(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
2022 年 9 月 29 日 (29.09.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/199569 A1

(51) 国际专利分类号:
H04W 4/40 (2018.01)

(21) 国际申请号: PCT/CN2022/082192

(22) 国际申请日: 2022 年 3 月 22 日 (22.03.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110304444.4 2021年3月22日 (22.03.2021) CN
202111217636.8 2021年10月19日 (19.10.2021) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION CO., LTD RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。 中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 田野 (TIAN, Ye); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。 粟栗 (SU, Li); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。 何申 (HE, Shen); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。 杜海涛 (DU, Haitao); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。 马洁 (MA, Jie); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。 姜文姝 (JIANG, Wenshu); 中国北京市西城区宣武门西大街32号, Beijing 100053 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路21号中关村知识产权大厦B座2层, Beijing 100080 (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, IT, JM, JO, 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,

(54) **Title:** CONFIGURATION METHOD AND APPARATUS FOR TERMINAL DEVICE, AND COMMUNICATION DEVICE

(54) **发明名称**: 一种终端设备的配置方法、装置和通信设备

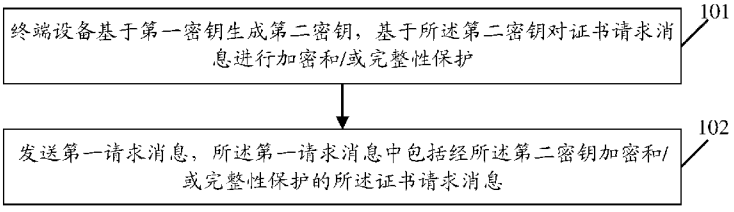

图 2

101 A TERMINAL DEVICE GENERATES A SECOND KEY ON THE BASIS OF A FIRST KEY, AND PERFORMS ENCRYPTION AND/OR INTEGRITY PROTECTION ON A CERTIFICATE REQUEST MESSAGE ON THE BASIS OF THE SECOND KEY

102 SEND A FIRST REQUEST MESSAGE, THE FIRST REQUEST MESSAGE COMPRISING THE CERTIFICATE REQUEST MESSAGE ENCRYPTED AND/OR INTEGRITY-PROTECTED VIA THE SECOND KEY

(57) **Abstract:** Disclosed in embodiments of the present application are a configuration method and apparatus for a terminal device, and a communication device. The method comprises: the terminal device generating a second key on the basis of a first key, and performing encryption and/or integrity protection on a certificate request message on the basis of the second key; and sending a first request message, the first request message comprising the certificate request message encrypted and/or integrity-protected via the second key.

(57) **摘要**: 本申请实施例公开了一种终端设备的配置方法、装置和通信设备，所述方法包括：终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护；发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

WO 2022/199569 A1

[见续页]

SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))。

一种终端设备的配置方法、装置和通信设备

相关申请的交叉引用

本申请基于申请号为202110304444.4、申请日为2021年03月22日的中国专利申请以及申请号为202111217636.8、申请日为2021年10月19日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此以引入方式并入本申请。

技术领域

本申请涉及车联网技术领域，具体涉及一种终端设备的配置方法、装置和通信设备。

背景技术

蜂窝车联网（C-V2X，Cellular-Vehicle to X）车联网中，车辆、交通设施、车联网管理系统之间传递大量的实时交通信息，包括车辆行驶状态、路况事件、信号灯信息等，这些关键的交通信息直接关系着公共交通安全与司乘人员的生命安全，在根本上决定着C-V2X技术能否产业落地。

为了保障信息的安全性，引入了数字证书，并基于数字证书对C-V2X系统中用户与设备的真实性、传递信息的真实性进行保障。因此，保障数字证书的安全性就成为C-V2X技术落地的关键。

目前的生产流程中，需要在车辆或车联网设备的生产过程中离线配置数字证书，这种方法对车辆厂商、C-V2X终端设备厂商有较高的安全生产要求，要么需要改造生产线以满足离线灌装的物理环境安全要求，要么需要将设备送到专业的安全机构进行灌装，因此该方法投资成本高，灵活性较差，部署难度大，技术实施的难度较大。

此外，采用现有标准通用引导架构（GBA，Generic Bootstrapping Architecture）方法，如图 1 所示，车辆或车联网设备和 CA 服务器间能够建立起安全连接，C-V2X 设备可通过在线方式完成数字证书配置，但是标准方案要求网络运营商为每一个 CA 服务器部署一个网络应用功能（NAF，Network Application Function）/认证代理（AP，Authentication Proxy）网元来提供 GBA 服务（参加图 1 中 C-V2X 服务提供者（C-V2X Service Provider）虚框，虚框中对于 CA 服务器（图中为 C-V2X 应用服务器（C-V2X Application Server））与 NAF/AP 网元一一对应），这对运营商而言增加了巨大的网络运营及维护的成本。除此之外，由于 CA 服务器与车联网设备通信所使用的 GBA 会话密钥是由 NAF/AP 网元中存储的，消息加解密、完整性保护等安全保护操作是由 NAF/AP 设备执行的，而 NAF/AP 是按照通信行业安全技术标准研发的，因此 CA 服务器不能够灵活使用 GBA 会话密钥，所执行的安全保护操作也不一定能够符合 C-V2X 车联网行业安全技术要求，这给 GBA 方案的产业应用带来的困难。

另外，在线配置方式完成数字证书配置对 C-V2X 设备的安全实现有着极高的设计要求。为了保证数字证书及敏感参数在设备侧的安全性，这些信息不能够简单地由客户端应用操作，在设备上通用 中央处理器（CPU，Central Processing Unit）、内/外部存储器等上运算执行，而应结合密钥的生成获取方式在可信的安全环境中处理。然而，现有配置方案缺乏设备侧整体安全设计与实现，无法确保数字证书的配置安全。

总而言之，如何安全、便捷地将数字证书及敏感安全参数在 C-V2X 设备上安全部署配置是当前 C-V2X 车联网行业在安全领域面临的一大挑战。

发明内容

本申请实施例提供一种终端设备的配置方法、装置和通信设备。

本申请实施例的技术方案是这样实现的：

第一方面，本申请实施例提供了一种终端设备的配置方法，所述方法包括:

终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护;

发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

在本申请的一些可选实施例中，所述方法还包括：所述终端设备接收来自服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和全球用户识别模块（USIM）;

所述终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护，包括:

所述应用客户端通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥;

所述应用客户端生成第一证书请求消息，并通过所述基带芯片向所述 USIM 发送所述第一证书请求消息;

所述 USIM 生成公私钥对，在所述第一证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息;

所述 USIM 基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，在所述第二证书请求消息中添加第一校验值;

所述 USIM 通过所述基带芯片向所述应用客户端发送经上述处理后的所述第二证书请求消息。

在本申请的一些可选实施例中，所述发送第一请求消息，包括：所述

应用客户端向服务器发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述第二证书请求消息；所述第一请求消息中还包括：引导事务标识（B-TID）和/或服务器的全限定域名（FQDN）。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和 USIM;

所述终端设备接收来自所述服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书，包括:

所述应用客户端接收来自所述服务器的第一响应消息，并通过所述基带芯片向所述 USIM 发送所述第一响应消息;

所述 USIM 基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密;

校验通过后，所述 USIM 获得所述第一响应消息中携带的数字证书，并在安全组件中存储所述数字证书。

在本申请的一些可选实施例中，所述方法还包括：所述终端设备执行通用引导架构（GBA）认证流程或面向应用的认证或密钥管理（AKMA）认证流程，与网络设备协商所述第一密钥。

第二方面，本申请实施例还提供了一种终端设备的配置方法，所述方法包括：服务器接收来自终端设备的第一请求消息；所述第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息;

所述服务器获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成;

所述服务器基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书;

所述服务器向所述终端设备发送第一响应消息，所述第一响应消息中

包括所述数字证书。

在本申请的一些可选实施例中，所述服务器向所述终端设备发送第一响应消息，包括:

所述服务器构建包含有所述数字证书的第一响应消息，基于所述第二密钥对所述第一响应消息进行加密和/或完整性保护，在所述第一响应消息中添加第二校验值;

向所述终端设备发送经上述处理后的第一响应消息。

在本申请的一些可选实施例中，所述第一请求消息中还包括：引导事务标识（B-TID）;

所述服务器获得来自网络设备的所述第二密钥，包括:

所述服务器查询是否存在与所述 B-TID 对应的第二密钥;

在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥。

在本申请的一些可选实施例中，所述服务器获得来自网络设备的所述第二密钥，包括:

所述服务器向所述网络设备发送第二请求消息，所述第二请求消息用于请求所述第二密钥;

所述服务器接收所述网络设备发送的第二响应消息，所述第二响应消息中包括所述第二密钥。

第三方面，本申请实施例还提供了一种终端设备的配置方法，所述方法包括：网络设备基于预先协商的第一密钥生成第二密钥，向服务器发送所述第二密钥。

在本申请的一些可选实施例中，所述方法还包括：所述网络设备与所述终端设备通过执行 GBA 认证流程或 AKMA 认证流程，与所述终端设备协商所述第一密钥。

在本申请的一些可选实施例中，所述网络设备基于预先协商的第一密钥生成第二密钥，向服务器发送所述第二密钥，包括:

所述网络设备接收所述服务器发送的第二请求信息，所述第二请求消息用于请求所述第二密钥;

所述网络设备基于预先协商的第一密钥生成第二密钥，向所述服务器发送第二响应消息，所述第二响应消息中包括所述第二密钥。

第四方面，本申请实施例还提供了一种终端设备的配置装置，所述装置包括：第一生成单元和第一通信单元；其中，

所述第一生成单元，配置为基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护;

所述第一通信单元，配置为发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

在本申请的一些可选实施例中，所述第一通信单元，还配置为接收来自服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书。

在本申请的一些可选实施例中，所述第一生成单元包括：应用客户端、基带芯片和 USIM;

所述应用客户端，配置为通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；还配置为生成第一证书请求消息，并通过所述基带芯片向所述 USIM 发送所述第一证书请求消息;

所述 USIM，配置为生成公私钥对，在所述第一证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息；基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，并在所述第二证书请求消息中添加第一校验值；通过所述基带芯片向所述应用客户端发送经所述第二密钥加

密和/或完整性保护的所述第二证书请求消息。

在本申请的一些可选实施例中，所述应用客户端，配置为通过所述第一通信单元向服务器发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述第二证书请求消息；所述第一请求消息中还包括：B-TID 和/或服务器 FQDN。

在本申请的一些可选实施例中，所述第一生成单元包括：应用客户端、基带芯片和 USIM;

所述应用客户端，配置为通过所述第一通信单元接收来自所述服务器的第一响应消息，并通过所述基带芯片向所述 USIM 发送所述第一响应消息；

所述 USIM，配置为基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密；校验通过后，获得所述第一响应消息中携带的数字证书，并在安全组件中存储所述数字证书。

在本申请的一些可选实施例中，所述装置还包括第一执行单元，配置为执行 GBA 认证流程或 AKMA 认证流程，与网络设备协商所述第一密钥。

第五方面，本申请实施例还提供了一种终端设备的配置装置，所述装置包括：第二通信单元和第一校验单元；其中，

所述第二通信单元，配置为接收来自终端设备的第一请求消息；所述第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息；

所述第一校验单元，配置为获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；还配置为基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书；

所述第二通信单元，还配置为向所述终端设备发送第一响应消息，所述第一响应消息中包括所述数字证书。

在本申请的一些可选实施例中，所述第二通信单元，配置为构建包含有所述数字证书的第一响应消息，基于所述第二密钥对所述第一响应消息进行加密和/或完整性保护，在所述第一响应消息中添加第二校验值，向所述终端设备发送经上述处理后的第一响应消息。

在本申请的一些可选实施例中，所述第一请求消息中还包括：引导事务标识（B-TID）；

所述装置还包括第二执行单元，配置为查询是否存在与所述 B-TID 对应的第二密钥；在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，通过所述第二通信单元获得来自网络设备的所述第二密钥。

第六方面，本申请实施例还提供了一种终端设备的配置装置，所述装置包括第二生成单元和第三通信单元；其中，

所述第二生成单元，配置为基于预先协商的第一密钥生成第二密钥；

所述第三通信单元，配置为向服务器发送所述第二密钥。

在本申请的一些可选实施例中，所述装置还包括第三执行单元，配置为与终端设备通过执行 GBA 认证流程或 AKMA 认证流程，与所述终端设备协商所述第一密钥。

在本申请的一些可选实施例中，所述第二生成单元，配置为基于预先协商的第一密钥，为每个服务器生成对应的第二密钥；

所述第三通信单元，配置为分别向每个服务器发送所述对应的第二密钥。

第七方面，本申请实施例还提供了一种终端设备的配置方法，所述方法包括：终端设备基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护；发送第一消息。

在本申请的一些可选实施例中，所述方法还包括：所述终端设备接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校

验和/或解密。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和全球用户识别模块（USIM）；

所述终端设备基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护，包括：

所述应用客户端通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；

所述应用客户端生成第一消息，并通过所述基带芯片向所述 USIM 发送所述第一消息；

所述 USIM 基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护；

所述 USIM 通过所述基带芯片向所述应用客户端发送经上述处理后的所述第一消息。

在本申请的一些可选实施例中，所述发送第一消息，包括：所述应用客户端向服务器发送所述第一消息；

所述第一消息中还包括：引导事务标识（B-TID）和/或服务器的全限定域名（FQDN）；或者包括：面向应用的认证或密钥管理（AKMA）密钥标识符（A-KID）和/或 FQDN。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和全球用户识别模块（USIM）；

所述终端设备接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密，包括：

所述应用客户端接收来自所述服务器的第二消息，并通过所述基带芯片向所述 USIM 发送所述第二消息；

所述 USIM 基于所述第二密钥对所述第二消息进行完整性校验和/或解

密。

第八方面，本申请实施例还提供了一种终端设备的配置方法，所述方法包括:

服务器接收来自终端设备的第一消息，所述第一消息的部分或全部经第二密钥加密和/或完整性保护;

所述服务器获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成;

所述服务器基于所述第二密钥对所述第一消息进行完整性校验和/或解密。

在本申请的一些可选实施例中，所述方法还包括：所述服务器基于所述第二密钥对第二消息的部分或全部进行加密和/或完整性保护；发送第二消息。

在本申请的一些可选实施例中，所述第一消息中还包括：引导事务标识（B-TID），或者包括面向应用的认证或密钥管理（AKMA）密钥标识符（A-KID）;

所述服务器获得来自网络设备的所述第二密钥，包括:

所述服务器查询是否存在与所述 B-TID 或所述 A-KID 对应的第二密钥;

在查询结果为不存在与所述 B-TID 或所述 A-KID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥。

第九方面，本申请实施例还提供了一种终端设备的配置装置，所述装置包括：第三生成单元和第四通信单元；其中，

所述第三生成单元，配置为基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护;

