

(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
2017 年 1 月 19 日 (19.01.2017)



(10) 国际公布号
WO 2017/008640 A1

- (51) 国际专利分类号:
H04W 28/16 (2009.01)
- (21) 国际申请号: PCT/CN2016/087973
- (22) 国际申请日: 2016 年 6 月 30 日 (30.06.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510419740.3 2015 年 7 月 16 日 (16.07.2015) CN
- (71) 申请人: 电信科学技术研究院 (CHINA ACADEMY OF TELECOMMUNICATIONS TECHNOLOGY) [CN/CN]; 中国北京市海淀区学院路 40 号, Beijing 100191 (CN)。
- (72) 发明人: 周巍 (ZHOU, Wei); 中国北京市海淀区学院路 40 号, Beijing 100191 (CN)。
- (74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市海淀区知春路 7 号致真大厦 A1304-05 室, Beijing 100191 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

(54) Title: METHOD FOR ISSUING ACCESS TOKEN AND RELATED DEVICE

(54) 发明名称: 一种访问令牌颁发方法及相关设备

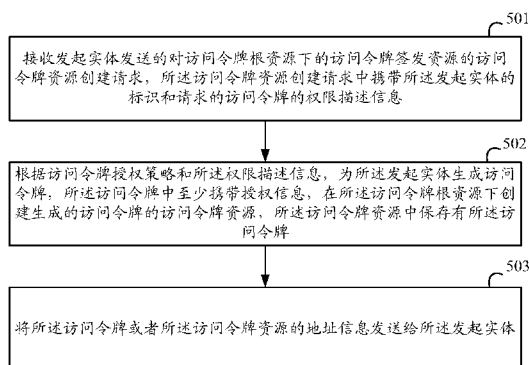


图 5

501 Receiving an access token resource creating request, transmitted by an initiating entity, for an access token issuing resource under an access token root resource, and the access token resource creating request carrying an identify of the initiating entity and authority description information of the requested access token
502 According to an access token authorization policy and the authority description information, generating an access token for the initiating entity, the access token carrying at least authorization information, and creating the access token resource of the generated access token under the access token root resource, the access token resource storing the access token therein
503 Transmitting the access token or address information of the access token resource to the initiating entity

(57) Abstract: A method for issuing an access token and a related device are used for giving a specific authorization mechanism in a oneM2M system. The method comprises: receiving an access token resource creating request, transmitted by an initiating entity, for an access token issuing resource under an access token root resource, and the access token resource creating request carrying an identify of the initiating entity and authority description information of the requested access token; according to an access token authorization policy and the authority description information, generating an access token for the initiating entity, the access token carrying at least authorization information, and creating the access token resource of the generated access token under the access token root resource; transmitting the access token or address information of the access token resource to the initiating entity; and the access token root resource being a common resource under an CSE root resource, the access token issuing resource being a virtual resource under the access token root resource, and the access token resource being a common resource under the access token root resource.

(57) 摘要:

[见续页]

WO 2017/008640 A1



一种访问令牌颁发方法及相关设备，用以给出 oneM2M 系统中具体的授权机制。该方法为：接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带所述发起实体的标识和请求的访问令牌的权限描述信息；根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，访问令牌中至少携带授权信息，在访问令牌根资源下创建生成的访问令牌的访问令牌资源；将访问令牌或者访问令牌资源的地址信息发送给所述发起实体；访问令牌根资源为 CSE 根资源下的普通资源，访问令牌签发资源为访问令牌根资源下的虚拟资源，访问令牌资源为访问令牌根资源下的普通资源。

一种访问令牌颁发方法及相关设备

本申请要求在 2015 年 7 月 16 日提交中国专利局、申请号为 201510419740.3、发明名称为“一种访问令牌颁发方法及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，尤其涉及一种访问令牌颁发方法及相关设备。

