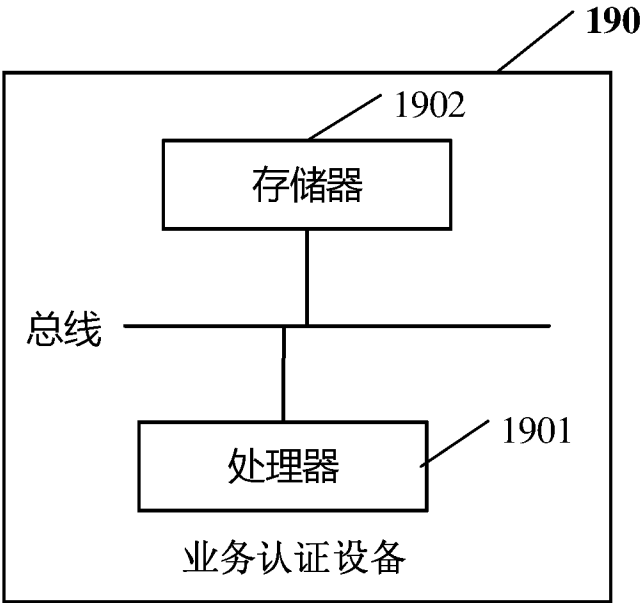


图 19

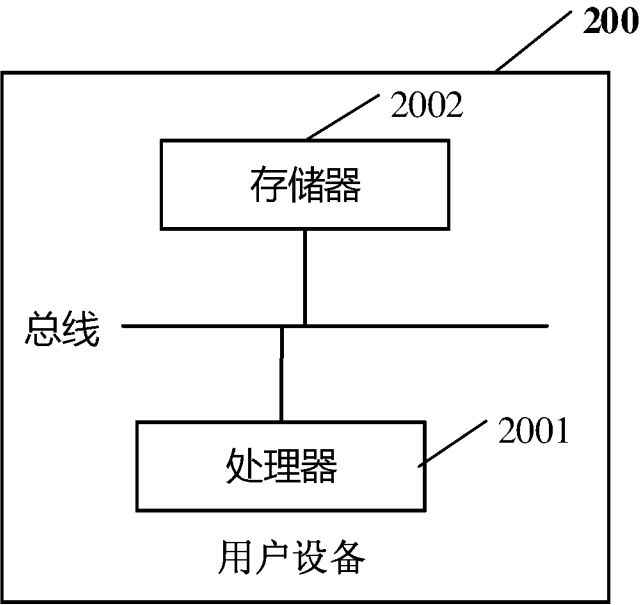


图 20

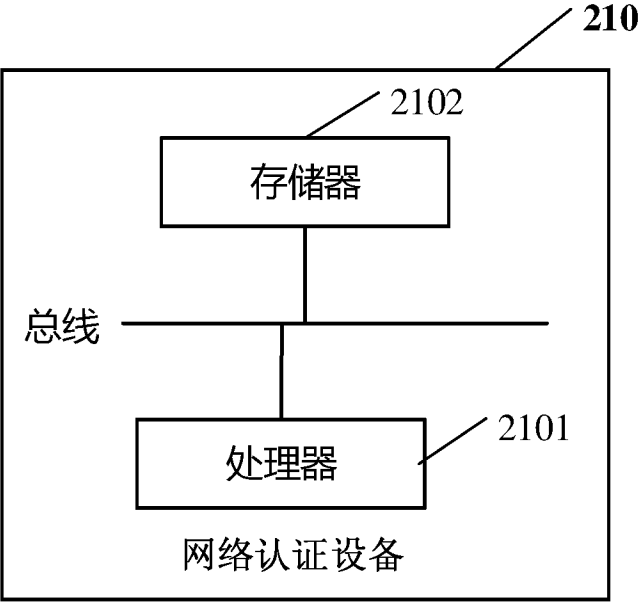


图 21

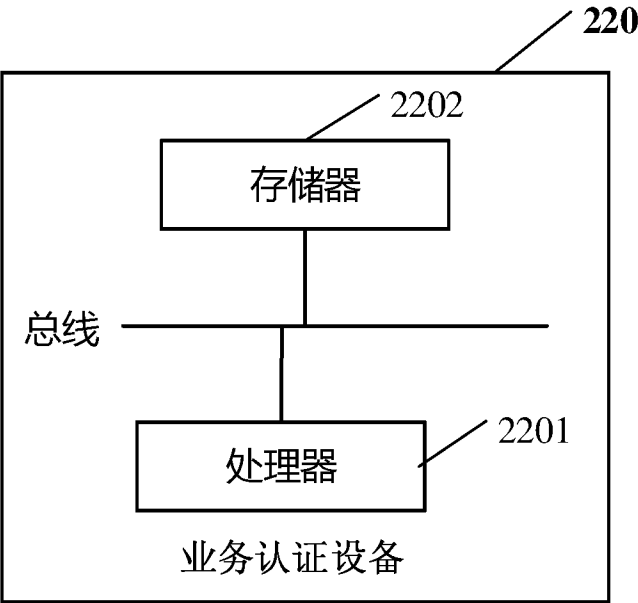


图 22

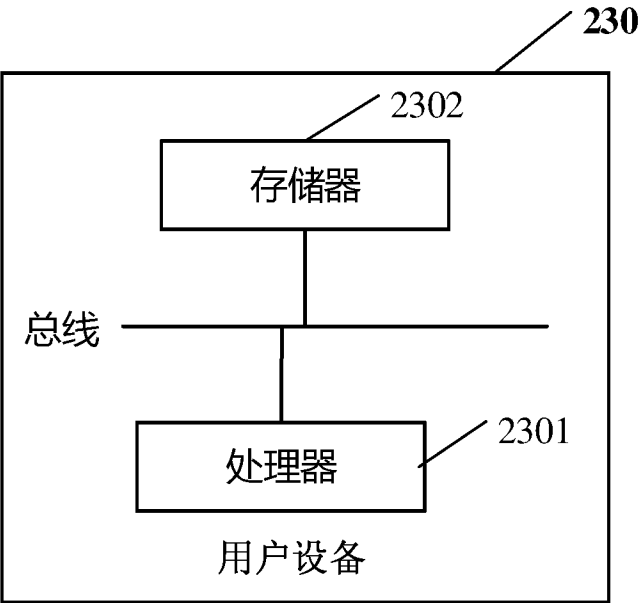


图 23

