

安全通道建立方法、装置、相关设备及存储介质

相关申请的交叉引用

本申请基于申请号为 202110910311.1、申请日为 2021 年 08 月 09 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引入本申请作为参考。

技术领域

本申请涉及网络安全领域，尤其涉及一种安全通道建立方法、装置、相关设备及存储介质。

背景技术

相关技术中，定义了第五代移动通信技术（5G）消息服务及该服务在应用层的架构和流程，如图 1 所示。如何解决 5G 消息服务的安全问题，尤其是如何保障 5G 消息终端（英文可以表示为 MSGin5G UE）与 5G 消息服务器（英文可以表示为 MSGin5G Server）之间的网络信息安全，成为亟待解决的问题。

发明内容

为解决相关技术问题，本申请实施例提供一种安全通道建立方法、装置、相关设备及存储介质。

本申请实施例的技术方案是这样实现的：

本申请实施例提供了一种安全通道建立方法，应用于 5G 消息终端，包括：

基于应用层认证和密钥管理（AKMA，Authentication and Key Management for Application）服务，生成第一密钥；

基于所述第一密钥，建立所述 5G 消息终端与 5G 消息服务器之间的安全通道。

上述方案中，所述基于所述第一密钥，建立所述 5G 消息终端与 5G 消息服务器之间的安全通道，包括：

基于所述第一密钥生成第三密钥，并向所述 5G 消息服务器发送携带第一标识的客户端密钥交换消息；

建立所述 5G 消息终端与 5G 消息服务器之间的安全传输协议（TLS，

Transport Layer Security) 安全通道。

上述方案中, 在所述基于 AKMA 服务生成第一密钥之前, 所述方法还包括:

进行终端和核心网之间的初始认证。

5 上述方案中, 所述基于 AKMA 服务, 生成第一密钥, 包括:

向所述 5G 消息服务器发送会话建立请求, 所述会话建立请求至少携带第一标识;

利用所述第一标识标识的第二密钥, 生成所述第一密钥; 所述第二密钥和第一标识是基于 AKMA 服务生成的。

10 上述方案中, 所述利用第一标识标识的第二密钥生成所述第一密钥是在向所述 5G 消息服务器发送所述会话建立请求之前或之后进行的。

上述方案中, 所述方法还包括:

接收 5G 消息服务器发送的会话建立响应;

所述生成第一密钥是在接收所述会话建立响应之前或之后进行的。

15 本申请实施例还提供了一种安全通道建立方法, 应用于 5G 消息服务器, 包括:

基于 AKMA 服务, 获得第一密钥;

基于所述第一密钥, 建立所述 5G 消息服务器与 5G 消息终端之间的安全通道。

20 上述方案中, 所述基于所述第一密钥, 建立所述 5G 消息服务器与 5G 消息终端之间的安全通道, 包括:

接收 5G 消息终端发送的携带第一标识的客户端密钥交换消息;

根据所述第一标识获得所述第一密钥, 利用所述第一密钥生成第三密钥, 建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道。

25 上述方案中, 所述基于 AKMA 服务, 获得第一密钥, 包括:

接收所述 5G 消息终端发送的会话建立请求; 所述会话建立请求至少携带第一标识;

向核心网发送密钥请求; 所述密钥请求至少携带所述第一标识;

30 接收所述核心网发送的第一信息; 所述第一信息至少包括基于所述第一标识标识的第二密钥生成的所述第一密钥; 所述第二密钥和第一标识是基于 AKMA 服务生成的。

上述方案中, 所述第一信息还包括所述第一密钥的周期。

本申请实施例还提供了一种安全通道建立装置, 包括:

第一处理单元, 配置为基于 AKMA 服务, 生成第一密钥;

35 第二处理单元, 配置为基于所述第一密钥, 建立 5G 消息终端与 5G 消息服务器之间的安全通道。

本申请实施例还提供了一种安全通道建立装置, 包括:

第三处理单元, 配置为基于 AKMA 服务, 获得第一密钥;

第四处理单元，配置为基于所述第一密钥，建立 5G 消息服务器与 5G 消息终端之间的安全通道。

本申请实施例还提供了一种 5G 消息终端，包括：第一通信接口及第一处理器；其中，

5 所述第一处理器，配置为：

基于 AKMA 服务，生成第一密钥；

基于所述第一密钥，建立所述 5G 消息终端与 5G 消息服务器之间的安全通道。

10 本申请实施例还提供了一种 5G 消息服务器，包括：第二通信接口及第二处理器；其中，

所述第二处理器，配置为：

基于 AKMA 服务，获得第一密钥；

基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的安全通道。

15 本申请实施例还提供了一种 5G 消息终端，包括：第一处理器和配置为存储能够在处理器上运行的计算机程序的第一存储器，

其中，所述第一处理器配置为运行所述计算机程序时，执行上述 5G 消息终端侧任一方法的步骤。

20 本申请实施例还提供了一种 5G 消息服务器，包括：第二处理器和配置为存储能够在处理器上运行的计算机程序的第二存储器，

其中，所述第二处理器配置为运行所述计算机程序时，执行上述 5G 消息服务器侧任一方法的步骤。

25 本申请实施例还提供了一种存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述 5G 消息终端侧任一方法的步骤，或者实现上述 5G 消息服务器侧任一方法的步骤。

30 本申请实施例提供的安全通道建立方法、装置、相关设备及存储介质，5G 消息终端基于 AKMA 服务，生成第一密钥；5G 消息服务器基于 AKMA 服务，获得第一密钥；所述 5G 消息终端和所述 5G 消息服务器基于所述第一密钥，建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道。本申请实施例的方案，5G 消息终端与 5G 消息服务器基于 AKMA 服务得到第一密钥，并基于所述第一密钥建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道；如此，对于 5G 消息终端与 5G 消息服务器之间接口的保护，无需在 5G 消息终端预置认证凭证，也无需额外的认证机制，比如利用 SEAL 架构、可扩展认证协议（EAP，Extensible Authentication Protocol）认证框架等认证机制，且不需要对终端新增要求，仅基于 AKMA 服务，即可
35 实现应用层 5G 消息终端与 5G 消息服务器之间的快速认证，从而能够保障 5G 消息终端与 5G 消息服务器之间接口的安全。

