(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
2017 年 12 月 14 日 (14.12.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/210852 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2016/085051

(22) 国际申请日: 2016 年 6 月 7 日 (07.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(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: 韦安妮 (WEI, Anni); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 熊春山(XIONG, Chunshan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 尤建洁(YOU, Jianjie); 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: 北京三高永信知识产权代理有限责任公司(BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市海淀区学院路蓟门里和景园A座1单元102室, Beijing 100088 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD,

(54) **Title:** SERVICE PROCESSING METHOD AND DEVICE

(54) **发明名称**: 业务处理方法及装置

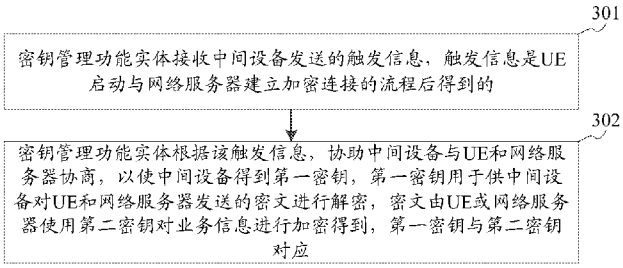

图 3

301 A key management entity receives triggering information sent by an intermediate device, wherein the triggering information is obtained after UE starts the procedure of establishing an encryption connection with a network server

302 The key management entity assists, according to the triggering information, the intermediate device to negotiate with the UE and the network server, so that the intermediate device obtains a first key, wherein the first key is used by the intermediate device to decrypt ciphertext sent by the UE and the network server, the ciphertext is obtained through encryption of service information by the UE or the network server by using a second key, and the first key corresponds to the second key

(57) **Abstract:** The present invention discloses a service processing method and device, and relates to the communications field. The method comprises: receiving triggering information sent by an intermediate device; and assisting, according to the triggering information, the intermediate device to negotiate with UE and a network server, so that the intermediate device obtains a first key, wherein the first key is used by the intermediate device to decrypt ciphertext sent by the UE and the network server, the ciphertext is obtained through encryption of service information by the UE or the network server by using a second key, and the first key corresponds to the second key. The invention solves a problem in which the intermediate device cannot decrypt the ciphertext and so cannot provide service optimization for the UE and the network server, and achieves the effect of expanding the application scope of service optimization.

(57) **摘要**: 本发明公开了一种业务处理方法及装置，涉及通信领域，所述方法包括：接收中间设备发送的触发信息；根据触发信息，协助中间设备与UE和网络服务器协商，以使中间设备得到第一密钥，第一密钥用于供中间设备对UE和网络服务器发送的密文进行解密，密文由UE或网络服务器使用第二密钥对业务信息进行加密得到，第一密钥与第二密钥对应。本发明解决了中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

WO 2017/210852 A1

[见续页]

GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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)。

根据细则4.17的声明：

— 关于申请人有权申请并被授予专利(细则4.17(ii))

本国际公布：

— 包括国际检索报告(条约第21条(3))。

业务处理方法及装置

技术领域

本发明涉及通信领域，特别涉及一种业务处理方法及装置。

背景技术

安全套接层（英文：security socket layer；简称：SSL）协议及其继任者传输层安全（英文：transport layer security；简称，TLS）协议用于为网络通信提供加密、身份认证及数据完整性等服务，已被广泛地应用于浏览器与网络服务器之间的安全通信。其中，SSL/TLS 协议位于传输层的传输控制协议（英文：transmission control protocol；简称：TCP）协议和应用层的超文本传送协议（英文：hypertext transfer protocol；简称：HTTP）之间。

相关技术提供的一种业务处理方法包括：用户设备（英文：user equipment；简称：UE）基于下层使用了 SSL/TLS 协议的超文本传输安全协议（英文：hyper text transfer protocol over secure socket layer；简称：HTTPS）与网络服务器建立加密连接，并约定密钥，用户设备使用密钥加密业务信息后发送给网络服务器，网络服务器使用密钥解密得到业务信息，根据该业务信息生成业务数据，加密业务数据后发送给用户设备，用户设备使用密钥解密得到业务数据。其中，业务信息可以用于请求网络服务器的网页，也可以用于请求网络服务器中的对象。

通常，还可以在用户设备和网络服务器之间设置中间设备，在中间设备存在的场景下，当在用户设备和网络服务器之间建立加密连接时，用户设备和网络服务器之间传输的是加密后得到的密文，由于中间设备不能获取到密钥，因此，中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化。

发明内容

为了解决中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，本发明实施例提供了一种业务处理方法及装置。所述技术方案如下：

第一方面，提供了一种业务处理方法，方法包括：密钥管理功能实体接收中间设备发送的触发信息，该触发信息是UE启动与网络服务器建立加密连接的流程后得到的；根据该触发信息，协助中间设备与UE和网络服务器协商，以使中间设备得到第一密钥，第一密钥用于供中间设备对UE和网络服务器发送的密文进行解密，密文由UE或网络服务器使用第二密钥对业务信息进行加密得到，第一密钥与第二密钥对应。

由于UE与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对UE来说是透明的，此时，中间设备需要在密钥管理功能实体的协助下与UE 和服务器进行协商，在协商成功后得到第一密钥，再使用第一密钥来解密UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

在第一方面的第一种可能的实现方式中，密钥管理功能实体根据触发信息，协助中间设备与UE和网络服务器协商，以使中间设备得到第一密钥，包括：密钥管理功能实体根据触发信息确定与网络服务器协商成功后，向UE获取第一密钥，将第一密钥发送给中间设备；或者，密钥管理功能实体根据触发信息与UE进行协商，协商成功后向网络服务器获取第一密钥，将第一密钥发送给中间设备；或者，密钥管理功能实体根据触发信息与UE进行协商，协商成功后触发中间设备向网络服务器获取第一密钥；或者，当密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能实体根据触发信息向网络服务器获取第一密钥，将第一密钥发送给中间设备。

密钥管理实体既可以协助中间设备向网络服务器获取第一密钥，也可以协助中间设备向UE获取第一密钥，为中间设备获取第一密钥提供了多种实现方式。

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，密钥管理功能实体根据触发信息确定与网络服务器协商成功后，向UE 获取第一密钥，将第一密钥发送给中间设备，包括：当触发信息是中间设备发送的第一密钥获取请求时，密钥管理功能实体向网络服务器发送第一解密请求，接收网络服务器发送的携带网络服务器的签名的第一解密应答，生成携带网络服务器的签名的第二密钥获取请求发送给 UE，接收 UE 使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥发送给中间设

备；或者，当触发信息是中间设备发送的，且携带网络服务器的签名的第三密钥获取请求时，密钥管理功能实体生成携带网络服务器的签名的第四密钥获取请求发送给 UE，接收 UE 使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备，网络服务器的签名是中间设备向网络服务器发送第二解密请求后，从得到的第二解密应答中得到的；其中，第三密钥是 UE 在建立加密连接时从网络服务器中得到的，网络服务器的签名是网络服务器使用第四密钥对协商成功的第一确认信息进行加密得到的，第四密钥与第三密钥对应。

结合第一方面的第一种可能的实现方式，在第一方面的第三种可能的实现方式中，密钥管理功能实体根据触发信息与 UE 进行协商，协商成功后向网络服务器获取第一密钥，将第一密钥发送给中间设备，包括：当触发信息是中间设备发送的第五密钥获取请求时，密钥管理功能实体向 UE 发送第三解密请求，接收 UE 发送的携带 UE 的签名和第五密钥的第三解密应答，生成携带 UE 的签名和第五密钥的第五密钥获取请求发送给网络服务器，接收网络服务器使用第五密钥对 UE 的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备；其中，UE 的签名信息是 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，第六密钥与第五密钥对应。

结合第一方面的第一种可能的实现方式，在第一方面的第四种可能的实现方式中，密钥管理功能实体根据触发信息与 UE 进行协商，协商成功后触发中间设备向网络服务器获取第一密钥，包括：当触发信息是中间设备发送的第四解密请求时，密钥管理功能实体将第四解密请求转发给 UE，接收 UE 发送的携带 UE 的签名和第五密钥的第四解密应答，将第四解密应答转发给中间设备，第四解密应答用于指示中间设备向网络服务器发送携带 UE 的签名和第五密钥的第六密钥获取请求，并接收网络服务器使用第五密钥对 UE 的签名验证通过后发送的第一密钥；其中，UE 的签名信息是 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，第六密钥与第五密钥对应。

结合第一方面的第一种可能的实现方式，在第一方面的第五种可能的实现方式中，当密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能实体根据触发信息向网络服务器获取第一密钥，将第一密钥发送给中间设备，包括：当触发信息是中间设备发送的第七密钥获取请求，且密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能实体将第七密钥获取

请求转发给网络服务器，并接收网络服务器在确定密钥管理功能实体与网络服务器之间建立有加密连接时发送的第一密钥，将第一密钥发送给中间设备。

第二方面，提供了一种业务处理方法，方法包括：在密钥管理功能实体和网络服务器的协助下，UE 协助中间设备获取第一密钥；UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文；或者，UE 接收中间设备转发的密文，密文由网络服务器使用第二密钥对业务信息进行加密得到并发送给中间设备；其中，第一密钥用于供中间设备对密文进行解密，且第一密钥与第二密钥对应。

由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

在第二方面的第一种可能的实现方式中，在密钥管理功能实体和网络服务器的协助下，UE 协助中间设备获取第一密钥，包括：UE 接收密钥管理功能实体发送的密钥获取请求，密钥获取请求中携带网络服务器的签名，服务器的签名是网络服务器使用第四密钥对协商成功的第一确认信息进行加密得到的；UE 使用第三密钥对网络服务器的签名进行解密，在得到第一确认信息时确定验证通过，第三密钥是 UE 在建立加密连接时从网络服务器中得到的，第三密钥与第四密钥对应；在验证通过后，UE 向密钥管理功能实体发送第一密钥，第一密钥由密钥管理功能实体发送给中间设备。

在第二方面的第二种可能的实现方式中，在密钥管理功能实体和网络服务器的协助下，UE 协助中间设备获取第一密钥，包括：UE 接收密钥管理功能实体发送的解密请求；UE 使用第六密钥对协商成功的第二确认信息进行加密，得到 UE 的签名；UE 生成携带 UE 的签名和第五密钥的解密应答发送给密钥管理功能实体，密钥管理功能实体用于将解密应答发送给中间设备，中间设备用于生成携带 UE 的签名和第五密钥的密钥获取请求发送给网络服务器，并接收网络服务器使用第五密钥对 UE 的签名的验证通过后发送的第一密钥；或者，密钥管理功能实体用于生成携带 UE 的签名和第五密钥的密钥获取请求发送给网络服务器，并获取网络服务器使用第五密钥对 UE 的签名的验证通过后发送

的第一密钥，将第一密钥发送给中间设备，第五密钥与第六密钥对应。

第三方面，提供了一种业务处理方法，方法包括：在密钥管理功能实体和UE 的协助下，网络服务器协助中间设备获取第一密钥；网络服务器接收中间设备转发的密文，密文由 UE 使用第二密钥对业务信息进行加密得到密文并发送给中间设备；或者，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文；其中，第一密钥用于供中间设备对密文进行解密，第一密钥与第二密钥对应。

网络服务器需要在密钥管理功能实体和 UE 的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

在第三方面的第一种可能的实现方式中，在密钥管理功能实体和 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括：网络服务器接收中间设备发送的解密请求；网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到网络服务器的签名；网络服务器生成携带网络服务器的签名的解密应答发送给中间设备，中间设备用于生成携带网络服务器的签名的密钥获取请求发送给密钥管理功能实体，密钥管理功能实体用于将密钥获取请求转发给 UE，并接收 UE 使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥转发给中间设备。

在第三方面的第二种可能的实现方式中，在密钥管理功能实体和 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括：网络服务器接收密钥管理功能实体发送的解密请求；网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到网络服务器的签名；网络服务器生成携带网络服务器的签名的解密应答发送给密钥管理功能实体，密钥管理功能实体生成携带网络服务器的签名的密钥获取请求发送给 UE，并接收 UE 使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥转发给中间设备。

在第三方面的第三种可能的实现方式中，在密钥管理功能实体和 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括：网络服务器接收中间设备发送的密钥获取请求，密钥获取请求中携带 UE 的签名和第五密钥，UE 的签名是 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，第五密钥和第六密钥对应；网络服务器使用第五密钥对 UE 的签名进行解密，在得到

第二确认信息时确定验证通过；在验证通过后，网络服务器向中间设备发送第一密钥。

在第三方面的第四种可能的实现方式中，在密钥管理功能实体和UE的协助下，网络服务器协助中间设备获取第一密钥，包括：网络服务器接收密钥管理功能实体发送的密钥获取请求，密钥获取请求中携带UE的签名和第五密钥，UE的签名是UE使用第六密钥对协商成功的第二确认信息进行加密得到的，第五密钥和第六密钥对应；网络服务器使用第五密钥对UE的签名进行解密，在得到第二确认信息时确定验证通过；在验证通过后，网络服务器向密钥管理功能实体发送第一密钥，第一密钥由密钥管理功能实体发送给中间设备。

在第三方面的第五种可能的实现方式中，所述在密钥管理功能实体和所述UE的协助下，所述网络服务器协助所述中间设备获取所述第一密钥，包括：所述网络服务器接收所述密钥管理功能实体发送的密钥获取请求；所述网络服务器在确定所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

第四方面，提供了一种业务处理装置，所述装置包括至少一个单元，该至少一个单元用于实现上述第一方面或第一方面的至少一种实现方式中所提供的业务处理方法。

第五方面，提供了一种业务处理装置，所述装置包括至少一个单元，该至少一个单元用于实现上述第二方面或第二方面的至少一种实现方式中所提供的业务处理方法。

第六方面，提供了一种业务处理装置，所述装置包括至少一个单元，该至少一个单元用于实现上述第三方面或第三方面的至少一种实现方式中所提供的业务处理方法。

第七方面，提供了一种业务处理装置，该装置包括：处理器、以及与处理耦合的收发信机；该收发信机被配置为由处理器控制，该处理器用于实现上述第一方面或第一方面的至少一种实现中所提供的业务处理方法。

第八方面，提供了一种业务处理装置，该装置包括：处理器、以及与处理耦合的收发信机；该收发信机被配置为由处理器控制，该处理器用于实现上述第二方面或第二方面的至少一种实现中所提供的业务处理方法。

第九方面，提供了一种业务处理装置，该装置包括：处理器、以及与处理

耦合的收发信机；该收发信机被配置为由处理器控制，该处理器用于实现上述第三方面或第三方面的至少一种实现中所提供的业务处理方法。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明实施例提供的业务处理系统的结构示意图；

图 2 是本发明实施例提供的设备的结构示意图；

图 3 是本发明实施例提供的一种业务处理方法的方法流程图；

图 4 是本发明实施例提供的一种业务处理方法的方法流程图；

图 5 是本发明实施例提供的一种业务处理方法的方法流程图；

图 6A 是本发明实施例提供的一种业务处理方法的方法流程图；

图 6B 是本发明实施例提供的一种业务处理方法的实施示意图；

图 7A 是本发明实施例提供的一种业务处理方法的方法流程图；

图 7B 是本发明实施例提供的一种业务处理方法的实施示意图；

图 8A 是本发明实施例提供的一种业务处理方法的方法流程图；

图 8B 是本发明实施例提供的一种业务处理方法的实施示意图；

图 9A 是本发明实施例提供的一种业务处理方法的方法流程图；

图 9B 是本发明实施例提供的一种业务处理方法的实施示意图；

图 10A 是本发明实施例提供的一种业务处理方法的方法流程图；

图 10B 是本发明实施例提供的一种业务处理方法的实施示意图；

图 11 是本发明实施例提供的一种业务处理装置的结构示意图；

图 12 是本发明实施例提供的一种业务处理装置的结构示意图；

图 13 是本发明实施例提供的一种业务处理装置的结构示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

请参考图 1，其示出了本发明一个示例性实施例提供的业务处理系统的结构示意图。该业务处理系统包括 UE120、密钥管理功能实体（key management function entity）140、中间设备 160 和网络服务器 180。

在第一种实施场景中，UE120 与密钥管理功能实体 140 建立加密连接，密钥管理功能实体 140 分别与中间设备 160 和网络服务器 180 建立加密连接。

在第二种实施场景中，UE120 与密钥管理功能实体 140 建立加密连接，密钥管理功能实体 140 与中间设备 160 建立加密连接，中间设备 160 与网络服务器 180 建立加密连接。

在第三种实施场景中，密钥管理功能实体 140 分别与中间设备 160 和网络服务器 180 建立加密连接。

其中，加密连接可以是基于下层使用了 SSL 协议/ TLS 协议的 HTTPS 的连接。

UE120 可以是移动电话（英文：cellphone），智能手机（英文：smartphone），计算机（英文：computer），平板电脑（英文：tablet computer），可穿戴设备（英文：wearable device），个人数码助理（英文：personal digital assistant，PDA），移动互联网设备（英文：mobile Internet device，MID）和电子书阅读器（英文：e-book reader）等。

密钥管理功能实体 140 用于管理密钥，可以是可信且权威的服务器，如运营商服务器等，可以通过数字证书向 UE 验证其身份。例如，密钥管理功能实体的域名为 KeyManagement function entity.node.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

中间设备 160 可以是 TLS 代理、边缘服务器（英文：edge server）等等，且边缘服务器可以包括内容分发网络（英文：Content Delivery Network；简称：CDN）服务器，本实施例不作限定。

请参考图 2，其示出了本发明另一个示例性实施例示出的设备 200 的结构示意图。该设备 200 可以是图 1 中所示出的 UE120 或密钥管理功能实体 140 或中间设备 160 或网络服务器 180，该无线设备 200 包括：处理器 220、与处理器 220 耦合的收发信机 240。

该收发信机 240 可由一个或多个天线组成，该天线使得设备 200 能够发送或接收无线电信号。

收发信机240可连接至通信电路260，该通信电路260可对经由收发信机240接收或经由收发信机240发送的信号执行各种处理，如：调制经由收发信机240发送的信号，解调经由收发信机240接收的信号，在实际实现时，该通信电路260可由射频（英文：radio frequency，RF）芯片和基带芯片组成。

