(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 2 月 9 日 (09.02.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/010608 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2021/112257

(22) 国际申请日: 2021 年 8 月 12 日 (12.08.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110880949.5 2021年8月2日 (02.08.2021) CN

(71) 申请人: 中国科学院深圳先进技术研究院 (**SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY CHINESE ACADEMY OF SCIENCES**) [CN/CN]; 中国广东省深圳市南山区深圳大学城学苑大道 1068 号, Guangdong 518055 (CN)。

(72) 发明人: **戴思佳 (DAI, Sijia)**; 中国广东省深圳市南山区深圳大学城学苑大道1068号, Guangdong 518055 (CN)。 **宁立 (NING, Li)**; 中国广东省深圳市南山区深圳大学城学苑大道1068号, Guangdong 518055 (CN)。 **张涌 (ZHANG, Yong)**; 中国广东省深圳市南山区深圳大学城学苑大道1068号, Guangdong 518055 (CN)。

(74) 代理人: 深圳市科进知识产权代理事务所（普通合伙） (**SHENZHEN KEJIN INTELLECTUAL PROPERTY OFFICE**); 中国广东省深圳市南山区粤兴三道二号虚拟大学园产业化基地A701室, Guangdong 518055 (CN)。

(54) **Title:** CROSS-DOMAIN SECURE INTERACTION METHOD AND SYSTEM, TERMINAL, AND STORAGE MEDIUM

(54) **发明名称:** 一种跨域安全交互方法、系统、终端以及存储介质

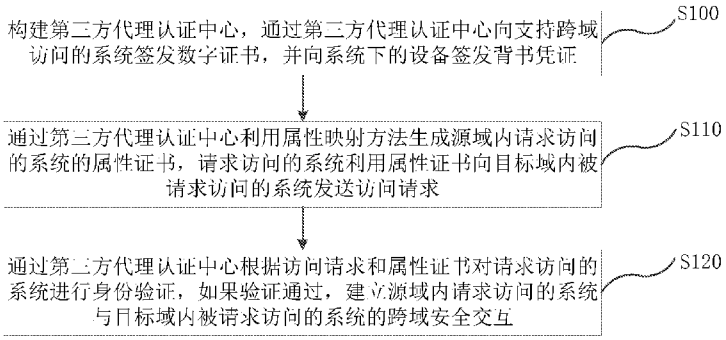

图 1

S100 Construct a third-party proxy authentication center, issue, by means of the third-party proxy authentication center, a digital certificate to a system supporting cross-domain access, and issue an endorsement credential to a device under the system

S110 By means of the third-party proxy authentication center, generate, by using an attribute mapping method, an attribute certificate of a system requesting access in a source domain, the system requesting access sending, by using the attribute certificate, an access request to a system requested in a target domain for access

S120 By means of the third-party proxy authentication center, perform, according to the access request and the attribute certificate, identity verification on the system requesting access, and if verified, establish a cross-domain security interaction between the system requesting access in the source domain and the system requested in the target domain for access

(57) **Abstract:** The present application relates to a cross-domain secure interaction method and system, a terminal, and a storage medium. The method comprises: constructing a third-party proxy authentication center, issuing, by means of the third-party proxy authentication center, a digital certificate to a system supporting cross-domain access, and issuing an endorsement credential to a device under the system; by means of the third-party proxy authentication center, generating, by using an attribute mapping method, an attribute certificate of a system requesting access in a source domain, the system requesting access sending, by using the attribute

WO 2023/010608 A1

[见续页]

(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, 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))。

certificate, an access request to a system requested in a target domain for access; by means of the third-party proxy authentication center, performing, according to the access request and the attribute certificate, identity verification on the system requesting access, and if verified, establishing a cross-domain security interaction between the system requesting access in the source domain and the system requested in the target domain for access. The embodiments of the present application achieves one-to-many cross-domain identity verification between heterogeneous systems, and improves access efficiency and the security of cross-domain access control.

(57) 摘要：本申请涉及一种跨域安全交互方法、系统、终端以及存储介质。所述方法包括：构建第三方代理认证中心，通过所述第三方代理认证中心向支持跨域访问的系统签发数字证书，并向所述系统下的设备签发背书凭证；通过所述第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，所述请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互。本申请实施例实现了异构系统之间一对多的跨域身份验证，提高了访问效率和跨域访问控制的安全性。

一种跨域安全交互方法、系统、终端以及存储介质

技术领域

本申请属于网络安全技术领域，特别涉及一种跨域安全交互方法、系统、终端以及存储介质。

背景技术

近年来，为了消除信息孤岛，实施互联互通，推进集约化建设，政务信息整合和共享受到各级政府的高度重视。用户注册数据库统一建立在省政务服务平台，用户注册统一由省政务服务平台提供，各市、部门政务服务页面不再提供用户注册功能。同样，用户登录界面也由省政务服务平台统一提供，各市、各部门只提供相应的跳转链接。各部门政务服务系统虽然不提供用户注册和登录检验功能，但是必须建立一个统一用户认证对接管理模块，统一处理和省政务服务平台用户认证子系统之间的相互调用。

异构系统是指节点分布在不同安全域中的系统结构，跨域认证也就是针对不同信任域下的用户在进行跨域访问、通信时进行身份验证。常见的网络安全方案中，服务器一般通过约定好的身份验证协议验证客户端的身份，由于物联网中存在种类繁多的设备和应用系统，这种传统的安全模式存在各种弊端。首先，如果设备数量过于庞大可能导致设备身份的管理困难，并导致系统服务器的性能要求高和身份管理代价大；其次，不同的应用系统独立存储设备的身份信息并独立完成身份验证，这种相互独立的模式，每个系统都将是一个信任孤岛，各个系统之间的资源、信息无法共享使用，造成资源的浪费；最后，相互独立的不同系统之间的认证机制可能不相同，不同种类的设备的安全性也不相同，这也导致客户端的身份的认证存在诸多的不确定性因素。