附图说明

- 图 1 为相关技术中 5G 消息服务的应用层架构示意图；
- 图 2 为相关技术中 5G 消息终端与 5G 消息服务器基于 SEAL 架构进行认证的流程图；
- 5 图 3 为相关技术中 5G 消息终端与 5G 消息服务器进行二次认证的流程图；
- 图 4 为本申请实施例一种安全通道建立方法的流程图；
- 图 5 为本申请实施例另一种安全通道建立方法的流程图；
- 图 6 为本申请应用实施例的网络架构示意图；
- 10 图 7 为本申请应用实施例 5G 消息终端与 5G 消息服务器之间的认证流程图；
- 图 8 为本申请实施例一种安全通道建立装置的结构示意图；
- 图 9 为本申请实施例另一种安全通道建立装置的结构示意图；
- 图 10 为本申请实施例 5G 消息终端的结构示意图；
- 15 图 11 为本申请实施例 5G 消息服务器的结构示意图；
- 图 12 为本申请实施例安全通道建立系统的结构示意图。

具体实施方式

下面结合附图及实施例对本申请再作进一步的描述。

- 20 相关技术中，为了保障 5G 消息终端与 5G 消息服务器之间的网络信息安全，可以采用以下两种方式对 5G 消息终端与 5G 消息服务器之间的认证、授权及相应接口（即图 1 所示的 MSGin5G-1 接口）进行安全保护。

方式一：5G 消息终端与 5G 消息服务器基于 SEAL 架构进行认证。

- 具体地，由 SEAL 服务器（英文可以表示为 SEAL Server）为 SEAL 终端（即安装有 SEAL 客户端（英文可以表示为 SEAL Client）的 5G 消息终端）颁发接入令牌（token）；5G 消息终端携带 token 接入 5G 消息服务器后，5G 消息服务器需要与 SEAL 服务器对接进行 token 验证，token 验证通过后 5G 消息服务器才允许终端的后续业务交互请求。
- 25

如图 2 所示，5G 消息终端与 5G 消息服务器基于 SEAL 架构进行认证的过程可以包括以下步骤：

- 30 步骤 201：5G 消息终端的 SEAL 客户端与 SEAL 服务器建立一个安全通道；之后执行步骤 202；

步骤 202：SEAL 客户端向 SEAL 服务器发送认证请求；之后执行步骤 203；

- 这里，5G 消息终端可以基于自身支持的认证方式发送所述认证请求，比如 OIDC（OpenID Connect）认证请求；
- 35

步骤 203：SEAL 服务器向 SEAL 客户端发送用于请求用户名和密码的

超文本标记语言 (HTML, Hyper Text Markup Language) 页面; 之后执行步骤 204;

步骤 204: SEAL 客户端向 SEAL 服务器发送用户名和密码; 之后执行步骤 205;

5 这里, SEAL 客户端基于所述 HTML 页面向 SEAL 服务器发送用户名和密码;

步骤 205: SEAL 服务器验证用户名和密码; 验证通过后执行步骤 206;

步骤 206: SEAL 服务器向 SEAL 客户端发送认证响应; 之后执行步骤 207;

10 这里, 所述认证响应携带授权码 (英文可以表示为 Authorization Code, 可以简称为 AuthCode); 所述认证响应与步骤 202 中的认证请求相对应, 即在所述认证请求为 OIDC 认证请求的情况下, 所述认证响应为 OIDC 认证响应;

步骤 207: SEAL 客户端向 SEAL 服务器发送 token 请求 (比如 OIDC token 请求); 之后执行步骤 208;

这里, 所述 token 请求携带 AuthCode;

步骤 208: SEAL 服务器向 SEAL 客户端发送 token 响应; 之后执行步骤 209;

这里, 所述 token 响应携带接入 token;

20 步骤 209: 5G 消息终端的 5G 消息服务客户端从 SEAL 客户端获取认证凭证 (即接入 token); 之后执行步骤 210;

步骤 210: 5G 消息服务客户端与 5G 消息服务器建立一个安全通道; 之后执行步骤 211;

步骤 211: 5G 消息服务客户端向 5G 消息服务器发送应用层注册请求; 25 之后执行步骤 212;

这里, 所述应用层注册请求携带接入 token;

步骤 212: 5G 消息服务器与 SEAL 服务器对接, 验证接入 token; 之后执行步骤 213;

步骤 213: 5G 消息服务器接受或拒绝 5G 消息服务客户端的应用层注册请求; 30

这里, 5G 消息服务器根据接入 token 的验证结果, 确定接受或拒绝 5G 消息服务客户端的应用层注册请求。

方式二: 5G 消息终端与 5G 消息服务器进行二次认证。

具体地, 在 5G 消息终端完成 5G 网络初始认证 (第一次认证), 由会话管理功能 (SMF, Session Management Function) 建立协议数据单元 (PDU, Protocol Data Unit) 会话时, 5G 消息终端与 5G 消息服务器进行二次认证 (第二次认证), 即由 5G 消息服务器对 5G 消息终端进行 EAP 认证, 认证成功后 SMF 为 5G 消息终端建立 PDU 会话以接入 5G 消息服务器。 35

如图 3 所示, 5G 消息终端与 5G 消息服务器进行二次认证的过程可以包括以下步骤:

步骤 301: 终端 (即 5G 消息终端) 与鉴权服务器功能 (AUSF, Authentication Server Function) 交互完成注册和初始认证程序; 之后执行步骤 302;

步骤 302: 终端向接入和移动性管理功能 (AMF, Access and Mobility Management Function) 或安全锚功能 (SEAF, SEcurity Anchor Function) 发送 PDU 会话建立请求; 之后执行步骤 303;

步骤 303: AMF 或 SEAF 向 SMF 发送 PDU 会话建立请求 (英文可以表示为 Nsmf_PDUSession_CreateSMContext Request); 之后执行步骤 304;

步骤 304: SMF 向 AMF 或 SEAF 发送 PDU 会话建立响应 (英文可以表示为 Nsmf_PDUSession_CreateSMContext Response); 之后执行步骤 305;

步骤 305: SMF 从统一数据管理 (UDM, Unified Data Management) 获取订阅数据并验证终端发送的请求; 之后执行步骤 306;

步骤 306: SMF 启动 EAP 认证; 之后执行步骤 307;