通信电路260可连接至处理器220。可替换的该通信电路260也可集成在处理器220中。处理器220是设备200的控制中心，该处理器220可以是中央处理器（英文：central processing unit ，CPU），网络处理器（英文：network processor，NP）或者CPU和NP的组合。处理器220还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路（英文：application-specific integrated circuit，ASIC），可编程逻辑器件（英文：programmable logic device，PLD）或其组合。上述PLD可以是复杂可编程逻辑器件（英文：complex programmable logic device，CPLD），现场可编程逻辑门阵列（英文：field-programmable gate array，FPGA），通用阵列逻辑（英文：generic array logic，GAL）或其任意组合。

存储器280用总线或其它方式与处理器220相连，存储器280可以为易失性存储器(英文: volatile memory)，非易失性存储器(英文: non-volatile memory)或者它们的组合。易失性存储器可以为随机存取存储器（英文：random-access memory，RAM），例如静态随机存取存储器(英文: static random access memory，SRAM)，动态随机存取存储器(英文: dynamic random access memory，DRAM)。非易失性存储器可以为只读存储器（英文：read only memory image，ROM），例如可编程只读存储器（英文：programmable read only memory，PROM），可擦除可编程只读存储器（英文：erasable programmable read only memory，EPROM)，电可擦除可编程只读存储器(英文: electrically erasable programmable read-only memory，EEPROM)。非易失性存储器也可以为快闪存储器（英文：flash memory)，磁存储器，例如磁带(英文: magnetic tape)，软盘(英文: floppy disk)，硬盘。非易失性存储器也可以为光盘。

请参见图3，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法可以包括:

步骤301，密钥管理功能实体接收中间设备发送的触发信息，触发信息是UE启动与网络服务器建立加密连接的流程后得到的。

步骤 302，密钥管理功能实体根据该触发信息，协助中间设备与 UE 和网络服务器协商，以使中间设备得到第一密钥，第一密钥用于供中间设备对 UE 和网络服务器发送的密文进行解密，密文由 UE 或网络服务器使用第二密钥对业务信息进行加密得到，第一密钥与第二密钥对应。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，中间设备需要在密钥管理功能实体的协助下与 UE 和服务器进行协商，在协商成功后得到第一密钥，再使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 4，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法可以包括:

步骤 401，在密钥管理功能实体和网络服务器的协助下，UE 协助中间设备获取第一密钥。

步骤 402，UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文。

步骤 403，UE 接收中间设备转发的密文，密文由网络服务器使用第二密钥对业务信息进行加密得到并发送给中间设备。

其中，第一密钥用于供中间设备对密文进行解密，且第一密钥与第二密钥对应。

其中，步骤 402 和步骤 403 可以择一执行。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备和网络服务器提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 5，其示出了本发明实施例提供的一种业务处理方法的方法流程

图。该业务处理方法可以包括:

步骤 501，在密钥管理功能实体和 UE 的协助下，网络服务器协助中间设备获取第一密钥。

步骤 502，网络服务器接收中间设备转发的密文，密文由 UE 使用第二密钥对业务信息进行加密得到并发送给中间设备。

步骤 503，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文。

其中，第一密钥用于供中间设备对密文进行解密，第一密钥与第二密钥对应。

其中，步骤 502 和步骤 503 可以择一执行。

综上所述，本发明实施例提供的业务处理方法，网络服务器需要在密钥管理功能实体和 UE 的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 6A，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法应用于第一种实施场景中，且密钥管理功能实体根据请求与网络服务器进行协商，协商成功后向 UE 获取所述第一密钥，将第一密钥发送给中间设备，该业务处理方法可以包括:

步骤 601，密钥管理功能实体接收中间设备发送的触发信息，该触发信息是 UE 启动与网络服务器建立加密连接的流程后得到的。

若 UE 需要访问网络服务器，需要先与网络服务器建立连接，该连接可以是基于 HTTP 的非加密连接，也可以是基于下层使用了 SSL 协议/ TLS 协议的 HTTPS 的加密连接，UE 再通过该连接访问网络服务器。

可选的，在 UE 与网络服务器之间还可以设置一个中间设备，该中间设备用于转发 UE 与网络服务器之间传输的数据。具体地，若 UE 与网络服务器建立的是非加密连接，UE 与网络服务器之间传输的数据是明文，此时，中间设备直接转发明文，不对明文进行业务优化；若 UE 与网络服务器建立的是加密连接，UE 与网络服务器之间传输的业务信息是密文，此时，中间设备需要对密文进行解密，并对解密得到的业务信息进行业务优化。由于中间设备对密文

进行解密时需要使用 UE 与网络服务器协商的密钥，因此，中间设备需要向 UE 或网络服务器获取该密钥。

为了获取 UE 与网络服务器协商的密钥，中间设备可以代替网络服务器与 UE 建立加密连接，代替 UE 与网络服务器建立加密连接。

具体地，UE 向网络服务器发送传输控制协议（英文：Transmission Control Protocol；简称：TCP）建立请求，该 TCP 建立请求包括 UE 的因特网协议（英文：Internet Protocol；简称：IP）地址和网络服务器的 IP 地址；中间设备截获 UE 向网络服务器发送的 TCP 建立请求；根据网络服务器的 IP 地址，代替网络服务器与 UE 建立 TCP 连接，并根据 UE 的 IP 地址，代替 UE 与网络服务器建立 TCP 连接；UE 通过 TCP 连接向网络服务器发送加密建立请求；中间设备截获 UE 通过 TCP 连接向网络服务器发送的加密建立请求，根据加密建立请求，代替网络服务器与 UE 建立加密连接，并根据加密建立请求，代替 UE 与网络服务器建立加密连接。

其中，TCP 建立请求中的信息包括源端 IP 地址，源端端口，目的端 IP 地址，目的端端口，源端为 UE，目的端为网络服务器。TCP 连接的端口包括 80 端口和 443 端口，若 UE 需要基于 HTTP 协议访问网络服务器，则 TCP 连接的端口为 80 端口；若 UE 需要基于 HTTPS 协议访问网络服务器，则 TCP 连接的端口为 443 端口。本实施例以 UE 基于 HTTPS 协议访问网络服务器为例进行说明，此时，TCP 连接的端口为 443 端口。

在 TCP 连接的三次握手阶段，中间设备使用网络服务器的 IP 地址作为中间设备的源端 IP 地址，UE 的 IP 地址作为目的端 IP 地址，与 UE 交互完成三次握手，代替网络服务器与 UE 建立 TCP 连接。中间设备向网络服务器发送 TCP 建立请求，该 TCP 建立请求中的源端 IP 地址为 UE 的 IP 地址，目的端 IP 地址为网络服务器的 IP 地址。在 TCP 连接的三次握手阶段，中间设备使用 UE 的 IP 地址作为中间设备的源端 IP 地址，网络服务器的 IP 地址作为目的端 IP 地址，与网络服务器交互完成三次握手，代替 UE 与网络服务器建立 TCP 连接。此时，在 UE 与中间设备之间以及中间设备与网络服务器之间的 TCP 连接建立完成后，UE、中间设备和网络服务器之间形成通路，此时，UE 可以通过 TCP 连接向网络服务器发送加密建立连接。

由于基于 SSL 协议的加密连接和基于 TLS 协议的加密连接的建立过程类似，下文以基于 TLS 协议的加密连接为例进行说明。

1），中间设备截获 UE 向网络服务器发送的 TLS 协议版本号、加密算法列表和第一随机数，并将 TLS 协议版本号、加密算法列表和第一随机数转发给网络服务器。

2），若网络服务器支持该 TLS 协议版本，则从加密算法列表中选择一个加密算法，向 UE 发送 TLS 协议版本号、加密算法、会话标识和第二随机数。

3），中间设备截获网络服务器向 UE 发送的 TLS 协议版本号、加密算法、会话标识和第二随机数，并将 TLS 协议版本号、加密算法、会话标识和第二随机数转发给 UE。

4），中间设备截获网络服务器向 UE 发送的网络服务器的数字证书，并将数字证书转发给 UE。

5），中间设备截获网络服务器向 UE 发送的第一完成消息，并将第一完成消息转发给 UE。

6），UE 对数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，向网络服务器发送得到的公钥交换信息。

此时，UE 根据第一随机数、第二随机数、预主密钥和加密算法生成第二密钥。其中，第二密钥包括客户端写消息验证码（英文：message authentication code；简称：MAC）密钥（client write MAC secret）、服务器写 MAC 密钥（server write MAC secret）、客户端写密钥（client write key）、服务器写密钥（server write key），且客户端写 MAC 密钥和服务器写 MAC 密钥用于验证消息有没有被中途篡改，客户端写密钥用于供客户端加密信息和服务器解密信息，服务器写密钥用于供服务器加密信息和客户端解密信息。

7），中间设备截获 UE 向网络服务器发送的公钥交换信息，并将公钥交换信息转发给网络服务器。

8），中间设备截获 UE 向网络服务器发送的更改密码说明，并将更改密码说明转发给网络服务器，通知网络服务器启动协商好的参数。

9），中间设备截获 UE 向网络服务器发送的第二完成消息，并将第二完成消息转发给网络服务器。

其中，第二完成消息包括哈希值，以便网络服务器根据哈希值进行验证，该哈希值是 UE 对发送给网络服务器的所有内容进行哈希运算得到的。

10），中间设备截获网络服务器向 UE 发送的更改密码说明，并将更改密

码说明转发给 UE，通知 UE 启动协商好的参数。

此时，网络服务器使用私钥解密公钥交换信息，得到预主密钥，根据第一随机数、第二随机数、预主密钥和加密算法生成第二密钥，网络服务器生成的第二密钥与 UE 生成的第二密钥相同。

11），中间设备截获网络服务器向 UE 发送的第三完成消息，并将第三完成消息转发给 UE。

其中，第三完成消息包括哈希值，以便 UE 根据哈希值进行验证，该哈希值是网络服务器对发送给 UE 的所有内容进行哈希运算得到的。

由于中间设备中没有网络服务器的私钥，因此，中间设备无法解密公钥交换信息，从而无法获取第一密钥。其中，第一密钥为预主密钥；或，第一密钥包括第一随机数、第二随机数、预主密钥和加密算法；或，第一密钥为 UE 或网络服务器根据第一随机数、第二随机数、预主密钥和加密算法生成的第二密钥。

本实施例中，中间设备可以从 UE 或网络服务器获取第一密钥。其中，在第一种实现方式中，中间设备从 UE 或网络服务器获取的第一密钥为预主密钥，中间设备再根据之前截获的一随机数、第二随机数和加密算法计算第二密钥；在第二种实现方式中，中间设备从 UE 或网络服务器获取的第一密钥包括第一随机数、第二随机数、预主密钥和加密算法，中间设备再根据第一密钥生成第二密钥；在第三种实现方式中，中间设备从网络服务器或 UE 获取的第一密钥是已经根据第一随机数、第二随机数、预主密钥和加密算法生成的第二密钥，本实施例不作限定。其中，中间设备获取第一密钥的步骤可以在确定 UE 需要与网络服务器建立加密连接之后执行，即，在 UE 向网络服务器发送 TLS 协议版本号、加密算法列表和第一随机数之后执行，且最晚需要在接收到 UE 或网络服务器发送的密文时执行，密文是 UE 或网络服务器使用第二密钥对业务信息进行加密后得到的。

本实施例中，中间设备在密钥管理功能实体的协助下，与 UE 和网络服务器进行协商得到第一密钥。其中，密钥管理功能实体与中间设备可以部署于同一实体，也可以部署于不同的实体，本实施例不作限定。当密钥管理功能实体和中间设备部署于同一实体时，密钥管理功能实体与中间设备可以通过内部模块交互；当密钥管理功能实体与中间设备部署于不同的实体时，密钥管理功能实体需要分别与 UE 和中间设备建立加密连接，密钥管理功能实体与 UE 之间

的交互可以基于 SSL/TLS 协议、IPSEC 等等，密钥管理功能实体与中间设备之间的交互可以基于 SSL/TLS 协议、IPSEC 等等。其中，UE 可以在开机时与密钥管理功能实体建立加密连接，也可以在通信过程中与密钥管理功能实体建立加密连接。密钥管理功能实体可以预先与中间设备建立加密连接，也可以在中间设备需要获取第一密钥时与中间设备建立加密连接。

其中，UE 在与密钥管理功能实体建立加密连接之前，还需要先发现密钥管理功能实体。本实施例提供了两种 UE 发现密钥管理功能实体的发现方式，下面分别对这两种发现方式进行介绍。在第一种发现方式中，在 UE 中配置多个密钥管理功能实体的 IP 地址或域名，UE 可以根据 IP 地址或域名轮流与密钥管理功能实体建立加密连接。在第二种发现方式中，当中间设备和密钥管理功能实体同时位于 PDN 网关（英文：PDN GateWay；简称：PGW）中时，由于 UE 需要接入 PGW，由 PGW 为 UE 分配 IP 地址，因此，UE 可以直接确定密钥管理功能实体，并与该密钥管理功能实体建立加密连接。

触发信息用于指示密钥管理功能实体协助中间设备获取第一密钥。当密钥管理功能实体与中间设备部署于同一实体时，触发信息可以是中间设备截获到的 TLS 协议版本号、加密算法列表和第一随机数，也可以是中间设备截获到的 UE 发送的密文，还可以是上述两种信息的接收时刻之间的任意时刻接收到的信息。当密钥管理功能实体与中间设备部署于不同实体时，触发信息可以是中间设备得到预定信息后向密钥管理功能实体发送的信息，预定信息可以是中间设备截获到的 TLS 协议版本号、加密算法列表和第一随机数，也可以是中间设备截获到的 UE 发送的密文，还可以是上述两种信息的接收时刻之间的任意时刻接收到的信息。

可选的，在密钥管理功能实体协助中间设备获取第一密钥之前，中间设备还可以获取网络服务器的标识，根据网络服务器的标识确定是否需要为 UE 和网络服务器之间传输的数据提供业务优化。具体地，中间设备中预设有白名单，在获取到网络服务器的标识后，检测该网络服务器的标识是否位于白名单中，当该网络服务器的标识位于白名单中时，向密钥管理功能实体发送请求；当该网络服务器的标识未位于白名单中时，结束流程。其中，网络服务器的标识可以是服务器名字指示（英文：Server Name Indication；简称：SNI）或 IP 地址。SNI 可以是中间设备截获 UE 向网络服务器发送的加密连接建立请求中携带的，IP 地址可以是中间设备结果 UE 向网络服务器发送的 TCP 建立请求中携带

的。

步骤 602，当触发信息是中间设备发送的第一密钥获取请求时，密钥管理功能实体向网络服务器发送第一解密请求。

其中，第一密钥获取请求和第一解密请求中都携带会话标识，该会话标识可以是 IP 五元组，以指示第一密钥与会话连接的对应关系。IP 五元组包括 UE 的 IP 地址，网络服务器的 IP 地址，UE 端口，Server 端口，传输协议 TCP。

在一种可能的实现方式中，第一密钥获取请求如下:

ClientKeyRequest:

POST / ClientKeyRequest HTTP/1.1

Host:

KeyManagementFunctionEntity.node.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Content-Type: application/json

Content-Length: 256

{

"protocol": "TLS 1.1",

"session-id": "

session-id-1:client-ip,server-ip,client-port,server-port,transport-protocol",

"decryption-reason":"network optimization",

}

第一解密请求如下:

keyComfirmRequest:

POST / keyComfirmRequest HTTP/1.1

Host : sever.example.com

Content-Type: application/json

Content-Length: 256

{

"protocol": "TLS 1.1",

"session-id": "

session-id-1:client-ip,server-ip,client-port,server-port,transport-protocol",

"decryption-reason":"network optimization",

}

步骤 603，网络服务器接收密钥管理功能实体发送的第一解密请求。

步骤 604，网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到网络服务器的签名。

网络服务器在根据会话标识确定协商成功后，生成第一确认信息，并使用第四密钥对第一确认信息进行加密，得到网络服务器的签名。其中，第四密钥可以是网络服务器的私钥。

步骤 605，网络服务器生成携带网络服务器的签名的第一解密应答发送给密钥管理功能实体。

其中，第一解密应答除了包括网络服务器的签名之外，还需要包括会话标识。

在一种可能的实现方式中，第一解密应答如下：

keyComfirmResponse:

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 13

{

"output": "ok(digital signature of server)"

}

步骤 606，密钥管理功能实体接收网络服务器发送的携带网络服务器的签名的第一解密应答，生成携带网络服务器的签名的第二密钥获取请求发送给 UE。

其中，第二密钥获取请求除了包括网络服务器的签名之外，还需要包括会话标识。

在一种可能的实现方式中，第二密钥获取请求如下：

ClientKeyRequest:

POST / ClientKeyRequest Request HTTP/1.1

Host:

KeyManagementFunctionEntity.node.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Content-Type: application/json

Content-Length: 256

{

"protocol": "TLS 1.1",

"session-id": "
session-id-1:client-ip,server-ip,client-port,server-port,transport-protocol",

“keyComfirmResponse”: "ok(digital signature of server)"

"decryption-reason":"network optimization",

}

步骤 607，UE 接收密钥管理功能实体发送的第二密钥获取请求。

步骤 608，UE 使用第三密钥对网络服务器的签名进行解密，在得到第一确认信息时确定验证通过，第三密钥是 UE 在建立加密连接时从网络服务器中得到的，第三密钥与第四密钥对应。

当第四密钥是网络服务器的私钥时，第三密钥是网络服务器的公钥，且网络服务器的公钥是网络服务器的数字证书中提供的。

步骤 609，在验证通过后，UE 向密钥管理功能实体发送第一密钥，第一密钥由密钥管理功能实体发送给中间设备。

具体地，UE 在验证通过后，根据会话标识确定第一密钥，生成携带第一密钥和会话标识的密钥应答发送给密钥管理功能实体。

若第一密钥为预主密钥，则在一种可能的实现方式中，密钥应答如下：

ClientKeyResponse:

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 64

{

"session-id": "
session-id-1:client-ip,server-ip,client-port,server-port,transport-protocol",

"output": "pre-master secret"