所述第四通信单元，配置为发送第一消息。

在本申请的一些可选实施例中，所述第四通信单元，还配置为接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

在本申请的一些可选实施例中，所述第三生成单元包括：应用客户端、基带芯片和全球用户识别模块（USIM）；

所述应用客户端，配置为通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；还配置为生成第一消息，并通过所述基带芯片向所述 USIM 发送所述第一消息；

所述 USIM，配置为基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护；还配置为通过所述基带芯片向所述应用客户端发送经上述处理后的所述第一消息。

在本申请的一些可选实施例中，所述应用客户端，还配置为向服务器发送所述第一消息；

所述第一消息中还包括：引导事务标识（B-TID）和/或服务器的全限定域名（FQDN）；或者包括：面向应用的认证或密钥管理（AKMA）密钥标识符（A-KID）和/或 FQDN。

在本申请的一些可选实施例中，所述第三生成单元包括：应用客户端、基带芯片和全球用户识别模块（USIM）；

所述应用客户端，配置为接收来自所述服务器的第二消息，并通过所述基带芯片向所述 USIM 发送所述第二消息；

所述 USIM，配置为基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

第十方面，本申请实施例还提供了一种终端设备的配置装置，所述装置包括：第五通信单元和第二校验单元；其中，

所述第五通信单元，配置为接收来自终端设备的第一消息，所述第一

消息的部分或全部经第二密钥加密和/或完整性保护；

所述第二校验单元，配置为获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；还配置为基于所述第二密钥对所述第一消息进行完整性校验和/或解密。

在本申请的一些可选实施例中，所述装置还包括第四生成单元，配置为基于所述第二密钥对第二消息的部分或全部进行加密和/或完整性保护；

所述第五通信单元，还配置为发送第二消息。

在本申请的一些可选实施例中，所述第一消息中还包括：引导事务标识（B-TID），或者包括面向应用的认证或密钥管理（AKMA）密钥标识符（A-KID）；

所述装置还包括第四执行单元，配置为查询是否存在与所述 B-TID 或所述 A-KID 对应的第二密钥；

所述第二校验单元，配置为在所述第四执行单元获得的查询结果为不存在与所述 B-TID 或所述 A-KID 对应的第二密钥的情况下，通过所述第五通信单元获得来自网络设备的所述第二密钥。

第十一方面，本申请实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本申请实施例第一方面、第二方面、第三方面、第七方面或第八方面所述方法的步骤。

第十二方面，本申请实施例还提供了一种通信设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现本申请实施例第一方面、第二方面、第三方面、第七方面或第八方面所述方法的步骤。

本申请实施例提供的终端设备的配置方法、装置和通信设备，终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护；发送请求消息，所述请求消息中包括经所述第二密钥

加密和/或完整性保护的所述证书请求消息；服务器接收来自终端设备的请求消息；所述请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息；获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；基于所述第二密钥对所述请求消息进行完整性校验和/或解密，并在对所述请求消息授权通过后签发数字证书；向所述终端设备发送响应消息，所述响应消息中包括所述数字证书。采用本申请实施例的技术方案，基于 GBA 机制，可通过“一键配置”的方式实现 C-V2X 终端设备的数字证书的安全配置，无需生产线安全环境的改造，也无需专业的安全机构进行灌装，提升数字证书配置的灵活性、降低部署难度以及投资成本。

附图说明

图 1 为 GBA 架构示意图；

图 2 为本申请实施例的终端设备的配置方法的流程示意图一；

图 3 为本申请实施例中的 GBA 增强架构示意图；

图 4 为本申请实施例的终端设备的一种可选架构示意图；

图 5 为本申请实施例的终端设备的配置方法的流程示意图二；

图 6 为本申请实施例的终端设备的配置方法的流程示意图三；

图 7 为本申请实施例的终端设备的配置方法的交互流程示意图一；

图 8 为本申请实施例的终端设备的配置装置的组成结构示意图一；

图 9 为本申请实施例的终端设备的配置装置的组成结构示意图二；

图 10 为本申请实施例的终端设备的配置装置的组成结构示意图三；

图 11 为本申请实施例的终端设备的配置方法的流程示意图四；

图 12 为本申请实施例的终端设备的配置方法的流程示意图五；

图 13 为本申请实施例的终端设备的配置方法的交互流程示意图二；

图 14 为本申请实施例的终端设备的配置装置的组成结构示意图四；

图 15 为本申请实施例的终端设备的配置装置的组成结构示意图五；

图 16 为本申请实施例的通信设备的硬件组成结构示意图。

具体实施方式

下面结合附图及具体实施例对本申请作进一步详细的说明。

本申请实施例提供了一种终端设备的配置方法。图 2 为本申请实施例的终端设备的配置方法的流程示意图一；如图 2 所示，所述方法包括:

步骤 101: 终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护;

步骤 102: 发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

本实施例的终端设备的配置方法（以下简称方法）应用于终端设备中，所述终端设备具体可以是车联网终端设备（也可以称为 C-V2X Device），在一些可选实施例中，所述车联网终端设备例如可以是车载单元（OBU，On Board Unit）、路侧单元（RSU，Road Side Unit）等等；在另一些可选实施例中，所述车联网终端设备也可以是行人的手持设备、可穿戴设备等等。

在本申请的一些可选实施例中，所述方法还包括: 所述终端设备执行 GBA 认证流程或面向应用的认证和密钥管理（AKMA，Authentication and Key Management for Applications）认证流程，与网络设备协商所述第一密钥。

具体来说，这里的网络设备在 GBA 认证流程下具体可以是 NAF 或 AP。进而，在 AKMA 认证流程下，网络设备可以是网络开放功能实体（NEF，Network Exposure Function），NEF 用于将网络能力开放给其他网元使用。

终端与网络设备预先协商第一密钥的一种可能的实现方式为（这里以 C-V2X 设备基于 GBA 认证流程为例）:

C-V2X 设备与 BSF 进行 AKA 认证，BSF 返回 200OK 响应后，C-V2X 设备生成 GBA 会话密钥，也即所述第一密钥。随后，在 C-V2X 设备访问

NAF/AP 时，NAF/AP 请求 BSF 为其协商生成同样的 GBA 会话密钥，也即所述第一密钥。这里的 NAF/AP 向 C-V2X 服务提供者（例如 C-V2X 应用服务器）提供 GBA 服务。NAF/AP 从 BSF 获得该 GBA 会话密钥，也即所述第一密钥，从而完成了终端与网络设备协商第一密钥的过程。

在 C-V2X 设备需要与服务器安全地进行业务消息交互（如申请数字证书）时，C-V2X 设备向服务器发起应用请求。此时，服务器通过与网络设备预先建立的安全连接访问 NAF/AP，请求 NAF/AP 基于第一密钥为本次业务生成第二密钥，并获取生成的第二密钥。基于第二密钥，C-V2X 终端与服务器间可对交互的业务消息进行加密、完整性保护等安全处理，相当于在 C-V2X 终端与服务器间建立起安全的通信通道。

其中，这里的服务器可以为 C-V2X 应用服务器（C-V2X application server），C-V2X 应用服务器可以是 CA 服务器（CA 为 Certificate Authority，也即证书颁发机构）。在这一架构下 CA 服务器可以：为注册 CA 服务器或授权 CA 服务器。也即如果 C-V2X 设备要申请注册证书，则服务器相应为注册 CA 服务器（Enrolment CA server 或 ECA）；如果 C-V2X 要申请授权证书或应用证书或身份证书，则服务器相应为授权 CA 服务器（Authorization CA server 或 ACA）。CA 服务器可由 MNO 自己部署或第三方部署，从而可以为 C-V2X 设备提供证书服务。

这里的 C-V2X 终端与服务器间建立起安全的通信通道是指：终端设备通过上述 GBA 认证流程后，会获得第一密钥，后续会基于第一密钥生成第二密钥。而服务器侧可以从网络设备处获得第二密钥（网络设备 NAF/AP 已经预先与终端协商好了第一密钥，并在服务器需要第二密钥时，基于第一密钥生成第二密钥，将第二密钥返回给服务器，后续会对这一流程进行详细说明）。可见，终端设备与服务器都获得了第二密钥，并且基于第二密钥进行消息的安全保护及收发，从而终端设备与服务器之间实际建立了一

个安全通道（或称为安全连接、安全链路等），用于基于第二密钥对所收发的消息进行良好地保护。

此外，这里的所述第一密钥也可称为共享会话密钥；基于第一密钥生成第二密钥，所述第二密钥也可称为应用会话密钥或会话密钥。

需要说明的是，应用该方法的终端设备可以部署在如图 3 所示的 GBA 增强架构中。在增强的架构中，网络设备 NAF/AP 由少数几个 C-V2X 应用服务器（例如 CA 服务器）共享（参见图 3 中 C-V2X 服务提供者（C-V2X Service Provider）虚框，虚框中不包含 NAF/AP 网元，而是将 NAF/AP 网元部署在移动网络运营商（MNO，Mobile Network Operator）侧，且多个 CA 服务器（图中为 C-V2X 应用服务器（C-V2X Application Server））共享一个 NAF/AP 网元）。不难理解，多个 CA 服务器共享一个 NAF/AP 网元能够大大降低部署成本，降低维护难度。

进一步的，基于引导服务器功能（BSF，Bootstrapping Server Function）在 GBA 引导的安全关联过程中提供的 GBA 会话密钥（例如 Ks_int_NAF），网络设备 NAF/AP 进一步为每个 C-V2X 应用服务器（例如 CA 服务器）派生出 GBA 应用会话密钥（用 K*表示），并将 K*共享给 CA 服务器。同时，C-V2X 设备（C-V2X Device）也从本地获取与 GBA 引导过程中相同的 K*，然后提供 K*给上层的 C-V2X 应用客户端（C-V2X Application Client）调用。这样，CA 服务器和 C-V2X 设备共享相同的 GBA 应用会话密钥 K*。他们可以使用 K*实现相互认证，保护传输的消息，建立安全通道等，然后用共享的 GBA 应用会话密钥 K*对 C-V2X 证书申请及发放过程进行保护。

本实施例的方法可允许用户通过“一键”触发方式实现数字证书配置，具体来说，用户通过终端上的人机界面点击触发或者通过其他接口软件触发，可以很容易地触发终端启动证书配置操作。接收到触发命令后，终端可自动与服务器完成接入认证、安全通道建立、密钥生成、数字证书申请

以及后续的数字证书下载及安全存储等操作，实现终端设备的初始安全配置。该方式相比于现有的离线部署以及在线部署方式来说，自动化程度高、应用及维护成本较低、人工操作步骤少、易于推广。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端（也可以称为 C-V2X application client）、基带芯片（也可以称为设备调制解调器 Device modem，用于接入 4G 或 5G 网络）和全球用户识别模块（USIM，Universal Subscriber Identity Module）；所述终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护，包括：所述应用客户端通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；所述应用客户端生成第一证书请求消息，并通过所述基带芯片向所述 USIM 发送所述第一证书请求消息；所述 USIM 生成公私钥对，在所述第一证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息；所述 USIM 基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，在所述第二证书请求消息中添加第一校验值；所述 USIM 通过所述基带芯片向所述应用客户端发送经过上述处理的所述第二证书请求消息。

其中，这里的第二密钥可以仅由一种密钥组成，也可以由多种密钥组成（也即这里的多种密钥都是基于第一密钥生成的，统称为第二密钥）。一种可行的实施方式中，第二密钥由多种密钥组成，例如可以包括加密密钥和/或完整性保护密钥，当然还可以根据实际需要包括其他类型的密钥，此处不再赘述。进而，USIM 基于所述第二密钥对所述第二证书请求消息进行加密的过程包括：USIM 利用第二密钥中的加密密钥对明文的第二证书请求消息进行加密，使其变成密文。和/或，USIM 基于所述第二密钥对所述第二证书请求消息进行完整性保护的过程包括：USIM 利用第二密钥中的完整

性保护密钥对消息进行完整性保护，例如可以对加密后的消息利用完整性保护密钥计算出第一校验值，然后将计算出的第一校验值添加到所述第二证书请求消息中。其中，可选地，所述第一校验值可以是哈希运算消息认证码（HMAC，Hash-based Message Authentication Code）值，示例性的，USIM 可基于消息中的某些比特位进行计算，得到所述第一校验值。需要说明的是，“将计算出的第一校验值添加到请求消息中”其实是消息完整性保护过程的一个步骤，这里为了能够更清晰的说明后续如何对于第二证书请求消息进行保护，才将此步骤重点强调。

图 4 为本申请实施例的终端设备的一种可选架构示意图；如图 4 所示，终端设备可包括应用（Application）层、用户库（User libraries）、Linux 内核（Linux Kernel）以及硬件（Hardware）层等等。其中，应用层可包括 CA 管理应用和 V2X 应用；用户库包括 GBA 接口库、USIM 接口库、硬件安全模块（HSM，Hardware Security Module）接口库以及 LTE-V2X 接口库等等；硬件层包括 HSM、LTE-V2X 通信模组和 LTE-Uu 通信模组，LTE-Uu 通信模组中可包括基带芯片和 USIM。其中，LTE-Uu 通信模组、LTE-V2X 通信模组以及 HSM 以分立模块或元器件的方式实现，或者也可封装集成为一个模块/模组，但这不影响它们之间的逻辑功能划分。

本示例中，CA 管理应用（也即 CA 应用客户端（CA application client））是终端设备（例如 C-V2X 终端设备）实现“初始安全一键配置”的控制软件，它负责整个业务流程的逻辑控制。V2X 应用（也可称为 C-V2X 应用）是终端设备通过 PC5/V5 接口实现 V2X 直连通信的业务应用模块，负责直连通信业务消息的收发控制。它通过调用 LTE-V2X 接口库访问硬件层的 LTE-V2X 通信模组，与其他终端设备实现 C-V2X 业务交互。

GBA 接口库、USIM 接口库，HSM 接口库是终端底层硬件模块开放给上层应用的调用接口，分别用于调用 LTE-Uu 通信模组支持的 GBA 安全接

入认证能力、USIM 提供的数字证书管理应用能力和安全能力以及 HSM 提供的安全存储及运算能力。

当然，本申请实施例中的终端设备的组成架构不限于图 4 中所示，其他的架构形式也可在本申请实施例的保护范围之内。

本实施例中的应用客户端负责实现 CA 管理应用的功能，负责终端设备数字证书的管理，具体可参照图 4 中的 CA 管理应用。

本实施例中，应用客户端通过所述基带芯片、调用 USIM 接口库触发所述 USIM 基于所述第一密钥生成第二密钥。应用客户端可根据“一键触发”生成第一证书请求消息，调用 USIM 重构证书请求接口（即第一 USIM 接口）、通过所述基带芯片向所述 USIM 发送所述第一证书请求消息；当然，本实施例中所述第一 USIM 接口不限于是 USIM 重构证书请求接口，其他用于重构证书请求的接口名称也可在本申请实施例的保护范围之内。USIM 接收到第一证书请求消息后，可基于通用集成电路卡（UICC，Universal Integrated Circuit Card）内部的随机数发生器生成公私钥对，按照 C-V2X 相关规范的协议格式的要求，完善证书请求消息，在第一证书请求消息中添加公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息，USIM 基于第二密钥对第二证书请求进行加密和/或完整性保护。接着，USIM 通过所述基带芯片并通过接口库向所述应用客户端发送经上述处理的所述第二证书请求消息。