步骤 307: 终端与数据网络认证、授权和计费 (DN-AAA, Data Network-Authentication, Authorization and Accounting) 服务器 (即 5G 消息服务器) 交互 EAP 认证请求和 EAP 认证响应消息; 完成 EAP 认证后执行步骤 308;

步骤 308: DN-AAA 向 SMF 通知 EAP 认证成功; 之后执行步骤 309;

步骤 309: SMF 向 AMF 或 SEAF 通知 EAP 认证成功; 之后执行步骤 310;

步骤 310: AMF 或 SEAF 向终端发送 PDU 会话建立响应; 终端接入 5G 消息服务器。

实际应用时, 上述方式一存在以下缺点:

1) 5G 消息终端需要安装 SEAL 客户端才能够实现 SEAL 的相关功能, 而对于轻量级的 5G 消息终端, 即计算资源和/或存储资源有限的 5G 消息终端, 比如物联网终端 (包含各类传感器等) 等, 受限于资源成本, 这类 5G 消息终端无法安装 SEAL 客户端;

2) 交互流程复杂; 具体地, 5G 消息终端携带接入 token 向 5G 消息服务器发送请求时, 5G 消息服务器需要向 SEAL 服务器请求 token 验证, 换句话说, 该流程中需要 5G 消息服务器和 SEAL 服务器的交互。

实际应用时, 上述方式二存在以下缺点:

1) 仅能够实现 5G 消息服务器对 5G 消息终端的接入认证, 而无法保证 5G 消息服务器与 5G 消息终端之间的通信通道的安全性, 因此仍然需要采用额外的方式对 5G 消息服务器和 5G 消息终端之间通信的接口进行保护;

2) 需要 5G 消息服务器必须使用 EAP 认证框架, 但相关技术中的一些

应用层的 5G 消息服务器并不支持 EAP 认证框架;

3) 需要提前在 5G 消息终端预置二次认证使用的认证凭证, 比如用户名、口令等; 而预置凭证的安全性无法保证。

基于此, 在本申请的各种实施例中, 5G 消息终端与 5G 消息服务器基于 AKMA 服务得到第一密钥, 并基于所述第一密钥建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道; 如此, 对于 5G 消息终端与 5G 消息服务器之间接口的保护, 与上述方式一和方式二相比, 本申请实施例的方案, 不需要在 5G 消息终端预置认证凭证, 也不需要额外的认证机制, 比如利用 SEAL 架构、EAP 认证框架等认证机制, 且不需要对终端新增要求, 仅基于 AKMA 服务, 即可实现应用层 5G 消息终端与 5G 消息服务器之间的快速认证, 并能够满足轻量级的 5G 消息终端与 5G 消息服务器之间的认证需求, 从而能够保障 5G 消息终端与 5G 消息服务器之间接口的安全。

本申请实施例提供一种安全通道建立方法, 应用于 5G 消息终端, 如图 4 所示, 该方法包括:

步骤 401: 基于 AKMA 服务, 生成第一密钥;

步骤 402: 基于所述第一密钥, 建立所述 5G 消息终端与 5G 消息服务器之间的安全通道。

这里, 所述建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道, 是指建立所述 5G 消息终端与所述 5G 消息服务器之间数据传输的安全通道, 建立所述安全通道后, 所述 5G 消息终端与所述 5G 消息服务器可以基于所述安全通道进行数据传输, 从而能够保障 5G 消息终端与 5G 消息服务器之间接口的安全。

实际应用时, 所述 5G 消息终端需要先接入网络, 进而基于 AKMA 服务与所述 5G 消息服务器建立安全通道。

基于此, 在一实施例中, 如图 4 所示, 在执行步骤 401 之前, 该方法还可以包括:

步骤 400: 进行网络初始认证;

也就是说, 所述 5G 消息终端进行终端和核心网之间的初始认证。

实际应用时, 在步骤 400 中, 所述 5G 消息终端可以基于相关技术中定义的网络初始认证流程, 通过与运营商的 5G 核心网(英文可以表示为 5GC)进行交互, 具体可以与 AUSF 等功能实体进行交互, 完成 5G 网络的初始认证, 本申请实施例对网络初始认证的具体方式不作限定。

本申请实施例中, 对于 5G 消息终端与 5G 消息服务器之间接口的保护, 无需在 5G 消息终端预置认证凭证, 也无需额外的认证机制, 且不需要对终端新增要求, 仅使用网络接入的初始认证凭证(即存储于用户身份识别模块(SIM, Subscriber Identification Module)卡和运营商网络的密钥, 用于用户接入运营商网络, 即进行网络初始认证), 并基于 AKMA 服务, 即可实现应用层 5G 消息终端与 5G 消息服务器之间的快速认证, 从而能够保障

5G 消息终端与 5G 消息服务器之间接口的安全。

对于步骤 401, 在一实施例中, 所述基于 AKMA 服务, 生成第一密钥, 具体可以包括:

5 向所述 5G 消息服务器发送接入请求; 所述接入请求至少携带第一标识; 并利用所述第一标识标识的第二密钥, 生成所述第一密钥; 所述第二密钥是基于 AKMA 服务生成的;

接收所述 5G 消息服务器发送的接入响应。

10 其中, 所述向所述 5G 消息服务器发送接入请求, 也可以理解为向所述 5G 消息服务器发送会话建立请求, 所述会话建立请求至少携带第一标识; 相应地, 所述接收所述 5G 消息服务器发送的接入响应, 也可以理解为接收所述 5G 消息服务器发送的会话建立响应。

在一实施例中, 该方法还可以包括:

网络初始认证完成后, 基于 AKMA 服务, 获得所述第二密钥和所述第一标识。

15 具体地, 实际应用时, 在步骤 400 中, 所述 5G 消息终端进行网络初始认证完成后, 所述 5G 消息终端和核心网会交互 (具体可以和所述核心网的 AUSF 等功能实体进行交互), 从而生成密钥 KAUSF; 如果所述 5G 消息终端支持 AKMA 服务, 且注册并签约了 AKMA 服务 (英文可以表示为 subscription), 所述 5G 消息终端和所述核心网会基于密钥 KAUSF 和 AKMA 服务生成 AKMA 中间密钥 KAKMA (即所述第二密钥) 及该密钥对应的密
20 钥标识符 A-KID (即所述第一标识)。