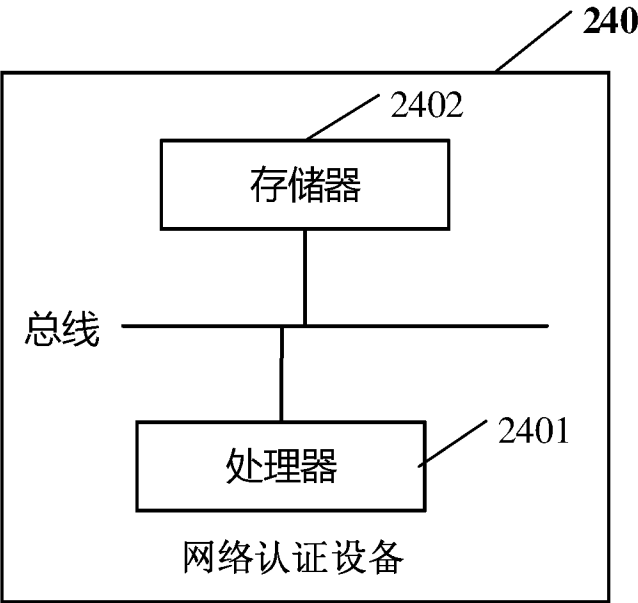


图 24

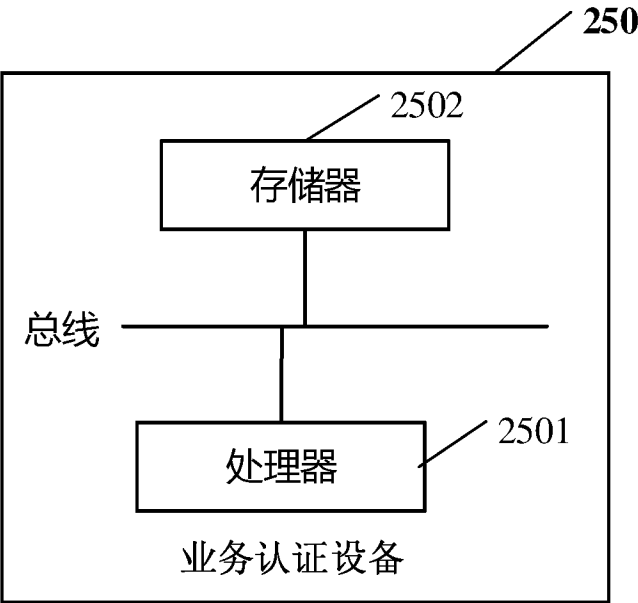


图 25

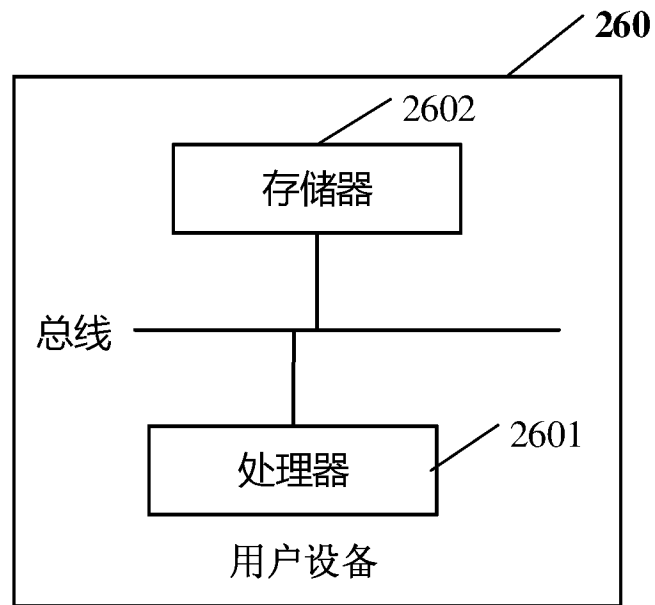


图 26

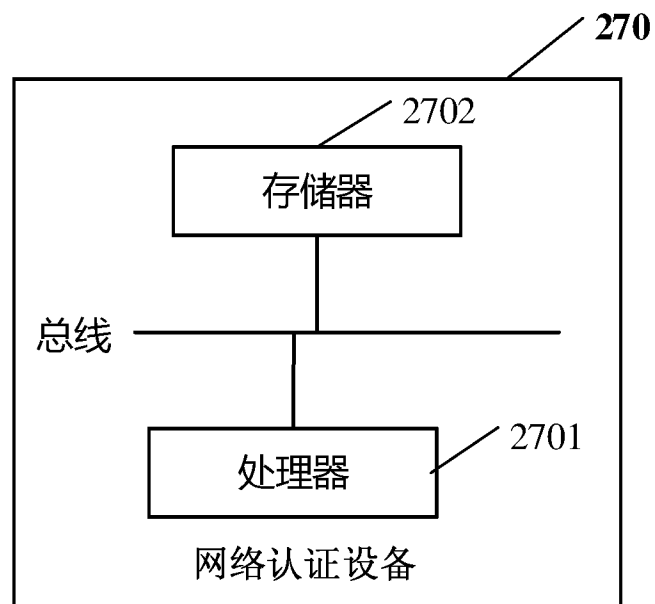


图 27

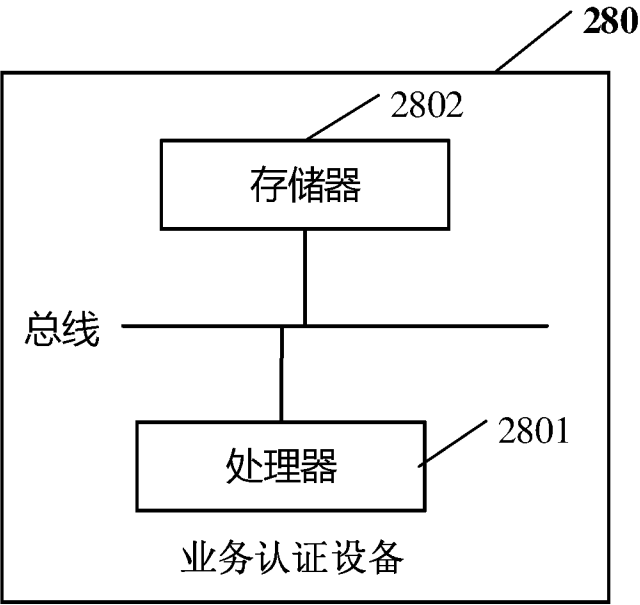


图 28

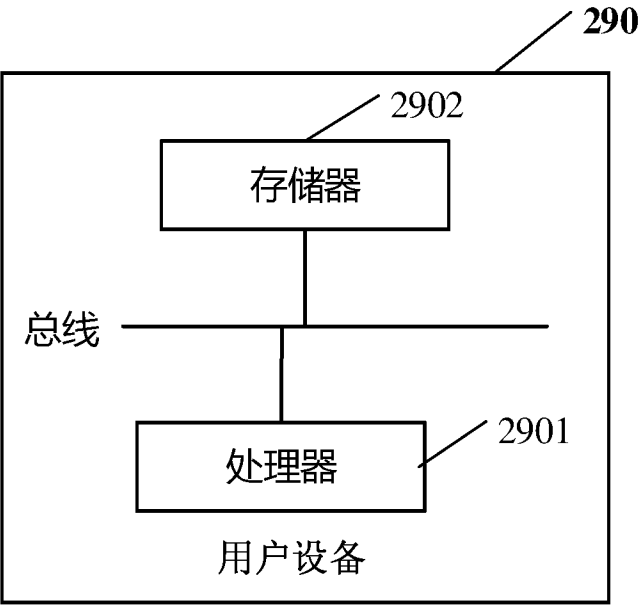