}

步骤 610，密钥管理功能实体接收 UE 使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备。

密钥管理功能实体可以将接收到的密钥应答转发给中间设备，中间设备从

中得到第一密钥。

中间设备在得到第一密钥后，根据第一密钥得到第二密钥，使用第二密钥对 UE 和网络服务器发送的密文进行解密。当中间设备使用第二密钥对 UE 发送的密文进行解密时，执行步骤 611-612；当中间设备使用第二密钥对网络服务器发送的密文进行解密时，执行步骤 613-614。

步骤 611，UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

中间设备在截获到 UE 发送的密文，且根据第一密钥得到第二密钥时，从第二密钥中读取客户端写密钥，使用客户端写密钥对密文进行解密，得到业务信息。在一种实现方式中，中间设备对业务信息进行业务优化，使用客户端写密钥对业务优化后的业务信息进行加密得到密文，将密文发送给网络服务器。在另一种实现方式中，中间设备不对业务信息进行业务优化，直接使用客户端写密钥对业务信息进行加密得到密文，将密文发送给网络服务器。

步骤 612，网络服务器接收中间设备转发的密文。

网络服务器接收到密文，使用客户端写密钥对密文进行解密，得到业务信息，对业务信息进行处理。

步骤 613，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

中间设备在截获到网络服务器发送的密文，且根据第一密钥得到第二密钥时，从第二密钥中读取服务器写密钥，使用服务器写密钥对密文进行解密，得到业务信息。在一种实现方式中，中间设备对业务信息进行业务优化，使用服务器写密钥对业务优化后的业务信息进行加密得到密文，将密文发送给 UE。在另一种实现方式中，中间设备不对业务信息进行业务优化，直接使用服务器写密钥对业务信息进行加密得到密文，将密文发送给 UE。

步骤 614，UE 接收中间设备转发的密文。

UE 接收到密文，使用服务器写密钥对密文进行解密，得到业务信息，对业务信息进行处理。

需要说明的是，当 UE 与中间设备、中间设备与网络服务器之间的加密连接断开时，中间设备继续维护一段时间会话标识和第一密钥的对应关系，使得

后续 UE 与中间设备、中间设备与网络服务器之间快速重连时，中间设备可以直接根据会话标识和对应关系确定第一密钥，而不需要重新向 UE 或网络服务器获取第一密钥，以提高处理效率，下文不再赘述。

请参考图 6B，为了便于理解，本实施例以密钥管理功能实体为 key management function entity、中间设备为 TLS Proxy、网络服务器为 Server 为例，对本实施例的实施过程进行描述。

1、UE 与 key management function entity 建立加密连接，key management function entity 与 Server 建立加密连接。

2、UE 与 TLS Proxy 建立 TCP 连接，TLS Proxy 与 Server 建立 TCP 连接。

具体地，TLS Proxy 截获 UE 向 Server 发送的 TCP 建立请求，根据 Server 的 IP 地址，代替 Server 与 UE 建立 TCP 连接，并根据 UE 的 IP 地址，代替 UE 与 Server 建立 TCP 连接。

3、TLS Proxy 截获 UE 向 Server 发送的 TLS 协议版本号、加密算法列表和第一随机数，并将 TLS 协议版本号、加密算法列表和第一随机数转发给 Server。

4、若 Server 支持该 TLS 协议版本，则从加密算法列表中选择一个加密算法，向 UE 发送 TLS 协议版本号、加密算法、会话标识和第二随机数，TLS Proxy 截获 Server 向 UE 发送的 TLS 协议版本号、加密算法、会话标识和第二随机数，并将 TLS 协议版本号、加密算法、会话标识和第二随机数转发给 UE。

5、Server 向 UE 发送数字证书，TLS Proxy 截获该数字证书，并将该数字证书转发给 UE。

6、Server 向 UE 发送第一完成消息，TLS Proxy 截获该第一完成消息，并将该第一完成消息转发给 UE。

7、UE 对数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，向 Server 发送得到的公钥交换信息，TLS Proxy 截获该公钥交换信息，并将该公钥交换信息转发给 Server。

8、TLS Proxy 与 key management function entity 建立加密连接。

其中，本实施例不限定步骤 1 和 8 与步骤 2-7 的先后执行顺序。

9、TLS Proxy 获取 Server 的标识，根据 Server 的标识确定是否需要启动解密流程，当确定需要启动解密流程时，执行下一步。

10、TLS Proxy 向 key management function entity 发送携带会话标识的密钥

获取请求。

11、key management function entity 向 Server 发送携带会话标识的解密请求。

12、Server 向 key management function entity 发送携带会话标识和 Server 的签名的解密请求应答。

13、key management function entity 向 UE 发送携带会话标识和 Server 的签名的密钥获取请求。

14、UE 在对 Server 的签名的验证通过后，向 key management function entity 发送携带会话标识和第一密钥的密钥应答。

15、key management function entity 向 TLS Proxy 发送携带会话标识和第一密钥的密钥应答。

16、UE 向 Server 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 Server。

17、UE 向 Server 发送第二完成消息，TLS Proxy 截获该第二完成消息，并将该第二完成消息转发给 Server。

18、Server 向 UE 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 UE，通知 UE 启动协商好的参数。

19、Server 向 UE 发送第三完成消息，TLS Proxy 截获该第三完成消息，并将该第三完成消息转发给 UE。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 7A，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法应用于第二种实施场景中，且密钥管理功能实体根据请求确定与网络服务器协商成功后，向 UE 获取第一密钥，将第一密钥发送给中间设备，该业务处理方法可以包括：

步骤 701，密钥管理功能实体接收中间设备发送的触发信息，该触发信息

是 UE 启动与网络服务器建立加密连接的流程后得到的。

其中，步骤 701 详见步骤 601 的描述，此处不作赘述。

步骤 702，中间设备向网络服务器发送第二解密请求。

由于中间设备与网络服务器建立了加密连接，因此，中间设备可以直接向网络服务器发送携带会话标识的第二解密请求。其中，会话标识详见步骤 604 中的描述。

步骤 703，网络服务器接收中间设备发送的第二解密请求。

步骤 704，网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到网络服务器的签名。

网络服务器在根据会话标识确定协商成功后，生成第一确认信息，并使用第四密钥对第一确认信息进行加密，得到网络服务器的签名。其中，第四密钥可以是网络服务器的私钥。

步骤 705，网络服务器生成携带网络服务器的签名的第二解密应答发送给中间设备。

其中，第二解密应答除了包括网络服务器的签名之外，还需要包括会话标识。

步骤 706，中间设备接收网络服务器发送的携带网络服务器的签名的第二解密应答，生成携带网络服务器的签名的第三密钥获取请求发送给密钥管理功能实体。

其中，第三密钥获取请求除了包括网络服务器的签名之外，还需要包括会话标识。

步骤 707，当触发信息是中间设备发送的，且携带网络服务器的签名的第三密钥获取请求时，密钥管理功能实体生成携带网络服务器的签名的第四密钥获取请求发送给 UE。

其中，第四密钥获取请求除了包括网络服务器的签名之外，还需要包括会话标识。

步骤 708，UE 接收密钥管理功能实体发送的第四密钥获取请求。

步骤 709，UE 使用第三密钥对网络服务器的签名进行解密，在得到第一确认信息时确定验证通过，第三密钥是 UE 在建立加密连接时从网络服务器中得到的，第三密钥与第四密钥对应。

当第四密钥是网络服务器的私钥时，第三密钥是网络服务器的公钥，且网

络服务器的公钥是网络服务器的数字证书中提供的。

步骤 710，在验证通过后，UE 向密钥管理功能实体发送第一密钥，第一密钥由密钥管理功能实体发送给中间设备。

具体地，UE 在验证通过后，根据会话标识确定第一密钥，生成携带第一密钥和会话标识的密钥应答发送给密钥管理功能实体。

步骤 711，密钥管理功能实体接收 UE 使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备。

密钥管理功能实体可以将接收到的密钥应答转发给中间设备，中间设备从中得到第一密钥。

中间设备在得到第一密钥后，根据第一密钥得到第二密钥，使用第二密钥对 UE 和网络服务器发送的密文进行解密。当中间设备使用第二密钥对 UE 发送的密文进行解密时，执行步骤 712-713，具体实现流程详见步骤 611-612 的描述；当中间设备使用第二密钥对网络服务器发送的密文进行解密时，执行步骤 714-715，具体实现流程详见步骤 613-614 的描述。

步骤 712，UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 713，网络服务器接收中间设备转发的密文。

步骤 714，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 715，UE 接收中间设备转发的密文。

请参考图 7B，为了便于理解，本实施例以密钥管理功能实体为 key management function entity、中间设备为 TLS Proxy、网络服务器为 Server 为例，对本实施例的实施过程进行描述。

1、UE 与 key management function entity 建立加密连接，key management function entity 与 TLS Proxy 建立加密连接，TLS Proxy 与 Server 建立加密连接。

2、UE 与 TLS Proxy 建立 TCP 连接，TLS Proxy 与 Server 建立 TCP 连接。

具体地，TLS Proxy 截获 UE 向 Server 发送的 TCP 建立请求，根据 Server 的 IP 地址，代替 Server 与 UE 建立 TCP 连接，并根据 UE 的 IP 地址，代替 UE 与 Server 建立 TCP 连接。

3、TLS Proxy 截获 UE 向 Server 发送的 TLS 协议版本号、加密算法列表和第一随机数，并将 TLS 协议版本号、加密算法列表和第一随机数转发给 Server。

4、若 Server 支持该 TLS 协议版本，则从加密算法列表中选择一个加密算法，向 UE 发送 TLS 协议版本号、加密算法、会话标识和第二随机数，TLS Proxy 截获 Server 向 UE 发送的 TLS 协议版本号、加密算法、会话标识和第二随机数，并将 TLS 协议版本号、加密算法、会话标识和第二随机数转发给 UE。

5、Server 向 UE 发送数字证书，TLS Proxy 截获该数字证书，并将该数字证书转发给 UE。

6、Server 向 UE 发送第一完成消息，TLS Proxy 截获该第一完成消息，并将该第一完成消息转发给 UE。

7、UE 对数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，向 Server 发送得到的公钥交换信息，TLS Proxy 截获该公钥交换信息，并将该公钥交换信息转发给 Server。

其中，本实施例不限定步骤 1 与步骤 2-7 的先后执行顺序。

8、TLS Proxy 获取 Server 的标识，根据 Server 的标识确定是否需要启动解密流程，当确定需要启动解密流程时，执行下一步。

9、TLS Proxy 向 Server 发送携带会话标识的解密请求。

10、Server 向 TLS Proxy 发送携带会话标识和 Server 的签名的解密请求应答。

11、TLS Proxy 向 key management function entity 发送携带会话标识和 Server 的签名的密钥获取请求。

12、key management function entity 向 UE 发送携带会话标识和 Server 的签名的密钥获取请求。

13、UE 在对 Server 的签名的验证通过后，向 key management function entity 发送携带会话标识和第一密钥的密钥应答。

14、key management function entity 向 TLS Proxy 发送携带会话标识和第一密钥的密钥应答。

15、UE 向 Server 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 Server。

16、UE 向 Server 发送第二完成消息，TLS Proxy 截获该第二完成消息，

并将该第二完成消息转发给 Server。

17、Server 向 UE 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 UE，通知 UE 启动协商好的参数。

18、Server 向 UE 发送第三完成消息，TLS Proxy 截获该第三完成消息，并将该第三完成消息转发给 UE。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 8A，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法应用于第一种实施场景中，且密钥管理功能实体根据请求与 UE 进行协商，协商成功后向网络服务器获取第一密钥，将第一密钥发送给中间设备，该业务处理方法可以包括:

步骤 801，密钥管理功能实体接收中间设备发送的触发信息，该触发信息是 UE 启动与网络服务器建立加密连接的流程后得到的。

其中，步骤 801 详见步骤 601 的描述，此处不作赘述。

步骤 802，当触发信息是中间设备发送的第五密钥获取请求时，密钥管理功能实体向 UE 发送第三解密请求。

其中，第五密钥获取请求和第三解密请求中都携带会话标识。

步骤 803，UE 接收密钥管理功能实体发送的第三解密请求。

步骤 804，UE 使用第六密钥对协商成功的第二确认信息进行加密，得到 UE 的签名。

UE 在根据会话标识确定协商成功后，生成第一确认信息，并使用第六密钥对第一确认信息进行加密，得到 UE 的签名。其中，第六密钥可以是 UE 的私钥。

步骤 805，UE 生成携带 UE 的签名和第五密钥的第三解密应答发送给密钥管理功能实体，第六密钥与第五密钥对应。

第三解密应答除了包括 UE 的签名之外，还需要包括会话标识和第五密钥。

其中，当第六密钥是UE的私钥时，第五密钥可以是UE的公钥。

可选的，由于第五密钥位于UE的数字证书中，因此，还可以将第三解密应答中的第五密钥替换为UE的数字证书。

步骤806，密钥管理功能实体接收UE发送的携带UE的签名和第五密钥的第三解密应答，生成携带UE的签名和第五密钥的第五密钥获取请求发送给网络服务器。

在一种可能的实现方式中，第三解密应答如下：

keyComfirmResponse:

HTTP/1.1 200 OK

Content-Type: application/json

Content-Length: 13

{

"UE Certificate": "(UE Certificate content)"

"output": "ok"

}

其中，第五密钥获取请求除了包括UE的签名之外，还需要包括会话标识。在一种可能的实现方式中，第五密钥获取如下：

ClientKeyRequest:

POST / ClientKeyRequest Request HTTP/1.1

Host:

KeyManagementFunctionEntity.node.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Content-Type: application/json

Content-Length: 256

{

"protocol": "TLS 1.1",

"session-id": "session-id-1:client-ip,server-ip,client-port,server-port,transport-protocol",

"UE Certificate": "(UE Certificate content)"

“keyComfirmResponse”: "ok(digital signature of UE)",

"decryption-reason":"network optimization",

}

步骤 807，网络服务器接收密钥管理功能实体发送的第五密钥获取请求。

步骤 808，网络服务器使用第五密钥对 UE 的签名进行解密，在得到第二确认信息时确定验证通过。

步骤 809，在验证通过后，网络服务器向密钥管理功能实体发送第一密钥。

具体地，网络服务器在验证通过后，根据会话标识确定第一密钥，生成携带第一密钥和会话标识的密钥应答发送给密钥管理功能实体。

步骤 810，密钥管理功能实体接收网络服务器使用第五密钥对 UE 的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备。

密钥管理功能实体可以将接收到的密钥应答转发给中间设备，中间设备从中得到第一密钥。

中间设备在得到第一密钥后，根据第一密钥得到第二密钥，使用第二密钥对 UE 和网络服务器发送的密文进行解密。当中间设备使用第二密钥对 UE 发送的密文进行解密时，执行步骤 811-812，具体实现流程详见步骤 611-612 的描述；当中间设备使用第二密钥对网络服务器发送的密文进行解密时，执行步骤 813-814，具体实现流程详见步骤 613-614 的描述。

步骤 811，UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 812，网络服务器接收中间设备转发的密文。

步骤 813，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 814，UE 接收中间设备转发的密文。

请参考图 8B，为了便于理解，本实施例以密钥管理功能实体为 key management function entity、中间设备为 TLS Proxy、网络服务器为 Server 为例，对本实施例的实施过程进行描述。

1、UE 与 key management function entity 建立加密连接，key management function entity 与 Server 建立加密连接。

2、UE 与 TLS Proxy 建立 TCP 连接，TLS Proxy 与 Server 建立 TCP 连接。

具体地，TLS Proxy 截获 UE 向 Server 发送的 TCP 建立请求，根据 Server

的 IP 地址，代替 Server 与 UE 建立 TCP 连接，并根据 UE 的 IP 地址，代替 UE 与 Server 建立 TCP 连接。

3、TLS Proxy 截获 UE 向 Server 发送的 TLS 协议版本号、加密算法列表和第一随机数，并将 TLS 协议版本号、加密算法列表和第一随机数转发给 Server。

4、若 Server 支持该 TLS 协议版本，则从加密算法列表中选择一个加密算法，向 UE 发送 TLS 协议版本号、加密算法、会话标识和第二随机数，TLS Proxy 截获 Server 向 UE 发送的 TLS 协议版本号、加密算法、会话标识和第二随机数，并将 TLS 协议版本号、加密算法、会话标识和第二随机数转发给 UE。

5、Server 向 UE 发送数字证书，TLS Proxy 截获该数字证书，并将该数字证书转发给 UE。

6、Server 向 UE 发送第一完成消息，TLS Proxy 截获该第一完成消息，并将该第一完成消息转发给 UE。

7、UE 对数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，向 Server 发送得到的公钥交换信息，TLS Proxy 截获该公钥交换信息，并将该公钥交换信息转发给 Server。

8、TLS Proxy 与 key management function entity 建立加密连接。

其中，本实施例不限定步骤 1 和 8 与步骤 2-7 的先后执行顺序。

9、TLS Proxy 获取 Server 的标识，根据 Server 的标识确定是否需要启动解密流程，当确定需要启动解密流程时，执行下一步。

10、TLS Proxy 向 key management function entity 发送携带会话标识的密钥获取请求。

11、key management function entity 向 UE 发送携带会话标识的解密请求。

12、UE 向 key management function entity 发送携带会话标识、UE 的签名和 UE 的数字证书的解密请求应答。

13、key management function entity 向 Server 发送携带会话标识、Server 的签名和 UE 的数字证书的密钥获取请求。

14、Server 在对 UE 的签名的验证通过后，向 key management function entity 发送携带会话标识和第一密钥的密钥应答。

15、key management function entity 向 TLS Proxy 发送携带会话标识和第一密钥的密钥应答。

16、UE 向 Server 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 Server。

17、UE 向 Server 发送第二完成消息，TLS Proxy 截获该第二完成消息，并将该第二完成消息转发给 Server。

18、Server 向 UE 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 UE，通知 UE 启动协商好的参数。

19、Server 向 UE 发送第三完成消息，TLS Proxy 截获该第三完成消息，并将该第三完成消息转发给 UE。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 9A，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法应用于第二种实施场景中，且密钥管理功能实体根据请求与 UE 进行协商，协商成功后触发中间设备向网络服务器获取第一密钥，该业务处理方法可以包括:

步骤 901，密钥管理功能实体接收中间设备发送的触发信息，该触发信息是 UE 启动与网络服务器建立加密连接的流程后得到的。

其中，步骤 901 详见步骤 601 的描述，此处不作赘述。

步骤 902，当触发信息是中间设备发送的第四解密请求时，密钥管理功能实体将第四解密请求转发给 UE。

其中，第四解密请求中都携带会话标识。

步骤 903，UE 接收密钥管理功能实体发送的第四解密请求。

步骤 904，UE 使用第六密钥对协商成功的第二确认信息进行加密，得到 UE 的签名。

UE 在根据会话标识确定协商成功后，生成第一确认信息，并使用第六密钥对第一确认信息进行加密，得到 UE 的签名。其中，第六密钥可以是 UE 的私钥。

步骤 905，UE 生成携带 UE 的签名和第五密钥的第四解密应答发送给密钥管理功能实体，第六密钥与第五密钥对应。

第四解密应答除了包括 UE 的签名之外，还需要包括会话标识和第五密钥。其中，当第六密钥是 UE 的私钥时，第五密钥可以是 UE 的公钥。

可选的，由于第五密钥位于 UE 的数字证书中，因此，还可以将第四解密应答中的第五密钥替换为 UE 的数字证书。

步骤 906，密钥管理功能实体接收 UE 发送的携带 UE 的签名和第五密钥的第四解密应答，将第四解密应答转发给中间设备。

步骤 907，中间设备生成携带 UE 的签名和第五密钥的第六密钥获取请求发送给网络服务器。

可选的，当第四解密应答包括 UE 的数字证书时，第六密钥请求中的第五密钥可以替换为 UE 的数字证书。

步骤 908，网络服务器接收中间设备发送的第六密钥获取请求。

步骤 909，网络服务器使用第五密钥对 UE 的签名进行解密，在得到第二确认信息时确定验证通过。

步骤 910，在验证通过后，网络服务器向中间设备发送第一密钥。

具体地，网络服务器在验证通过后，根据会话标识确定第一密钥，生成携带第一密钥和会话标识的密钥应答发送给中间设备。

中间设备在得到第一密钥后，根据第一密钥得到第二密钥，使用第二密钥对 UE 和网络服务器发送的密文进行解密。当中间设备使用第二密钥对 UE 发送的密文进行解密时，执行步骤 911-912，具体实现流程详见步骤 611-612 的描述；当中间设备使用第二密钥对网络服务器发送的密文进行解密时，执行步骤 913-914，具体实现流程详见步骤 613-614 的描述。

步骤 911，UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 912，网络服务器接收中间设备转发的密文。

步骤 913，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 914，UE 接收中间设备转发的密文。

请参考图 9B，为了便于理解，本实施例以密钥管理功能实体为 key management function entity、中间设备为 TLS Proxy、网络服务器为 Server 为例，对本实施例的实施过程进行描述。

1、UE 与 key management function entity 建立加密连接，key management function entity 与 TLS Proxy 建立加密连接，TLS Proxy 与 Server 建立加密连接。

2、UE 与 TLS Proxy 建立 TCP 连接，TLS Proxy 与 Server 建立 TCP 连接。

具体地，TLS Proxy 截获 UE 向 Server 发送的 TCP 建立请求，根据 Server 的 IP 地址，代替 Server 与 UE 建立 TCP 连接，并根据 UE 的 IP 地址，代替 UE 与 Server 建立 TCP 连接。

3、TLS Proxy 截获 UE 向 Server 发送的 TLS 协议版本号、加密算法列表和第一随机数，并将 TLS 协议版本号、加密算法列表和第一随机数转发给 Server。

4、若 Server 支持该 TLS 协议版本，则从加密算法列表中选择一个加密算法，向 UE 发送 TLS 协议版本号、加密算法、会话标识和第二随机数，TLS Proxy 截获 Server 向 UE 发送的 TLS 协议版本号、加密算法、会话标识和第二随机数，并将 TLS 协议版本号、加密算法、会话标识和第二随机数转发给 UE。

5、Server 向 UE 发送数字证书，TLS Proxy 截获该数字证书，并将该数字证书转发给 UE。

6、Server 向 UE 发送第一完成消息，TLS Proxy 截获该第一完成消息，并将该第一完成消息转发给 UE。

7、UE 对数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，向 Server 发送得到的公钥交换信息，TLS Proxy 截获该公钥交换信息，并将该公钥交换信息转发给 Server。

其中，本实施例不限定步骤 1 与步骤 2-7 的先后执行顺序。

8、TLS Proxy 获取 Server 的标识，根据 Server 的标识确定是否需要启动解密流程，当确定需要启动解密流程时，执行下一步。

9、TLS Proxy 向 key management function entity 发送携带会话标识的解密请求。

10、key management function entity 向 UE 发送携带会话标识的解密请求。

11、UE 向 key management function entity 发送携带会话标识、UE 的签名和 UE 的数字证书的解密请求应答。

12、key management function entity 向 TLS Proxy 发送携带会话标识、UE 的签名和 UE 的数字证书的解密请求应答。

13、TLS Proxy 向 Server 发送携带会话标识、UE 的签名和 UE 的数字证书的密钥获取请求。

14、Server 向 TLS Proxy 发送携带会话标识和第一密钥的密钥应答。

15、UE 向 Server 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 Server。

16、UE 向 Server 发送第二完成消息，TLS Proxy 截获该第二完成消息，并将该第二完成消息转发给 Server。

17、Server 向 UE 发送更改密码说明，TLS Proxy 截获该更改密码说明，并将该更改密码说明转发给 UE，通知 UE 启动协商好的参数。

18、Server 向 UE 发送第三完成消息，TLS Proxy 截获该第三完成消息，并将该第三完成消息转发给 UE。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参见图 10A，其示出了本发明实施例提供的一种业务处理方法的方法流程图。该业务处理方法应用于第三种实施场景中，中间设备是边缘服务器，且当密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能实体根据请求向网络服务器获取第一密钥，将第一密钥发送给中间设备，该业务处理方法可以包括:

步骤 1001，密钥管理功能实体接收中间设备发送的。

其中，步骤 1001 详见步骤 601 的描述，此处不作赘述。

步骤 1002，当触发信息是中间设备发送的第七密钥获取请求，且密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能实体将第七密钥获取请求转发给网络服务器。

当密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能

实体不需要与 UE 协商，即可向网络服务器获取第一密钥。具体地，密钥管理功能实体可以将中间设备发送的第七密钥获取请求转发给网络服务器。其中，第七密钥获取请求中携带会话标识。

步骤 1003，网络服务器接收第七密钥获取请求，在确定密钥管理功能实体与网络服务器之间建立有加密连接时，向密钥管理功能实体发送第一密钥。

网络服务器生成携带第一密钥和会话标识的密钥应答发送给密钥管理功能实体。

步骤 1004，密钥管理功能实体接收网络服务器在确定密钥管理功能实体与网络服务器之间建立有加密连接时发送的第一密钥，将第一密钥发送给中间设备。

密钥管理功能实体可以将接收到的密钥应答转发给中间设备，中间设备从中得到第一密钥。

中间设备在得到第一密钥后，根据第一密钥得到第二密钥，使用第二密钥对 UE 和网络服务器发送的密文进行解密。当中间设备使用第二密钥对 UE 发送的密文进行解密时，执行步骤 1005-1006，具体实现流程详见步骤 611-612 的描述；当中间设备使用第二密钥对网络服务器发送的密文进行解密时，执行步骤 1007-1008，具体实现流程详见步骤 613-614 的描述。

步骤 1005，UE 使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 1006，网络服务器接收中间设备转发的密文。

步骤 1007，网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向 UE 发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密。

步骤 1008，UE 接收中间设备转发的密文。

请参考图 10B，为了便于理解，本实施例以密钥管理功能实体为 key management function entity、中间设备为 Edge Server、网络服务器为 Server 为例，对本实施例的实施过程进行描述。

1、key management function entity 与 Edge Server 建立加密连接，key management function entity 与 Server 建立加密连接。

2、UE 与 Edge Server 建立 TCP 连接，Edge Server 与 Server 建立 TCP 连

接。

具体地，Edge Server 截获 UE 向 Server 发送的 TCP 建立请求，根据 Server 的 IP 地址，代替 Server 与 UE 建立 TCP 连接，并根据 UE 的 IP 地址，代替 UE 与 Server 建立 TCP 连接。

3、Edge Server 截获 UE 向 Server 发送的 TLS 协议版本号、加密算法列表和第一随机数，并将 TLS 协议版本号、加密算法列表和第一随机数转发给 Server。

4、若 Server 支持该 TLS 协议版本，则从加密算法列表中选择一个加密算法，向 UE 发送 TLS 协议版本号、加密算法、会话标识和第二随机数，Edge Server 截获 Server 向 UE 发送的 TLS 协议版本号、加密算法、会话标识和第二随机数，并将 TLS 协议版本号、加密算法、会话标识和第二随机数转发给 UE。

5、Server 向 UE 发送数字证书，Edge Server 截获该数字证书，并将该数字证书转发给 UE。

6、Server 向 UE 发送第一完成消息，Edge Server 截获该第一完成消息，并将该第一完成消息转发给 UE。

7、UE 对数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，向 Server 发送得到的公钥交换信息，Edge Server 截获该公钥交换信息，并将该公钥交换信息转发给 Server。

8、Edge Server 获取 Server 的标识，根据 Server 的标识确定是否需要启动解密流程，当确定需要启动解密流程时，执行下一步。

9、Edge Server 向 key management function entity 发送携带会话标识的密钥获取请求。

10、key management function entity 向 Server 发送携带会话标识的密钥获取请求。

11、Server 向 key management function entity 发送携带会话标识和第一密钥的密钥应答。

12、key management function entity 向 Edge Server 发送携带会话标识和第一密钥的密钥应答。

13、UE 向 Server 发送更改密码说明，Edge Server 截获该更改密码说明，并将该更改密码说明转发给 Server。

14、UE 向 Server 发送第二完成消息，Edge Server 截获该第二完成消息，

并将该第二完成消息转发给 Server。

15、Server 向 UE 发送更改密码说明，Edge Server 截获该更改密码说明，并将该更改密码说明转发给 UE，通知 UE 启动协商好的参数。

16、Server 向 UE 发送第三完成消息，Edge Server 截获该第三完成消息，并将该第三完成消息转发给 UE。

综上所述，本发明实施例提供的业务处理方法，由于 UE 与网络服务器之间传输的数据需要经过中间设备转发，且中间设备对 UE 来说是透明的，此时，UE 需要在密钥管理功能实体和网络服务器的协助下触发中间设备获取第一密钥，以便中间设备使用第一密钥来解密 UE 与网络服务器之间传输的密文，提供业务优化，解决了中间设备无法解密密文，导致中间设备无法为用户设备提供业务优化的问题，达到了扩大业务优化的使用范围的效果。

请参考图 11，其示出了本发明实施例提供的一种业务处理装置的结构示意图。该业务处理装置可由硬件或者软硬件的集合实现成为上述密钥管理功能实体的全部或一部分。该业务处理装置可以包括：

接收单元 1110 用于实现上述实施例步骤 301 中的功能；

协助单元 1120 用于实现上述实施例步骤 302 中的功能。

需要说明的是，上述的接收单元 1110 可以通过密钥管理功能实体中的收发信机来实现；上述的协助单元 1120 可以通过密钥管理功能实体中的处理器来实现。

请参考图 12，其示出了本发明实施例提供的一种业务处理装置的结构示意图。该业务处理装置可由硬件或者软硬件的集合实现成为上述 UE 的全部或一部分。该业务处理装置可以包括：

协助单元 1210 用于实现上述实施例步骤 401 中的功能；

发送单元 1220 用于实现上述实施例步骤 402 中的功能；

接收单元 1230 用于实现上述实施例步骤 403 中的功能。

需要说明的是，上述的协助单元 1210 可以通过 UE 中的处理器来实现；上述的发送单元 1220 和接收单元 1230 可以通过 UE 中的收发信机来实现。

请参考图 13，其示出了本发明实施例提供的一种业务处理装置的结构示意

图。该业务处理装置可由硬件或者软硬件的集合实现成为上述网络服务器的全部或一部分。该业务处理装置可以包括:

协助单元 1310 用于实现上述实施例步骤 501 的功能;

接收单元 1320 用于实现上述实施例步骤 502 中的功能;

发送单元 1330 用于实现上述实施例步骤 503 中的功能。

需要说明的是,上述的协助单元 1310 可以通过网络服务器中的处理器来实现;上述的接收单元 1320 和发送单元 1330 可以通过网络服务器中的收发信机来实现。

需要说明的是:上述实施例提供的业务处理装置在进行业务处理时,仅以上述各功能模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能模块完成,即将业务处理装置的内部结构划分成不同的功能模块,以完成以上描述的全部或者部分功能。另外,上述实施例提供的业务处理装置与业务处理方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

本领域普通技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能,但是这种实现不应认为超出本发明的范围。

所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

在本申请所提供的几个实施例中,应该理解到,所揭露的系统、装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,可以仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

权 利 要 求 书

1、一种业务处理方法，其特征在于，所述方法包括:

密钥管理功能实体接收触发信息，所述触发信息是用户设备 UE 启动与网络服务器建立加密连接的流程后得到的;

所述密钥管理功能实体根据所述触发信息，协助中间设备与所述 UE 和所述网络服务器协商，以使所述中间设备得到第一密钥，所述第一密钥用于供所述中间设备对所述 UE 和所述网络服务器发送的密文进行解密，所述密文由所述 UE 或所述网络服务器使用第二密钥对业务信息进行加密得到，所述第一密钥与所述第二密钥对应。

2、根据权利要求 1 所述的方法，其特征在于，所述密钥管理功能实体根据所述触发信息，协助中间设备与所述 UE 和所述网络服务器协商，以使所述中间设备得到第一密钥，包括:

所述密钥管理功能实体根据所述触发信息确定与所述网络服务器协商成功后，向所述 UE 获取所述第一密钥，将所述第一密钥发送给所述中间设备; 或者，

所述密钥管理功能实体根据所述触发信息与所述 UE 进行协商，协商成功后向所述网络服务器获取所述第一密钥，将所述第一密钥发送给所述中间设备; 或者，

所述密钥管理功能实体根据所述触发信息与所述 UE 进行协商，协商成功后触发所述中间设备向所述网络服务器获取所述第一密钥; 或者，

当所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，所述密钥管理功能实体根据所述触发信息向所述网络服务器获取所述第一密钥，将所述第一密钥发送给所述中间设备。

3、根据权利要求 2 所述的方法，其特征在于，所述密钥管理功能实体根据所述触发信息确定与所述网络服务器协商成功后，向所述 UE 获取所述第一密钥，将所述第一密钥发送给所述中间设备，包括:

当所述触发信息是所述中间设备发送的第一密钥获取请求时，所述密钥管理功能实体向所述网络服务器发送第一解密请求，接收所述网络服务器发送的携带所述网络服务器的签名的第一解密应答，生成携带所述网络服务器的签名的第二密钥获取请求发送给所述 UE，接收所述 UE 使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间

设备；或者，

当所述触发信息是所述中间设备发送的，且携带所述网络服务器的签名的第三密钥获取请求时，所述密钥管理功能实体生成携带所述网络服务器的签名的第四密钥获取请求发送给所述 UE，接收所述 UE 使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间设备，所述网络服务器的签名是所述中间设备向所述网络服务器发送第二解密请求后，从得到的第二解密应答中得到的；

其中，所述第三密钥是所述 UE 在建立所述加密连接时从所述网络服务器中得到的，所述网络服务器的签名是所述网络服务器使用第四密钥对协商成功的第一确认信息进行加密得到的，所述第四密钥与所述第三密钥对应。

4、根据权利要求 2 所述的方法，其特征在于，所述密钥管理功能实体根据所述触发信息与所述 UE 进行协商，协商成功后向所述网络服务器获取所述第一密钥，将所述第一密钥发送给所述中间设备，包括：

当所述触发信息是所述中间设备发送的第五密钥获取请求时，所述密钥管理功能实体向所述 UE 发送第三解密请求，接收所述 UE 发送的携带所述 UE 的签名和第五密钥的第三解密应答，生成携带所述 UE 的签名和所述第五密钥的第五密钥获取请求发送给所述网络服务器，接收所述网络服务器使用所述第五密钥对所述 UE 的签名验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间设备；

其中，所述 UE 的签名信息是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第六密钥与所述第五密钥对应。

5、根据权利要求 2 所述的方法，其特征在于，所述密钥管理功能实体根据所述触发信息与所述 UE 进行协商，协商成功后触发所述中间设备向所述网络服务器获取所述第一密钥，包括：

当所述触发信息是所述中间设备发送的第四解密请求时，所述密钥管理功能实体将所述第四解密请求转发给所述 UE，接收所述 UE 发送的携带所述 UE 的签名和第五密钥的第四解密应答，将所述第四解密应答转发给所述中间设备，所述第四解密应答用于指示所述中间设备向所述网络服务器发送携带所述 UE 的签名和所述第五密钥的第六密钥获取请求，并接收所述网络服务器使用所述第五密钥对所述 UE 的签名验证通过后发送的所述第一密钥；

其中，所述 UE 的签名信息是所述 UE 使用第六密钥对协商成功的第二确认

信息进行加密得到的，所述第六密钥与所述第五密钥对应。

6、根据权利要求 2 所述的方法，其特征在于，当所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，所述密钥管理功能实体根据所述触发信息向所述网络服务器获取所述第一密钥，将所述第一密钥发送给所述中间设备，包括:

当所述触发信息是所述中间设备发送的第七密钥获取请求，且所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，所述密钥管理功能实体将所述第七密钥获取请求转发给所述网络服务器，并接收所述网络服务器在确定所述密钥管理功能实体与所述网络服务器之间建立有加密连接时发送的所述第一密钥，将所述第一密钥发送给所述中间设备。

7、一种业务处理方法，其特征在于，所述方法包括:

在密钥管理功能实体和网络服务器的协助下，用户设备 UE 协助中间设备获取第一密钥;

所述 UE 使用第二密钥对业务信息进行加密得到密文，经过所述中间设备向所述网络服务器发送所述密文；或者，

所述 UE 接收所述中间设备转发的密文，所述密文由所述网络服务器使用第二密钥对业务信息进行加密得到并发送给所述中间设备;

