(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
2023 年 8 月 31 日 (31.08.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/160632 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

(21) 国际申请号: PCT/CN2023/077968

(22) 国际申请日: 2023 年 2 月 23 日 (23.02.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210176632.8 2022年2月25日 (25.02.2022) CN
202210605661.1 2022年5月30日 (30.05.2022) CN

(71) 申请人: 华为云计算技术有限公司 (HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.) [CN/CN]; 中国贵州省贵阳市贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。

(72) 发明人: 李俊 (LI, Jun); 中国贵州省贵阳市贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。 孙智喜 (SUN, Zhixi); 中国贵州省贵阳市贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。 章奇 (ZHANG, Qi); 中国贵州省贵阳市贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区西城区裕民路 18 号北环中心 A 座 2002, Beijing 100029 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI,

(54) **Title:** METHOD FOR SETTING CLOUD SERVICE ACCESS PERMISSIONS OF ENCLAVE INSTANCE, AND CLOUD MANAGEMENT PLATFORM

(54) **发明名称:** 针对飞地实例的云服务访问权限设置方法和云管理平台

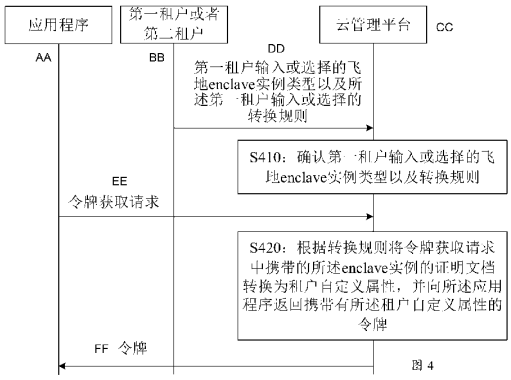


图 4

S410 CONFIRM ENCLAVE INSTANCE TYPE AND CONVERSION RULE INPUTTED OR SELECTED BY FIRST TENANT
S420 USE CONVERSION RULE TO CONVERT INTO A TENANT CUSTOM PROPERTY AN ATTESTATION DOCUMENT OF AN ENCLAVE INSTANCE CARRIED IN TOKEN ACQUISITION REQUEST, AND RETURNING TO THE APPLICATION PROGRAM A TOKEN CARRYING THE TENANT CUSTOM PROPERTY
AA APPLICATION PROGRAM
BB FIRST TENANT OR SECOND TENANT
CC CLOUD MANAGEMENT PLATFORM
DD ENCLAVE INSTANCE TYPE INPUTTED OR SELECTED BY FIRST TENANT AND CONVERSION RULE INPUTTED OR SELECTED BY FIRST TENANT
EE TOKEN ACQUISITION REQUEST
FF TOKEN

(57) **Abstract:** A method for setting cloud service access permissions of an enclave instance, and a cloud management platform. The cloud management platform provides an IAM service and an STS; the IAM service is used for confirming an enclave instance type inputted or selected by a first tenant and a conversion rule inputted or selected by the first tenant; the conversion rule is used for converting to a tenant custom property an attestation document of an enclave instance provided by an enclave instance corresponding to the enclave instance type; the STS is used for receiving a token acquisition request sent by an application program in an enclave instance,

WO 2023/160632 A1

[见续页]

GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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 token acquisition request carrying the attestation document of the enclave instance; and the STS is further used for converting the attestation document into a tenant custom property according to the conversion rule, and returning to the application program a token carrying the tenant custom property, wherein the token is used for indicating that the application program in the enclave instance has permission to access a target cloud service.

(57) 摘要：一种针对飞地实例的云服务访问权限设置方法和云管理平台。该云管理平台提供IAM服务和STS，IAM服务用于确认第一租户输入或选择的飞地enclave实例类型以及第一租户输入或选择的转换规则，转换规则用于将飞地enclave实例类型对应的enclave实例提供的enclave实例的证明文档转换成租户自定义属性；STS用于接收enclave实例中的应用程序发送的令牌获取请求，令牌获取请求携带有enclave实例的证明文档，STS还用于根据转换规则将证明文档转换为租户自定义属性，并向应用程序返回携带有租户自定义属性的令牌，令牌用于指示enclave实例中的应用程序具有访问目标云服务的权限。