另外，为了保护用户的隐私，在域中传输数据时需要对数据进行加密。传统方法是使用对称或非对称加密算法，但该方法不适用于政务系统的复杂场景。

基于上述，如何在分布式的多域环境下，对原本独立安全的单个域构建安全高效的跨域访问控制模型进而与外域进行安全交互成为研究难点。

发明内容

本申请提供了一种跨域安全交互方法、系统、终端以及存储介质，旨在至少在一定程度上解决现有技术中的上述技术问题之一。

为了解决上述问题，本申请提供了如下技术方案：

一种跨域安全交互方法，包括：

构建第三方代理认证中心，通过所述第三方代理认证中心向支持跨域访问的系统签发数字证书，并向所述系统下的设备签发背书凭证；

通过所述第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，所述请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；所述访问请求中包括背书凭证；

通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互。

本申请实施例采取的技术方案还包括：所述向支持跨域访问的系统签发数字证书，并向所述系统下的设备签发背书凭证具体为：

识别请求接入所述第三方代理认证中心的系统信息，向支持跨域访问的系统签发数字证书；

接收所述系统下的设备发送的注册请求，并对所述注册请求进行解析后，根据所述系统的认证方式向所述设备签发背书凭证。

本申请实施例采取的技术方案还包括：所述向设备签发背书凭证具体包括：

解析所述设备的注册请求，验证设备的用户身份信息以及注册请求是否合法，如何合法，查询所述设备期待访问的目标域信息，并生成一对密钥，根据所述密钥和用户身份信息生成背书凭证；

使用所述数字证书中的密钥对背书凭证进行数字签名；

将所述背书凭证、数字签名以及私钥签发给设备，并将所述背书凭证签发记录写入到第三方代理认证中心；

所述背书凭证中包括设备的唯一身份标识、凭证出具系统的标识、凭证出具系统的名称、凭证出具系统的认证方式、设备认证结果、凭证有效时间以及时间戳、数字签名、期待访问的目标域系统标识、目标域内被请求访问的系统支持的属性操作以及与设备加密通信的密钥。

本申请实施例采取的技术方案还包括：所述属性证书中包括设备的身份信息、密钥信息，唯一的证书序列号、证书的有效使用期限、属性信息、使用域、签发单位、签发单位的公钥信息以及证书类型；

所述访问请求中包括设备的唯一身份标识、请求访问的内容、请求支持的操作、请求访问的有效期和时间戳以及背书凭证。

本申请实施例采取的技术方案还包括：所述通过第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书具体包括：

构造属性表存储模块，所述属性表存储模块用于存储域与域之间的属性转换关系；

构造属性映射表，所述属性映射表用于记录源域和目标域的所有属性，以

及属性间的相互映射关系;

在属性映射服务模块构造缓冲区,通过所述缓冲区存储常用域间的属性映射表;

利用所述属性映射表对属性证书进行属性映射,如果属性映射表对应可完全映射,则代表支持跨域访问以及同步修改操作;如果属性映射表对应不能映射,则代表不能进行跨域访问;如果属性映射表部分映射,则代表可进行跨域访问但不能进行修改操作。

本申请实施例采取的技术方案还包括:所述通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证还包括:

通过所述目标域内被请求访问的系统对所述访问请求和属性证书进行解析;所述解析过程包括:

对所述访问请求进行解析,查看所述访问请求的时间戳和请求内容;

通过所述第三方代理认证中心查询背书凭证签发方的信息,验证数字签名,并验证所述背书凭证是否完整;

检查所述背书凭证的有效期以及签发方状态,验证所述访问请求是否合规,并查看所述背书凭证签发方是否在本域的信任列表中。

本申请实施例采取的技术方案还包括:所述如果验证通过,建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互具体包括:

在所述目标域内被请求访问的系统的数据域中开辟可支持读写操作的数据共享域,所述数据共享域支持源域内请求访问的系统下的设备进行同步修改操作;

所述数据共享域由第三方代理认证中心向目标域指明。

本申请实施例采取的另一技术方案为:一种跨域安全交互系统,包括:

认证中心构建模块：用于构建第三方代理认证中心，通过所述第三方代理认证中心向支持跨域访问的系统签发数字证书，并向所述系统下的设备签发背书凭证；

请求发送模块：用于通过所述第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，所述请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；所述访问请求中包括背书凭证；

系统验证模块：用于通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互。

本申请实施例采取的又一技术方案为：一种终端，所述终端包括处理器、与所述处理器耦接的存储器，其中，

所述存储器存储有用于实现所述跨域安全交互方法的程序指令；

所述处理器用于执行所述存储器存储的所述程序指令以控制跨域安全交互。

本申请实施例采取的又一技术方案为：一种存储介质，存储有处理器可运行的程序指令，所述程序指令用于执行所述跨域安全交互方法。

相对于现有技术，本申请实施例产生的有益效果在于：本申请实施例的跨域安全交互方法、系统、终端以及存储介质通过建立一个可信的第三方代理认证中心，通过该第三方代理认证中心为不同系统和系统下的设备构建统一的身份标识，利用数字证书对不同系统在物联网环境下的跨域身份进行验证，实现异构系统之间一对多的跨域身份验证；并在身份验证成功之后在被请求访问的系统的数据域中划分出可支持读写操作的数据共享域，实现不同域间安全互操作的同时，保证了某些不可被修改访问的数据域的安全性，且避免了资源的浪