其中，这里的 UICC 是一种安全级别达到 EAL 4+的安全硬件，可基于它实现 USIM 功能，可以保证 Ks_int_NAF（也即第一密钥）的安全性。具体来说，UICC 可以理解为是一种通用架构，或者可以理解为是一种安全载体，当 USIM 功能（function）被实施在这一通用架构中，则实现了 USIM 功能，也即成为 USIM。UICC 其实还可以实现很多应用，也即该架构中可以支持实施很多功能，在本申请实施例中实现的是 USIM，因此 USIM 也具

有很高的安全性，进而在 USIM 中进行证书公私钥对生成、密码运算、安全存储等操作能够有效保证终端的安全性。避免出现现有技术中，由于密钥在不安全的终端 CPU、内存等器件中运算、存储所带来的敏感信息泄露之类的安全隐患。且通过将已有的 USIM 作为终端上的安全器件进行上述安全操作，能够避免在终端上增加新的安全硬件，从而降低终端的硬件实现成本。

示例性的，本实施例中的数字证书也可称为注册证书（EC，Enrollment Certificate），用于标识一个可信的终端设备，因此需要以安全的方法实现数字证书在终端设备上的初始安全配置。相应的，本实施例中的服务器可以为 ECA 服务器，也即授权 CA 服务器。

在本申请的一些可选实施例中，所述发送第一请求消息，包括：所述应用客户端向服务器发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述第二证书请求消息；所述第一请求消息中还包括：引导事务标识（B-TID，Bootstrapping-Transaction Identifier）和/或服务器全限定域名（FQDN，Fully Qualified Domain Name）。

在本申请的一些可选实施例中，所述方法还包括：所述终端设备接收来自服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书。

本实施例中，示例性的，所述第一响应消息可通过超文本传输协议（HTTP，HyperText Transfer Protocol）消息承载，例如可通过 HTTP 200 OK 消息承载。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和 USIM；所述终端设备接收来自所述服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书，包括：所述应用客户端接收来自所述服务

器的第一响应消息，并通过所述基带芯片向所述 USIM 发送所述第一响应消息；所述 USIM 基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密；校验通过后，所述 USIM 获得所述第一响应消息中携带的数字证书，并在安全组件中存储所述数字证书。

本实施例中，应用客户端接收来自所述CA服务器的第一响应消息，调用USIM安全检验接口(即第二USIM接口)通过所述基带芯片向所述USIM发送所述第一响应消息；当然，本实施例中所述第二 USIM 接口不限于是USIM 安全检验接口，其他用于安全检验的接口也可在本申请实施例的保护范围之内。USIM 基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，其中，第一响应消息中携带第二校验值，所述完整性校验即校验所述第一响应消息中携带的第二校验值；其中，可选地，所述第二校验值也可以是 HMAC 值，示例性的，USIM 可基于消息中的某些比特位进行计算，得到一个校验值，再将该校验值与所述第二校验值进行比对，比对一致则表明所述完整性校验通过。校验通过后，所述 USIM 获得所述第一响应消息中携带的数字证书。

本实施例中，所述 USIM 在安全组件中存储所述数字证书。示例性的，USIM（还可包括 HSM）是终端设备本地的安全实体/模块，能够为数据的运算、存储、处理提供可靠的安全环境。为了确保 V2X 业务数据的安全性，密钥（例如第一密钥、公私钥对等敏感参数）、数字证书等以及涉及它们的运算通常应在终端设备本地的安全实体/模块中处理，因此保证 C-V2X 终端设备数字证书安全配置过程的安全性。

基于前述实施例，本申请实施例还提供了一种终端设备的配置方法。图 5 为本申请实施例的终端设备的配置方法的流程示意图二；如图 5 所示，所述方法包括:

步骤 201：服务器接收来自终端设备的第一请求消息；所述第一请求消

息中包括经第二密钥加密和/或完整性保护的证书请求消息；

步骤 202：获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；

步骤 203：基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书；

步骤 204：向所述终端设备发送第一响应消息，所述第一响应消息中包括所述数字证书。

本实施例中，在用户的“一键”触发下，终端设备可基于 GBA 技术机制或 AKMA 认证机制自动完成服务器接入认证以及安全通道的建立、密钥生成以及数字证书的申请以及后续的数字证书的下载及安全存储等操作，实现终端设备的初始安全配置。

本实施例中，所述服务器通过上述建立的安全通道接收来自终端设备的第一请求消息。示例性的，所述服务器可通过网络设备接收来自终端设备的第一请求消息，即，第一请求消息经终端设备发出、到达网络设备，再经由网络设备将第一请求消息发送至服务器。

本实施例中，由于第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息，则服务器需要获得上述第二密钥。示例性的，服务器从网络设备处获得所述第二密钥。在终端设备执行 GBA 认证流程或 AKMA 认证流程过程中，终端设备与网络设备协商第一密钥，所述第一密钥也可称为共享会话密钥。

在一些可选实施方式中，所述服务器获得来自网络设备的所述第二密钥，包括：所述服务器向所述网络设备发送第二请求消息，所述第二请求消息用于请求所述第二密钥；所述服务器接收所述网络设备发送的第二响应消息，所述第二响应消息中包括所述第二密钥。

本实施例中，服务器可向网络设备发送第二请求消息，所述第二请求

消息用于请求第二密钥；则网络设备接收到所述第二请求消息后，基于预先协商的第一密钥生成第二密钥，再向服务器发送第二响应消息，所述第二响应消息中包括所述第二密钥，由此使得服务器获得所述第二密钥。

在另一些可选实施方式中，网络设备在接收到终端设备发送的用于请求数字证书的第一请求消息后，也可基于预先协商的第一密钥生成第二密钥，在向服务器发送该第一请求消息的过程中，将所述第二密钥发送至所述服务器。

在本申请的一些可选实施例中，所述第一请求消息中还包括：B-TID；所述服务器获得来自网络设备的所述第二密钥，包括：所述服务器查询是否存在与所述 B-TID 对应的第二密钥；在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥。

本实施例中，服务器中可能预先获得与 B-TID 对应的第二密钥。则在接收到第一请求消息后，可先通过第一请求消息中携带的 B-TID 查询是否存在与所述 B-TID 对应的第二密钥；在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥；在存在与所述 B-TID 对应的第二密钥的情况下，可直接获得所述 B-TID 对应的第二密钥。

本实施例中，由于终端设备发送的消息是经过第二密钥加密和/或完整性保护的，服务器获得第二密钥后，基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书。

本实施例中，所述证书请求消息中还包括第一校验值，所述第一校验值可以是 HAMC 值，所述服务器可基于第一请求消息中的某些比特位进行计算，得到一个校验值，再将该校验值与所述第一校验值进行比对，比对一致则表明完整性校验通过。

在本申请的一些可选实施例中，所述服务器向所述终端设备发送第一响应消息，包括：所述服务器构建包含有所述数字证书的第一响应消息，基于所述第二密钥对所述第一响应消息进行加密和/或完整性保护，在所述第一响应消息中添加第二校验值，向所述终端设备发送经过上述处理的第一响应消息。同样的，这里的添加第二校验值也属于对第一响应消息进行完整性保护过程的一部分，为便于更清晰的说明后续终端如何基于第一响应消息进行处理，本实施例中才将添加第二校验值这一步骤重点强调。

本实施例中，服务器在签发数字证书后，按照 C-V2X 相关规范的协议格式要求，构建第一响应消息（或证书响应消息），并基于第一响应消息中的某些比特位进行计算，得到第二校验值，将第二校验值添加至所述第一响应消息中，并向所述终端设备发送经上述处理的第一响应消息。示例性的，所述第一响应消息可通过 HTTP 消息承载，例如可通过 HTTP 200 OK 消息承载。

基于前述实施例，本申请实施例还提供了一种终端设备的配置方法。图 6 为本申请实施例的终端设备的配置方法的流程示意图三；如图 6 所示，所述方法包括：

步骤 301：网络设备基于预先协商的第一密钥生成第二密钥；

步骤 302：向服务器发送所述第二密钥。

本实施例中，所述网络设备具体可以是 NAF/AP。终端设备执行 GBA 认证流程或 AKMA 认证流程，开始建立与服务器之间的安全访问连接（或安全通道、安全链路等等），认证完成后，终端设备与网络设备已协商好第一密钥，所述第一密钥也可称为共享会话密钥。

在一些可选实施例中，网络设备可接收服务器的第二请求消息，所述第二请求消息用于请求第二密钥，则所述网络设备基于预先协商的第一密钥生成第二密钥，再向服务器发送第二响应消息，所述第二响应消息中包

括所述第二密钥，由此使得服务器获得所述第二密钥。在另一些可选实施例中，网络设备在接收到终端设备发送的用于请求数字证书的第一请求消息后，也可基于预先协商的第一密钥生成第二密钥，在向服务器发送该第一请求消息的过程中，将所述第二密钥发送至所述服务器。

在本申请的一些可选实施例中，所述方法还包括：所述网络设备与终端设备通过执行 GBA 认证流程或 AKMA 认证流程，与所述终端设备协商所述第一密钥。

采用本申请实施例的技术方案，基于 GBA 机制，可通过“一键配置”的方式实现 C-V2X 终端设备的数字证书的安全配置，无需生产线安全环境的改造，也无需专业的安全机构进行灌装，提升数字证书配置的灵活性、降低部署难度以及投资成本。

下面结合具体的场景对本申请实施例的终端设备的配置方法进行说明。

本示例中，以终端设备为 C-V2X 设备（C-V2X Device）、网络设备为 NAF/AP 为例进行说明。其中，C-V2X 设备中包括 USIM、基带芯片和应用客户端；基带芯片也可称为设备调制解调器（Device Modem），应用客户端也可称为（C-V2X Application Client），上述实施例中的 CA 服务器在本示例中称为应用服务器或 C-V2X 应用服务器（C-V2X Application Server）。图 7 为本申请实施例的终端设备的配置方法的交互流程示意图一；如图 7 所示，所述方法包括：

步骤 401、C-V2X 应用客户端向基带芯片发起 GBA 启动请求。

在需要对 C-V2X 设备进行初始化、配置数字证书时，应用客户端通过 GBA 接口库调用底层基带芯片启动 GBA 认证流程，开始建立至 CA 服务器（如 ECA 服务器）的安全访问连接。

步骤 402、执行 GBA 认证流程，与 NAF/AP 协商共享会话密钥

Ks_int_NAF（即前述实施例中的第一密钥）。

步骤403、基带芯片向C-V2X应用客户端发送对应于GBA启动请求的GBA响应。

步骤404-步骤408、在采用GBA增强技术的情况下，C-V2X应用客户端通过接口调用，即调用USIM接口库（例如USIM重构证书请求接口）向USIM传送消息，以触发USIM基于Ks_int_NAF生成应用会话密钥K*（即第二密钥）；USIM通过基带芯片以及接口返回，即调用USIM接口库向C-V2X应用客户端进行消息传送，以告知C-V2X应用客户端已生成应用会话密钥K*。

示例性的，C-V2X应用客户端向USIM传送的消息可携带B-TID、IMPI和NAF标识（ID）；USIM接收到消息后，基于Ks_int_NAF生成应用会话密钥K*。

步骤409-步骤410、C-V2X应用客户端组建证书请求消息（即前述第一证书请求消息），准备向CA服务器申请数字证书。C-V2X应用客户端通过接口调用，即调用USIM重构证书请求接口、通过基带芯片向USIM进行消息传送，传送的消息中携带准备好的证书请求消息（即前述实施例中的第一证书请求消息）。

步骤411、接收到证书请求消息后，USIM生成公私钥对，在证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对证书请求消息进行签名，获得第二证书请求消息；基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，在所述第二证书请求消息中添加HMAC值。

具体的，USIM执行如下操作：

1）使用UICC内部的随机数发生器为EC数字证书生成所需的密码公私钥对；

2）按照 C-V2X 相关规范的协议要求，完善证书请求消息，其中增加所生成的公私钥对中的公钥;

3）使用公私钥对中的私钥对证书请求消息进行签名;

4）使用应用会话密钥 K*对证书请求消息进行加密及完整性保护，并将 HMAC 值加入到消息中，得到第二证书请求消息。

步骤 412-步骤 413、USIM 通过基带芯片以及接口返回，即通过调用 USIM 接口库向 C-V2X 应用客户端进行消息传送，传送的消息中包含经过应用会话密钥 K*加密和/或完整性保护的第二证书请求消息。

步骤 414、C-V2X 应用客户端向 CA 服务器发送请求消息，请求消息中携带受 K*保护的第二证书请求消息以及 B-TID、Server FQDN 等信息。

其中，示例性的，所述请求消息经 NAF/AP 传输至 CA 服务器。

步骤 415-步骤 417、CA 服务器通过预先建立的安全通道与 NAF/AP 交互，请求 NAF/AP 基于 Ks_int_NAF 生成应用会话密钥 K*，并获取应用会话密钥 K*及其相关信息。所述相关信息例如可包括应用会话密钥 K*的生存时间等等。

其中，NAF/AP 可通过 HTTP 200 OK 响应消息向 CA 服务器发送应用会话密钥 K*及其相关信息。

其中，CA 服务器向 NAF/AP 发送的请求消息中还可包括 B-TID、服务器 FQDN（Server FQDN）等信息。

步骤 418、CA 服务器获取应用会话密钥 K*之后，基于应用会话密钥 K*对请求消息进行完整性校验和/或解密，并在对请求消息授权通过后签发数字证书；构建包含有所述数字证书的响应消息，基于应用会话密钥 K*对所述响应消息进行加密和/或完整性保护，在所述响应消息中添加 HMAC 值。

具体的，CA 服务器可执行如下操作:

1）使用应用会话密钥 K*校验请求消息的 HMAC 值，解密消息；

2)对证书请求消息进行授权检验；在授权检验通过的情况下，为 C-V2X 设备签发数字证书；

3）按照 C-V2X 相关规范的协议要求，构建响应消息，响应消息中包含签发的数字证书；

4）使用应用会话密钥 K*对响应消息进行加密及完整性保护，并将 HMAC 值加入到响应消息中。

步骤 419、CA 服务器向 C-V2X 应用客户端返回经应用会话密钥 K*保护的响应消息；示例性的，该响应消息可通过 HTTP 200 OK 消息承载。

步骤 420-步骤 421、C-V2X 应用客户端通过接口调用，即调用 USIM 安全检验接口、并经基带芯片向 USIM 进行消息传送，传送的消息中携带上述经应用会话密钥 K*保护的响应消息。

