

(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 2022/156580 A1

(43) 国际公布日
2022 年 7 月 28 日 (28.07.2022)

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(72) 发明人: 李飞 (LI, Fei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(21) 国际申请号: PCT/CN2022/071670

(74) 代理人: 北京中博世达专利商标代理有限公司 (BEIJING ZBSD PATENT&TRADEMARK AGENT LTD.); 中国北京市海淀区交大东路31号11号楼8层, Beijing 100044 (CN)。

(22) 国际申请日: 2022 年 1 月 12 日 (12.01.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

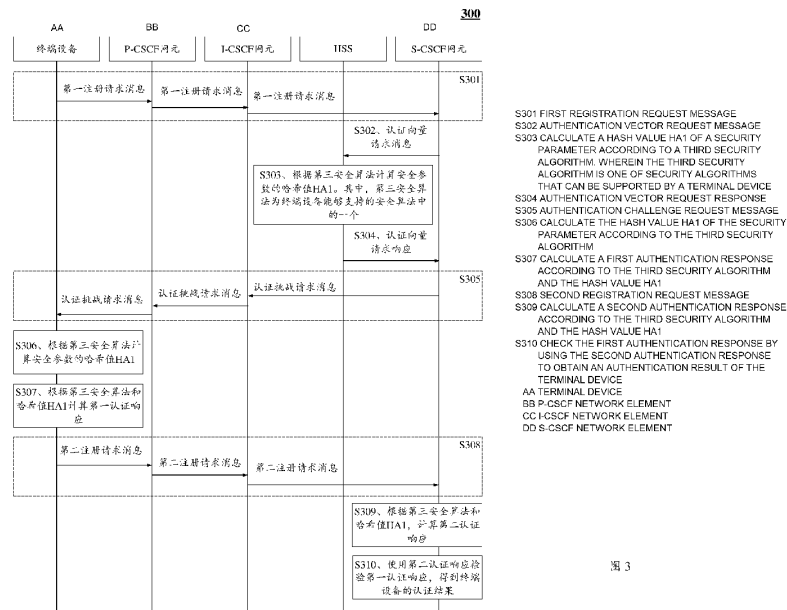
(30) 优先权:
202110090637.4 2021年1月22日 (22.01.2021) CN

(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)。

(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,

(54) Title: AUTHENTICATION METHOD AND COMMUNICATION APPARATUS

(54) 发明名称: 认证方法及通信装置



(57) Abstract: The present application relates to the technical field of communications, provides an authentication method and a communication apparatus, and is capable of authenticating a terminal device supporting different security algorithms. The method comprises: a terminal device sends a first registration request message to a service call session control function network element, wherein the first registration request message carries information of a security algorithm that can be supported by the terminal device; the terminal device receives an authentication challenge message from the service call session control function network element, wherein

[见续页]

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))。

the authentication challenge message comprises information of a third security algorithm, and the third security algorithm is one of security algorithms that can be supported by the terminal device; the terminal device calculates a hash value of a security parameter according to the third security algorithm, and the terminal device calculates an authentication response according to the third security algorithm and the hash value; and the terminal device sends a second registration request message to the service call session control function network element, wherein the second registration request message carries the authentication response, and the authentication response is used for authenticating the terminal device.

(57) 摘要: 本申请提供了认证方法及通信装置, 涉及通信技术领域, 能够认证支持不同安全算法的终端设备。该方法包括: 终端设备向服务呼叫会话控制功能网元发送第一注册请求消息。其中, 第一注册请求消息携带终端设备能够支持的安全算法的信息。终端设备接收来自服务呼叫会话控制功能网元的认证挑战消息。其中, 认证挑战消息包括第三安全算法的信息, 第三安全算法为终端设备能够支持的安全算法中的一个。终端设备根据第三安全算法计算安全参数的哈希值, 终端设备根据第三安全算法和哈希值计算认证响应。终端设备向服务呼叫会话控制功能网元发送第二注册请求消息。其中, 第二注册请求消息携带认证响应, 认证响应用于认证终端设备。