费。本发明在跨域访问过程中采用基于属性证书加密算法的数据传输方式，提高了访问效率和跨域访问控制的安全性。

附图说明

图 1 是本申请第一实施例的跨域安全交互方法的流程图；

图 2 是本申请第二实施例的跨域安全交互方法的流程图；

图 3 为本申请实施例的属性证书示意图；

图 4 为本申请实施例的跨域安全交互系统结构示意图；

图 5 为本申请实施例的终端结构示意图；

图 6 为本申请实施例的存储介质的结构示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。

请参阅图 1，是本申请第一实施例的跨域安全交互方法的流程图。本申请第一实施例的跨域安全交互方法包括以下步骤：

S100：构建第三方代理认证中心，通过第三方代理认证中心向支持跨域访问的系统签发数字证书，并向系统下的设备签发背书凭证；

其中，第三方代理认证中心包括数字认证中心、属性映射中心以及数据操作记录缓存中心，具有所有支持跨域访问的系统的信息，并具有私钥生成功能，用于协助系统与系统下的设备之间进行密钥协商。通过第三方代理认证中心为不同的系统和系统下的设备构建统一的身份标识，实现异构身份系统之间一对多的跨域认证。

S110：通过第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；

其中，属性证书中包括设备的身份信息、密钥信息，唯一的证书序列号、证书的有效使用期限、属性的相关信息、使用域、签发单位、签发单位的公钥信息以及证书类型等信息。访问请求具体包括设备的唯一身份标识、请求访问的内容、请求支持的操作、请求访问的有效期和时间戳以及背书凭证等信息。

S120：通过第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互；

其中，如果验证通过，表示请求访问的系统可信任，则在被请求访问的系统的数据域中开辟支持读写操作的数据共享域，该数据共享域可支持源域系统的设备进行数据读写等修改操作，在能够支持源域系统修改操作的同时，保障了目标域系统的隐秘性。

请参阅图 2，是本申请第二实施例的跨域安全交互方法的流程图。本申请第二实施例的跨域安全交互方法包括以下步骤：

S200：构建第三方代理认证中心；

本步骤中，通过在第三方系统或者云服务器中建立一个被不同系统信任的认证中心，不同的系统接入该认证中心，通过设备在系统中进行注册并登录所注册的系统。第三方代理认证中心包括数字认证中心、属性映射中心以及数据操作记录缓存中心，具有所有支持跨域访问的系统的信息，并具有私钥生成功能，用于协助系统与系统下的设备之间进行密钥协商。通过第三方代理认证中心为不同的系统和系统下的设备构建统一的身份标识，实现异构身份系统之间

一对多的跨域认证。

S210：通过第三方代理认证中心识别请求接入该认证中心的系统信息，并向支持跨域访问的系统签发数字证书；

本步骤中，数字证书用于验证是否支持具有背书凭证的系统访问。

S220：通过第三方代理认证中心接收支持跨域访问的系统下的设备发送的注册请求，并对注册请求进行解析后，根据不同系统的认证方式向对应的设备签发背书凭证；

具体的，背书凭证是数字证书的一种，系统下的每个设备只需要在第三方代理认证中心中注册一次即可凭签发的背书凭证直接访问支持代理的其他系统，不会因为跨域访问而给设备造成额外的负担。第三方代理认证中心向设备签发背书凭证的过程具体包括：解析设备的注册请求，验证设备身份信息以及注册请求是否合法，如何合法，则查询设备期待访问的目标域系统信息，并生成一对密钥，根据密钥和设备身份信息生成背书凭证；然后，使用第三方代理认证中心签发的数字证书中的密钥对背书凭证进行数字签名；最后，将背书凭证、数字签名以及私钥发送给设备，同时将背书凭证签发记录写入到第三方代理认证中心的数据操作记录缓存中心。其中，背书凭证中包括设备的唯一身份标识、凭证出具系统的标识、凭证出具系统的名称、凭证出具系统的认证方式、设备认证结果、凭证有效时间以及时间戳、凭证出具的数字签名、期待访问的目标域系统标识、目标域内被请求访问的系统支持的属性操作以及与设备加密通信的密钥等信息。

S230：通过第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，源域内请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；

本步骤中，如图 3 所示，为本申请实施例的属性证书示意图。属性证书由第三方代理认证中心里的属性映射中心和用户密钥生成，用户密钥是指不同系统访问的对应密钥，即不同系统的识别号。属性映射中心使用混合加密的方式将密钥和属性访问权限进行加密后再放到链路上进行传输，保证在属性证书生成过程中的安全传输。属性证书中包括设备的身份信息、密钥信息，唯一的证书序列号、证书的有效使用期限、属性的相关信息、使用域、签发单位、签发单位的公钥信息以及证书类型等信息。访问请求具体包括设备的唯一身份标识、请求访问的内容、请求支持的操作、请求访问的有效期和时间戳以及背书凭证等信息。

本申请实施例中，属性映射方法具体包括：

S231：构造属性表存储模块；属性表存储模块用于存储域与域之间的属性转换关系，属性表存储模块采用哈希表的索引结构，便于提取被请求访问的系统支持的相应属性。

S232：构造属性映射表；属性映射表是一个二维矩阵，第一列和第一行分别记录了源域和目标域中的所有属性;表中的数字记录了属性间的相互映射关系;其中 1 表示完全映射，0 表示不能映射，介于 0、1 之间的数字表示部分映射。