步骤 422-步骤 424、USIM 使用应用会话密钥 K*对响应消息进行完整性校验和/或解密；校验成功之后，USIM 将 CA 服务器签发的数字证书在安全组件中安全存储，并通过接口返回、经基带芯片向 C-V2X 应用客户端传送结果状态指示。

本申请实施例还提供了一种终端设备的配置装置，应用于终端设备中。图 8 为本申请实施例的终端设备的配置装置的组成结构示意图一；如图 8 所示，所述装置包括：第一生成单元 11 和第一通信单元 12；其中，

所述第一生成单元 11，配置为基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护；

所述第一通信单元 12，配置为发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

在本申请的一些可选实施例中，所述第一通信单元 12，还配置为接收来自服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行

完整性校验和/或解密，获得所述第一响应消息中携带的数字证书。

在本申请的一些可选实施例中，所述第一生成单元 11 包括：应用客户端、基带芯片和 USIM;

所述应用客户端，配置为通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；还配置为生成第一证书请求消息，并通过所述基带芯片向所述 USIM 发送所述第一证书请求消息;

所述 USIM，配置为生成公私钥对，在所述第一证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息；基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，并在所述第二证书请求消息中添加第一校验值；通过所述基带芯片向所述应用客户端发送经所述第二密钥加密和/或完整性保护的所述第二证书请求消息。

在本申请的一些可选实施例中，所述应用客户端，配置为通过所述第一通信单元 12 向服务器发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述第二证书请求消息；所述第一请求消息中还包括：B-TID 和/或服务器 FQDN。

在本申请的一些可选实施例中，所述第一生成单元 11 包括：应用客户端、基带芯片和 USIM;

所述应用客户端，配置为通过所述第一通信单元 12 接收来自所述服务器的第一响应消息，并通过所述基带芯片向所述 USIM 发送所述第一响应消息;

所述 USIM，配置为基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密；校验通过后，获得所述第一响应消息中携带的数字证书，并在安全组件中存储所述数字证书。

在本申请的一些可选实施例中，所述装置还包括第一执行单元，配置

为执行GBA认证流程或AKMA认证流程，与网络设备协商所述第一密钥。

本申请实施例中，所述装置中的第一生成单元11、第一通信单元12和第一执行单元，在实际应用中均可由中央处理器（CPU，Central Processing Unit）、数字信号处理器（DSP，Digital Signal Processor）、微控制单元（MCU，Microcontroller Unit）或可编程门阵列（FPGA，Field－Programmable Gate Array）结合通信模组（包含：基础通信套件、操作系统、通信模块、标准化接口和协议等）及收发天线实现。

本申请实施例还提供了一种终端设备的配置装置，应用于服务器中。图9为本申请实施例的终端设备的配置装置的组成结构示意图二；如图9所示，所述装置包括：第二通信单元21和校验单元22；其中，

所述第二通信单元21，配置为接收来自终端设备的第一请求消息；所述第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息；

所述校验单元22，配置为获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；还配置为基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书；

所述第二通信单元21，还配置为向所述终端设备发送第一响应消息，所述第一响应消息中包括所述数字证书。

在本申请的一些可选实施例中，所述第二通信单元21，配置为构建包含有所述数字证书的第一响应消息，基于所述第二密钥对所述第一响应消息进行加密和/或完整性保护，在所述第一响应消息中添加第二校验值，向所述终端设备发送经上述处理后的第一响应消息。

在本申请的一些可选实施例中，所述第一请求消息中还包括：B-TID；

所述装置还包括第二执行单元，配置为查询是否存在与所述B-TID对应的第二密钥；在查询结果为不存在与所述B-TID对应的第二密钥的情况

下，通过所述第二通信单元获得来自网络设备的所述第二密钥。

在本申请的一些可选实施例中，所述第二通信单元 21，配置为向所述网络设备发送第二请求消息，所述第二请求消息用于请求所述第二密钥；接收所述网络设备发送的第二响应消息，所述第二响应消息中包括所述第二密钥。

本申请实施例中，所述装置中的第二通信单元 21、校验单元 22 和第二执行单元，在实际应用中均可由 CPU、DSP、MCU 或 FPGA 结合通信模组（包含：基础通信套件、操作系统、通信模块、标准化接口和协议等）及收发天线实现。

本申请实施例还提供了一种终端设备的配置装置，应用于网络设备中。图 10 为本申请实施例的终端设备的配置装置的组成结构示意图三；如图 10 所示，所述装置包括第二生成单元 31 和第三通信单元 32；其中，

所述第二生成单元 31，配置为基于预先协商的第一密钥生成第二密钥；

所述第三通信单元 32，配置为向服务器发送所述第二密钥。

在本申请的一些可选实施例中，所述装置还包括第三执行单元，配置为与终端设备通过执行 GBA 认证流程或 AKMA 认证流程，与所述终端设备协商所述第一密钥。

在本申请的一些可选实施例中，所述第二生成单元 31，配置为基于预先协商的第一密钥，为每个服务器生成对应的第二密钥；

所述第三通信单元 32，配置为分别向每个服务器发送所述对应的第二密钥。

在本申请的一些可选实施例中，所述第三通信单元 32，配置为接收所述服务器发送的第二请求信息，所述第二请求消息用于请求所述第二密钥；向所述服务器发送第二响应消息，所述第二响应消息中包括所述第二生成单元 31 生成的所述第二密钥。

本申请实施例中，所述装置中的第二生成单元31、第三通信单元32和第三执行单元，在实际应用中均可由CPU、DSP、MCU或FPGA结合通信模组（包含：基础通信套件、操作系统、通信模块、标准化接口和协议等）及收发天线实现。

需要说明的是：上述实施例提供的终端设备的配置装置在进行配置时，仅以上述各程序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处理分配由不同的程序模块完成，即将装置的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的终端设备的配置装置与终端设备的配置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。

本申请实施例还提供了一种终端设备的配置方法。图11为本申请实施例的终端设备的配置方法的流程示意图四；如图11所示，所述方法包括：

步骤501：终端设备基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护；

步骤502：发送第一消息。

本实施例的终端设备的配置方法（以下简称方法）应用于终端设备中，所述终端设备具体可以是车联网终端设备（也可以称为C-V2X Device），在一些可选实施例中，所述车联网终端设备例如可以是OBU、RSU等等；在另一些可选实施例中，所述车联网终端设备也可以是行人的手持设备、可穿戴设备等等。

在本申请的一些可选实施例中，所述方法还包括：所述终端设备执行GBA认证流程或AKMA认证流程，与网络设备协商所述第一密钥。具体过程可参见前述实施例中终端设备的配置方法的详细记载，这里不再赘述。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和USIM；所述终端设备基于第一密钥生成第二密钥，基于所述第二

密钥对第一消息的部分或全部进行加密和/或完整性保护，包括：所述应用客户端通过所述基带芯片触发所述USIM基于所述第一密钥生成第二密钥；所述应用客户端生成第一消息，并通过所述基带芯片向所述 USIM 发送所述第一消息；所述 USIM 基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护；所述 USIM 通过所述基带芯片向所述应用客户端发送经上述处理后的所述第一消息。

本实施例中，第二密钥可以仅由一种密钥组成，也可以由多种密钥组成（也即这里的多种密钥都是基于第一密钥生成的，统称为第二密钥）。一种可行的实施方式中，第二密钥由多种密钥组成，例如可以包括加密密钥和/或完整性保护密钥，当然还可以根据实际需要包括其他类型的密钥，此处不再赘述。进而，USIM基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护，其加密和/或完整性保护的具体过程可参照前述实施例中所述，这里不再赘述。

本实施例中，所述第一消息可以是终端设备发送给服务器的任意消息、信息等。

在本申请的一些可选实施例中，所述发送第一消息，包括：所述应用客户端向服务器发送所述第一消息；所述第一消息中还包括：B-TID 和/或服务器的 FQDN；或者包括：AKMA 密钥标识符（A-KID）和/或 FQDN。

在本申请的一些可选实施例中，所述方法还包括：所述终端设备接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

本实施例中，所述第二消息可以是服务器发送给终端设备的任意消息、信息等。

在本申请的一些可选实施例中，所述终端设备包括：应用客户端、基带芯片和 USIM；所述终端设备接收来自服务器的第二消息，基于所述第二

密钥对所述第二消息进行完整性校验和/或解密，包括：所述应用客户端接收来自所述服务器的第二消息，并通过所述基带芯片向所述 USIM 发送所述第二消息；所述 USIM 基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

本实施例中，应用客户端接收来自服务器的第二消息，调用 USIM 安全检验接口通过所述基带芯片向所述 USIM 发送所述第二消息；当然，本实施例中接口不限于是 USIM 安全检验接口，其他用于安全检验的接口也可在本申请实施例的保护范围之内。USIM 基于所述第二密钥对所述第二消息进行完整性校验和/或解密，其完整性校验和/或解密的具体过程可参照前述实施例中所述，这里不再赘述。进而，USIM 将解密获得的明文信息和/或处理结果返回给应用客户端。

基于上述实施例，本申请实施例还提供了一种终端设备的配置方法。图 12 为本申请实施例的终端设备的配置方法的流程示意图四；如图 12 所示，所述方法包括：

步骤 601：服务器接收来自终端设备的第一消息，所述第一消息的部分或全部经第二密钥加密和/或完整性保护；

步骤 602：所述服务器获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；

步骤 603：所述服务器基于所述第二密钥对所述第一消息进行完整性校验和/或解密。

本实施例中，在用户的“一键”触发下，终端设备可基于 GBA 技术机制或 AKMA 认证机制自动完成服务器接入认证以及安全通道的建立和密钥生成等操作，实现终端设备的初始安全配置。

本实施例中，所述服务器通过上述建立的安全通道接收来自终端设备的第一消息。示例性的，所述服务器可通过网络设备接收来自终端设备的

第一消息，即，第一请求消息经终端设备发出、到达网络设备，再经由网络设备将第一消息发送至服务器。

本实施例中，由于第一消息的部分或全部经第二密钥加密和/或完整性保护处理，则服务器需要获得上述第二密钥。示例性的，服务器从网络设备处获得所述第二密钥。在终端设备执行 GBA 认证流程或 AKMA 认证流程过程中，终端设备与网络设备协商第一密钥，所述第一密钥也可称为共享会话密钥。

在一些可选实施方式中，所述服务器获得来自网络设备的所述第二密钥，包括：所述服务器向所述网络设备发送第三消息，所述第三消息用于请求所述第二密钥；所述服务器接收所述网络设备发送的第四消息，所述第四消息中包括所述第二密钥。

本实施例中，服务器可向网络设备发送第三消息，所述第三消息用于请求第二密钥；则网络设备接收到所述第三消息后，基于预先协商的第一密钥生成第二密钥，再向服务器发送第四消息，所述第四消息中包括所述第二密钥，由此使得服务器获得所述第二密钥。

另一些可选实施方式中，网络设备在接收到终端设备发送的第一消息后，也可基于预先协商的第一密钥生成第二密钥，在向服务器发送该第一消息的过程中，将所述第二密钥发送至所述服务器。

在本申请的一些可选实施例中，所述第一消息中还包括：B-TID，或者包括 AKMA 密钥标识符（A-KID）；所述服务器获得来自网络设备的所述第二密钥，包括：所述服务器查询是否存在与所述 B-TID 或所述 A-KID 对应的第二密钥；在查询结果为不存在与所述 B-TID 或所述 A-KID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥。

本实施例中，服务器中可能预先获得与 B-TID 对应的第二密钥。则在接收到第一请求消息后，可先通过第一请求消息中携带的 B-TID 查询是否

存在与所述 B-TID 对应的第二密钥；在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥；在存在与所述 B-TID 对应的第二密钥的情况下，可直接获得所述 B-TID 对应的第二密钥。

在本申请的一些可选实施例中，所述方法还包括：所述服务器基于所述第二密钥对第二消息的部分或全部进行加密和/或完整性保护；发送第二消息。

本实施例中，服务器在待向终端设备发送第二消息时，按照相关规范的协议格式要求，构建第二消息，具体是基于第二密钥对第二消息的部分或全部进行加密和/或完整性保护，其加密和/或完整性保护的具体过程可参照前述实施例中所述，这里不再赘述。

下面结合具体的场景对本申请实施例的终端设备的配置方法进行说明。

本示例中，以终端设备为 UE、网络设备为 AF 为例进行说明。其中，UE 中包括 USIM、基带芯片和应用客户端；基带芯片也可称为设备调制解调器（Device Modem），应用客户端也可称为（C-V2X Application Client），上述实施例中的服务器在本示例中称为应用服务器（Application Server）或 C-V2X 应用服务器（C-V2X Application Server）。图 13 为本申请实施例的终端设备的配置方法的交互流程示意图二；如图 13 所示，所述方法包括：

步骤 701、UE 启动 AKMA。

在需要对 C-V2X 设备进行初始化、配置数字证书时，应用客户端通过 GBA 接口库调用底层基带芯片启动 GBA 认证流程，开始建立至 CA 服务器（如 ECA 服务器）的安全访问连接。

步骤 702、执行 AKMA 认证流程，与 AF 协商共享会话密钥 K_{AF}（即前述实施例中的第一密钥）。

步骤 703、UE 获得共享会话密钥 K_{AF}。

步骤 704-步骤 705、UE 基于共享会话密钥 K_{AF} 生成应用会话密钥 K*，使用应用会话密钥 K*对消息（上行消息）进行加密和/或完整性保护。

示例性的，应用客户端通过基带芯片向 USIM 传送消息，消息中可携带 B-TID 等信息；USIM 接收到消息后，基于共享会话密钥 K_{AF} 生成应用会话密钥 K*，并利用应用会话密钥 K*对消息的部分或全部进行加密或完整性保护，通过基带芯片向应用客户端发送经上述处理后的消息。

步骤 706、UE 向应用服务器发送消息（即上行消息），消息中携带受应用会话密钥 K*保护的上行消息以及 B-TID、服务器 FQDN（Server FQDN）等信息。

其中，示例性的，所述消息经 AF 传输至应用服务器。

步骤 707-步骤 709、应用服务器通过预先建立的安全通道与 AF 交互，请求 AF 基于共享会话密钥 K_{AF} 生成应用会话密钥 K*，并获取应用会话密钥 K*及其相关信息。所述相关信息例如可包括应用会话密钥 K*的生存时间等等。

其中，AF 可通过 HTTP 200 OK 响应消息向应用服务器发送应用会话密钥 K*及其相关信息。

其中，应用服务器向 AF 发送的请求消息中还可包括 B-TID、服务器 FQDN（Server FQDN）等信息。

步骤 710、应用服务器获取应用会话密钥 K*之后，使用应用会话密钥 K*对消息进行完整性校验和/或解密。

以上为终端与应用服务器之间的上行消息的传输过程。

步骤 711、应用服务器使用应用会话密钥 K*对消息（下行消息）进行加密和/或完整性保护。

步骤 712、应用服务器向 UE 发送消息（下行消息）。

步骤 713、UE 使用应用会话密钥 K*对消息进行完整性校验和/或解密。

步骤 714、UE 与应用服务器之间可使用应用会话密钥 K*安全传输上下行消息。

基于上述实施例，本申请实施例还提供了一种终端设备的配置装置，应用于终端设备中。图 14 为本申请实施例的终端设备的配置装置的组成结构示意图四；如图 14 所示，所述装置包括：第三生成单元 51 和第四通信单元 52；其中，