实际应用时, 向所述 5G 消息服务器发送接入请求、接收所述 5G 消息服务器发送的接入响应与生成所述第一密钥在时间顺序上不分先后。换句话说, 所述 5G 消息终端既可以先向所述 5G 消息服务器发送接入请求, 再
25 生成所述第一密钥, 即所述利用所述第一标识标识的第二密钥生成所述第一密钥是在向所述 5G 消息服务器发送所述会话建立请求之后进行的; 所述 5G 消息终端也可以先生成所述第一密钥再发送所述接入请求, 即所述利用所述第一标识标识的第二密钥生成所述第一密钥是在向所述 5G 消息服务器发送所述会话建立请求之前进行的。相应地, 所述 5G 消息终端既可以先
30 接收所述 5G 消息服务器发送的接入响应, 再生成所述第一密钥, 即所述生成所述第一密钥是在接收所述会话建立响应之后进行的; 所述 5G 消息终端也可以先生成所述第一密钥再接收所述接入响应, 即所述生成所述第一密钥是在接收所述会话建立响应之前进行的。

实际应用时, 所述 5G 消息服务器接收到所述 5G 消息终端发送的携带
35 所述第一标识的接入请求后, 可以向所述核心网发送携带所述第一标识的密钥请求; 所述核心网可以根据所述第一标识确定所述第二密钥, 利用所述第二密钥生成第一密钥, 并向所述 5G 消息服务器返回生成的第一密钥; 所述 5G 消息服务器接收到所述第一密钥后, 可以向所述 5G 消息终端发送

所述接入响应。

实际应用时,所述核心网和所述 5G 消息终端利用所述第二密钥生成所述第一密钥的具体方式可以根据需求设置,本申请实施例对此不作限定。示例性地,所述核心网和所述 5G 消息终端可以利用所述第二密钥和所述 5G 消息服务器对应的标识(英文可以表示为 MSGin5G Server ID),结合预设的算法生成所述第一密钥,比如密钥导出函数(KDF, Key Derivation Function)等;所述预设的算法可以是所述 5G 消息终端和所述核心网协商确定的,也可以是运营商预置算法,本申请实施例对此不作限定。

实际应用时,所述核心网可以利用预设的策略确定所述第一密钥的周期(也可以称为生命周期),比如,可以由 AKMA 密钥锚定功能(AAnF, AKMA Anchor Function)等功能实体确定所述第一密钥的周期;本申请实施例对确定所述第一密钥的周期的具体方式不作限定。示例性地,所述核心网可以根据 5G 消息业务(即 5G 消息服务)的需求及运营商的密钥管理策略确定所述第一密钥的周期。

实际应用时,所述核心网向所述 5G 消息服务器返回生成的第一密钥时,还可以向所述 5G 消息服务器发送所述第一密钥的周期;所述 5G 消息服务器可以根据所述第一密钥的周期对所述第一密钥进行维护,即根据所述第一密钥的周期确定所述第一密钥即将过期时,所述 5G 消息服务器可以向所述核心网发送密钥更新请求;所述核心网接收到密钥更新请求时,可以根据 AKMA 服务生成新的第一密钥,并向所述 5G 消息服务器返回新的第一密钥;所述 5G 消息服务器接收到新的第一密钥后,可以向所述 5G 消息终端发送密钥更新指示,以指示所述 5G 消息终端更新所述第一密钥;这里,所述 5G 消息终端更新所述第一密钥的方式可以根据需求设置,本申请实施例对此不作限定。示例性地,所述 5G 消息终端可以重新接入 5G 网络,即重新进行网络初始认证。

在步骤 403 中,实际应用时,所述基于所述第一密钥建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道,一种实现方式可以是所述 5G 消息终端和所述 5G 消息服务器利用所述第一密钥对传输的数据进行加密。另一种实现方式可以是所述 5G 消息终端和所述 5G 消息服务器基于所述第一密钥建立 TLS 通道等类型的安全通道。

基于此,在一实施例中,所述基于所述第一密钥,建立所述 5G 消息终端与 5G 消息服务器之间的安全通道,可以包括:

基于所述第一密钥,建立所述 5G 消息终端与 5G 消息服务器之间的 TLS 安全通道(也可以称为 TLS 隧道)。

其中,所述基于所述第一密钥,建立所述 5G 消息终端与 5G 消息服务器之间的 TLS 安全通道,可以包括:

基于所述第一密钥生成第三密钥,并向所述 5G 消息服务器发送携带第一标识的客户端密钥交换(英文可以表示为 ClientKeyExchange)消息;

建立所述 5G 消息终端与 5G 消息服务器之间的 TLS 安全通道,即基于所述第三密钥,建立所述 5G 消息终端与 5G 消息服务器之间的 TLS 安全通道。

具体地,实际应用时,所述 5G 消息终端可以向所述 5G 消息服务器发送 TLS 安全通道建立请求;所述 TLS 安全通道建立请求可以携带第二信息和第三信息;所述第二信息表征基于预共享密钥(PSK, Pre-Shared Key)的加密算法;所述第三信息表征所述 5G 消息终端支持基于 PSK 的 TLS。

所述 5G 消息服务器接收到所述 TLS 安全通道建立请求后,可以从所述第二信息表征的加密算法中选择加密算法,并发送携带选择的加密算法的 TLS 安全通道建立响应;同时,所述 5G 消息服务器可以向所述 5G 消息终端发送第四信息;所述第四信息表征所述 5G 消息服务器支持 AKMA 协议。

所述 5G 消息终端接收到所述 TLS 安全通道建立响应后,可以与所述 5G 消息服务器进行 TLS 握手;在 TLS 握手过程中,所述 5G 消息终端可以利用所述第一密钥生成 TLS 安全通道的预主密钥(英文可以表示为 premaster key,后续描述中记作第三密钥),并向所述 5G 消息服务器发送携带所述第一标识的客户端密钥交换(英文可以表示为 ClientKeyExchange)消息;所述 5G 消息服务器可以根据所述第一标识获得所述第一密钥,利用所述第一密钥生成所述第三密钥,并向所述 5G 消息终端发送更改密码套件(英文可以表示为 ChangeCipherSuite)消息和完成(Finished)消息结束 TLS 握手,建立 TLS 安全通道;所述 TLS 安全通道能够保护所述 5G 消息终端与所述 5G 消息服务器之间的数据交互,从而能够保障 5G 消息终端与 5G 消息服务器之间接口的安全。

