

(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



(10) 国际公布号  
WO 2021/218978 A1

(43) 国际公布日  
2021 年 11 月 4 日 (04.11.2021)

(51) 国际专利分类号:  
H04W 12/04 (2021.01) H04W 12/06 (2021.01)

(21) 国际申请号: PCT/CN2021/090348

(22) 国际申请日: 2021 年 4 月 27 日 (27.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
202010368028.6 2020 年 4 月 30 日 (30.04.2020) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 郭龙华(GUO, Longhua); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李赫(LI, He); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 吴荣(WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 吴

义壮(WU, Yizhuang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, 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, 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,

(54) Title: KEY MANAGEMENT METHOD, DEVICE AND SYSTEM

(54) 发明名称: 密钥管理方法、设备及系统

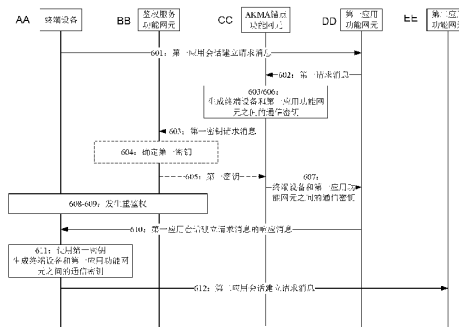


图 10

- 601 First application session establishment request message
- 602 First request message
- 603/606 Generate a communication key between the terminal device and the first application function network element
- 603 First key request message
- 604 Determine a first key
- 605 First key
- 607 The communication key between the terminal device and the first application function network element
- 608-609 Re-authentication occurs
- 610 Response message of the first application session establishment request message
- 611 Use the first key to generate the communication key between the terminal device and the first application function network element
- 612 Second application session establishment request message
- AA Terminal device
- BB Authentication service function network element
- CC AKMA anchor point function network element
- DD First application function network element
- EE Second application function network element

(57) Abstract: Provided are a key management method, device and system, which are used for ensuring that a communication key between an application function network element and a terminal device can still be successfully negotiated between the terminal device and the application function network element after re-authentication occurs during an AKMA process. The method comprises: a terminal device sending a first application session establishment request message to a first application function network element, wherein the establishment request message carries identification information of a first key, and the first key is a key for authentication and key management for applications (AKMA); the terminal device receiving a first authentication request message during a re-authentication process; the terminal device sending a response message of the first authentication request message during the re-authentication process; the terminal device receiving a response message that is from the establishment request message; and the terminal device using the first key to deduce a communication key between the terminal device and the first application function network element.

[见续页]

RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

---

**(57) 摘要：**本申请提供一种密钥管理方法、设备及系统，用以保证AKMA流程中发生重鉴权后终端设备与应用功能网元之间仍能成功协商该应用功能网元与该终端设备之间的通信密钥。该方法包括：终端设备向第一应用功能网元发送第一应用会话的建立请求消息，该建立请求消息携带第一密钥的标识信息，该第一密钥为应用的认证和密钥管理AKMA密钥；该终端设备接收重鉴权流程中的第一鉴权请求消息；该终端设备发送该重鉴权流程中的该第一鉴权请求消息的响应消息；该终端设备接收来自该建立请求消息的响应消息；该终端设备使用该第一密钥推演该终端设备和该第一应用功能网元之间的通信密钥。