所述第三生成单元 51，配置为基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护；

所述第四通信单元 52，配置为发送第一消息。

在本申请的一些可选实施例中，所述第四通信单元 52，还配置为接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

在本申请的一些可选实施例中，所述第三生成单元 51 包括：应用客户端、基带芯片和 USIM;

所述应用客户端，配置为通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；还配置为生成第一消息，并通过所述基带芯片向所述 USIM 发送所述第一消息;

所述 USIM，配置为基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护；还配置为通过所述基带芯片向所述应用客户端发送经上述处理后的所述第一消息。

在本申请的一些可选实施例中，所述应用客户端，还配置为向服务器发送所述第一消息;

所述第一消息中还包括：B-TID 和/或服务器的 FQDN；或者包括：AKMA 密钥标识符（A-KID）和/或 FQDN。

在本申请的一些可选实施例中，所述第三生成单元 51 包括：应用客户端、基带芯片和 USIM;

所述应用客户端，配置为接收来自所述服务器的第二消息，并通过所述基带芯片向所述 USIM 发送所述第二消息;

所述 USIM，配置为基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

本申请实施例中，所述装置中的第三生成单元 51 和第四通信单元 52，在实际应用中均可由 CPU、DSP、MCU 或 FPGA 结合通信模组（包含：基础通信套件、操作系统、通信模块、标准化接口和协议等）及收发天线实现。

本申请实施例还提供了一种终端设备的配置装置，应用于服务器中。图 15 为本申请实施例的终端设备的配置装置的组成结构示意图四；如图 15 所示，所述装置包括：第五通信单元 61 和第二校验单元 62；其中，

所述第五通信单元 61，配置为接收来自终端设备的第一消息，所述第一消息的部分或全部经第二密钥加密和/或完整性保护;

所述第二校验单元 62，配置为获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；还配置为基于所述第二密钥对所述第一消息进行完整性校验和/或解密。

在本申请的一些可选实施例中，所述装置还包括第四生成单元，配置为基于所述第二密钥对第二消息的部分或全部进行加密和/或完整性保护;

所述第五通信单元 61，还配置为发送第二消息。

在本申请的一些可选实施例中，所述第一消息中还包括：B-TID，或者包括 AKMA 密钥标识符（A-KID）;

所述装置还包括第四执行单元，配置为查询是否存在与所述 B-TID 或所述 A-KID 对应的第二密钥;

所述第二校验单元 62，配置为在所述第四执行单元获得的查询结果为不存在与所述 B-TID 或所述 A-KID 对应的第二密钥的情况下，通过所述第五通信单元 61 获得来自网络设备的所述第二密钥。

本申请实施例中，所述装置中的第五通信单元 61、第二校验单元 62 和第三执行单元，在实际应用中均可由 CPU、DSP、MCU 或 FPGA 结合通信模组（包含：基础通信套件、操作系统、通信模块、标准化接口和协议等）及收发天线实现。

需要说明的是：上述实施例提供的终端设备的配置装置在进行配置时，仅以上述各程序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处理分配由不同的程序模块完成，即将装置的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的终端设备的配置装置与终端设备的配置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。

本申请实施例还提供了一种通信设备。图 16 为本申请实施例的通信设备的硬件组成结构示意图，如图 16 所示，所述通信设备包括存储器 42、处理器 41 及存储在存储器 42 上并可在处理器 41 上运行的计算机程序，所述处理器 41 执行所述程序时实现本申请实施例前述应用于终端设备中的终端设备的配置方法的步骤；或者，所述处理器 41 执行所述程序时实现本申请实施例前述应用于服务器中的终端设备的配置方法的步骤；或者，所述处理器 41 执行所述程序时实现本申请实施例前述应用于网络设备中的终端设备的配置方法的步骤，

可选地，通信设备还可包括一个或多个网络接口 43。可以理解，通信设备中的各个组件通过总线系统 44 耦合在一起。可理解，总线系统 44 用于实现这些组件之间的连接通信。总线系统 44 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 16

中将各种总线都标为总线系统 44。

可以理解，存储器 42 可以是易失性存储器或非易失性存储器，也可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（ROM，Read Only Memory）、可编程只读存储器（PROM，Programmable Read-Only Memory）、可擦除可编程只读存储器（EPROM，Erasable Programmable Read-Only Memory）、电可擦除可编程只读存储器（EEPROM，Electrically Erasable Programmable Read-Only Memory）、磁性随机存取存储器（FRAM，ferromagnetic random access memory）、快闪存储器（Flash Memory）、磁表面存储器、光盘、或只读光盘（CD-ROM，Compact Disc Read-Only Memory）；磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器（RAM，Random Access Memory），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（SRAM，Static Random Access Memory）、同步静态随机存取存储器（SSRAM，Synchronous Static Random Access Memory）、动态随机存取存储器（DRAM，Dynamic Random Access Memory）、同步动态随机存取存储器（SDRAM，Synchronous Dynamic Random Access Memory）、双倍数据速率同步动态随机存取存储器（DDRSDRAM，Double Data Rate Synchronous Dynamic Random Access Memory）、增强型同步动态随机存取存储器（ESDRAM，Enhanced Synchronous Dynamic Random Access Memory）、同步连接动态随机存取存储器（SLDRAM，SyncLink Dynamic Random Access Memory）、直接内存总线随机存取存储器（DRRAM，Direct Rambus Random Access Memory）。本申请实施例描述的存储器 42 旨在包括但不限于这些和任意其它适合类型的存储器。

上述本申请实施例揭示的方法可以应用于处理器 41 中，或者由处理器 41 实现。处理器 41 可能是一种集成电路芯片，具有信号的处理能力。在实

现过程中，上述方法的各步骤可以通过处理器 41 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器 41 可以是通用处理器、DSP，或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器 41 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器 42，处理器 41 读取存储器 42 中的信息，结合其硬件完成前述方法的步骤。

在示例性实施例中，通信设备可以被一个或多个应用专用集成电路（ASIC，Application Specific Integrated Circuit）、DSP、可编程逻辑器件（PLD，Programmable Logic Device）、复杂可编程逻辑器件（CPLD，Complex Programmable Logic Device）、FPGA、通用处理器、控制器、MCU、微处理器（Microprocessor）、或其他电子元件实现，用于执行前述方法。

在示例性实施例中，本申请实施例还提供了一种计算机可读存储介质，例如包括计算机程序的存储器 42，上述计算机程序可由通信设备的处理器 41 执行，以完成前述方法所述步骤。计算机可读存储介质可以是 FRAM、ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或 CD-ROM 等存储器；也可以是包括上述存储器之一或任意组合的各种设备。

本申请实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现本申请实施例前述应用于终端设备中的终端设备的配置方法的步骤；或者，该程序被处理器执行时实现本申请实施例前述应用于服务器中的终端设备的配置方法的步骤；或者，该程序被处理器执行时实现本申请实施例前述应用于网络设备中的终端设备的配置

方法的步骤。

本申请所提供的几个方法实施例中所揭露的方法，在不冲突的情况下可以任意组合，得到新的方法实施例。

本申请所提供的几个产品实施例中所揭露的特征，在不冲突的情况下可以任意组合，得到新的产品实施例。

本申请所提供的几个方法或设备实施例中所揭露的特征，在不冲突的情况下可以任意组合，得到新的方法实施例或设备实施例。

在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，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，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元，即可以位于一个地方，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全部单元来实现本实施例方案的目的。

另外，在本申请各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；

而前述的存储介质包括：移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

或者，本申请上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也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，本申请实施例的技术方案本质上或者说对现有技术做出贡献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）执行本申请各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、 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，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权利要求书

1、一种终端设备的配置方法，所述方法包括:

终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护;

发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

2、根据权利要求 1 所述的方法，其中，所述方法还包括:

所述终端设备接收来自服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书。

3、根据权利要求 1 所述的方法，其中，所述终端设备包括: 应用客户端、基带芯片和全球用户识别模块 USIM;

所述终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护，包括:

所述应用客户端通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥;

所述应用客户端生成第一证书请求消息，并通过所述基带芯片向所述 USIM 发送所述第一证书请求消息;

所述 USIM 生成公私钥对，在所述第一证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息;

所述 USIM 基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，在所述第二证书请求消息中添加第一校验值;

所述 USIM 通过所述基带芯片向所述应用客户端发送经上述处理后的所述第二证书请求消息。

4、根据权利要求 3 所述的方法，其中，所述发送第一请求消息，包括：

所述应用客户端向服务器发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述第二证书请求消息；

所述第一请求消息中还包括：引导事务标识 B-TID 和/或服务器的全限定域名 FQDN。

5、根据权利要求 2 所述的方法，其中，所述终端设备包括：应用客户端、基带芯片和 USIM；

所述终端设备接收来自所述服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书，包括：

所述应用客户端接收来自所述服务器的第一响应消息，并通过所述基带芯片向所述 USIM 发送所述第一响应消息；

所述 USIM 基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密；

校验通过后，所述 USIM 获得所述第一响应消息中携带的数字证书，并在安全组件中存储所述数字证书。

6、根据权利要求 1 所述的方法，其中，所述方法还包括：

所述终端设备执行通用引导架构 GBA 认证流程或面向应用的认证或密钥管理 AKMA 认证流程，与网络设备协商所述第一密钥。

7、一种终端设备的配置方法，所述方法包括：

服务器接收来自终端设备的第一请求消息；所述第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息；

所述服务器获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；

所述服务器基于所述第二密钥对所述第一请求消息进行完整性校验和/

或解密，并在对所述第一请求消息授权通过后签发数字证书；

所述服务器向所述终端设备发送第一响应消息，所述第一响应消息中包括所述数字证书。

8、根据权利要求 7 所述的方法，其中，所述服务器向所述终端设备发送第一响应消息，包括：

所述服务器构建包含有所述数字证书的第一响应消息，基于所述第二密钥对所述第一响应消息进行加密和/或完整性保护，在所述第一响应消息中添加第二校验值；

向所述终端设备发送经上述处理后的第一响应消息。

9、根据权利要求 7 所述的方法，其中，所述第一请求消息中还包括：引导事务标识 B-TID；

所述服务器获得来自网络设备的所述第二密钥，包括：

所述服务器查询是否存在与所述 B-TID 对应的第二密钥；

在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥。

10、根据权利要求 7 所述的方法，其中，所述服务器获得来自网络设备的所述第二密钥，包括：

所述服务器向所述网络设备发送第二请求消息，所述第二请求消息用于请求所述第二密钥；

所述服务器接收所述网络设备发送的第二响应消息，所述第二响应消息中包括所述第二密钥。

11、一种终端设备的配置方法，所述方法包括：

网络设备基于预先协商的第一密钥生成第二密钥，向服务器发送所述第二密钥。

12、根据权利要求 11 所述的方法，其中，所述方法还包括：

所述网络设备与所述终端设备通过执行通用引导架构GBA认证流程或面向应用的认证和密钥管理 AKMA 认证流程，与所述终端设备协商所述第一密钥。

13、根据权利要求 11 所述的方法，其中，所述网络设备基于预先协商的第一密钥生成第二密钥，向服务器发送所述第二密钥，包括:

所述网络设备基于预先协商的第一密钥，为每个服务器生成对应的第二密钥，向每个服务器发送所述对应的第二密钥。

14、根据权利要求 11 至 13 任一项所述的方法，其中，所述网络设备基于预先协商的第一密钥生成第二密钥，向服务器发送所述第二密钥，包括:

所述网络设备接收所述服务器发送的第二请求信息，所述第二请求消息用于请求所述第二密钥;

所述网络设备基于预先协商的第一密钥生成第二密钥，向所述服务器发送第二响应消息，所述第二响应消息中包括所述第二密钥。

15、一种终端设备的配置装置，所述装置包括：第一生成单元和第一通信单元；其中，

所述第一生成单元，配置为基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护;

所述第一通信单元，配置为发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息。

16、根据权利要求 15 所述的装置，其中，所述第一通信单元，还配置为接收来自服务器的第一响应消息，基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密，获得所述第一响应消息中携带的数字证书。

17、根据权利要求 15 所述的装置，其中，所述第一生成单元包括：应用客户端、基带芯片和全球用户识别模块 USIM;

所述应用客户端，配置为通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；还配置为生成第一证书请求消息，并通过所述基带芯片向所述 USIM 发送所述第一证书请求消息；

所述 USIM，配置为生成公私钥对，在所述第一证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对所述第一证书请求消息进行签名，获得第二证书请求消息；基于所述第二密钥对所述第二证书请求消息进行加密和/或完整性保护，并在所述第二证书请求消息中添加第一校验值；通过所述基带芯片向所述应用客户端发送经所述第二密钥加密和/或完整性保护的所述第二证书请求消息。

18、根据权利要求 17 所述的装置，其中，所述应用客户端，配置为通过所述第一通信单元向服务器发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述第二证书请求消息；所述第一请求消息中还包括：引导事务标识 B-TID 和/或服务器全限定域名 FQDN。

19、根据权利要求 16 所述的装置，其中，所述第一生成单元包括：应用客户端、基带芯片和全球用户识别模块 USIM；

所述应用客户端，配置为通过所述第一通信单元接收来自所述服务器的第一响应消息，并通过所述基带芯片向所述 USIM 发送所述第一响应消息；

所述 USIM，配置为基于所述第二密钥对所述第一响应消息进行完整性校验和/或解密；校验通过后，获得所述第一响应消息中携带的数字证书，并在安全组件中存储所述数字证书。

20、根据权利要求 15 所述的装置，其中，所述装置还包括第一执行单元，配置为执行通用引导架构 GBA 认证流程或面向应用的认证和密钥管理 AKMA 认证流程，与网络设备协商所述第一密钥。

21、一种终端设备的配置装置，所述装置包括：第二通信单元和第一

校验单元；其中，

所述第二通信单元，配置为接收来自终端设备的第一请求消息；所述第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息；

所述第一校验单元，配置为获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；还配置为基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书；

所述第二通信单元，还配置为向所述终端设备发送第一响应消息，所述第一响应消息中包括所述数字证书。

22、根据权利要求 21 所述的装置，其中，所述第二通信单元，配置为构建包含有所述数字证书的第一响应消息，基于所述第二密钥对所述第一响应消息进行加密和/或完整性保护，在所述第一响应消息中添加第二校验值，向所述终端设备发送经上述处理后的第一响应消息。

23、根据权利要求 21 所述的装置，其中，所述第一请求消息中还包括：引导事务标识 B-TID;