S233：在属性映射服务模块构造缓冲区，通过缓冲区存储常用域间的属性映射表；由于在多域环境中，进行跨域访问控制的往往是固定的几个常用域，因此，在属性映射服务模块构造一个缓冲区，通过该缓冲区存储常用域间的属性映射表，便于在进行属性映射时先在该缓冲区中寻找常用域的属性映射表。

S234：利用属性映射表对属性证书进行属性映射，如果属性映射表对应可完全映射，则代表支持跨域访问以及同步修改操作；如果属性映射表对应不能

映射，则代表不能进行跨域访问；如果属性映射表部分映射，则代表可进行跨域访问但不能进行修改操作；其中，本申请实施例在属性证书上加入属性映射的操作，在实现跨域系统身份验证的同时，保障了数据的安全，并且在一定程度上减少了数据读取的难度。属性映射的方法可以适用于多个控制域环境，提升了整个数据网络处理数据的性能。

通过上述操作，拥有属性证书的源域系统可以直接利用属性证书向目标域系统请求进行数据访问，并通过数据解密的方式获得明文，提高了访问效率和跨域访问控制的安全性。

S240：通过目标域内被请求访问的系统对访问请求和属性证书进行解析，通过第三方代理认证中心根据解析后的访问请求和属性证书验证请求访问的系统是否可信任，并将验证结果返回至目标域的被请求访问的系统；

本步骤中，对访问请求和属性证书的解析过程具体包括：首先被请求访问的系统对访问请求进行解析，查看访问请求的时间戳和请求内容;然后通过第三方代理认证中心查询背书凭证签发方的信息，验证数字签名，并验证背书凭证是否完整;最后检查背书凭证的有效期以及签发方状态，验证访问请求是否合规，并查看背书凭证签发方是否在本域的信任列表中。

S250:根据第三方代理认证中心返回的验证结果在被请求访问的系统的数据域中开辟数据共享域，建立源域系统与目标域系统的安全连接以及数据共享操作；

本步骤中，目标域系统基于自身系统的安全性考虑根据第三方代理认证中心返回的验证结果开辟数据共享域，该数据共享域可支持源域系统的设备进行数据读写等修改操作，并将操作记录传输至第三方代理认证中心进行维护，在能够支持源域系统修改操作的同时，保障了目标域系统的隐秘性，实现了跨域

访问的安全交互，解决现有技术中跨域操作难以实现以及跨域操作被请求访问的系统安全性较低的技术缺陷。其中数据共享域由第三方代理认证中心向目标域指明。

基于上述，本申请实施例的跨域安全交互方法通过建立一个可信的第三方代理认证中心，通过该第三方代理认证中心为不同系统和系统下的设备构建统一的身份标识，利用数字证书对不同系统在物联网环境下的跨域身份进行验证，实现异构系统之间一对多的跨域身份验证；并在身份验证成功之后在被请求访问的系统的数据域中划分出可支持读写操作的数据共享域，实现不同域间安全互操作的同时，保证了某些不可被修改访问的数据域的安全性，且避免了资源的浪费。本发明在跨域访问过程中采用基于属性证书加密算法的数据传输方式，提高了访问效率和跨域访问控制的安全性。

请参阅图 4，为本申请实施例的跨域安全交互系统结构示意图。本申请实施例的跨域安全交互系统 40 包括：

认证中心构建模块 41：用于构建第三方代理认证中心，通过第三方代理认证中心向支持跨域访问的系统签发数字证书，并向系统下的设备签发背书凭证；

请求发送模块 42：用于通过第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；访问请求中包括背书凭证；

系统验证模块 43：用于通过第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互。

请参阅图 5，为本申请实施例的终端结构示意图。该终端 50 包括处理器 51、与处理器 51 耦接的存储器 52。

存储器 52 存储有用于实现上述跨域安全交互方法的程序指令。

处理器 51 用于执行存储器 52 存储的程序指令以控制跨域安全交互。

其中，处理器 51 还可以称为 CPU（Central Processing Unit，中央处理单元）。处理器 51 可能是一种集成电路芯片，具有信号的处理能力。处理器 51 还可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现成可编程门阵列（FPGA）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。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

请参阅图 6，为本申请实施例的存储介质的结构示意图。本申请实施例的存储介质存储有能够实现上述所有方法的程序文件 61，其中，该程序文件 61 可以以软件产品的形式存储在上述存储介质中，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）或处理器（processor）执行本发明各个实施方式方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质，或者是计算机、服务器、手机、平板等终端设备。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本发明中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本发明所示的这些实施例，而是要符合与本发明所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求

1、一种跨域安全交互方法，其特征在于，包括：

构建第三方代理认证中心，通过所述第三方代理认证中心向支持跨域访问的系统签发数字证书，并向所述系统下的设备签发背书凭证；

通过所述第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，所述请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；所述访问请求中包括背书凭证；

通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互。

2、根据权利要求 1 所述的跨域安全交互方法，其特征在于，所述向支持跨域访问的系统签发数字证书，并向所述系统下的设备签发背书凭证具体为：

识别请求接入所述第三方代理认证中心的系统信息，向支持跨域访问的系统签发数字证书；

接收所述系统下的设备发送的注册请求，并对所述注册请求进行解析后，根据所述系统的认证方式向所述设备签发背书凭证。

3、根据权利要求 2 所述的跨域安全交互方法，其特征在于，所述向设备签发背书凭证具体包括：

解析所述设备的注册请求，验证设备的用户身份信息以及注册请求是否合法，如何合法，查询所述设备期待访问的目标域信息，并生成一对密钥，根据所述密钥和用户身份信息生成背书凭证；