其中,为了建立 TLS 安全通道,对于 5G 消息终端与 5G 消息服务器来说,需要一个对称的密钥,而本申请实施例中,不需要额外的认证机制,也无需在 5G 消息终端预置认证凭证,且不需要对终端新增要求,借助 AKMA 服务即可获得对称的密钥,从而即可实现应用层 5G 消息终端与 5G 消息服务器之间的快速认证、鉴权以及对 5G 消息终端与 5G 消息服务器之间接口的保护。

相应地,本申请实施例还提供了一种安全通道建立方法,应用于 5G 消息服务器,如图 5 所示,该方法包括:

步骤 501: 基于 AKMA 服务,获得第一密钥;

步骤 502: 基于所述第一密钥,建立所述 5G 消息服务器与 5G 消息终端之间的安全通道。

这里,所述建立所述 5G 消息服务器与所述 5G 消息终端之间的安全通道,是指建立所述 5G 消息服务器与所述 5G 消息终端之间数据传输的安全通道,建立所述安全通道后,所述 5G 消息服务器与所述 5G 消息终端可以基于所述安全通道进行数据传输,从而能够保障 5G 消息终端与 5G 消息服

务器之间接口的安全。

其中，在一实施例中，所述基于 AKMA 服务，获得第一密钥，可以包括：

5 接收所述 5G 消息终端发送的接入请求；所述接入请求至少携带第一标识；

向核心网发送密钥请求；所述密钥请求至少携带所述第一标识；

接收所述核心网发送的第一信息；所述第一信息至少包括基于所述第一标识标识的第二密钥生成的所述第一密钥；所述第二密钥和第一标识是基于 AKMA 服务生成的。

10 这里，所述接收所述 5G 消息终端发送的接入请求，也可以理解为接收所述 5G 消息终端发送的会话建立请求，所述会话建立请求至少携带第一标识。

具体地，实际应用时，所述 5G 消息终端可以基于相关技术中定义的网络初始认证流程，通过与运营商的 5G 核心网进行交互，完成 5G 网络的初始认证。在所述 5G 消息终端接入所述核心网进行网络初始认证完成后，所述 5G 消息终端和所述核心网会生成密钥 KAUSF；如果所述 5G 消息终端支持 AKMA 服务，且注册并签约了 AKMA 服务，所述 5G 消息终端和所述核心网会基于密钥 KAUSF 和 AKMA 服务生成第二密钥及该密钥对应的第一标识；获得所述第二密钥和所述第一标识后，所述 5G 消息终端可以向所述 5G 消息服务器发送所述接入请求。

20 实际应用时，所述核心网接收到所述密钥请求后，可以利用所述第一标识确定所述第二密钥，利用所述第二密钥生成第一密钥，并通过所述第一信息向所述 5G 消息服务器返回生成的第一密钥；所述 5G 消息服务器接收到所述第一密钥后，可以向所述 5G 消息终端发送接入响应。

25 其中，所述向所述 5G 消息终端发送接入响应，也可以理解为向所述 5G 消息终端发送会话建立响应。

实际应用时，所述 5G 消息服务器还可以对所述第一密钥进行维护。

基于此，在一实施例中，所述第一信息还可以包括所述第一密钥的周期；该方法还包括：

30 根据所述第一密钥的周期对所述第一密钥进行维护。

具体地，实际应用时，所述 5G 消息服务器根据所述第一密钥的周期确定所述第一密钥即将过期时，可以向所述核心网发送密钥更新请求；所述核心网接收到密钥更新请求时，可以根据 AKMA 服务生成新的第一密钥，并向所述 5G 消息服务器返回新的第一密钥；所述 5G 消息服务器接收到新的第一密钥后，可以向所述 5G 消息终端发送密钥更新指示，以指示所述 5G 消息终端更新所述第一密钥。

在步骤 502 中，实际应用时，所述基于所述第一密钥建立所述 5G 消息服务器与 5G 消息终端之间的安全通道，一种实现方式可以是所述 5G 消息

服务器和所述 5G 消息终端利用所述第一密钥对传输的数据进行加密。另一种实现方式可以是所述 5G 消息服务器和所述 5G 消息终端基于所述第一密钥建立 TLS 通道等类型的安全通道。

基于此，在一实施例中，所述基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的安全通道，可以包括：

基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道。

其中，所述基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道，可以包括：

接收 5G 消息终端发送的携带第一标识的客户端密钥交换消息；

根据所述第一标识获得所述第一密钥，利用所述第一密钥生成第三密钥，建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道，即基于所述第三密钥，建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道。

这里，所述 5G 消息终端与所述 5G 消息服务器建立 TLS 安全通道的过程已在上文详述，这里不再赘述。

本申请实施例提供的安全通道建立方法，5G 消息终端基于 AKMA 服务，生成第一密钥；5G 消息服务器基于 AKMA 服务，获得第一密钥；所述 5G 消息终端和所述 5G 消息服务器基于所述第一密钥，建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道。本申请实施例的方案，5G 消息终端与 5G 消息服务器基于 AKMA 服务得到第一密钥，并基于所述第一密钥建立所述 5G 消息终端与所述 5G 消息服务器之间的安全通道；如此，对于 5G 消息终端与 5G 消息服务器之间接口的保护，无需在 5G 消息终端预置认证凭证，也无需额外的认证机制，比如利用 SEAL 架构、EAP 认证框架等认证机制，且不需要对终端新增要求，仅基于 AKMA 服务，即可实现应用层 5G 消息终端与 5G 消息服务器之间的快速认证，从而能够保障 5G 消息终端与 5G 消息服务器之间接口的安全。

下面结合应用实施例对本申请再作进一步的描述。

在本应用实施例中，利用运营商 5G 网络接入的初始凭证（即存储于用户 SIM 卡与运营商网络的，用于用户接入运营商网络的密钥）为 5G 消息终端和 5G 消息服务器建立接口保护的安全凭证（即上述第一密钥），即网络初始认证完成后，利用 5G 核心网生成的 KAKMA（即上述第二密钥）作为中间密钥生成应用层密钥（即上述第一密钥），实现对图 6 所示的 MSGin5G-1 接口的保护。

在本应用实施例中，在 5G 消息终端与核心网交互，完成了网络初始认证并建立（即获得）了 KAKMA 的前提下，如图 7 所示，5G 消息终端与 5G 消息服务器之间的认证过程具体可以包括以下步骤：