所述装置还包括第二执行单元，配置为查询是否存在与所述 B-TID 对应的第二密钥；在查询结果为不存在与所述 B-TID 对应的第二密钥的情况下，通过所述第二通信单元获得来自网络设备的所述第二密钥。

24、一种终端设备的配置装置，所述装置包括第二生成单元和第三通信单元；其中，

所述第二生成单元，配置为基于预先协商的第一密钥生成第二密钥；

所述第三通信单元，配置为向服务器发送所述第二密钥。

25、根据权利要求 24 所述的装置，其中，所述装置还包括第三执行单元，配置为与终端设备通过执行通用引导架构 GBA 认证流程或面向应用的认证和密钥管理 AKMA 认证流程，与所述终端设备协商所述第一密钥。

26、根据权利要求 24 所述的装置，其中，所述第二生成单元，配置为基于预先协商的第一密钥，为每个服务器生成对应的第二密钥；

所述第三通信单元，配置为分别向每个服务器发送所述对应的第二密钥。

27、一种终端设备的配置方法，所述方法包括：

终端设备基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护；

发送第一消息。

28、根据权利要求 27 所述的方法，其中，所述方法还包括：

所述终端设备接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

29、根据权利要求 27 所述的方法，其中，所述终端设备包括：应用客户端、基带芯片和全球用户识别模块 USIM；

所述终端设备基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护，包括：

所述应用客户端通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；

所述应用客户端生成第一消息，并通过所述基带芯片向所述 USIM 发送所述第一消息；

所述 USIM 基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护；

所述 USIM 通过所述基带芯片向所述应用客户端发送经上述处理后的所述第一消息。

30、根据权利要求 29 所述的方法，其中，所述发送第一消息，包括：

所述应用客户端向服务器发送所述第一消息；

所述第一消息中还包括：引导事务标识 B-TID 和/或服务器的全限定域名 FQDN；或者包括：面向应用的认证或密钥管理 AKMA 密钥标识符 A-KID 和/或 FQDN。

31、根据权利要求 28 所述的方法，其中，所述终端设备包括：应用客户端、基带芯片和全球用户识别模块 USIM；

所述终端设备接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密，包括：

所述应用客户端接收来自所述服务器的第二消息，并通过所述基带芯片向所述 USIM 发送所述第二消息；

所述 USIM 基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

32、一种终端设备的配置方法，所述方法包括：

服务器接收来自终端设备的第一消息，所述第一消息的部分或全部经第二密钥加密和/或完整性保护；

所述服务器获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；

所述服务器基于所述第二密钥对所述第一消息进行完整性校验和/或解密。

33、根据权利要求 32 所述的方法，其中，所述方法还包括：

所述服务器基于所述第二密钥对第二消息的部分或全部进行加密和/或完整性保护；

发送第二消息。

34、根据权利要求 32 所述的方法，其中，所述第一消息中还包括：引导事务标识 B-TID，或者包括面向应用的认证或密钥管理 AKMA 密钥标识符 A-KID；

所述服务器获得来自网络设备的所述第二密钥，包括:

所述服务器查询是否存在与所述 B-TID 或所述 A-KID 对应的第二密钥;

在查询结果为不存在与所述 B-TID 或所述 A-KID 对应的第二密钥的情况下，获得来自网络设备的所述第二密钥。

35、一种终端设备的配置装置，所述装置包括：第三生成单元和第四通信单元；其中，

所述第三生成单元，配置为基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护;

所述第四通信单元，配置为发送第一消息。

36、根据权利要求 35 所述的装置，其中，所述第四通信单元，还配置为接收来自服务器的第二消息，基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

37、根据权利要求 35 所述的装置，其中，所述第三生成单元包括：应用客户端、基带芯片和全球用户识别模块 USIM;

所述应用客户端，配置为通过所述基带芯片触发所述 USIM 基于所述第一密钥生成第二密钥；还配置为生成第一消息，并通过所述基带芯片向所述 USIM 发送所述第一消息;

所述 USIM，配置为基于所述第二密钥对所述第一消息的部分或全部进行加密和/或完整性保护；还配置为通过所述基带芯片向所述应用客户端发送经上述处理后的所述第一消息。

38、根据权利要求 37 所述的装置，其中，所述应用客户端，还配置为向服务器发送所述第一消息;

所述第一消息中还包括：引导事务标识 B-TID 和/或服务器的全限定域名 FQDN; 或者包括: 面向应用的认证或密钥管理 AKMA 密钥标识符 A-KID

和/或 FQDN。

39、根据权利要求 36 所述的装置，其中，所述第三生成单元包括：应用客户端、基带芯片和全球用户识别模块 USIM;

所述应用客户端，配置为接收来自所述服务器的第二消息，并通过所述基带芯片向所述 USIM 发送所述第二消息;

所述 USIM，配置为基于所述第二密钥对所述第二消息进行完整性校验和/或解密。

40、一种终端设备的配置装置，所述装置包括：第五通信单元和第二校验单元；其中，

所述第五通信单元，配置为接收来自终端设备的第一消息，所述第一消息的部分或全部经第二密钥加密和/或完整性保护;

所述第二校验单元，配置为获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成；还配置为基于所述第二密钥对所述第一消息进行完整性校验和/或解密。

41、根据权利要求 40 所述的装置，其中，所述装置还包括第四生成单元，配置为基于所述第二密钥对第二消息的部分或全部进行加密和/或完整性保护;

所述第五通信单元，还配置为发送第二消息。

42、根据权利要求 40 所述的装置，其中，所述第一消息中还包括：引导事务标识 B-TID，或者包括面向应用的认证或密钥管理 AKMA 密钥标识符 A-KID;

所述装置还包括第四执行单元，配置为查询是否存在与所述 B-TID 或所述 A-KID 对应的第二密钥;

所述第二校验单元，配置为在所述第四执行单元获得的查询结果为不存在与所述 B-TID 或所述 A-KID 对应的第二密钥的情况下，通过所述第五

通信单元获得来自网络设备的所述第二密钥。

43、一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现权利要求 1 至 6 任一项所述方法的步骤；或者，

该程序被处理器执行时实现权利要求 7 至 10 任一项所述方法的步骤；或者，

该程序被处理器执行时实现权利要求 11 至 14 任一项所述方法的步骤；或者，

该程序被处理器执行时实现权利要求 27 至 31 任一项所述方法的步骤；或者，

该程序被处理器执行时实现权利要求 32 至 34 任一项所述方法的步骤。

44、一种通信设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现权利要求 1 至 6 任一项所述方法的步骤；或者，

所述处理器执行所述程序时实现权利要求 7 至 10 任一项所述方法的步骤；或者，

所述处理器执行所述程序时实现权利要求 11 至 14 任一项所述方法的步骤；或者，

所述处理器执行所述程序时实现权利要求 27 至 31 任一项所述方法的步骤；或者，

所述处理器执行所述程序时实现权利要求 32 至 34 任一项所述方法的步骤。

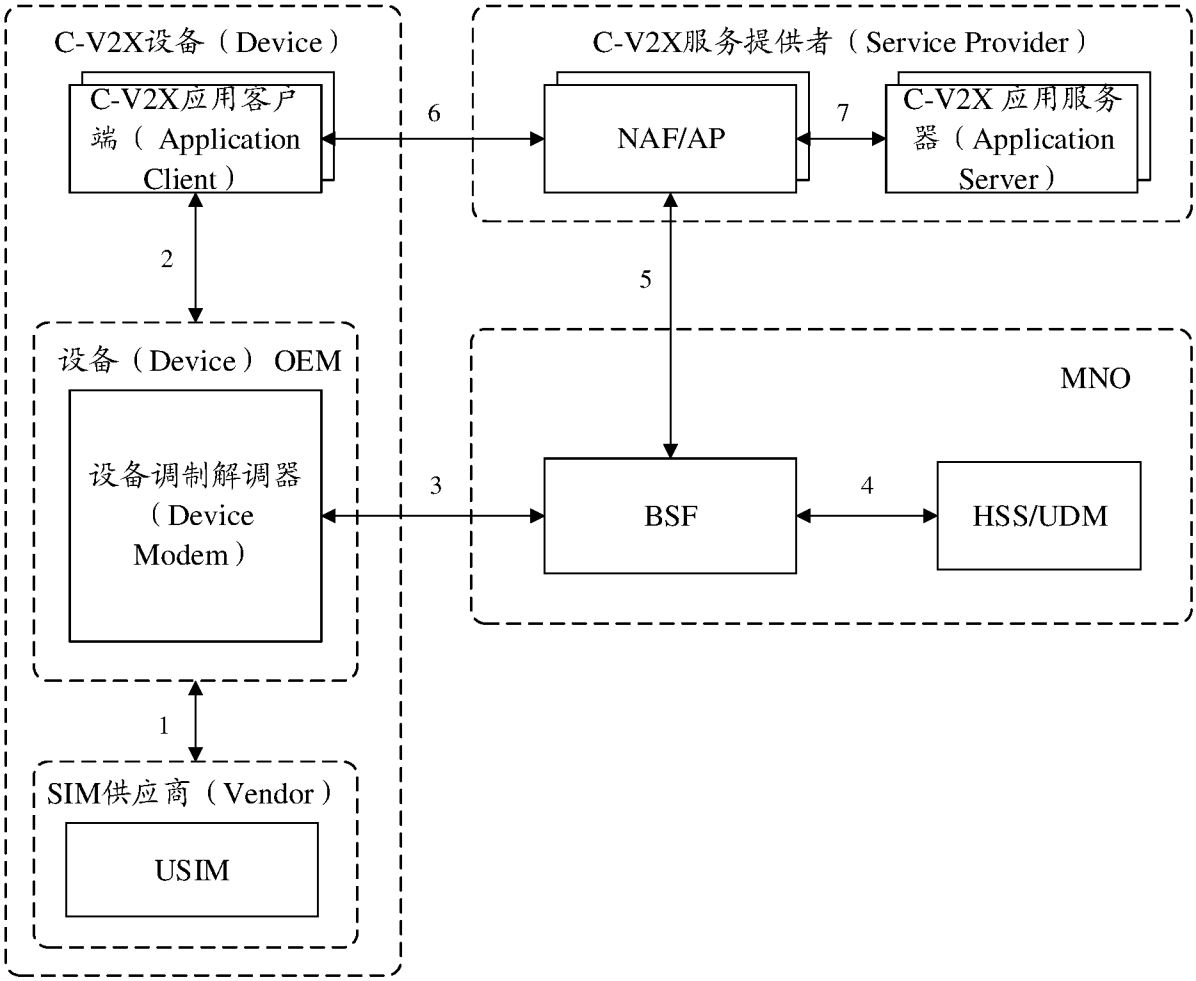
C-V2X设备（Device）
C-V2X应用客户端（Application Client）
C-V2X服务提供者（Service Provider）
NAF/AP
C-V2X 应用服务器（Application Server）
6
7
2
5
设备（Device）OEM
设备调制解调器（Device Modem）
MNO
3
4
BSF
HSS/UDM
1
SIM供应商（Vendor）
USIM

图 1

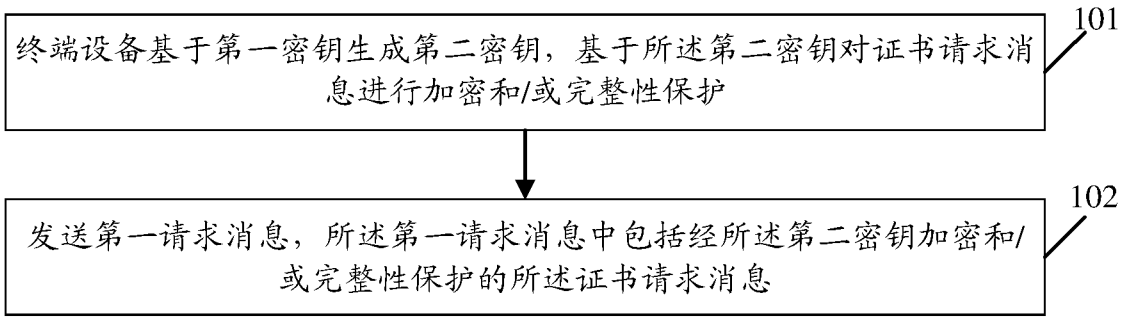
终端设备基于第一密钥生成第二密钥，基于所述第二密钥对证书请求消息进行加密和/或完整性保护
101
发送第一请求消息，所述第一请求消息中包括经所述第二密钥加密和/或完整性保护的所述证书请求消息
102

图 2

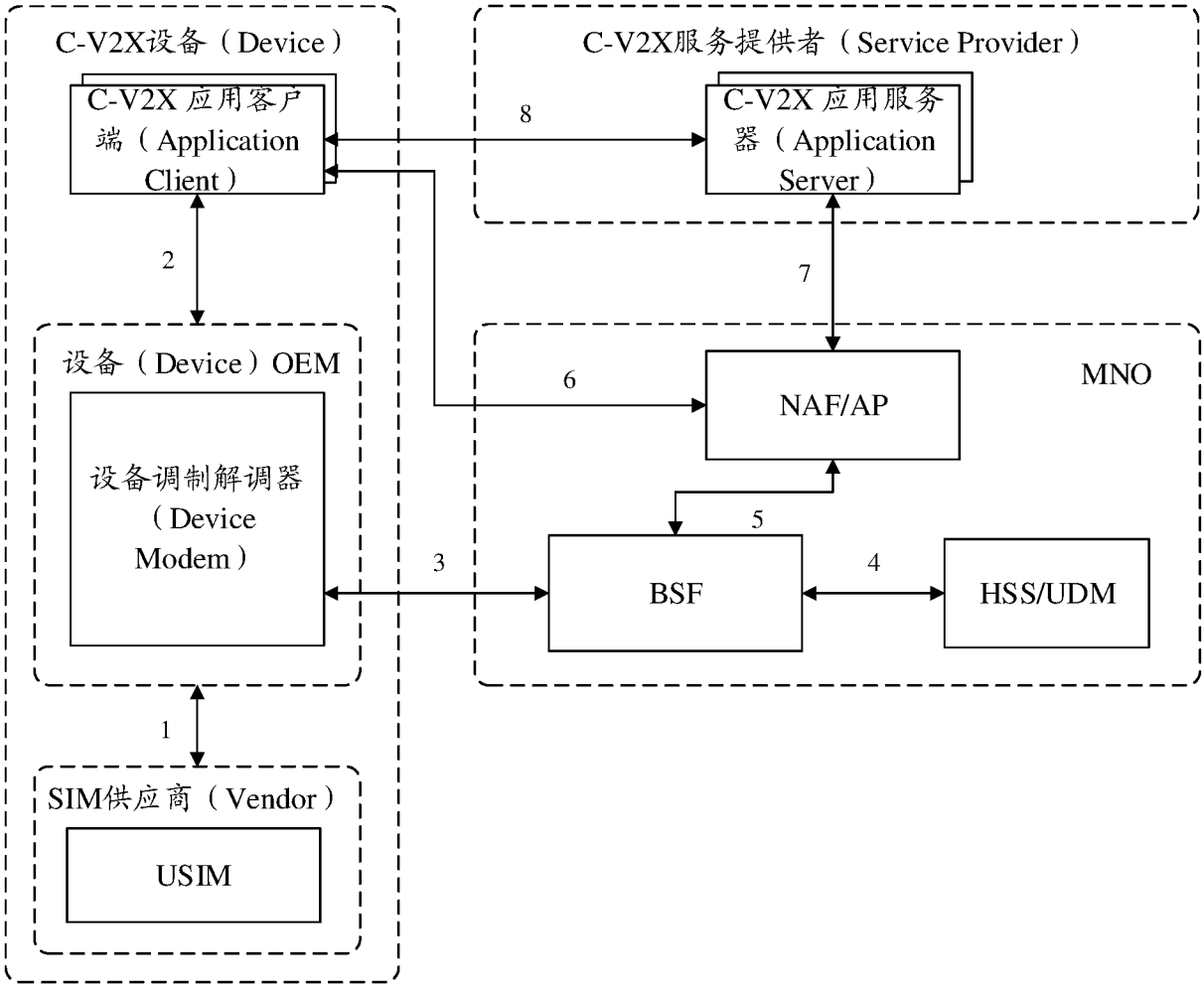
C-V2X设备（Device）
C-V2X 应用客户端（Application Client）
C-V2X服务提供者（Service Provider）
C-V2X 应用服务器（Application Server）
8
2
7
设备（Device）OEM
设备调制解调器（Device Modem）
6
NAF/AP
MNO
5
3
BSF
4
HSS/UDM
1
SIM供应商（Vendor）
USIM