使用所述数字证书中的密钥对背书凭证进行数字签名；

将所述背书凭证、数字签名以及私钥签发给设备，并将所述背书凭证签发记录写入到第三方代理认证中心；

所述背书凭证中包括设备的唯一身份标识、凭证出具系统的标识、凭证出具系统的名称、凭证出具系统的认证方式、设备认证结果、凭证有效时间以及时间戳、数字签名、期待访问的目标域系统标识、目标域内被请求访问的系统支持的属性操作以及与设备加密通信的密钥。

4、根据权利要求 1 至 3 任一项所述的跨域安全交互方法，其特征在于，所述属性证书中包括设备的身份信息、密钥信息，唯一的证书序列号、证书的有效使用期限、属性信息、使用域、签发单位、签发单位的公钥信息以及证书类型；

所述访问请求中包括设备的唯一身份标识、请求访问的内容、请求支持的操作、请求访问的有效期和时间戳以及背书凭证。

5、根据权利要求 4 所述的跨域安全交互方法，其特征在于，所述通过第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书具体包括：

构造属性表存储模块，所述属性表存储模块用于存储域与域之间的属性转换关系；

构造属性映射表，所述属性映射表用于记录源域和目标域的所有属性，以及属性间的相互映射关系；

在属性映射服务模块构造缓冲区，通过所述缓冲区存储常用域间的属性映射表；

利用所述属性映射表对属性证书进行属性映射，如果属性映射表对应可完全映射，则代表支持跨域访问以及同步修改操作；如果属性映射表对应不能映射，则代表不能进行跨域访问；如果属性映射表部分映射，则代表可进行跨域访问但

不能进行修改操作。

6、根据权利要求5所述的跨域安全交互方法，其特征在于，所述通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证还包括：

通过所述目标域内被请求访问的系统对所述访问请求和属性证书进行解析；所述解析过程包括：

对所述访问请求进行解析，查看所述访问请求的时间戳和请求内容;

通过所述第三方代理认证中心查询背书凭证签发方的信息,验证数字签名，并验证所述背书凭证是否完整;

检查所述背书凭证的有效期以及签发方状态,验证所述访问请求是否合规，并查看所述背书凭证签发方是否在本域的信任列表中。

7、根据权利要求6所述的跨域安全交互方法，其特征在于，所述如果验证通过，建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互具体包括：

在所述目标域内被请求访问的系统的数据域中开辟可支持读写操作的数据共享域，所述数据共享域支持源域内请求访问的系统下的设备进行同步修改操作；

所述数据共享域由第三方代理认证中心向目标域指明。

8、一种跨域安全交互系统，其特征在于，包括：

认证中心构建模块：用于构建第三方代理认证中心，通过所述第三方代理认证中心向支持跨域访问的系统签发数字证书,并向所述系统下的设备签发背书凭证；

请求发送模块：用于通过所述第三方代理认证中心利用属性映射方法生成源

域内请求访问的系统的属性证书，所述请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求；所述访问请求中包括背书凭证；

系统验证模块：用于通过所述第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立所述源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互。

9、一种终端，其特征在于，所述终端包括处理器、与所述处理器耦接的存储器，其中，

所述存储器存储有用于实现权利要求1-7任一项所述的跨域安全交互方法的程序指令；

所述处理器用于执行所述存储器存储的所述程序指令以控制跨域安全交互。

10、一种存储介质，其特征在于，存储有处理器可运行的程序指令，所述程序指令用于执行权利要求 1 至 7 任一项所述跨域安全交互方法。

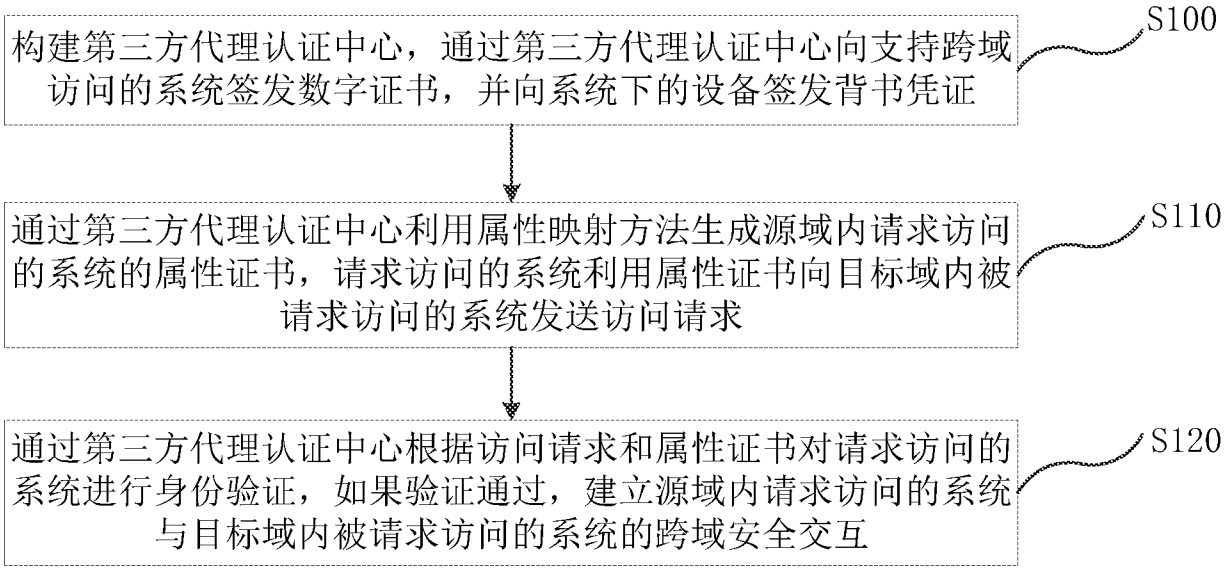
构建第三方代理认证中心，通过第三方代理认证中心向支持跨域访问的系统签发数字证书，并向系统下的设备签发背书凭证
S100
通过第三方代理认证中心利用属性映射方法生成源域内请求访问的系统的属性证书，请求访问的系统利用属性证书向目标域内被请求访问的系统发送访问请求
S110
通过第三方代理认证中心根据访问请求和属性证书对请求访问的系统进行身份验证，如果验证通过，建立源域内请求访问的系统与目标域内被请求访问的系统的跨域安全交互
S120