步骤 701：5G 消息终端向 5G 消息服务器发送应用层会话建立请求（携

带 A-KID, 即上述第一标识); 之后执行步骤 702。

步骤 702: 5G 消息服务器从核心网获得 K5GMSG (即上述第一密钥); 之后执行步骤 703。

这里, 5G 消息服务器接收到所述会话建立请求后, 携带 A-KID 和 MSGin5G Server ID 向核心网请求密钥; 所述核心网根据 A-KID 确定 KAKMA, 利用 KAKMA 和 MSGin5G Server ID 生成 K5GMSG, 并将生成的 K5GMSG 和 K5GMSG 的密钥周期返回给 5G 消息服务器。

实际应用时, 所述核心网可以利用以下公式生成 K5GMSG:

$$K5GMSG = KDF(KAKMA, MSGin5G Server ID) \quad (1)$$

实际应用时, K5GMSG 的生命周期由 AAnF 根据 5G 消息业务的需求和运营商的密钥管理策略进行设置。当密钥即将过期时, 5G 消息服务器可以向 5G 核心网请求密钥更新, 5G 核心网收到密钥更新请求时, 可以根据 AKMA 服务生成新的 K5GMSG。

步骤 703: 5G 消息服务器向 5G 消息终端发送应用层会话建立响应; 之后执行步骤 704;

这里, 所述应用层会话建立响应携带 MSGin5G Server ID, 所述应用层会话建立响应用于指示 5G 消息终端生成 K5GMSG; 所述 5G 消息终端接收到应用层会话建立响应后, 可以利用上述公式 (1) 生成 K5GMSG。

步骤 704: 5G 消息终端和 5G 消息服务器根据 K5GMSG 建立安全通道。

实际应用时, 5G 消息终端和 5G 消息服务器可以根据 K5GMSG 建立 TLS 安全通道, 以对 MSGin5G-1 接口进行安全保护。具体地, 利用 K5GMSG 建立 TLS 安全通道的过程可以包括以下步骤:

1) 5G 消息终端向 5G 消息服务器发送连接请求 (即上述 TLS 安全通道建立请求), 并在所述连接请求携带的 client hello 消息中携带基于 PSK 的加密算法信息 (即上述第二信息) 以及表示其支持基于 PSK 的 TLS 信息 (即上述第三信息)。

2) 5G 消息服务器在 server hello 消息 (即上述 TLS 安全通道建立响应) 中携带选中的加密算法发给 5G 消息终端, 同时向 5G 消息终端发送携带 “3GPP-AKMA” 的 ServerKeyExchange 消息 (即上述第四信息), 以向 5G 消息终端表示 5G 消息服务器支持 AKMA 协议。

3) 5G 消息终端使用 K5GMSG 推导出 (即生成) TLS 的 premaster key (即上述第三密钥), 之后向 5G 消息服务器发送携带 A-KID 的 ClientKeyExchange 消息。

4) 5G 消息服务器根据收到的 A-KID 获得 K5GMSG, 利用 K5GMSG 推导出 TLS 的 premaster key, 并向 UE 发送 ChangeCipherSuite 和 Finished 消息结束 TLS 握手, 建立 TLS 隧道。

5) 5G 消息终端和 5G 消息服务器之间的数据交互受到该 TLS 隧道的保护。

本应用实施例提供的方案，具有以下优点：

1) 5G 消息终端不需要为二次认证预置凭证，使用 5G 网络接入的初始认证凭证，并基于 AKMA 服务，即可实现 5G 消息终端和 5G 消息服务器之间的认证；

5 2) 利用 5G 核心网的初始认证凭证和应用层密钥（即 K5GMSG），进行应用层 5G 消息终端和 5G 消息服务器之间的认证，无需额外的认证机制，即不需要 5G 消息服务器支持 EAP 认证框架；

3) 对 5G 消息终端无新增要求（即不需要安装 SEAL 客户端），可以满足轻量级终端与 5G 消息服务器之间的认证需求。

10 为了实现本申请实施例 5G 消息终端侧的方法，本申请实施例还提供了
一种安全通道建立装置，设置在 5G 消息终端上，如图 8 所示，该装置包括：

第一处理单元 801，配置为基于 AKMA 服务，生成第一密钥；

第二处理单元 802，配置为基于所述第一密钥，建立所述 5G 消息终端
与 5G 消息服务器之间的安全通道。

15 其中，在一实施例中，所述第二处理单元 802，还配置为：

基于所述第一密钥生成第三密钥，并向所述 5G 消息服务器发送携带第
一标识的客户端密钥交换消息；

建立所述 5G 消息终端与 5G 消息服务器之间的 TLS 安全通道。

20 在一实施例中，所述第一处理单元 801，还配置为在所述基于 AKMA
服务生成第一密钥之前，进行终端和核心网之间的初始认证。

在一实施例中，所述第一处理单元 801，还配置为：

向所述 5G 消息服务器发送会话建立请求，所述会话建立请求至少携带
第一标识；

25 利用所述第一标识标识的第二密钥，生成所述第一密钥；所述第二密
钥和第一标识是基于 AKMA 服务生成的。

在一实施例中，所述第一处理单元 801，还配置为在向所述 5G 消息服
务器发送所述会话建立请求之前或之后，利用第一标识标识的第二密钥生
成所述第一密钥。

在一实施例中，所述第一处理单元 801，还配置为：

30 接收 5G 消息服务器发送的会话建立响应；

所述生成第一密钥是在接收所述会话建立响应之前或之后进行的。

实际应用时，所述第一处理单元 801 和所述第二处理单元 802 可由安
全通道建立装置中的处理器结合通信接口实现。

35 为了实现本申请实施例 5G 消息服务器侧的方法，本申请实施例还提供
了一种安全通道建立装置，设置在 5G 消息服务器上，如图 9 所示，该装置
包括：

第三处理单元 901，配置为基于 AKMA 服务，获得第一密钥；

第四处理单元 902，配置为基于所述第一密钥，建立所述 5G 消息服务

器与 5G 消息终端之间的安全通道。

其中，在一实施例中，所述第四处理单元 902，还配置为：

接收 5G 消息终端发送的携带第一标识的客户端密钥交换消息；

根据所述第一标识获得所述第一密钥，利用所述第一密钥生成第三密
5 钥，建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道。