图 3

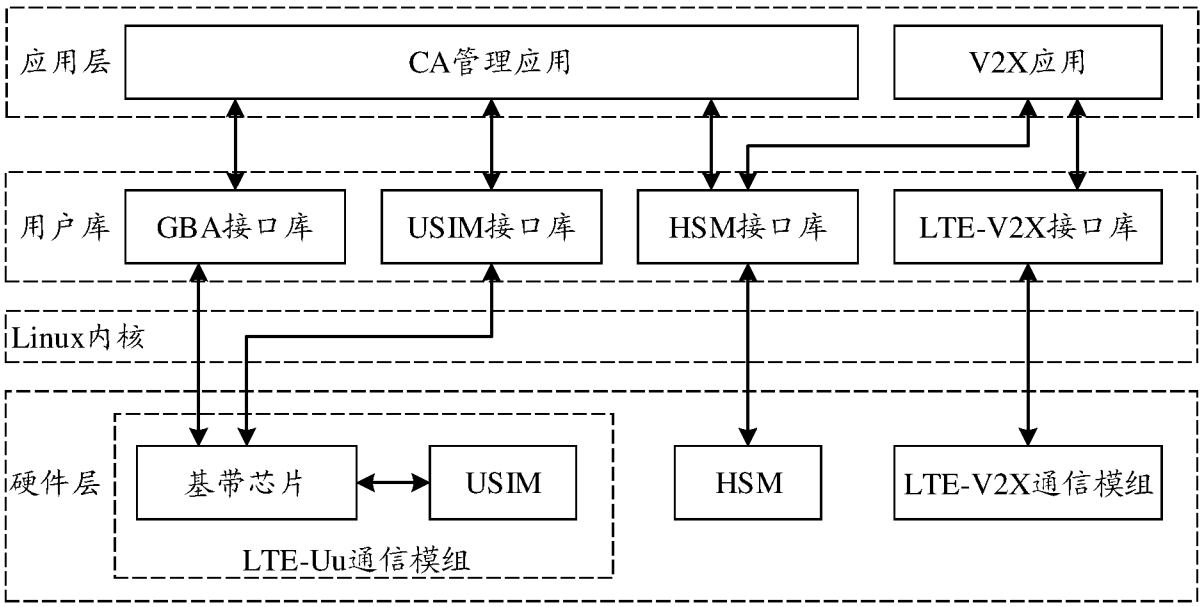
应用层
CA管理应用
V2X应用
用户库
GBA接口库
USIM接口库
HSM接口库
LTE-V2X接口库
Linux内核
硬件层
基带芯片
USIM
HSM
LTE-V2X通信模组
LTE-Uu通信模组

图 4

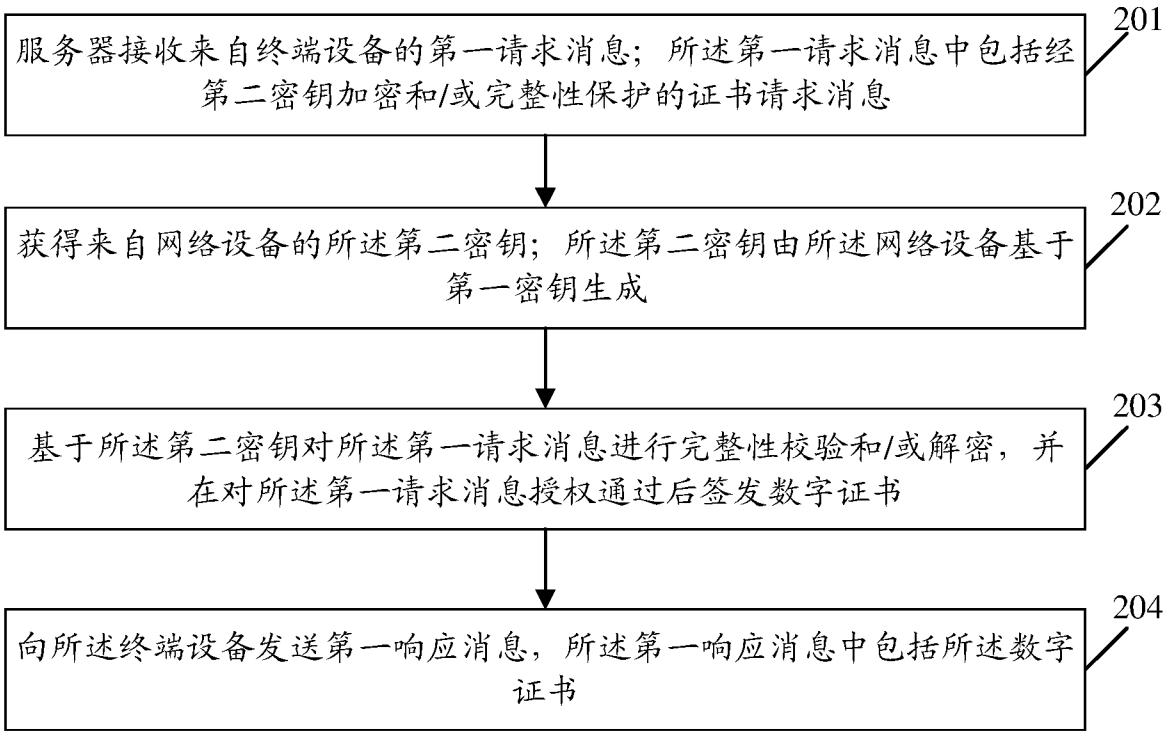
服务器接收来自终端设备的第一请求消息；所述第一请求消息中包括经第二密钥加密和/或完整性保护的证书请求消息
201
获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成
202
基于所述第二密钥对所述第一请求消息进行完整性校验和/或解密，并在对所述第一请求消息授权通过后签发数字证书
203
向所述终端设备发送第一响应消息，所述第一响应消息中包括所述数字证书
204

图 5

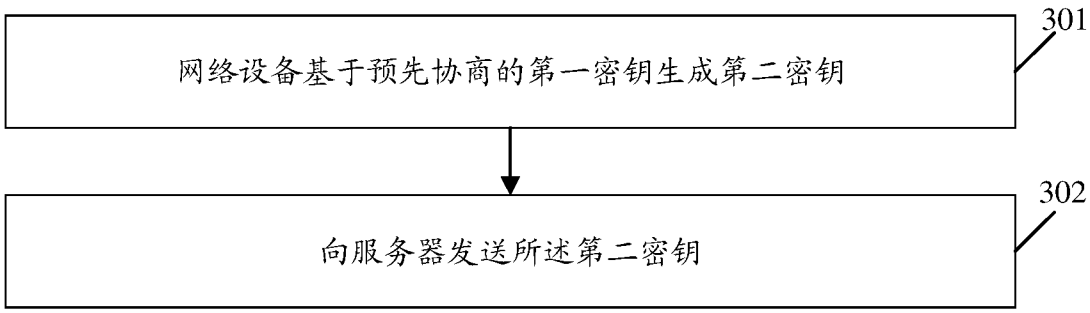
网络设备基于预先协商的第一密钥生成第二密钥
301
向服务器发送所述第二密钥
302

图 6

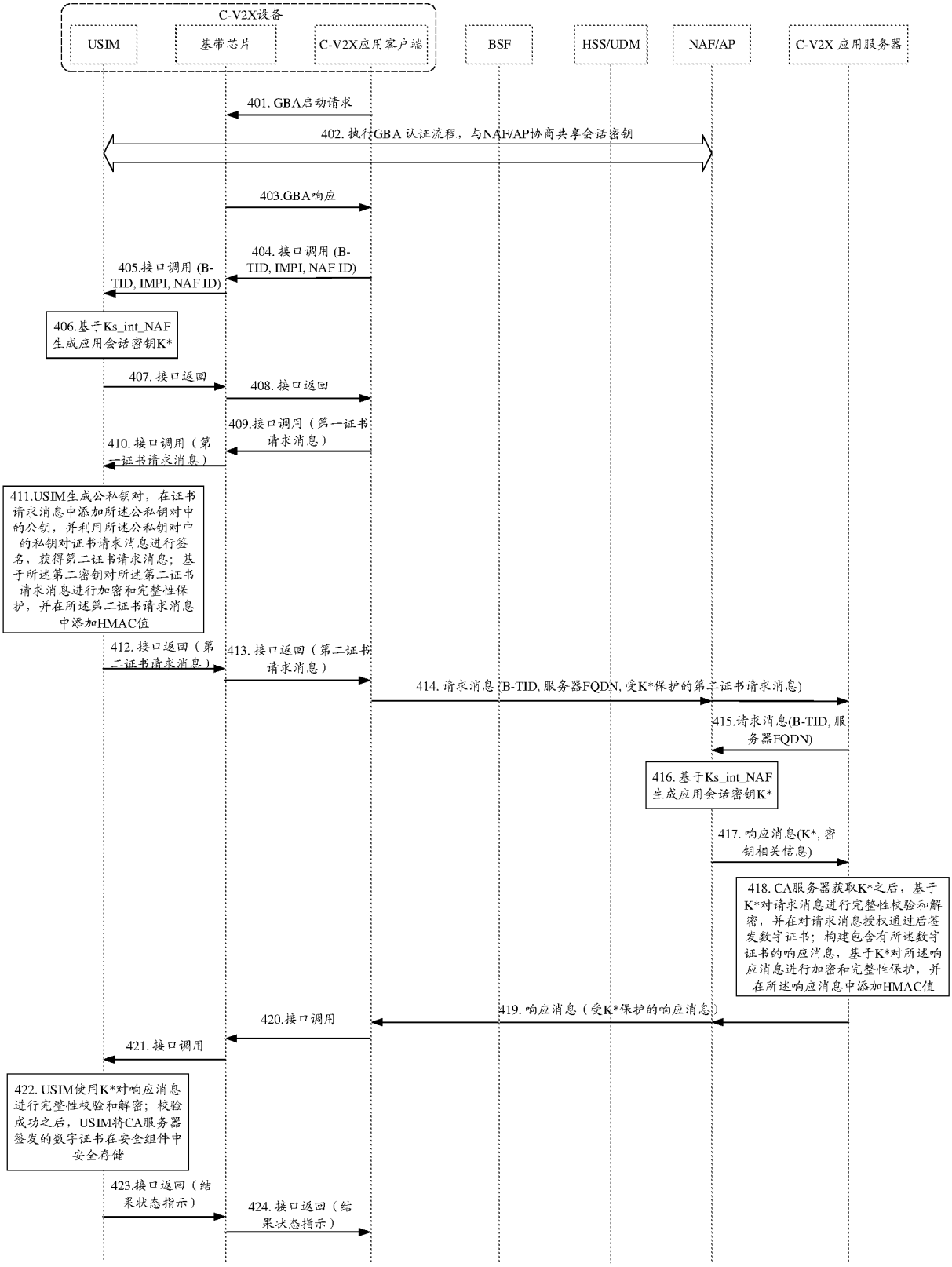
C-V2X设备
USIM
基带芯片
C-V2X应用客户端
BSF
HSS/UDM
NAF/AP
C-V2X 应用服务器
401. GBA启动请求
402. 执行GBA 认证流程，与NAF/AP协商共享会话密钥
403.GBA响应
404. 接口调用 (B-TID, IMPI, NAF ID)
405.接口调用 (B-TID, IMPI, NAF ID)
406.基于Ks_int_NAF生成应用会话密钥K*
407. 接口返回
408. 接口返回
409.接口调用（第一证书请求消息）
410. 接口调用（第一证书请求消息）
411.USIM生成公私钥对，在证书请求消息中添加所述公私钥对中的公钥，并利用所述公私钥对中的私钥对证书请求消息进行签名，获得第二证书请求消息；基于所述第二密钥对所述第二证书请求消息进行加密和完整性保护，并在所述第二证书请求消息中添加HMAC值
412. 接口返回（第二证书请求消息）
413. 接口返回（第二证书请求消息）
414. 请求消息 (B-TID, 服务器FQDN, 受K*保护的第二证书请求消息)
415.请求消息(B-TID, 服务器FQDN)
416. 基于Ks_int_NAF生成应用会话密钥K*
417. 响应消息(K*, 密钥相关信息)
418. CA服务器获取K*之后，基于K*对请求消息进行完整性校验和解密，并在对请求消息授权通过后签发数字证书；构建包含有所述数字证书的响应消息，基于K*对所述响应消息进行加密和完整性保护，并在所述响应消息中添加HMAC值
419. 响应消息（受K*保护的响应消息）
420.接口调用
421. 接口调用
422. USIM使用K*对响应消息进行完整性校验和解密；校验成功之后，USIM将CA服务器签发的数字证书在安全组件中安全存储
423.接口返回（结果状态指示）
424. 接口返回（结果状态指示）