其中，所述第一密钥用于供所述中间设备对所述密文进行解密，且所述第一密钥与所述第二密钥对应。

8、根据权利要求 7 所述的方法，其特征在于，所述在密钥管理功能实体和网络服务器的协助下，用户设备 UE 协助中间设备获取第一密钥，包括:

所述 UE 接收所述密钥管理功能实体发送的密钥获取请求，所述密钥获取请求中携带所述网络服务器的签名，所述服务器的签名是所述网络服务器使用第四密钥对协商成功的第一确认信息进行加密得到的;

所述 UE 使用第三密钥对所述网络服务器的签名进行解密，在得到所述第一确认信息时确定验证通过，所述第三密钥是所述 UE 在建立所述加密连接时从所述网络服务器中得到的，所述第三密钥与所述第四密钥对应;

在验证通过后，所述 UE 向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

9、根据权利要求 7 所述的方法，其特征在于，所述在密钥管理功能实体和网络服务器的协助下，用户设备 UE 协助中间设备获取第一密钥，包括:

所述 UE 接收所述密钥管理功能实体发送的解密请求;

所述 UE 使用第六密钥对协商成功的第二确认信息进行加密，得到所述 UE 的签名;

所述 UE 生成携带所述 UE 的签名和第五密钥的解密应答发送给所述密钥管理功能实体，所述密钥管理功能实体用于将所述解密应答发送给所述中间设备，所述中间设备用于生成携带所述 UE 的签名和所述第五密钥的密钥获取请求发送给所述网络服务器，并接收所述网络服务器使用所述第五密钥对所述 UE 的签名的验证通过后发送的所述第一密钥；或者，所述密钥管理功能实体用于生成携带所述 UE 的签名和所述第五密钥的密钥获取请求发送给所述网络服务器，并获取所述网络服务器使用所述第五密钥对所述 UE 的签名的验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间设备，所述第五密钥与所述第六密钥对应。

10、一种业务处理方法，其特征在于，所述方法包括:

在密钥管理功能实体和用户设备 UE 的协助下，网络服务器协助中间设备获取第一密钥;

所述网络服务器接收所述中间设备转发的密文，所述密文由所述 UE 使用第二密钥对业务信息进行加密得到并发送给所述中间设备；或者，

所述网络服务器使用第二密钥对业务信息进行加密得到密文，经过所述中间设备向所述 UE 发送所述密文;

其中，所述第一密钥用于供所述中间设备对所述密文进行解密，所述第一密钥与所述第二密钥对应。

11、根据权利要求 10 所述的方法，其特征在于，所述在密钥管理功能实体和用户设备 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括:

所述网络服务器接收所述中间设备发送的解密请求;

所述网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到所述网络服务器的签名;

所述网络服务器生成携带所述网络服务器的签名的解密应答发送给所述中间设备，所述中间设备用于生成携带所述网络服务器的签名的密钥获取请求发送给所述密钥管理功能实体，所述密钥管理功能实体用于将所述密钥获取请求转发给所述 UE，并接收所述 UE 使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥转发给所述中间设备。

12、根据权利要求 10 所述的方法，其特征在于，所述在密钥管理功能实体和用户设备 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括:

所述网络服务器接收所述密钥管理功能实体发送的解密请求;

所述网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到所述网络服务器的签名;

所述网络服务器生成携带所述网络服务器的签名的解密应答发送给所述密钥管理功能实体，所述密钥管理功能实体生成携带所述网络服务器的签名的密钥获取请求发送给所述 UE，并接收所述 UE 使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥转发给所述中间设备。

13、根据权利要求 10 所述的方法，其特征在于，所述在密钥管理功能实体和用户设备 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括:

所述网络服务器接收所述中间设备发送的密钥获取请求，所述密钥获取请求中携带所述 UE 的签名和第五密钥，所述 UE 的签名是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第五密钥和所述第六密钥对应;

所述网络服务器使用所述第五密钥对所述 UE 的签名进行解密，在得到所述第二确认信息时确定验证通过;

在验证通过后，所述网络服务器向所述中间设备发送所述第一密钥。

14、根据权利要求 10 所述的方法，其特征在于，所述在密钥管理功能实体和用户设备 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括:

所述网络服务器接收所述密钥管理功能实体发送的密钥获取请求，所述密钥获取请求中携带所述 UE 的签名和第五密钥，所述 UE 的签名是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第五密钥和所述第六密钥对应;

所述网络服务器使用所述第五密钥对所述 UE 的签名进行解密，在得到所述第二确认信息时确定验证通过;

在验证通过后，所述网络服务器向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

15、根据权利要求 10 所述的方法，其特征在于，所述在密钥管理功能实体和用户设备 UE 的协助下，网络服务器协助中间设备获取第一密钥，包括:

所述网络服务器接收所述密钥管理功能实体发送的密钥获取请求;

所述网络服务器在确定所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

16、一种业务处理装置，其特征在于，用于密钥管理功能实体中，所述装置包括:

接收单元，用于接收中间设备发送的触发信息，所述触发信息是用户设备UE启动与网络服务器建立加密连接的流程后得到的;

协助单元，用于根据所述接收单元接收的所述触发信息，协助中间设备与所述UE和所述网络服务器协商，以使所述中间设备得到第一密钥，所述第一密钥用于供所述中间设备对所述UE和所述网络服务器发送的密文进行解密，所述密文由所述UE或所述网络服务器使用第二密钥对业务信息进行加密得到，所述第一密钥与所述第二密钥对应。

17、根据权利要求16所述的装置，其特征在于，所述协助单元，包括:

根据所述触发信息确定与所述网络服务器协商成功后，向所述UE获取所述第一密钥，将所述第一密钥发送给所述中间设备；或者，

根据所述触发信息与所述UE进行协商，协商成功后向所述网络服务器获取所述第一密钥，将所述第一密钥发送给所述中间设备；或者，

根据所述触发信息与所述UE进行协商，协商成功后触发所述中间设备向所述网络服务器获取所述第一密钥；或者，

当所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，根据所述触发信息向所述网络服务器获取所述第一密钥，将所述第一密钥发送给所述中间设备。

18、根据权利要求17所述的装置，其特征在于，所述协助单元，还用于:

当所述触发信息是所述中间设备发送的第一密钥获取请求时，向所述网络服务器发送第一解密请求，接收所述网络服务器发送的携带所述网络服务器的签名的第一解密应答，生成携带所述网络服务器的签名的第二密钥获取请求发送给所述UE，接收所述UE使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间设备；或者，

当所述触发信息是所述中间设备发送的，且携带所述网络服务器的签名的第三密钥获取请求时，生成携带所述网络服务器的签名的第四密钥获取请求发送给所述UE，接收所述UE使用第三密钥对所述网络服务器的签名验证通过后

发送的所述第一密钥，将所述第一密钥发送给所述中间设备，所述网络服务器的签名是所述中间设备向所述网络服务器发送第二解密请求后，从得到的第二解密应答中得到的；

其中，所述第三密钥是所述 UE 在建立所述加密连接时从所述网络服务器中得到的，所述网络服务器的签名是所述网络服务器使用第四密钥对协商成功的第一确认信息进行加密得到的，所述第四密钥与所述第三密钥对应。

19、根据权利要求 17 所述的装置，其特征在于，所述协助单元，还用于：

当所述触发信息是所述中间设备发送的第五密钥获取请求时，向所述 UE 发送第三解密请求，接收所述 UE 发送的携带所述 UE 的签名和第五密钥的第三解密应答，生成携带所述 UE 的签名和所述第五密钥的第五密钥获取请求发送给所述网络服务器，接收所述网络服务器使用所述第五密钥对所述 UE 的签名验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间设备；

其中，所述 UE 的签名信息是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第六密钥与所述第五密钥对应。

20、根据权利要求 17 所述的装置，其特征在于，所述协助单元，还用于：

当所述触发信息是所述中间设备发送的第四解密请求时，将所述第四解密请求转发给所述 UE，接收所述 UE 发送的携带所述 UE 的签名和第五密钥的第四解密应答，将所述第四解密应答转发给所述中间设备，所述第四解密应答用于指示所述中间设备向所述网络服务器发送携带所述 UE 的签名和所述第五密钥的第六密钥获取请求，并接收所述网络服务器使用所述第五密钥对所述 UE 的签名验证通过后发送的所述第一密钥；

其中，所述 UE 的签名信息是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第六密钥与所述第五密钥对应。

21、根据权利要求 17 所述的装置，其特征在于，所述协助单元，还用于：

当所述触发信息是所述中间设备发送的第七密钥获取请求，且所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，将所述第七密钥获取请求转发给所述网络服务器，并接收所述网络服务器在确定所述密钥管理功能实体与所述网络服务器之间建立有加密连接时发送的所述第一密钥，将所述第一密钥发送给所述中间设备。

22、一种业务处理装置，其特征在于，用于用户设备 UE 中，所述装置包括：

协助单元，用于在密钥管理功能实体和网络服务器的协助下，协助中间设

备获取第一密钥;

发送单元，用于使用第二密钥对业务信息进行加密得到密文，经过所述中间设备向所述网络服务器发送所述密文；或者，

接收单元，用于接收所述中间设备转发的密文，所述密文由所述网络服务器使用第二密钥对业务信息进行加密得到并发送给所述中间设备;

其中，所述第一密钥用于供所述中间设备对所述密文进行解密，且所述第一密钥与所述第二密钥对应。

23、根据权利要求 22 所述的装置，其特征在于，所述协助单元，还用于:

接收所述密钥管理功能实体发送的密钥获取请求，所述密钥获取请求中携带所述网络服务器的签名，所述服务器的签名是所述网络服务器使用第四密钥对协商成功的第一确认信息进行加密得到的;

使用第三密钥对所述网络服务器的签名进行解密，在得到所述第一确认信息时确定验证通过，所述第三密钥是所述 UE 在建立所述加密连接时从所述网络服务器中得到的，所述第三密钥与所述第四密钥对应;

在验证通过后，向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

24、根据权利要求 22 所述的装置，其特征在于，所述协助单元，还用于:

接收所述密钥管理功能实体发送的解密请求;

使用第六密钥对协商成功的第二确认信息进行加密，得到所述 UE 的签名;

生成携带所述 UE 的签名和第五密钥的解密应答发送给所述密钥管理功能实体，所述密钥管理功能实体用于将所述解密应答发送给所述中间设备，所述中间设备用于生成携带所述 UE 的签名和所述第五密钥的密钥获取请求发送给所述网络服务器，并接收所述网络服务器使用所述第五密钥对所述 UE 的签名的验证通过后发送的所述第一密钥；或者，所述密钥管理功能实体用于生成携带所述 UE 的签名和所述第五密钥的密钥获取请求发送给所述网络服务器，并获取所述网络服务器使用所述第五密钥对所述 UE 的签名的验证通过后发送的所述第一密钥，将所述第一密钥发送给所述中间设备，所述第五密钥与所述第六密钥对应。

25、一种业务处理装置，其特征在于，用于网络服务器中，所述装置包括:

协助单元，用于在密钥管理功能实体和用户设备 UE 的协助下，协助中间设备获取第一密钥;

接收单元，用于接收所述中间设备转发的密文，所述密文由所述 UE 使用第二密钥对业务信息进行加密得到并发送给所述中间设备；或者，

发送单元，用于使用第二密钥对业务信息进行加密得到密文，经过所述中间设备向所述 UE 发送所述密文；

其中，所述第一密钥用于供所述中间设备对所述密文进行解密，所述第一密钥与所述第二密钥对应。

26、根据权利要求 25 所述的装置，其特征在于，所述协助单元，还用于：

接收所述中间设备发送的解密请求；

使用第四密钥对协商成功的第一确认信息进行加密，得到所述网络服务器的签名；

生成携带所述网络服务器的签名的解密应答发送给所述中间设备，所述中间设备用于生成携带所述网络服务器的签名的密钥获取请求发送给所述密钥管理功能实体，所述密钥管理功能实体用于将所述密钥获取请求转发给所述 UE，并接收所述 UE 使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥转发给所述中间设备。

27、根据权利要求 25 所述的装置，其特征在于，所述协助单元，还用于：

接收所述密钥管理功能实体发送的解密请求；

使用第四密钥对协商成功的第一确认信息进行加密，得到所述网络服务器的签名；

生成携带所述网络服务器的签名的解密应答发送给所述密钥管理功能实体，所述密钥管理功能实体生成携带所述网络服务器的签名的密钥获取请求发送给所述 UE，并接收所述 UE 使用第三密钥对所述网络服务器的签名验证通过后发送的所述第一密钥，将所述第一密钥转发给所述中间设备。

28、根据权利要求 25 所述的装置，其特征在于，所述协助单元，还用于：

接收所述中间设备发送的密钥获取请求，所述密钥获取请求中携带所述 UE 的签名和第五密钥，所述 UE 的签名是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第五密钥和所述第六密钥对应；

使用所述第五密钥对所述 UE 的签名进行解密，在得到所述第二确认信息时确定验证通过；

在验证通过后，向所述中间设备发送所述第一密钥。

29、根据权利要求 25 所述的装置，其特征在于，所述协助单元，还用于：

接收所述密钥管理功能实体发送的密钥获取请求，所述密钥获取请求中携带所述 UE 的签名和第五密钥，所述 UE 的签名是所述 UE 使用第六密钥对协商成功的第二确认信息进行加密得到的，所述第五密钥和所述第六密钥对应；

使用所述第五密钥对所述 UE 的签名进行解密，在得到所述第二确认信息时确定验证通过；

在验证通过后，向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

30、根据权利要求 25 所述的装置，其特征在于，所述协助单元，还用于：

接收所述密钥管理功能实体发送的密钥获取请求；

在确定所述密钥管理功能实体与所述网络服务器之间建立有加密连接时，向所述密钥管理功能实体发送所述第一密钥，所述第一密钥由所述密钥管理功能实体发送给所述中间设备。

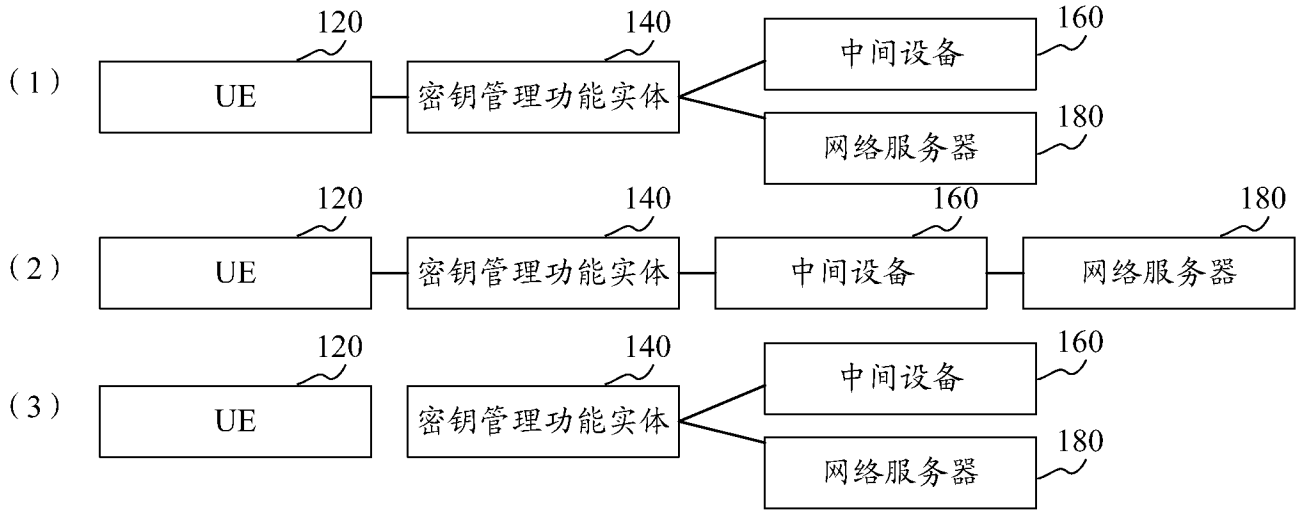
(1)
120
UE
140
密钥管理功能实体
160
中间设备
180
网络服务器
(2)
120
UE
140
密钥管理功能实体
160
中间设备
180
网络服务器
(3)
120
UE
140
密钥管理功能实体
160
中间设备
180
网络服务器

图 1

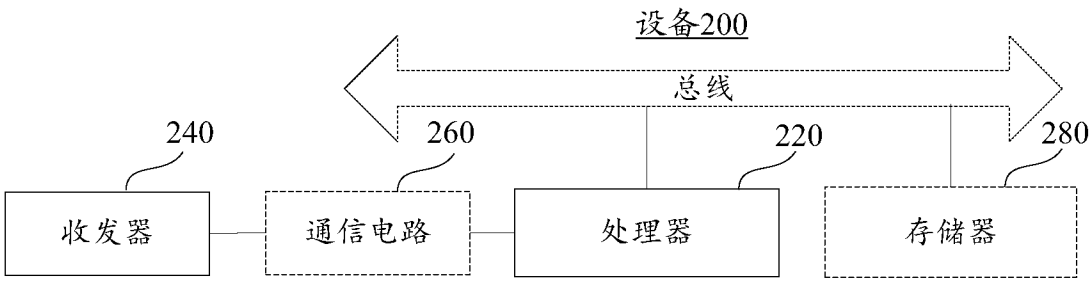
设备200
总线
240
收发器
260
通信电路
220
处理器
280
存储器