在一实施例中，所述第三处理单元 901，还配置为：

接收所述 5G 消息终端发送的会话建立请求；所述会话建立请求至少携
带第一标识；

向核心网发送密钥请求；所述密钥请求至少携带所述第一标识；

10 接收所述核心网发送的第一信息；所述第一信息至少包括基于所述第一
标识标识的第二密钥生成的所述第一密钥；所述第二密钥和第一标识是
基于 AKMA 服务生成的。

实际应用时，所述第三处理单元 901 和所述第四处理单元 902 可由安
全通道建立装置中的处理器结合通信接口实现。

15 需要说明的是：上述实施例提供的安全通道建立装置在建立安全通道
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
例提供的安全通道建立装置与安全通道建立方法实施例属于同一构思，其
20 具体实现过程详见方法实施例，这里不再赘述。

基于上述程序模块的硬件实现，且为了实现本申请实施例 5G 消息终端
侧的方法，本申请实施例还提供了一种 5G 消息终端，如图 10 所示，该 5G
消息终端 1000 包括：

第一通信接口 1001，能够与 5G 消息服务器进行信息交互；

25 第一处理器 1002，与所述第一通信接口 1001 连接，以实现与 5G 消息
服务器进行信息交互，用于运行计算机程序时，执行上述 5G 消息终端侧一
个或多个技术方案提供的方法；

第一存储器 1003，所述计算机程序存储在所述第一存储器 1003 上。

具体地，所述第一处理器 1002，配置为：

30 基于 AKMA 服务，生成第一密钥；

基于所述第一密钥，建立所述 5G 消息终端 1000 与 5G 消息服务器之
间的安全通道。

其中，在一实施例中，所述第一处理器 1002，还配置为：

基于所述第一密钥生成第三密钥，并通过所述第一通信接口 1001 向所
35 述 5G 消息服务器发送携带第一标识的客户端密钥交换消息；

建立所述 5G 消息终端与 5G 消息服务器之间的 TLS 安全通道。

在一实施例中，所述第一处理器 1002，还配置为在所述基于 AKMA 服
务生成第一密钥之前，进行终端和核心网之间的初始认证。

在一实施例中，所述第一处理器 1002，还配置为：

通过所述第一通信接口 1001 向所述 5G 消息服务器发送会话建立请求，所述会话建立请求至少携带第一标识；

利用所述第一标识标识的第二密钥，生成所述第一密钥；所述第二密钥和第一标识是基于 AKMA 服务生成的。

在一实施例中，所述第一处理器 1002，还配置为在向所述 5G 消息服务器发送所述会话建立请求之前或之后，利用第一标识标识的第二密钥生成所述第一密钥。

在一实施例中，所述第一处理器 1002，还配置为：

通过所述第一通信接口 1001 接收 5G 消息服务器发送的会话建立响应；所述生成第一密钥是在接收所述会话建立响应之前或之后进行的。

需要说明的是：第一处理器 1002 和第一通信接口 1001 的具体处理过程可参照上述方法理解。

当然，实际应用时，5G 消息终端 1000 中的各个组件通过总线系统 1004 耦合在一起。可理解，总线系统 1004 用于实现这些组件之间的连接通信。总线系统 1004 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 10 中将各种总线都标为总线系统 1004。

本申请实施例中的第一存储器 1003 用于存储各种类型的数据以支持 5G 消息终端 1000 的操作。这些数据的示例包括：用于在 5G 消息终端 1000 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第一处理器 1002 中，或者由所述第一处理器 1002 实现。所述第一处理器 1002 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所述第一处理器 1002 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第一处理器 1002 可以是通用处理器、数字信号处理器(DSP, Digital Signal Processor)，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。所述第一处理器 1002 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，该存储介质位于第一存储器 1003，所述第一处理器 1002 读取第一存储器 1003 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，5G 消息终端 1000 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)、现场可编程门阵列(FPGA,

Field-Programmable Gate Array)、通用处理器、控制器、微控制器 (MCU, Micro Controller Unit)、微处理器 (Microprocessor)、或者其他电子元件实现, 用于执行前述方法。

5 基于上述程序模块的硬件实现, 且为了实现本申请实施例 5G 消息服务器侧的方法, 本申请实施例还提供了一种 5G 消息服务器, 如图 11 所示, 该 5G 消息服务器 1100 包括:

第二通信接口 1101, 能够与 5G 消息终端进行信息交互;

10 第二处理器 1102, 与所述第二通信接口 1101 连接, 以实现与 5G 消息终端进行信息交互, 用于运行计算机程序时, 执行上述 5G 消息服务器侧一个或多个技术方案提供的方法;

第二存储器 1103, 所述计算机程序存储在所述第二存储器 1103 上。

具体地, 所述第二处理器 1102, 配置为:

基于 AKMA 服务, 获得第一密钥;

15 基于所述第一密钥, 建立所述 5G 消息服务器 1100 与 5G 消息终端之间的安全通道。

其中, 在一实施例中, 所述第二处理器 1102, 还配置为:

通过所述第二通信接口 1101 接收 5G 消息终端发送的携带第一标识的客户端密钥交换消息;

20 根据所述第一标识获得所述第一密钥, 利用所述第一密钥生成第三密钥, 建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道。

在一实施例中, 所述第二处理器 1102, 还配置为:

通过所述第二通信接口 1101 接收所述 5G 消息终端发送的会话建立请求; 所述会话建立请求至少携带第一标识;

25 通过所述第二通信接口 1101 向核心网发送密钥请求; 所述密钥请求至少携带所述第一标识;

通过所述第二通信接口 1101 接收所述核心网发送的第一信息; 所述第一信息至少包括基于所述第一标识标识的第二密钥生成的所述第一密钥; 所述第二密钥和第一标识是基于 AKMA 服务生成的。

30 需要说明的是: 第二处理器 1102 和第二通信接口 1101 的具体处理过程可参照上述方法理解。

当然, 实际应用时, 5G 消息服务器 1100 中的各个组件通过总线系统 1104 耦合在一起。可理解, 总线系统 1104 用于实现这些组件之间的连接通信。总线系统 1104 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 11 中将各种总线都标为总线系统 1104。