图 1

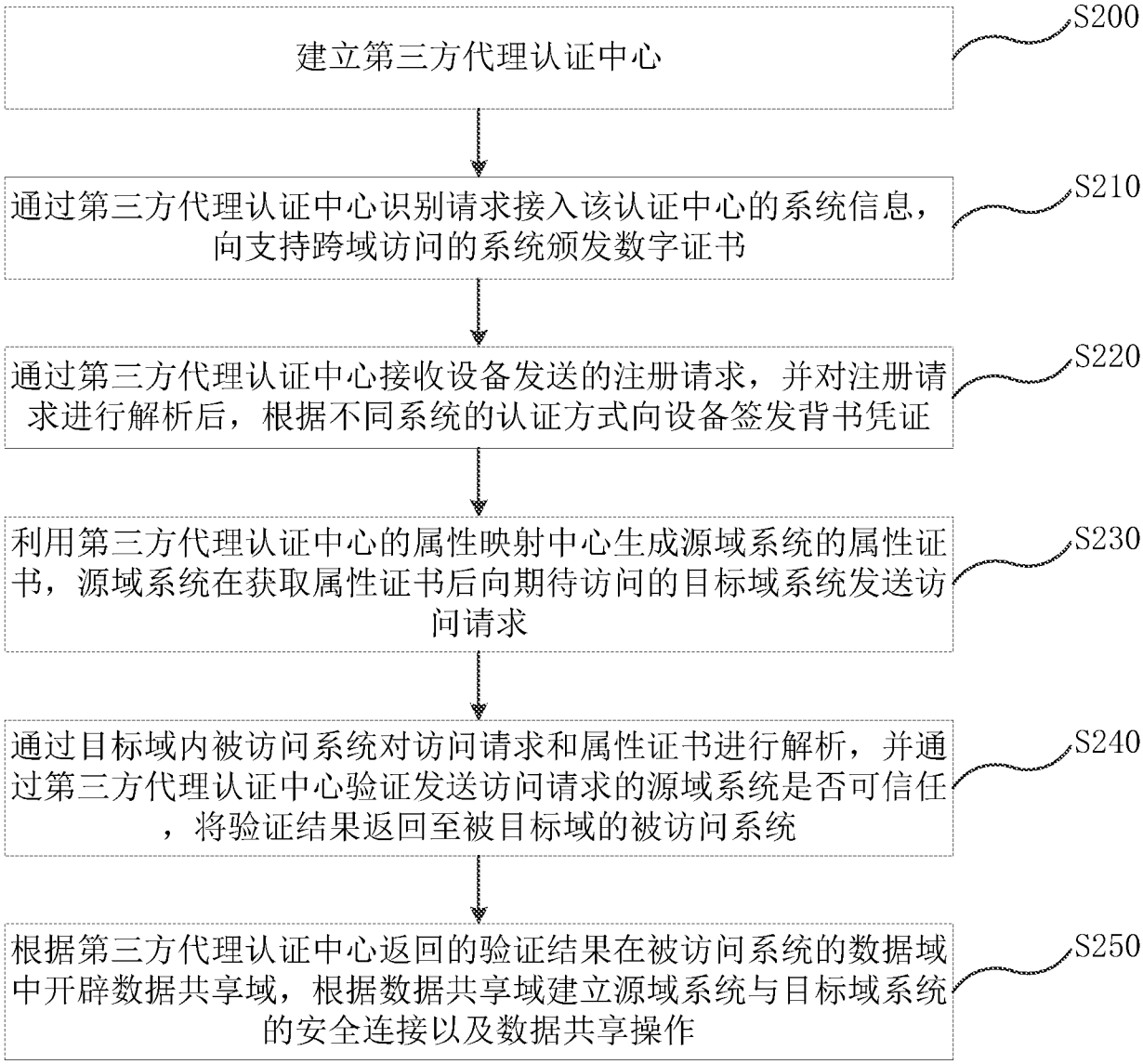
建立第三方代理认证中心
S200
通过第三方代理认证中心识别请求接入该认证中心的系统信息，向支持跨域访问的系统颁发数字证书
S210
通过第三方代理认证中心接收设备发送的注册请求，并对注册请求进行解析后，根据不同系统的认证方式向设备签发背书凭证
S220
利用第三方代理认证中心的属性映射中心生成源域系统的属性证书，源域系统在获取属性证书后向期待访问的目标域系统发送访问请求
S230
通过目标域内被访问系统对访问请求和属性证书进行解析，并通过第三方代理认证中心验证发送访问请求的源域系统是否可信任，将验证结果返回至被目标域的被访问系统
S240
根据第三方代理认证中心返回的验证结果在被访问系统的数据域中开辟数据共享域，根据数据共享域建立源域系统与目标域系统的安全连接以及数据共享操作
S250