图 2

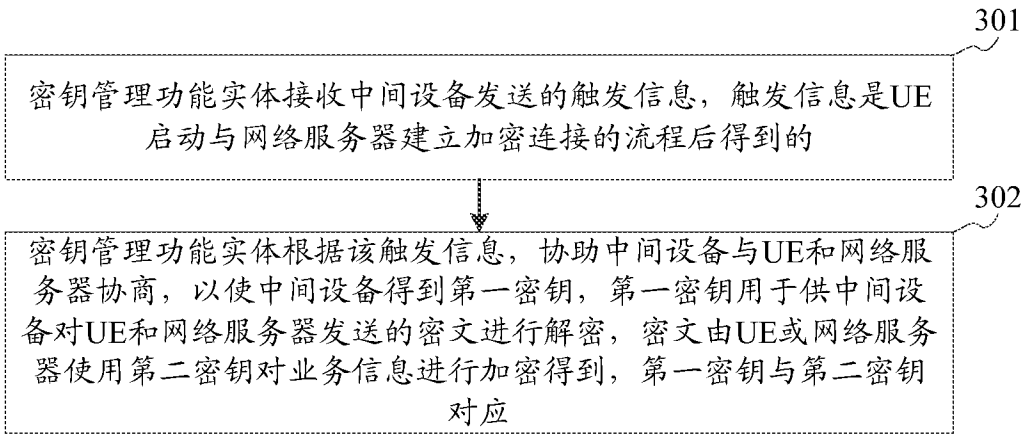
301
密钥管理功能实体接收中间设备发送的触发信息，触发信息是UE启动与网络服务器建立加密连接的流程后得到的
302
密钥管理功能实体根据该触发信息，协助中间设备与UE和网络服务器协商，以使中间设备得到第一密钥，第一密钥用于供中间设备对UE和网络服务器发送的密文进行解密，密文由UE或网络服务器使用第二密钥对业务信息进行加密得到，第一密钥与第二密钥对应

图 3

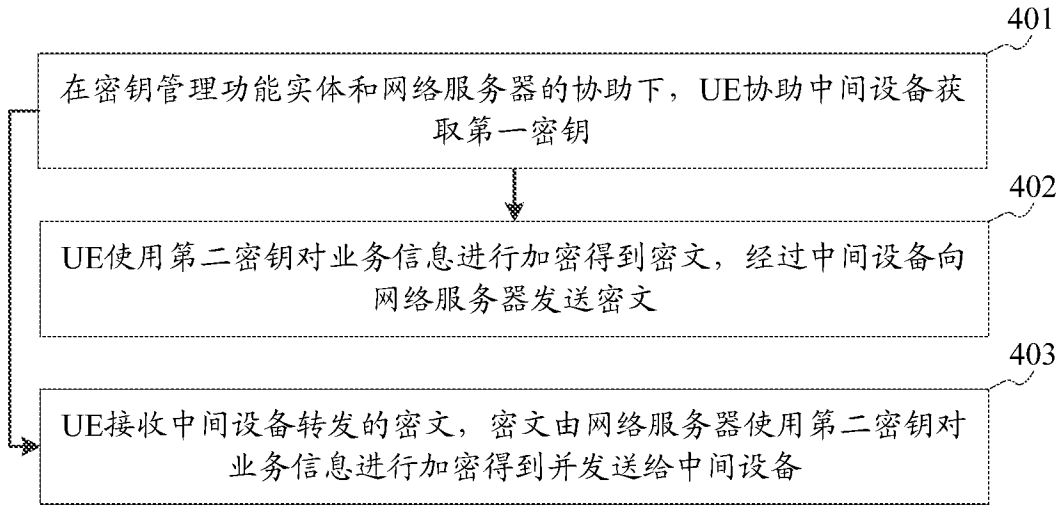
401
在密钥管理功能实体和网络服务器的协助下，UE协助中间设备获取第一密钥
402
UE使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文
403
UE接收中间设备转发的密文，密文由网络服务器使用第二密钥对业务信息进行加密得到并发送给中间设备

图 4

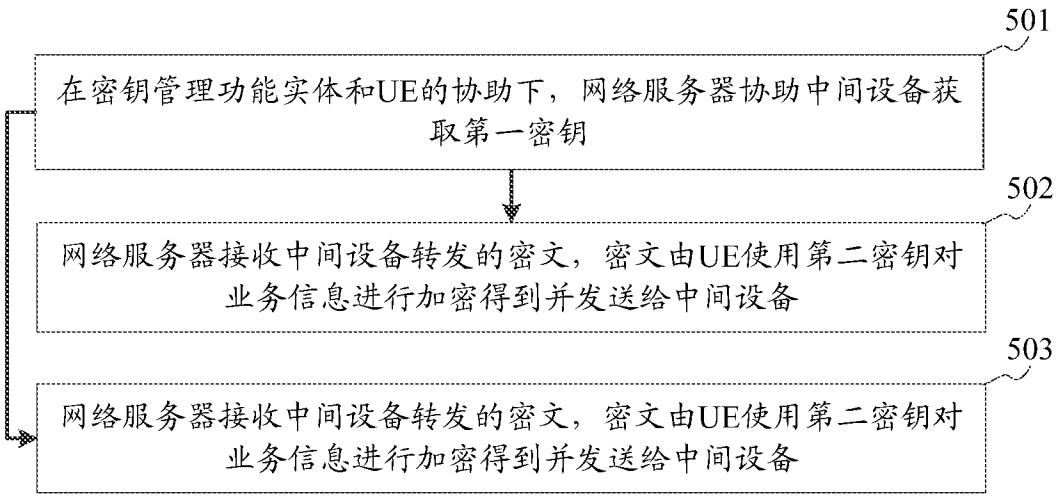
501
在密钥管理功能实体和UE的协助下，网络服务器协助中间设备获取第一密钥
502
网络服务器接收中间设备转发的密文，密文由UE使用第二密钥对业务信息进行加密得到并发送给中间设备
503
网络服务器接收中间设备转发的密文，密文由UE使用第二密钥对业务信息进行加密得到并发送给中间设备

图 5

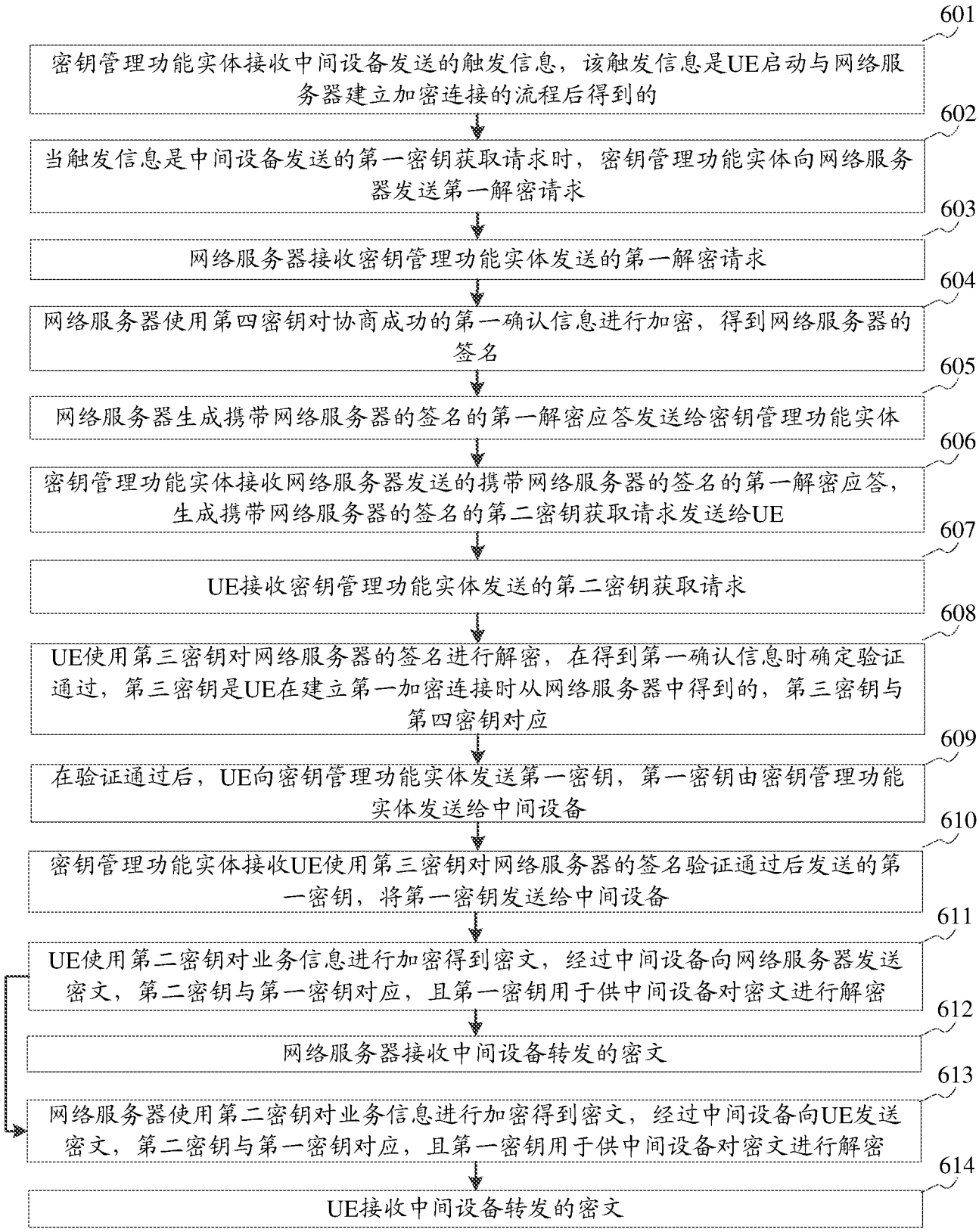
601
密钥管理功能实体接收中间设备发送的触发信息，该触发信息是UE启动与网络服务器建立加密连接的流程后得到的
602
当触发信息是中间设备发送的第一密钥获取请求时，密钥管理功能实体向网络服务器发送第一解密请求
603
网络服务器接收密钥管理功能实体发送的第一解密请求
604
网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到网络服务器的签名
605
网络服务器生成携带网络服务器的签名的第一解密应答发送给密钥管理功能实体
606
密钥管理功能实体接收网络服务器发送的携带网络服务器的签名的第一解密应答，生成携带网络服务器的签名的第二密钥获取请求发送给UE
607
UE接收密钥管理功能实体发送的第二密钥获取请求
608
UE使用第三密钥对网络服务器的签名进行解密，在得到第一确认信息时确定验证通过，第三密钥是UE在建立第一加密连接时从网络服务器中得到的，第三密钥与第四密钥对应
609
在验证通过后，UE向密钥管理功能实体发送第一密钥，第一密钥由密钥管理功能实体发送给中间设备
610
密钥管理功能实体接收UE使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备
611
UE使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
612
网络服务器接收中间设备转发的密文
613
网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向UE发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
614
UE接收中间设备转发的密文

图 6A

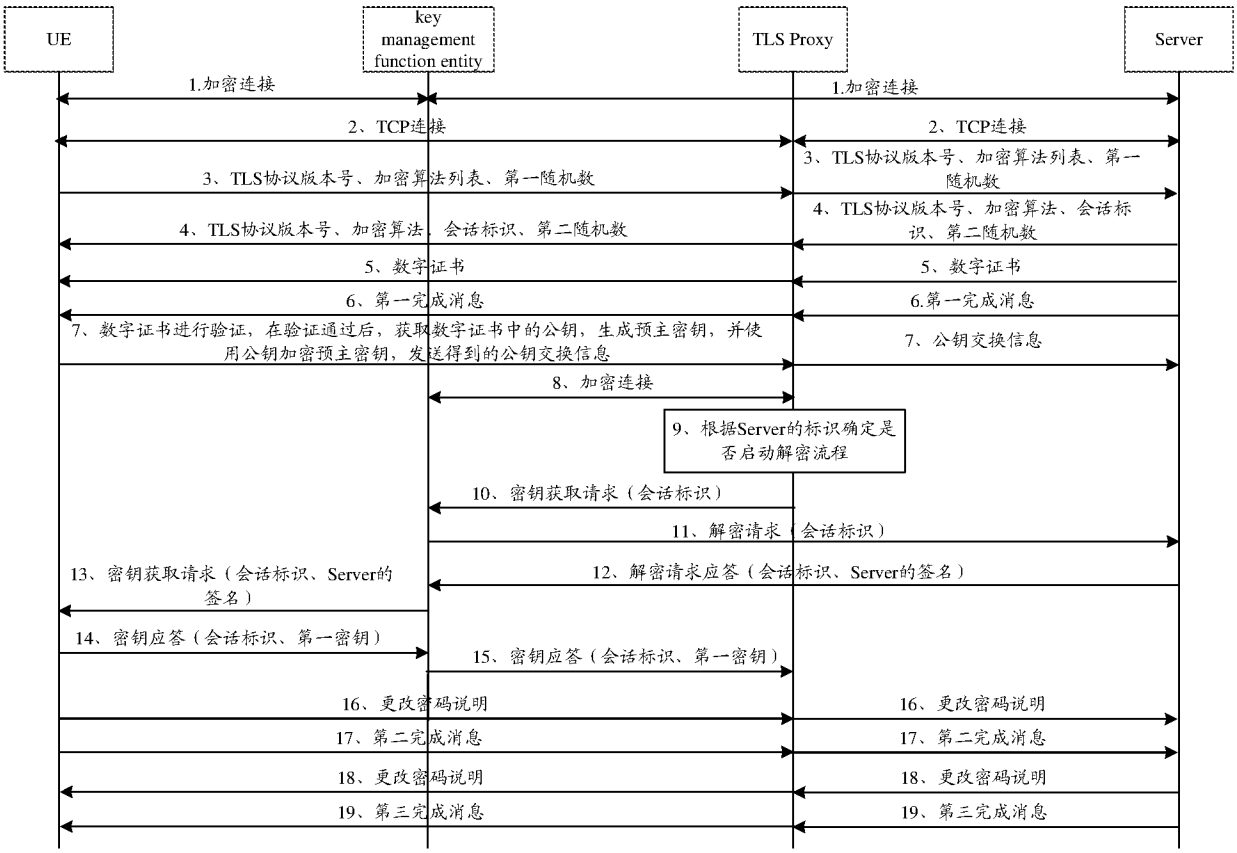
UE
key management function entity
TLS Proxy
Server
1.加密连接
1.加密连接
2、TCP连接
2、TCP连接
3、TLS协议版本号、加密算法列表、第一随机数
3、TLS协议版本号、加密算法列表、第一随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
5、数字证书
5、数字证书
6、第一完成消息
6.第一完成消息
7、数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，发送得到的公钥交换信息
7、公钥交换信息
8、加密连接
9、根据Server的标识确定是否启动解密流程
10、密钥获取请求（会话标识）
11、解密请求（会话标识）
13、密钥获取请求（会话标识、Server的签名）
12、解密请求应答（会话标识、Server的签名）
14、密钥应答（会话标识、第一密钥）
15、密钥应答（会话标识、第一密钥）
16、更改密码说明
16、更改密码说明
17、第二完成消息
17、第二完成消息
18、更改密码说明
18、更改密码说明
19、第三完成消息
19、第三完成消息

图 6B

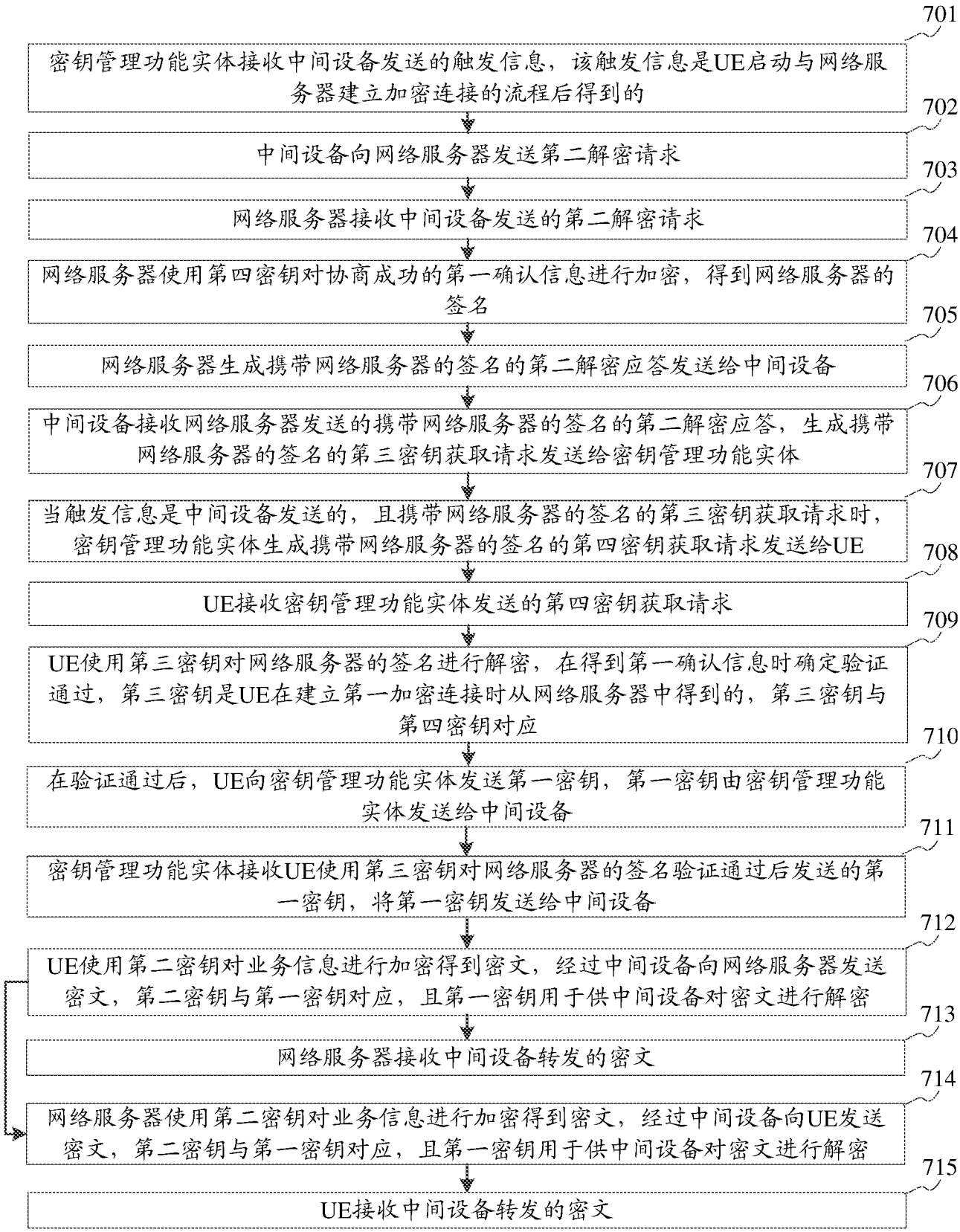
701
密钥管理功能实体接收中间设备发送的触发信息，该触发信息是UE启动与网络服务器建立加密连接的流程后得到的
702
中间设备向网络服务器发送第二解密请求
703
网络服务器接收中间设备发送的第二解密请求
704
网络服务器使用第四密钥对协商成功的第一确认信息进行加密，得到网络服务器的签名
705
网络服务器生成携带网络服务器的签名的第二解密应答发送给中间设备
706
中间设备接收网络服务器发送的携带网络服务器的签名的第二解密应答，生成携带网络服务器的签名的第三密钥获取请求发送给密钥管理功能实体
707
当触发信息是中间设备发送的，且携带网络服务器的签名的第三密钥获取请求时，密钥管理功能实体生成携带网络服务器的签名的第四密钥获取请求发送给UE
708
UE接收密钥管理功能实体发送的第四密钥获取请求
709
UE使用第三密钥对网络服务器的签名进行解密，在得到第一确认信息时确定验证通过，第三密钥是UE在建立第一加密连接时从网络服务器中得到的，第三密钥与第四密钥对应
710
在验证通过后，UE向密钥管理功能实体发送第一密钥，第一密钥由密钥管理功能实体发送给中间设备
711
密钥管理功能实体接收UE使用第三密钥对网络服务器的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备
712
UE使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
713
网络服务器接收中间设备转发的密文
714
网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向UE发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
715
UE接收中间设备转发的密文