35 本申请实施例中的第二存储器 1103 用于存储各种类型的数据以支持接 5G 消息服务器 1100 操作。这些数据的示例包括: 用于在 5G 消息服务器 1100 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第二处理器 1102 中，或者由所述第二处理器 1102 实现。所述第二处理器 1102 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所述第二处理器 1102 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第二处理器 1102 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。所述第二处理器 1102 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，该存储介质位于第二存储器 1103，所述第二处理器 1102 读取第二存储器 1103 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，5G 消息服务器 1100 可以被一个或多个 ASIC、DSP、PLD、CPLD、FPGA、通用处理器、控制器、MCU、Microprocessor、或其他电子元件实现，用于执行前述方法。

可以理解，本申请实施例的存储器（第一存储器 1003、第二存储器 1103）可以是易失性存储器或者非易失性存储器，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旨在包括但不限于这些和任意其它适合类型的存储器。

为了实现本申请实施例提供的方法，本申请实施例还提供了一种安全通道建立系统，如图 12 所示，该系统包括：5G 消息终端 1201 及 5G 消息服务器 1202。

5 这里，需要说明的是：所述 5G 消息终端 1201 及所述 5G 消息服务器 1202 的具体处理过程已在上文详述，这里不再赘述。

在示例性实施例中，本申请实施例还提供了一种存储介质，即计算机存储介质，具体为计算机可读存储介质，例如包括存储计算机程序的第一存储器 1003，上述计算机程序可由 5G 消息终端 1000 的第一处理器 1002 执行，以完成前述 5G 消息终端侧方法所述步骤。再比如包括存储计算机程序的第二存储器 1103，上述计算机程序可由 5G 消息服务器 1100 的第二处理器 1102 执行，以完成前述 5G 消息服务器侧方法所述步骤。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。

15 需要说明的是：“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

另外，本申请实施例所记载的技术方案之间，在不冲突的情况下，可以任意组合。

以上所述，仅为本申请的较佳实施例而已，并非用于限定本申请的保护范围。

20

权利要求书

- 1、一种安全通道建立方法，应用于 5G 消息终端，包括：
基于应用层认证和密钥管理 AKMA 服务，生成第一密钥；
基于所述第一密钥，建立所述 5G 消息终端与 5G 消息服务器之间的安全通道。
- 2、根据权利要求 1 所述的方法，其中，所述基于所述第一密钥，建立所述 5G 消息终端与 5G 消息服务器之间的安全通道，包括：
基于所述第一密钥生成第三密钥，并向所述 5G 消息服务器发送携带第一标识的客户端密钥交换消息；
建立所述 5G 消息终端与 5G 消息服务器之间的安全传输协议 TLS 安全通道。
- 3、根据权利要求 1 或 2 所述的方法，其中，在所述基于 AKMA 服务生成第一密钥之前，所述方法还包括：
进行终端和核心网之间的初始认证。
- 4、根据权利要求 1 或 2 所述的方法，其中，所述基于 AKMA 服务，生成第一密钥，包括：
向所述 5G 消息服务器发送会话建立请求，所述会话建立请求至少携带第一标识；
利用所述第一标识标识的第二密钥，生成所述第一密钥；所述第二密钥和第一标识是基于 AKMA 服务生成的。
- 5、根据权利要求 4 所述的方法，其中，所述利用第一标识标识的第二密钥生成所述第一密钥是在向所述 5G 消息服务器发送所述会话建立请求之前或之后进行的。
- 6、根据权利要求 4 所述的方法，其中，所述方法还包括：
接收 5G 消息服务器发送的会话建立响应；
所述生成第一密钥是在接收所述会话建立响应之前或之后进行的。
- 7、一种安全通道建立方法，应用于 5G 消息服务器，包括：
基于 AKMA 服务，获得第一密钥；
基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的安全通道。
- 8、根据权利要求 7 所述的方法，其中，所述基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的安全通道，包括：
接收 5G 消息终端发送的携带第一标识的客户端密钥交换消息；
根据所述第一标识获得所述第一密钥，利用所述第一密钥生成第三密钥，建立所述 5G 消息服务器与 5G 消息终端之间的 TLS 安全通道。
- 9、根据权利要求 7 或 8 所述的方法，其中，所述基于 AKMA 服务，

获得第一密钥，包括：

接收所述 5G 消息终端发送的会话建立请求；所述会话建立请求至少携带第一标识；

向核心网发送密钥请求；所述密钥请求至少携带所述第一标识；

- 5 接收所述核心网发送的第一信息；所述第一信息至少包括基于所述第一标识标识的第二密钥生成的所述第一密钥；所述第二密钥和第一标识是基于 AKMA 服务生成的。

10、根据权利要求 7 或 8 所述的方法，其中，所述第一信息还包括所述第一密钥的周期。

- 10 11、一种安全通道建立装置，包括：

第一处理单元，配置为基于 AKMA 服务，生成第一密钥；

第二处理单元，配置为基于所述第一密钥，建立 5G 消息终端与 5G 消息服务器之间的安全通道。

12、一种安全通道建立装置，包括：

- 15 第三处理单元，配置为基于 AKMA 服务，获得第一密钥；

第四处理单元，配置为基于所述第一密钥，建立 5G 消息服务器与 5G 消息终端之间的安全通道。

13、一种 5G 消息终端，包括：第一通信接口及第一处理器；其中，所述第一处理器，配置为：

- 20 基于 AKMA 服务，生成第一密钥；

基于所述第一密钥，建立所述 5G 消息终端与 5G 消息服务器之间的安全通道。

14、一种 5G 消息服务器，包括：第二通信接口及第二处理器；其中，所述第二处理器，配置为：

- 25 基于 AKMA 服务，获得第一密钥；

基于所述第一密钥，建立所述 5G 消息服务器与 5G 消息终端之间的安全通道。

15、一种 5G 消息终端，包括：第一处理器和配置为存储能够在处理器上运行的计算机程序的第一存储器，

- 30 其中，所述第一处理器配置为运行所述计算机程序时，执行权利要求 1 至 6 任一项所述方法的步骤。

16、一种 5G 消息服务器，包括：第二处理器和配置为存储能够在处理器上运行的计算机程序的第二存储器，

- 35 其中，所述第二处理器配置为运行所述计算机程序时，执行权利要求 7 至 10 任一项所述方法的步骤。

17、一种存储介质，其上存储有计算机程序，所述计算机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，或者实现权利要求 7 至 10 任一项所述方法的步骤。