图 2

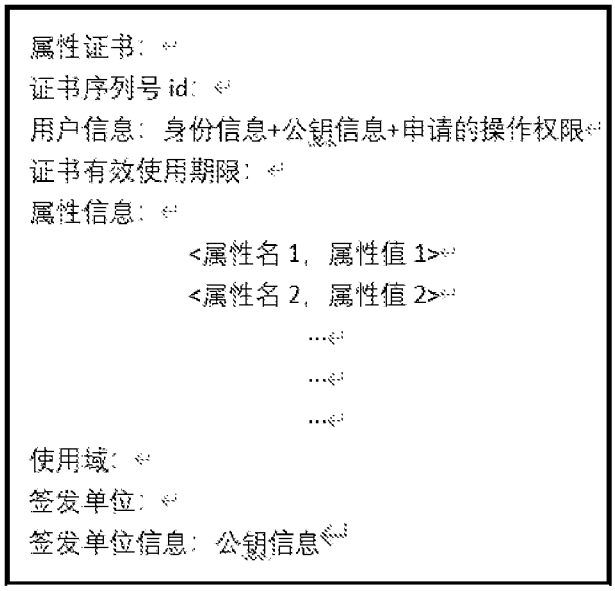
属性证书：
证书序列号 id：
用户信息：身份信息+公钥信息+申请的操作权限
证书有效使用期限：
属性信息：
<属性名 1，属性值 1>
<属性名 2，属性值 2>
…
…
…
使用域：
签发单位：
签发单位信息：公钥信息