图 7

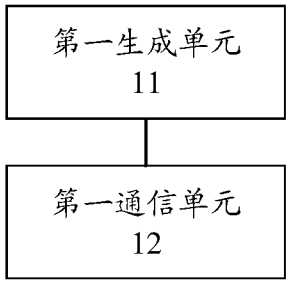
第一生成单元
11
第一通信单元
12

图 8

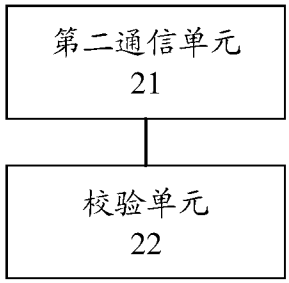
第二通信单元
21
校验单元
22

图 9

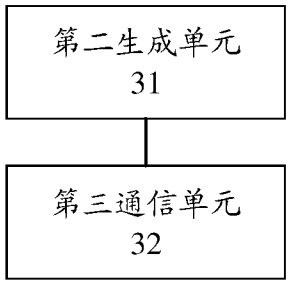
第二生成单元
31
第三通信单元
32

图 10

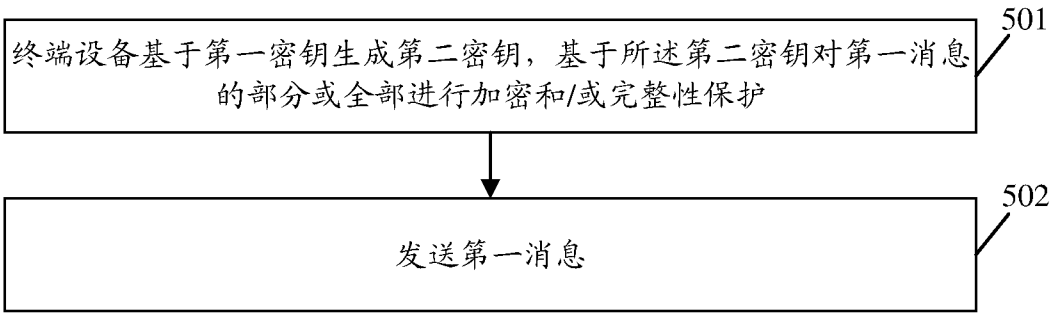
终端设备基于第一密钥生成第二密钥，基于所述第二密钥对第一消息的部分或全部进行加密和/或完整性保护
501
发送第一消息
502

图 11

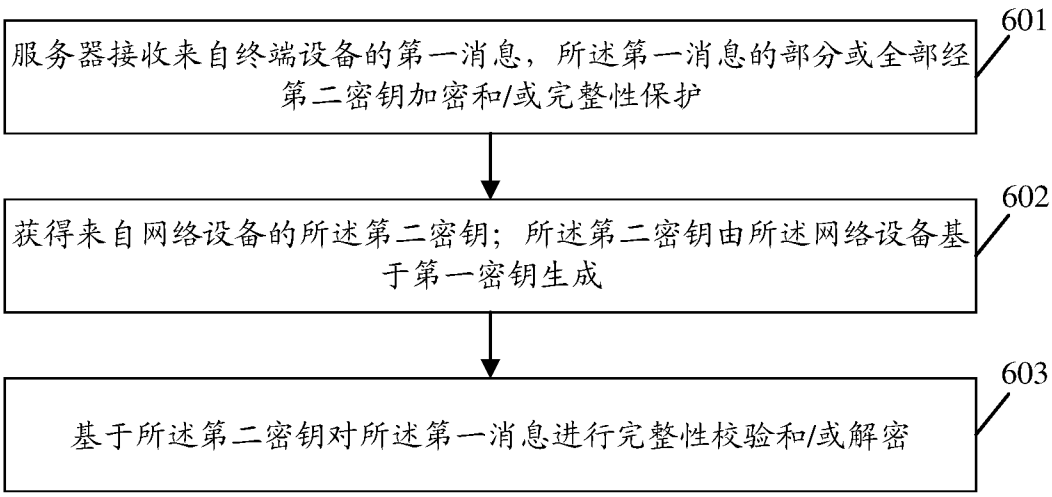
服务器接收来自终端设备的第一消息，所述第一消息的部分或全部经第二密钥加密和/或完整性保护
601
获得来自网络设备的所述第二密钥；所述第二密钥由所述网络设备基于第一密钥生成
602
基于所述第二密钥对所述第一消息进行完整性校验和/或解密
603

图 12

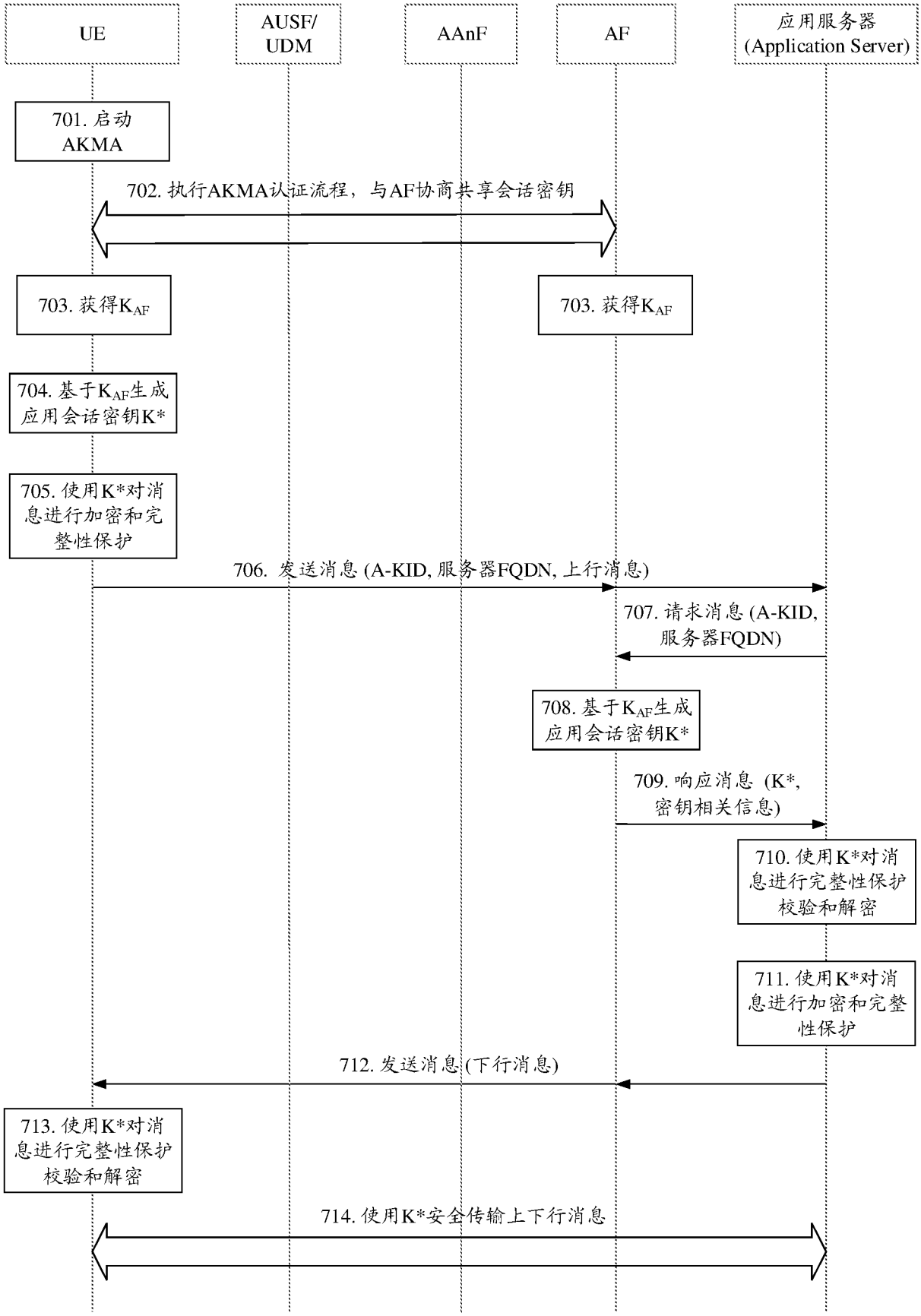
UE
AUSF/ UDM
AAnF
AF
应用服务器 (Application Server)
701. 启动 AKMA
702. 执行AKMA认证流程，与AF协商共享会话密钥
703. 获得K_{AF}
703. 获得K_{AF}
704. 基于K_{AF}生成应用会话密钥K*
705. 使用K*对消息进行加密和完整性保护
706. 发送消息 (A-KID, 服务器FQDN, 上行消息)
707. 请求消息 (A-KID, 服务器FQDN)
708. 基于K_{AF}生成应用会话密钥K*
709. 响应消息 (K*, 密钥相关信息)
710. 使用K*对消息进行完整性保护校验和解密
711. 使用K*对消息进行加密和完整性保护
712. 发送消息 (下行消息)
713. 使用K*对消息进行完整性保护校验和解密
714. 使用K*安全传输上下行消息

图 13

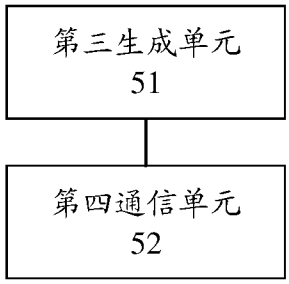
第三生成单元
51
第四通信单元
52

图 14

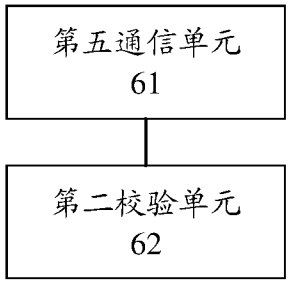
第五通信单元
61
第二校验单元
62

图 15

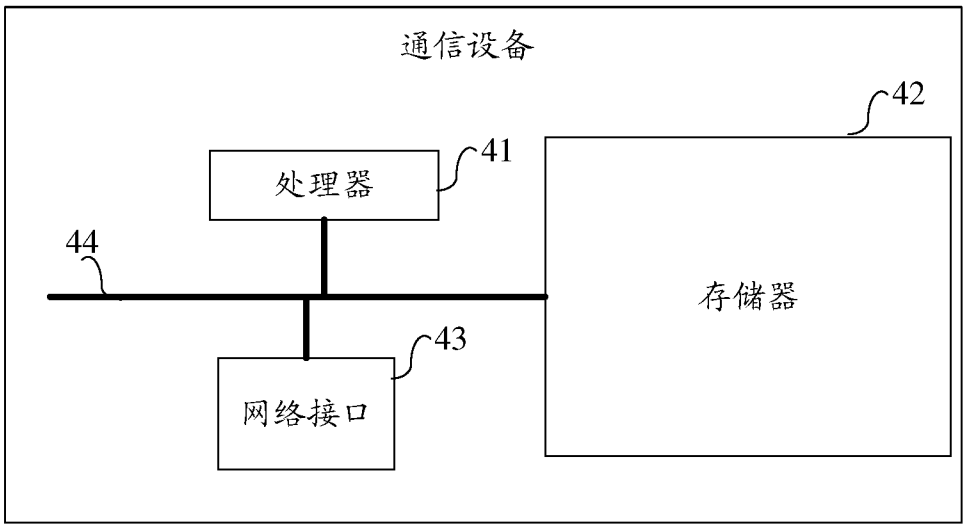
通信设备
42
41
处理器
44
存储器
43
网络接口

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/082192

A. CLASSIFICATION OF SUBJECT MATTER

H04W 4/40(2018.01)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)

H04W; H04L

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)

CNTXT; WPABS; CNKI; ENTXT; 3GPP: 密钥, 解密, 加密, 完整性, 验证, 第一, 第二, 证书, 授权; Key, decrypt, encrypt, integrity, verify, first, second, certificate, authorization

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101808286 A (CHINA IWNCOMM CO., LTD.) 18 August 2010 (2010-08-18) description, paragraphs 25-34	1, 11, 15, 24, 27, 35, 43-44
A	CN 112449323 A (HUAWEI TECHNOLOGIES CO., LTD.) 05 March 2021 (2021-03-05) entire document	1-44
A	CN 106797564 A (QUALCOMM INC.) 31 May 2017 (2017-05-31) entire document	1-44
A	CN 110958229 A (NANJING UNIVERSITY OF SCIENCE AND TECHNOLOGY et al.) 03 April 2020 (2020-04-03) entire document	1-44
A	WO 2015144042 A1 (CHINA IWNCOMM CO., LTD.) 01 October 2015 (2015-10-01) entire document	1-44

☐ 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
19 May 2022	**26 May 2022**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/082192

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 101808286 A	18 August 2010	WO 2011113227 A1	22 September 2011
CN 112449323 A	05 March 2021	None	
CN 106797564 A	31 May 2017	US 2016094542 A1	31 March 2016
		EP 3198910 A1	02 August 2017
		BR 112017006191 A2	10 April 2018
		JP 2017535998 A	30 November 2017
		AU 2015321928 A1	09 March 2017
		PE 20170739 A1	04 July 2017
		CU 20170034 A7	04 July 2017
		WO 2016048575 A1	31 March 2016
		US 2018295125 A1	11 October 2018
		AU 2009321928 B2	08 August 2013
		KR 20170062459 A	07 June 2017
CN 110958229 A	03 April 2020	None	
WO 2015144042 A1	01 October 2015	CN 104955040 A	30 September 2015

国际检索报告

国际申请号
PCT/CN2022/082192

A. 主题的分类

H04W 4/40(2018.01)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)

H04W; H04L

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））

CNTXT;WPABS;CNKI;ENTXT;3GPP: 密钥, 解密, 加密, 完整性, 验证, 第一, 第二, 证书, 授权; Key, decrypt, encrypt, integrity, verify, first, second, certificate, authorization

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 101808286 A (西安西电捷通无线网络通信股份有限公司) 2010年8月18日 (2010-08-18) 说明书第25-34段	1，11，15，24，27，35，43-44
A	CN 112449323 A (华为技术有限公司) 2021年3月5日 (2021-03-05) 全文	1-44
A	CN 106797564 A (高通股份有限公司) 2017年5月31日 (2017-05-31) 全文	1-44
A	CN 110958229 A (南京理工大学等) 2020年4月3日 (2020-04-03) 全文	1-44
A	WO 2015144042 A1 (CHINA IWNCOMM CO LTD) 2015年10月1日 (2015-10-01) 全文	1-44

☐ 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
2022年5月19日	2022年5月26日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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 孙蓉蓉 电话号码 86-(010)-62411361

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/082192

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	101808286	A	2010年8月18日	WO	2011113227	A1	2011年9月22日
CN	112449323	A	2021年3月5日		无		
CN	106797564	A	2017年5月31日	US	2016094542	A1	2016年3月31日
				EP	3198910	A1	2017年8月2日
				BR	112017006191	A2	2018年4月10日
				JP	2017535998	A	2017年11月30日
				AU	2015321928	A1	2017年3月9日
				PE	20170739	A1	2017年7月4日
				CU	20170034	A7	2017年7月4日
				WO	2016048575	A1	2016年3月31日
				US	2018295125	A1	2018年10月11日
				AU	2009321928	B2	2013年8月8日
				KR	20170062459	A	2017年6月7日
CN	110958229	A	2020年4月3日		无		
WO	2015144042	A1	2015年10月1日	CN	104955040	A	2015年9月30日