图 29

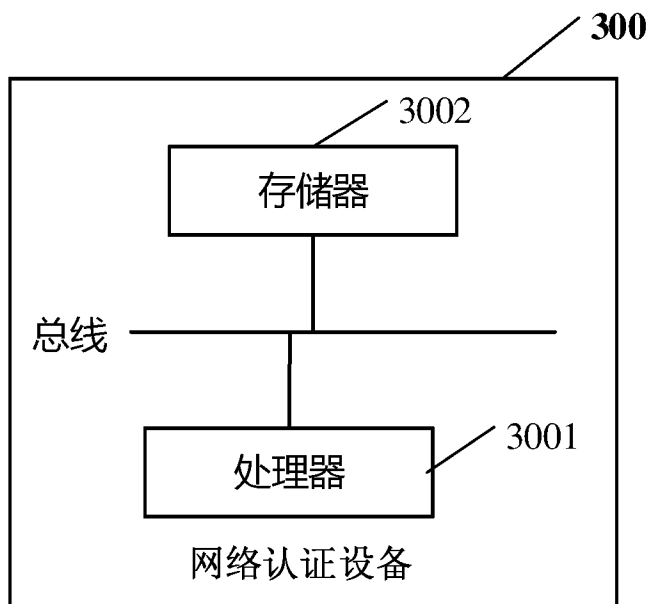


图 30

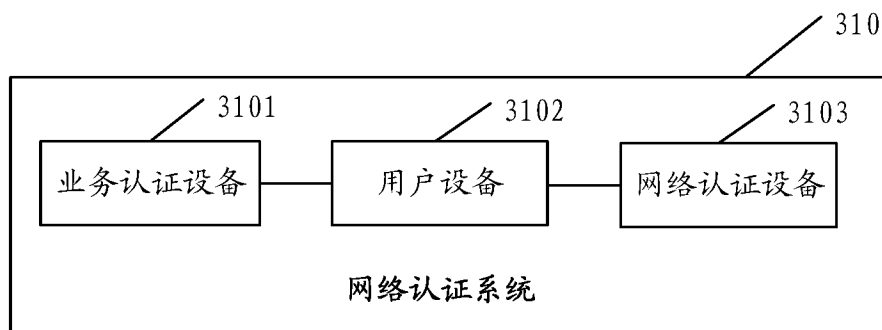


图 31

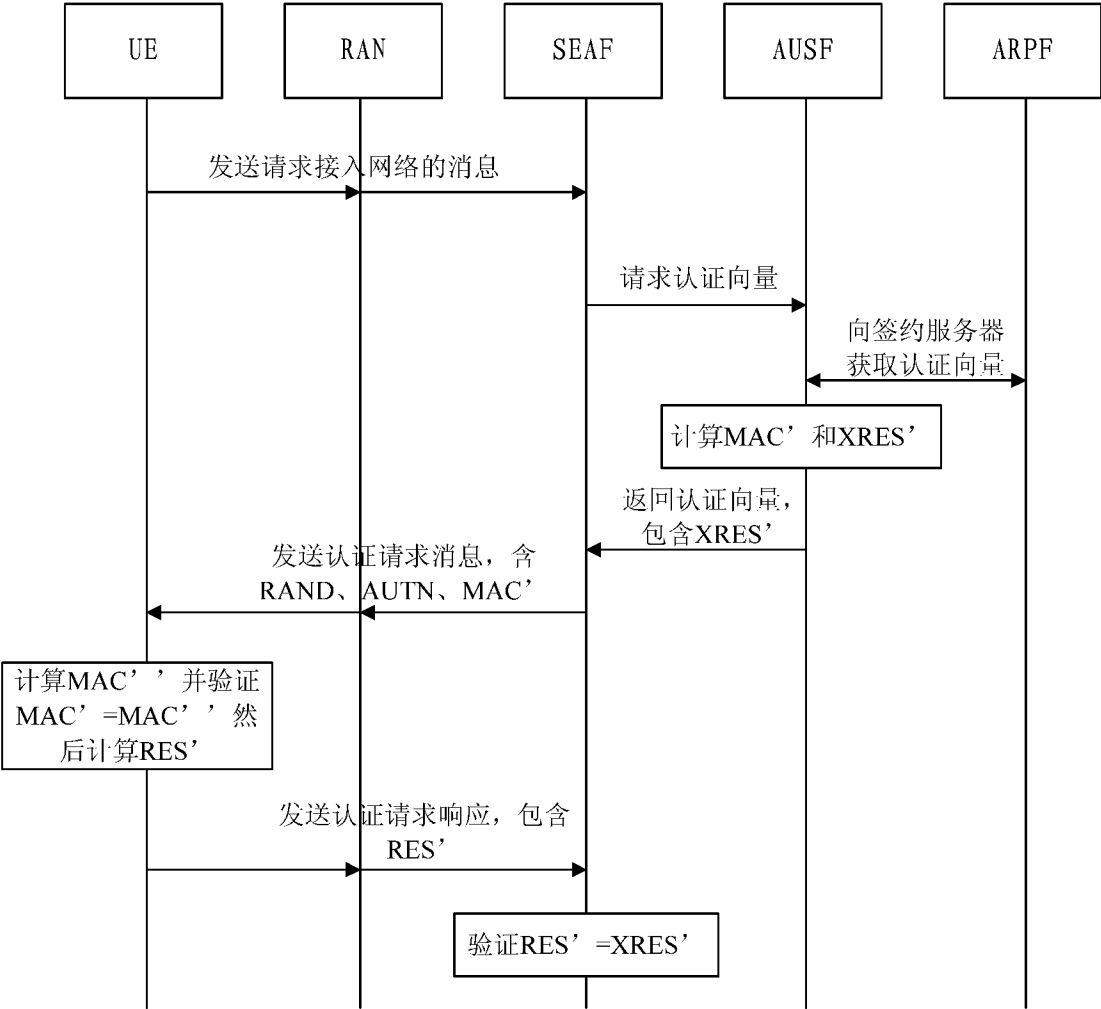


图 32

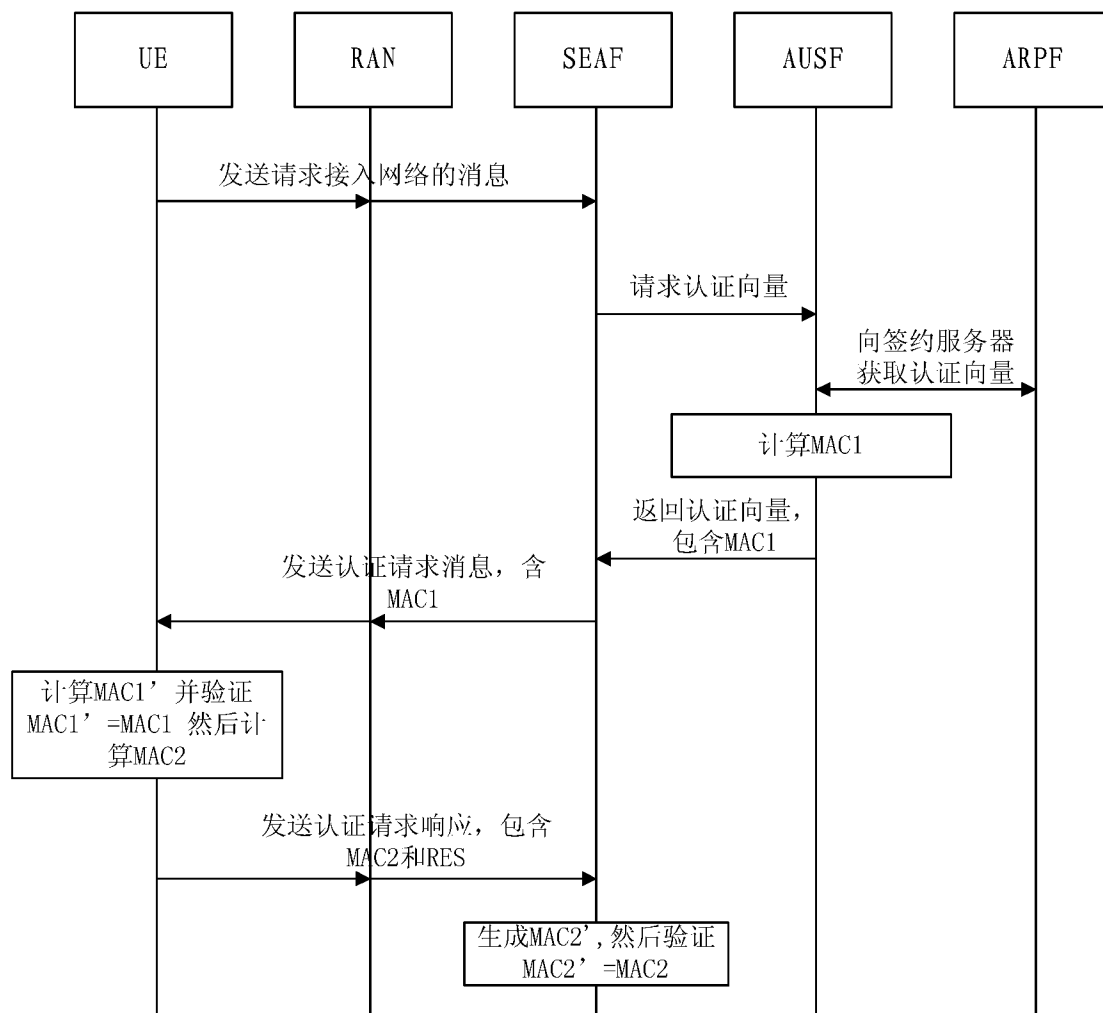


图 33

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/072253

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)

H04L 9/-

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)

CPRSABS, CNTXT, CNKI, VEN, DWPI: authentication, message authentication code, ID, shared key, symmetric key, generate, produce, service, certificate, identifier, pre-shared key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101052033 A (HUAWEI TECHNOLOGIES CO., LTD.), 10 October 2007 (10.10.2007), the whole document	1-101
A	CN 101156352 A (HUAWEI TECHNOLOGIES CO., LTD.), 02 April 2008 (02.04.2008), the whole document	1-101
A	CN 103023856 A (ZTE CORP.), 03 April 2013 (03.04.2013), the whole document	1-101
A	CN 1859097 A (HUAWEI TECHNOLOGIES CO., LTD.), 08 November 2006 (08.11.2006), the whole document	1-101