图 3

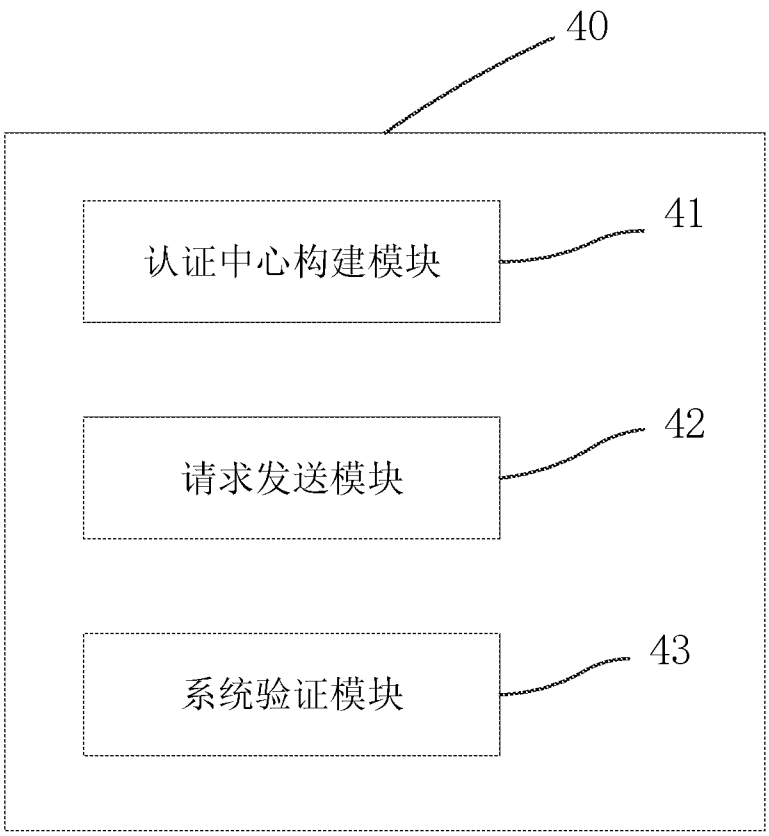
40
认证中心构建模块
41
请求发送模块
42
系统验证模块
43

图 4

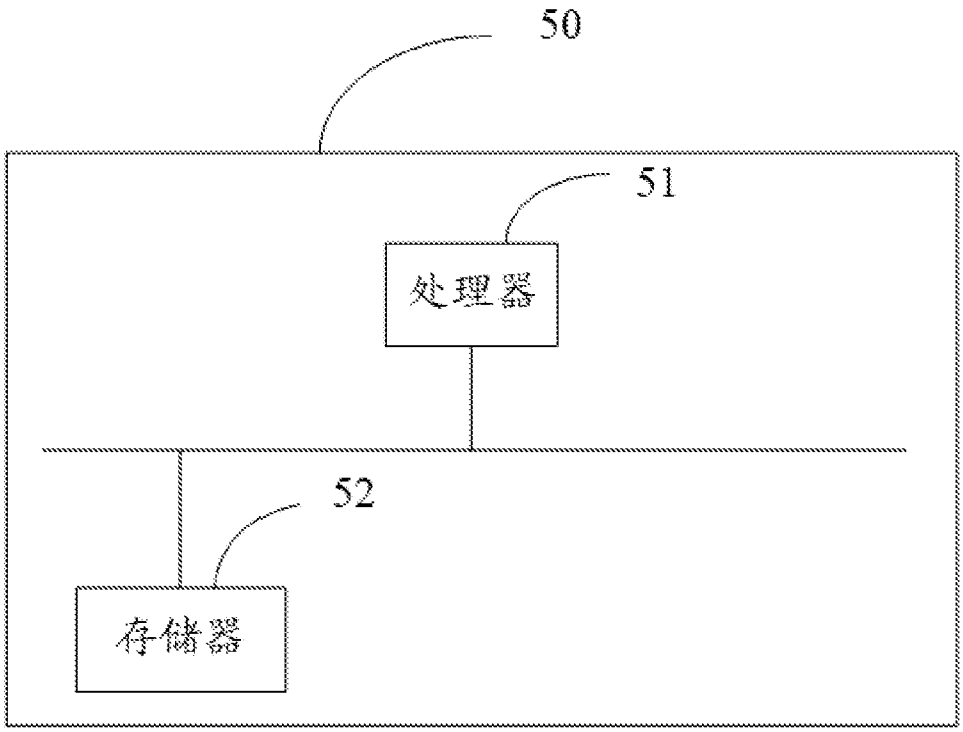

图 5

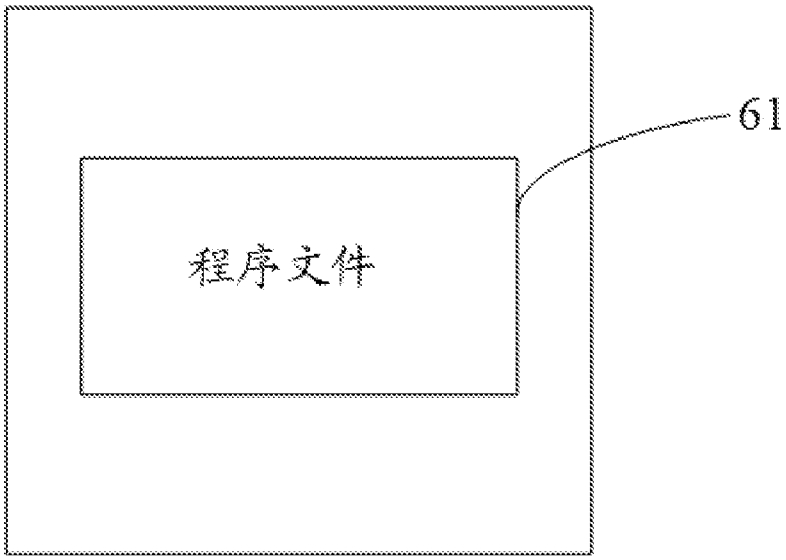

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/112257

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)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)

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)

CNPAT, WPI, EPODOC, CNKI, IEEE: 跨域, 第三方, 代理, 认证, 证书, 背书, 验证, 属性, 注册, 转换, 映射, 表, cross-domain, third, verification, proxy, authentication, certificate, verify, endorse, map

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 111447187 A (CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 24 July 2020 (2020-07-24) description, paragraphs [0055]-[0094], and figures 1-4	1-10
Y	CN 112532591 A (XIDIAN UNIVERSITY) 19 March 2021 (2021-03-19) description, paragraphs [0090]-[0174], and figures 1-4	1-10
A	CN 110166444 A (GUILIN UNIVERSITY OF ELECTRONIC TECHNOLOGY) 23 August 2019 (2019-08-23) entire document	1-10
A	CN 101399671 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCES) 01 April 2009 (2009-04-01) entire document	1-10
A	US 2014245417 A1 (ALCATEL LUCENT) 28 August 2014 (2014-08-28) entire document	1-10

☐ 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
01 April 2022	**25 April 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/CN2021/112257

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111447187 A	24 July 2020	None	
CN 112532591 A	19 March 2021	None	
CN 110166444 A	23 August 2019	None	
CN 101399671 A	01 April 2009	None	
US 2014245417 A1	28 August 2014	CN 103067338 A	24 April 2013
		JP 2014531163 A	20 November 2014
		KR 20140084217 A	04 July 2014
		EP 2770662 A1	27 August 2014
		WO 2013056674 A1	25 April 2013

国际检索报告

国际申请号
PCT/CN2021/112257

A. 主题的分类

H04L 9/32(2006.01)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)

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））

CNPAT, WPI, EPODOC, CNKI, IEEE: 跨域，第三方，代理，认证，证书，背书，验证，属性，注册，转换，映射，表，cross-domain, third, verification, proxy, authentication, certificate, verify, endorse, map

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
Y	CN 111447187 A (重庆邮电大学) 2020年7月24日 (2020-07-24) 说明书第[0055]-[0094]段，附图1-4	1-10
Y	CN 112532591 A (西安电子科技大学) 2021年3月19日 (2021-03-19) 说明书第[0090]-[0174]段，附图1-4	1-10
A	CN 110166444 A (桂林电子科技大学) 2019年8月23日 (2019-08-23) 全文	1-10
A	CN 101399671 A (中国科学院软件研究所) 2009年4月1日 (2009-04-01) 全文	1-10
A	US 2014245417 A1 (ALCATEL LUCENT) 2014年8月28日 (2014-08-28) 全文	1-10

☐ 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4月1日	2022年4月25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 周亚楠 电话号码 86-(10)-53961530

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/112257

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	111447187	A	2020年7月24日	无			
CN	112532591	A	2021年3月19日	无			
CN	110166444	A	2019年8月23日	无			
CN	101399671	A	2009年4月1日	无			
US	2014245417	A1	2014年8月28日	CN	103067338	A	2013年4月24日
				JP	2014531163	A	2014年11月20日
				KR	20140084217	A	2014年7月4日
				EP	2770662	A1	2014年8月27日
				WO	2013056674	A1	2013年4月25日