图 7A

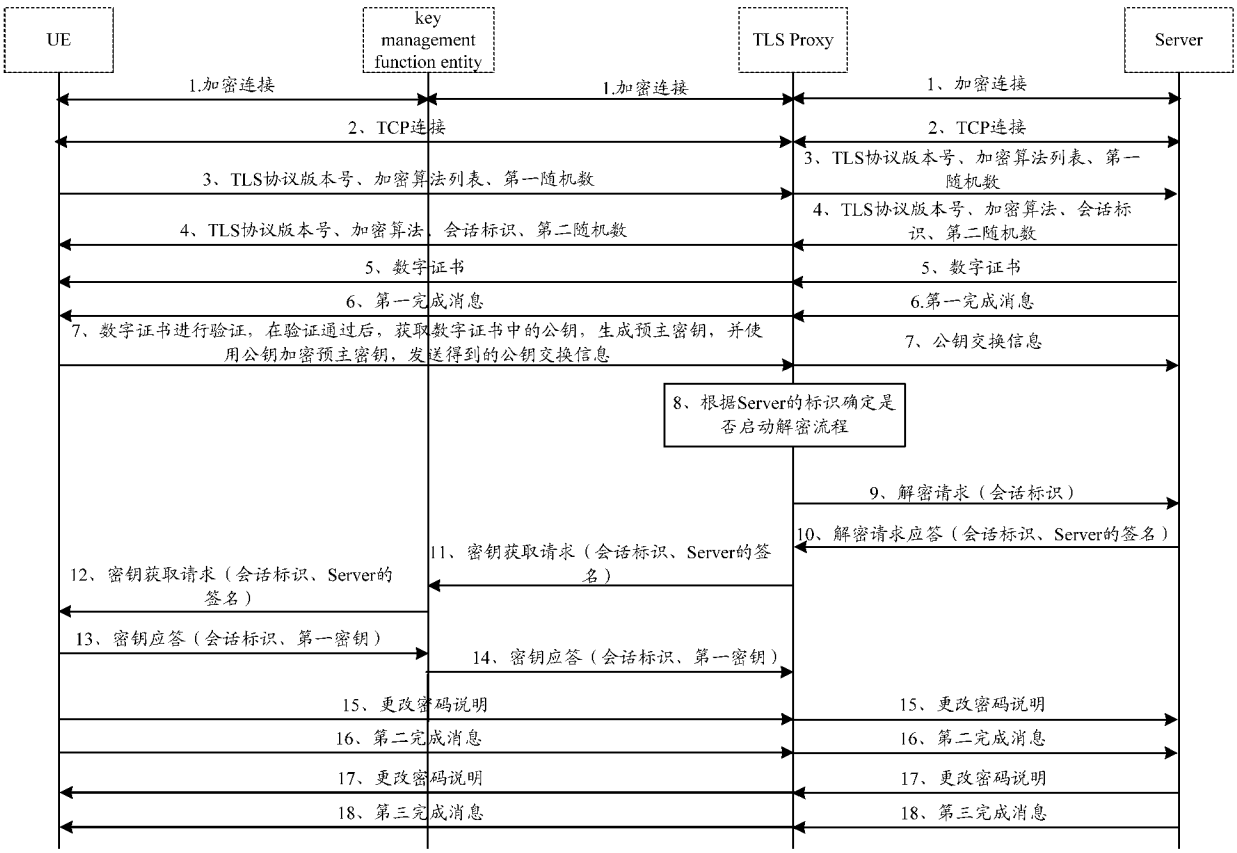
UE
key management function entity
TLS Proxy
Server
1.加密连接
1.加密连接
1、加密连接
2、TCP连接
2、TCP连接
3、TLS协议版本号、加密算法列表、第一随机数
3、TLS协议版本号、加密算法列表、第一随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
5、数字证书
5、数字证书
6、第一完成消息
6.第一完成消息
7、数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，发送得到的公钥交换信息
7、公钥交换信息
8、根据Server的标识确定是否启动解密流程
9、解密请求（会话标识）
10、解密请求应答（会话标识、Server的签名）
11、密钥获取请求（会话标识、Server的签名）
12、密钥获取请求（会话标识、Server的签名）
13、密钥应答（会话标识、第一密钥）
14、密钥应答（会话标识、第一密钥）
15、更改密码说明
15、更改密码说明
16、第二完成消息
16、第二完成消息
17、更改密码说明
17、更改密码说明
18、第三完成消息
18、第三完成消息

图 7B

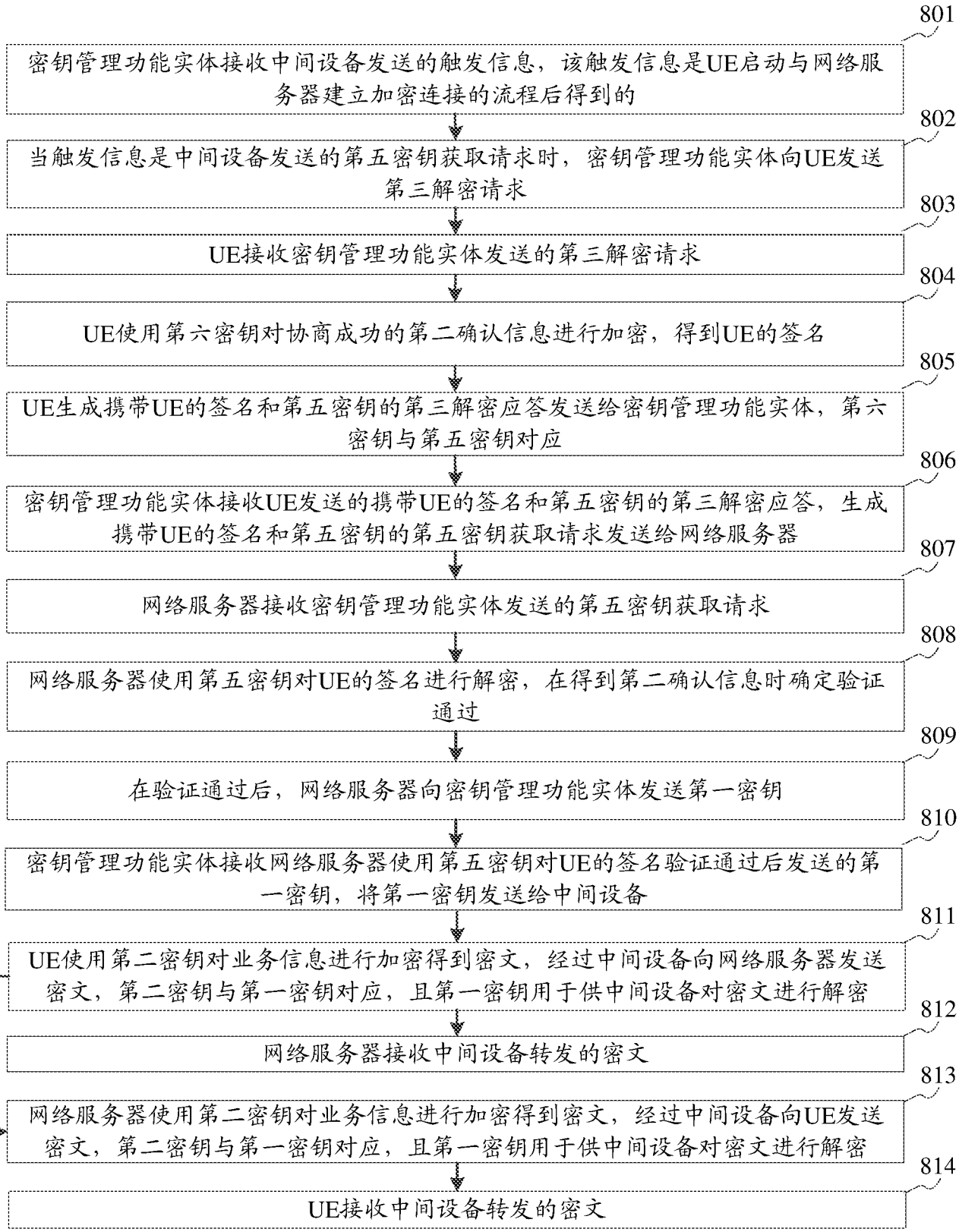
801
密钥管理功能实体接收中间设备发送的触发信息，该触发信息是UE启动与网络服务器建立加密连接的流程后得到的
802
当触发信息是中间设备发送的第五密钥获取请求时，密钥管理功能实体向UE发送第三解密请求
803
UE接收密钥管理功能实体发送的第三解密请求
804
UE使用第六密钥对协商成功的第二确认信息进行加密，得到UE的签名
805
UE生成携带UE的签名和第五密钥的第三解密应答发送给密钥管理功能实体，第六密钥与第五密钥对应
806
密钥管理功能实体接收UE发送的携带UE的签名和第五密钥的第三解密应答，生成携带UE的签名和第五密钥的第五密钥获取请求发送给网络服务器
807
网络服务器接收密钥管理功能实体发送的第五密钥获取请求
808
网络服务器使用第五密钥对UE的签名进行解密，在得到第二确认信息时确定验证通过
809
在验证通过后，网络服务器向密钥管理功能实体发送第一密钥
810
密钥管理功能实体接收网络服务器使用第五密钥对UE的签名验证通过后发送的第一密钥，将第一密钥发送给中间设备
811
UE使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
812
网络服务器接收中间设备转发的密文
813
网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向UE发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
814
UE接收中间设备转发的密文

图 8A

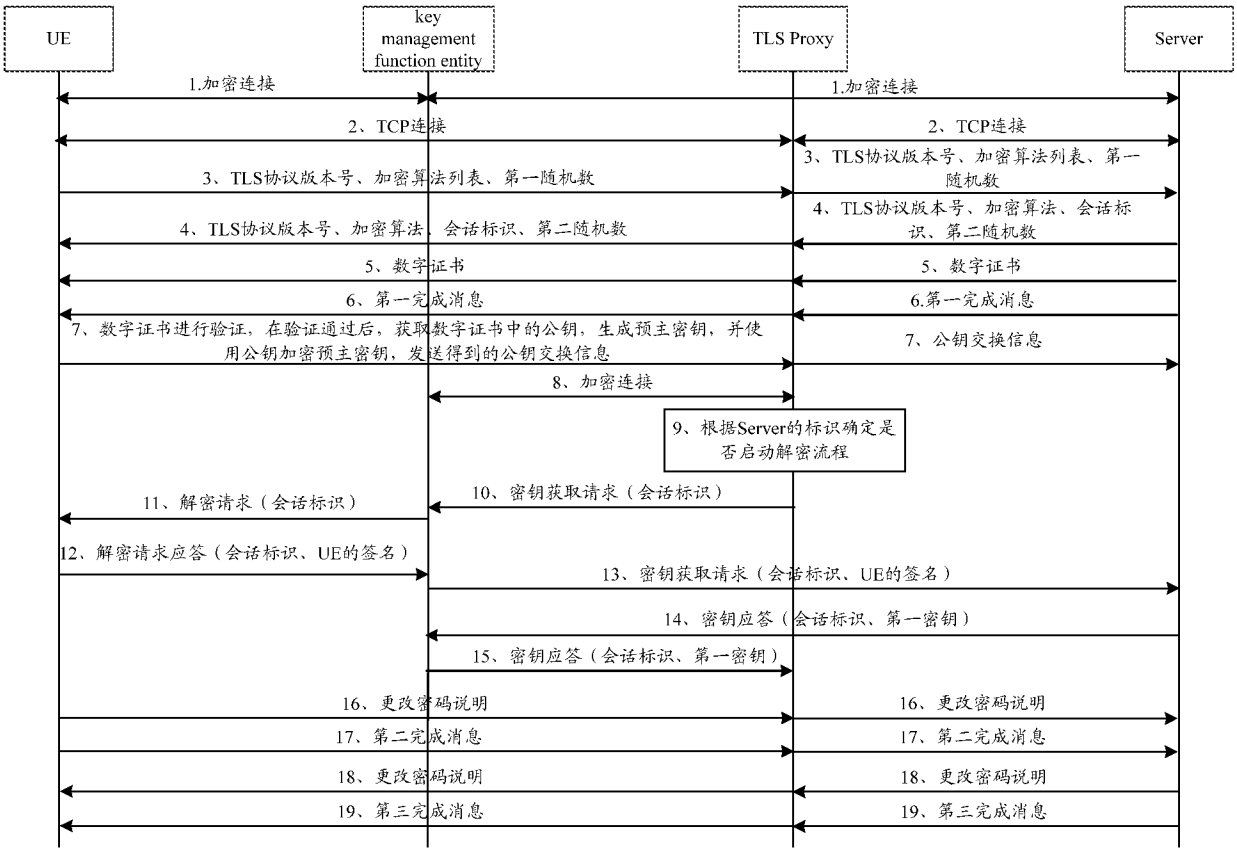
UE
key management function entity
TLS Proxy
Server
1.加密连接
1.加密连接
2、TCP连接
2、TCP连接
3、TLS协议版本号、加密算法列表、第一随机数
3、TLS协议版本号、加密算法列表、第一随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
5、数字证书
5、数字证书
6、第一完成消息
6.第一完成消息
7、数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，发送得到的公钥交换信息
7、公钥交换信息
8、加密连接
9、根据Server的标识确定是否启动解密流程
11、解密请求（会话标识）
10、密钥获取请求（会话标识）
12、解密请求应答（会话标识、UE的签名）
13、密钥获取请求（会话标识、UE的签名）
14、密钥应答（会话标识、第一密钥）
15、密钥应答（会话标识、第一密钥）
16、更改密码说明
16、更改密码说明
17、第二完成消息
17、第二完成消息
18、更改密码说明
18、更改密码说明
19、第三完成消息
19、第三完成消息

图 8B

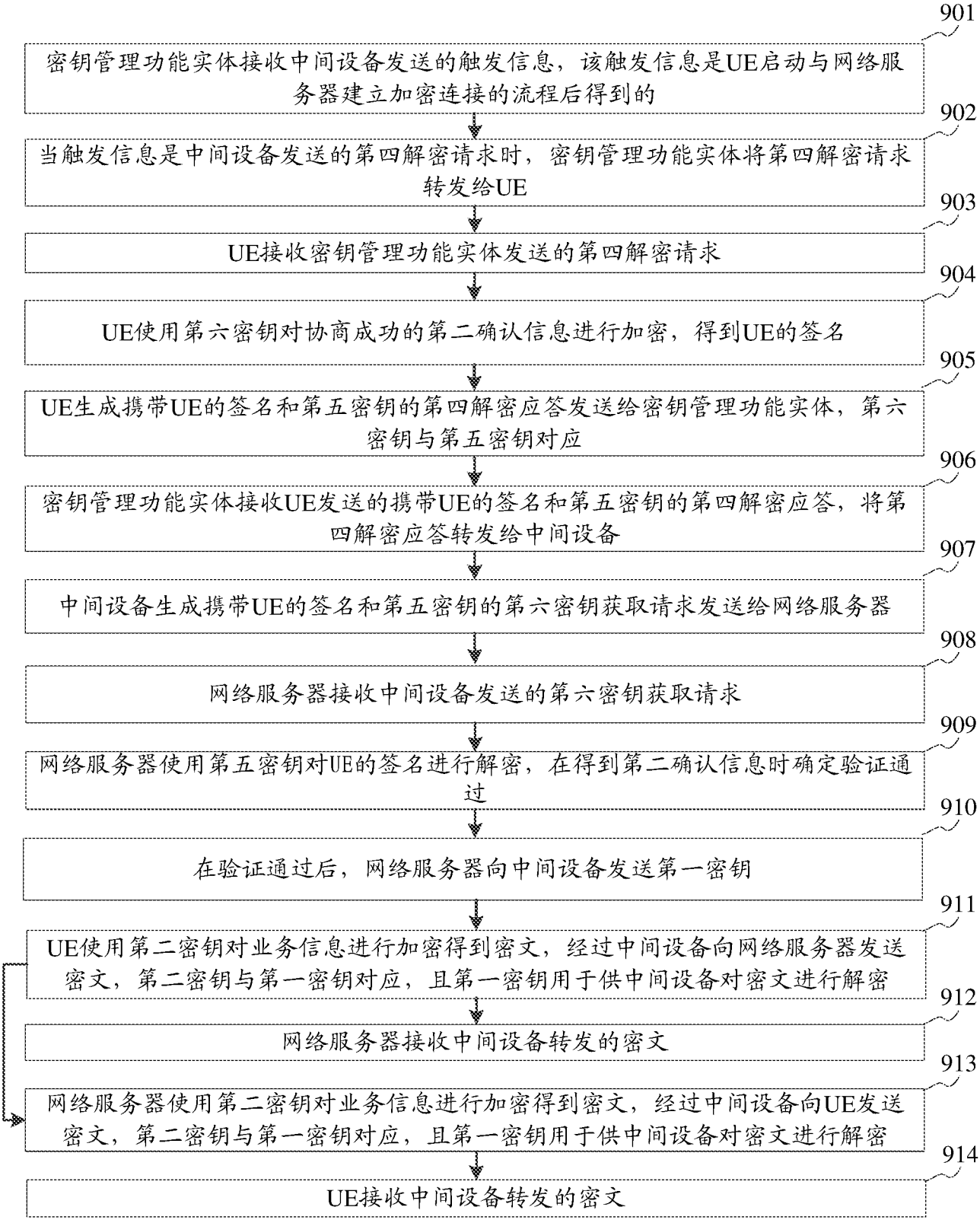
901
密钥管理功能实体接收中间设备发送的触发信息，该触发信息是UE启动与网络服务器建立加密连接的流程后得到的
902
当触发信息是中间设备发送的第四解密请求时，密钥管理功能实体将第四解密请求转发给UE
903
UE接收密钥管理功能实体发送的第四解密请求
904
UE使用第六密钥对协商成功的第二确认信息进行加密，得到UE的签名
905
UE生成携带UE的签名和第五密钥的第四解密应答发送给密钥管理功能实体，第六密钥与第五密钥对应
906
密钥管理功能实体接收UE发送的携带UE的签名和第五密钥的第四解密应答，将第四解密应答转发给中间设备
907
中间设备生成携带UE的签名和第五密钥的第六密钥获取请求发送给网络服务器
908
网络服务器接收中间设备发送的第六密钥获取请求
909
网络服务器使用第五密钥对UE的签名进行解密，在得到第二确认信息时确定验证通过
910
在验证通过后，网络服务器向中间设备发送第一密钥
911
UE使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
912
网络服务器接收中间设备转发的密文
913
网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向UE发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
914
UE接收中间设备转发的密文