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 06 April 2017 (06.04.2017)	Date of mailing of the international search report 26 April 2017 (26.04.2017)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer WANG, Zhiwei Telephone No.: (86-10) 62089565

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/072253

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101052033 A	10 October 2007	CN 101052033 B	04 April 2012
CN 101156352 A	02 April 2008	CN 101156352 B	17 November 2010
		CN 101009919 A	01 August 2007
		CN 101052032 B	12 May 2010
		CN 101052032 A	10 October 2007
		CN 101060406 B	12 May 2010
		CN 101060406 A	24 October 2007
		KR 1009330 B1	18 January 2011
		KR 20080089500 A	06 October 2008
		EP 1811744 A1	25 July 2007
		EP 1811744 B1	09 September 2009
		US 7984298 B2	19 July 2011
		US 2008178004 A1	24 July 2008
		US 8468353 B2	18 June 2013
		US 2011258447 A1	20 October 2011
		WO 2007085175 A1	02 August 2007
		JP 2012253817 A	20 December 2012
		JP 2009524369 A	25 June 2009
		JP 5123209 B2	23 January 2013
		DE 602007002308 D1	22 October 2009
		AT 442730 T	15 September 2009
CN 103023856 A	03 April 2013	CN 106254386 A	21 December 2016
		WO 2013040957 A1	28 March 2013
CN 1859097 A	08 November 2006	CN 1859097 B	04 August 2010

A. 主题的分类 H04L 9/32 (2006.01) i 按照国际专利分类 (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) H04L9/- 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)) CPRSABS, CNTXT, CNKI, VEN, DWPI: 业务, 认证, 共享密钥, 对称密钥, 产生, 生成, 消息认证码, 预共享密钥, 标识, ID, shared key, symmetric key, generate, produce, service, certificate, identifier, pre-shared key		
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
A	CN 101052033 A (华为技术有限公司) 2007年 10月 10日 (2007 - 10 - 10) 全文	1-101
A	CN 101156352 A (华为技术有限公司) 2008年 4月 2日 (2008 - 04 - 02) 全文	1-101
A	CN 103023856 A (中兴通讯股份有限公司) 2013年 4月 3日 (2013 - 04 - 03) 全文	1-101
A	CN 1859097 A (华为技术有限公司) 2006年 11月 8日 (2006 - 11 - 08) 全文	1-101
☐ 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 (如具体说明的) “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 2017年 4月 6日		国际检索报告邮寄日期 2017年 4月 26日
ISA/CN的名称和邮寄地址 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 王志伟 电话号码 (86-10) 62089565

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/072253

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101052033	A	2007年 10月 10日	CN	101052033	B	2012年 4月 4日
CN	101156352	A	2008年 4月 2日	CN	101156352	B	2010年 11月 17日
				CN	101009919	A	2007年 8月 1日
				CN	101052032	B	2010年 5月 12日
				CN	101052032	A	2007年 10月 10日
				CN	101060406	B	2010年 5月 12日
				CN	101060406	A	2007年 10月 24日
				KR	1009330	B1	2011年 1月 18日
				KR	20080089500	A	2008年 10月 6日
				EP	1811744	A1	2007年 7月 25日
				EP	1811744	B1	2009年 9月 9日
				US	7984298	B2	2011年 7月 19日
				US	2008178004	A1	2008年 7月 24日
				US	8468353	B2	2013年 6月 18日
				US	2011258447	A1	2011年 10月 20日
				WO	2007085175	A1	2007年 8月 2日
				JP	2012253817	A	2012年 12月 20日
				JP	2009524369	A	2009年 6月 25日
				JP	5123209	B2	2013年 1月 23日
				DE	602007002308	D1	2009年 10月 22日
				AT	442730	T	2009年 9月 15日
CN	103023856	A	2013年 4月 3日	CN	106254386	A	2016年 12月 21日
				WO	2013040957	A1	2013年 3月 28日
CN	1859097	A	2006年 11月 8日	CN	1859097	B	2010年 8月 4日

表 PCT/ISA/210 (同族专利附件) (2009年7月)