图 9A

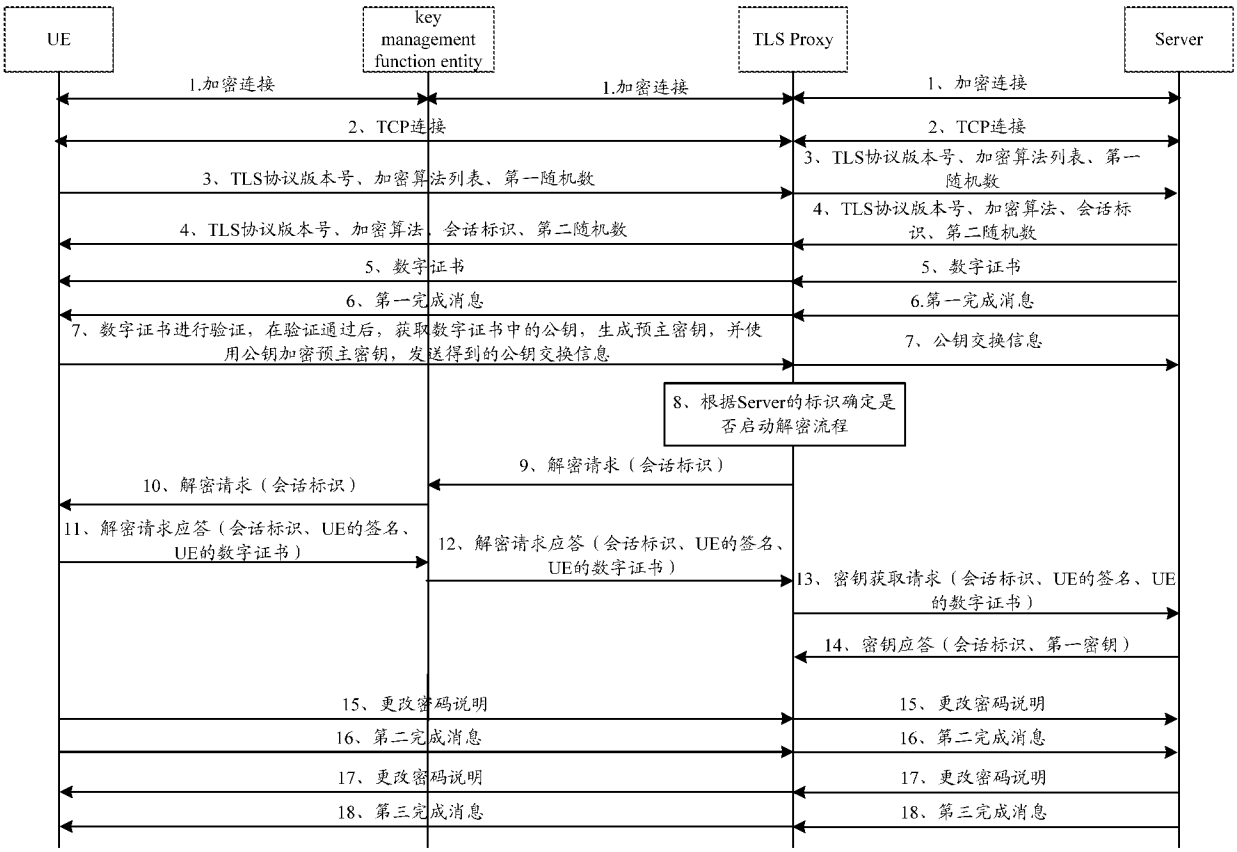
UE
key management function entity
TLS Proxy
Server
1.加密连接
1.加密连接
1、加密连接
2、TCP连接
2、TCP连接
3、TLS协议版本号、加密算法列表、第一随机数
3、TLS协议版本号、加密算法列表、第一随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
5、数字证书
5、数字证书
6、第一完成消息
6.第一完成消息
7、数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，发送得到的公钥交换信息
7、公钥交换信息
8、根据Server的标识确定是否启动解密流程
9、解密请求（会话标识）
10、解密请求（会话标识）
11、解密请求应答（会话标识、UE的签名、UE的数字证书）
12、解密请求应答（会话标识、UE的签名、UE的数字证书）
13、密钥获取请求（会话标识、UE的签名、UE的数字证书）
14、密钥应答（会话标识、第一密钥）
15、更改密码说明
15、更改密码说明
16、第二完成消息
16、第二完成消息
17、更改密码说明
17、更改密码说明
18、第三完成消息
18、第三完成消息

图 9B

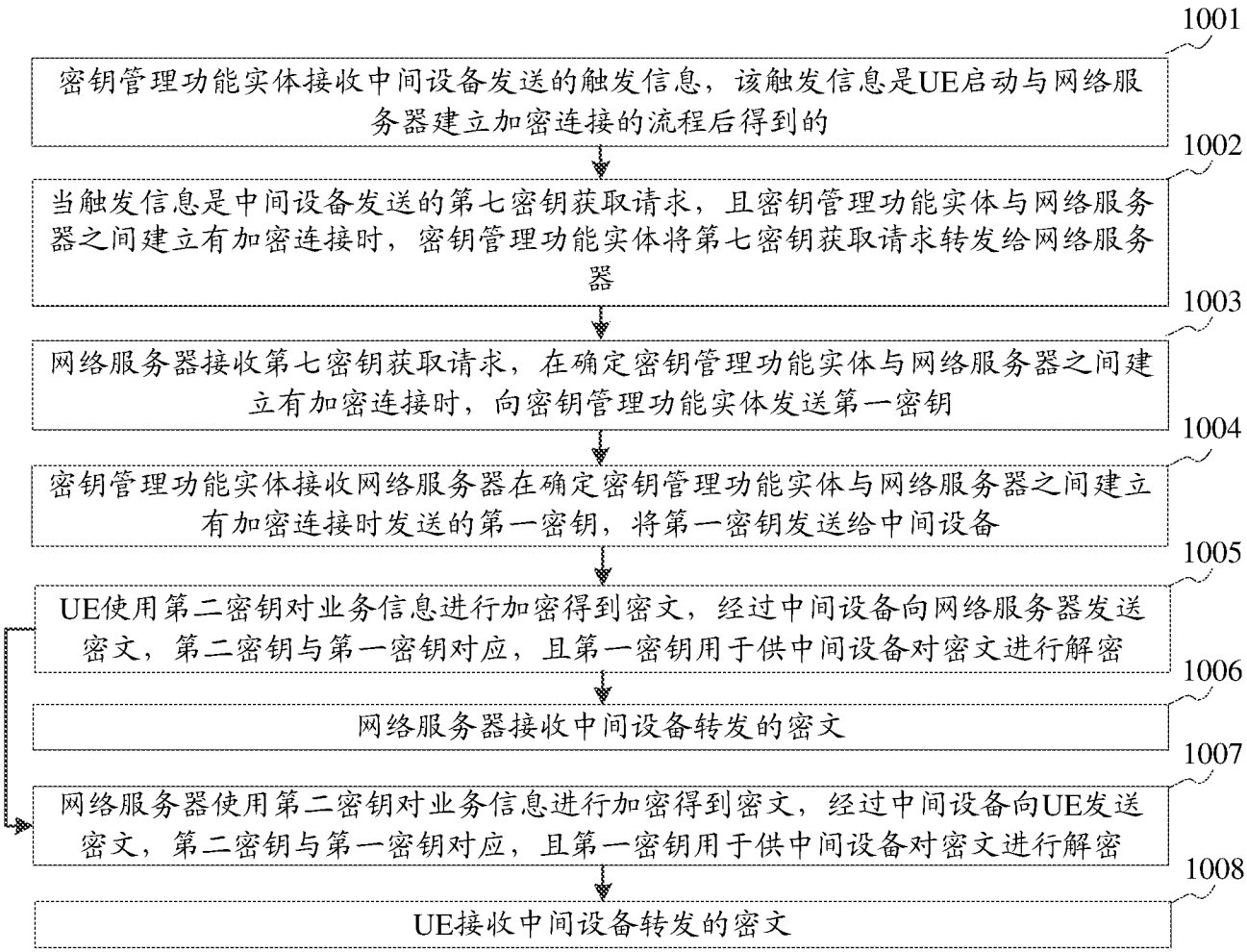
1001
密钥管理功能实体接收中间设备发送的触发信息，该触发信息是UE启动与网络服务器建立加密连接的流程后得到的
1002
当触发信息是中间设备发送的第七密钥获取请求，且密钥管理功能实体与网络服务器之间建立有加密连接时，密钥管理功能实体将第七密钥获取请求转发给网络服务器
1003
网络服务器接收第七密钥获取请求，在确定密钥管理功能实体与网络服务器之间建立有加密连接时，向密钥管理功能实体发送第一密钥
1004
密钥管理功能实体接收网络服务器在确定密钥管理功能实体与网络服务器之间建立有加密连接时发送的第一密钥，将第一密钥发送给中间设备
1005
UE使用第二密钥对业务信息进行加密得到密文，经过中间设备向网络服务器发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
1006
网络服务器接收中间设备转发的密文
1007
网络服务器使用第二密钥对业务信息进行加密得到密文，经过中间设备向UE发送密文，第二密钥与第一密钥对应，且第一密钥用于供中间设备对密文进行解密
1008
UE接收中间设备转发的密文

图 10A

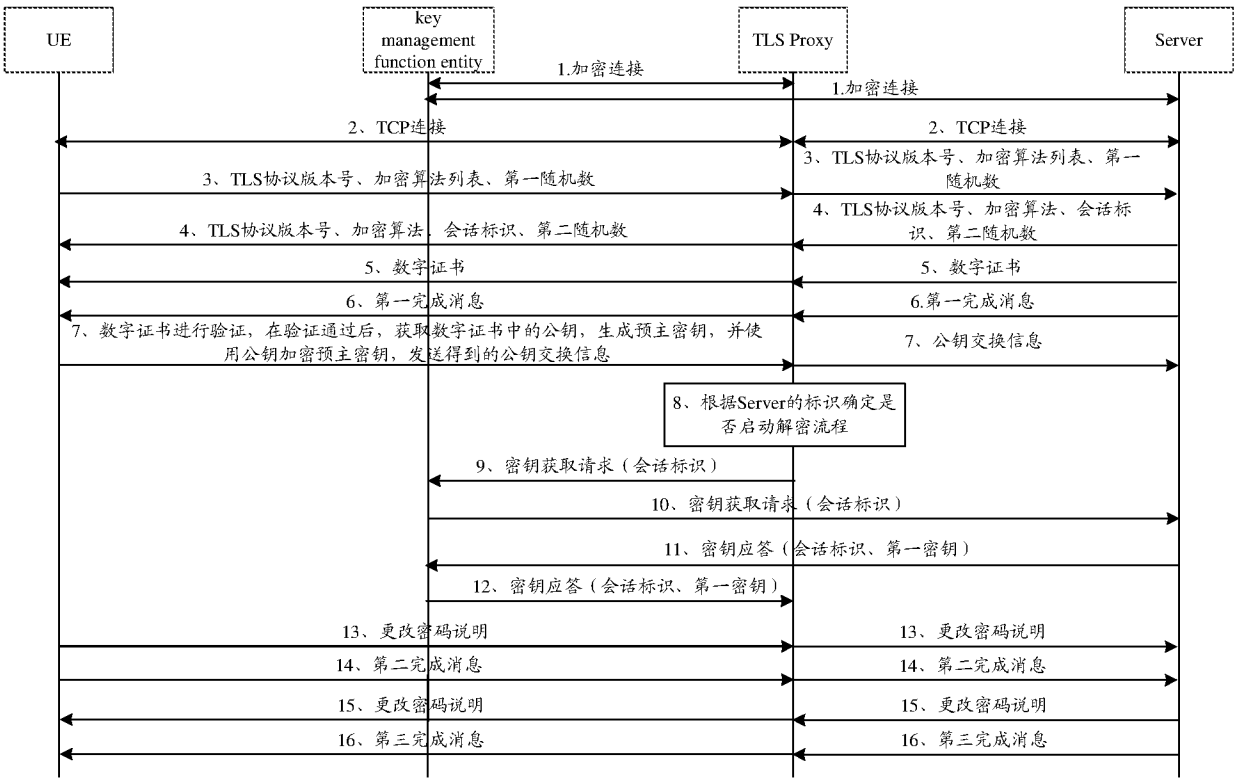
UE
key management function entity
TLS Proxy
Server
1.加密连接
1.加密连接
2、TCP连接
2、TCP连接
3、TLS协议版本号、加密算法列表、第一随机数
3、TLS协议版本号、加密算法列表、第一随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
4、TLS协议版本号、加密算法、会话标识、第二随机数
5、数字证书
5、数字证书
6、第一完成消息
6.第一完成消息
7、数字证书进行验证，在验证通过后，获取数字证书中的公钥，生成预主密钥，并使用公钥加密预主密钥，发送得到的公钥交换信息
7、公钥交换信息
8、根据Server的标识确定是否启动解密流程
9、密钥获取请求（会话标识）
10、密钥获取请求（会话标识）
11、密钥应答（会话标识、第一密钥）
12、密钥应答（会话标识、第一密钥）
13、更改密码说明
13、更改密码说明
14、第二完成消息
14、第二完成消息
15、更改密码说明
15、更改密码说明
16、第三完成消息
16、第三完成消息

图 10B

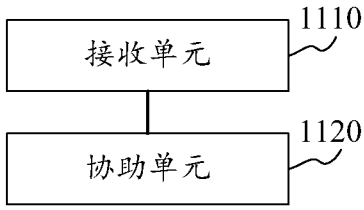
接收单元
1110
协助单元
1120

图 11

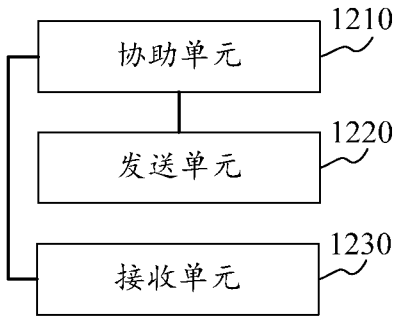

图 12

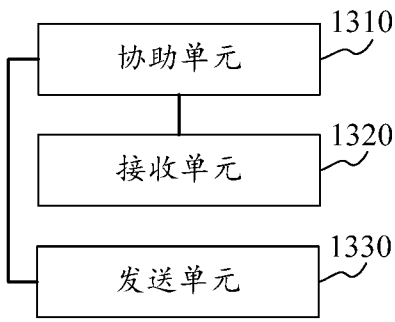

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/085051

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (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; H04W

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)

CNPAT; WPI; EPODOC; CNKI: SSL, TLS, relay, middle, node?, device?, key, decryption, terminal, middleware, intermediate, relay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105429962 A (TSINGHUA UNIVERSITY) 23 March 2016 (23.03.2016) description, paragraphs [0028]-[0047], and figures 1-3	1-30
A	CN 101515896 A (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.) 26 August 2009 (26.08.2009) the whole document	1-30
A	WO 2010088813 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 12 August 2010 (12.08.2010) the whole document	1-30

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 February 2017	23 February 2017
Name and mailing address of the ISA 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 XU, Hongyan Telephone No. (86-10) 62413251

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/085051

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105429962 A	23 March 2016	None	
CN 101515896 A	26 August 2009	None	
WO 2010088813 A1	12 August 2010	CN 101800734 A	11 August 2010

国际检索报告

国际申请号
PCT/CN2016/085051

A. 主题的分类

H04L 9/08(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)

H04L; H04W

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）)

CNPAT;WPI;EPODOC;CNKI:密钥，解密，终端，中间，设备，用户，中间设备，中间节点，节点，中继，SSL，TLS，relay，middle，node?，device?，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
X	CN 105429962 A (清华大学) 2016年 3月 23日 (2016-03-23) 说明书第[0028]-[0047]段、附图1-3	1-30
A	CN 101515896 A (成都市华为赛门铁克科技有限公司) 2009年 8月 26日 (2009-08-26) 全文	1-30
A	WO 2010088813 A1 (华为技术有限公司) 2010年 8月 12日 (2010-08-12) 全文	1-30

☐ 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	国际检索报告邮寄日期
2017年 2月 7日	2017年 2月 23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 许洪岩 电话号码 (86-10)62413251

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/085051

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 105429962 A	2016年 3月 23日	无	
CN 101515896 A	2009年 8月 26日	无	
WO 2010088813 A1	2010年 8月 12日	CN 101800734 A	2010年 8月 11日