背景技术

物联网标准化组织 oneM2M 致力于开发用于构造一个公共的机器对机器通信 (Machine-To-Machine, 简称 M2M) 服务层 (Service Layer) 的技术规范。

oneM2M 功能架构如图 1 所示，定义了三种基本实体：

一，应用实体 (Application Entity, 简称 AE)，位于应用层，该实体可实现一个 M2M 应用服务逻辑。一个应用服务逻辑既可以驻留在多个 M2M 节点中，也可以在单个节点中存在多个执行实例。应用服务逻辑的每个执行实例被称为一个应用实体，每个应用实体由唯一的 AE 身份标识 (AE-ID) 标识。

例如，车队跟踪应用实例、远程血糖监测应用实例、远程电力计量实例或控制应用实例等都属于应用实体。

二，公共服务实体 (Common Services Entity, 简称 CSE)，一个公共服务实体由一组 M2M 环境中的公共服务功能 (common service functions) 构成。公共服务功能通过参考点 Mca 和参考点 Mcc 公开给其他实体。参考点 Mcn 用于访问底层网络服务实体。每个公共服务实体由唯一的 CSE-ID 标识。

三，底层网络服务实体 (Underlying Network Services Entity, 简称 NSE)，一个底层网络服务实体向多个 CSE 提供底层网络服务，例如提供设备管理、位置服务和设备触发服务。

oneM2M 通过对标准化的资源树的操作实现服务层资源共享和交互。

oneM2M 资源树存在于 oneM2M 系统定义的 CSE 中。

根据 oneM2M TS-0001 中关于功能架构的定义，oneM2M 资源树的形式如图 2 所示。其中，CSEBase1 表示一个 CSE 根资源<CSEBase>，CSE1 表示一个资源<remoteCSE>，APP1 表示一个资源<AE>，CONT1 和 CONT2 分别代表一个资源 <container>，ACP1 和 ACP2 分别代表一个资源 <accessControlPolice>。对于 oneM2M 资源可进行创建（Create，简称 C）、查询（Retrieve，简称 R）、修改（Update，简称 U）和删除（Delete，简称 D）等操作。

oneM2M 定义的资源中与授权相关的资源为访问控制策略资源 <accessControlPolicy>，其中定义有访问控制策略（Access Control Policy，简称 ACP），<accessControlPolicy>资源由资源身份标识（ID）唯一标识。其他资源通过资源中的 accessControlPolicyIDs 属性指定适用的访问控制策略。

oneM2M 系统中服务签约信息存储在<m2mServiceSubscriptionProfile>资源中，该资源的 serviceRoles 属性保存有可签约的服务角色 ID（Service Role ID）列表，AE 通过获取可签约的服务角色而获得相应的签约服务，也就是拥有管理<m2mServiceSubscriptionProfile>资源中 <serviceSubscribedNode>子资源中所描述的 M2M 节点（M2M Node）的权限。

oneM2M 定义有三种资源类型：

普通资源（Normal Resource），具有具体的资源结构以及资源属性；

虚拟资源（Virtual Resource），不具有具体的资源结构以及资源属性，主要用于触发特定的处理过程；

公布资源（Announced Resource），具有具体的资源结构及资源属性，该资源为其他实体上普通资源中某些内容的复制，主要目的是为资源发现提供便利。

目前，oneM2M 系统中仅给出了服务签约信息以及授权相关的资源，并没有给出具体的授权机制。

发明内容

本发明实施例提供一种访问令牌颁发方法及相关设备,用以给出 oneM2M 系统中具体的授权机制。

本发明实施例提供的具体技术方案如下:

第一方面,提供了一种访问令牌颁发方法,包括:

接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求,所述访问令牌资源创建请求中携带所述发起实体的标识和请求的访问令牌的权限描述信息;

根据访问令牌授权策略和所述权限描述信息,为所述发起实体生成访问令牌,所述访问令牌中至少携带授权信息,在所述访问令牌根资源下创建生成的访问令牌的访问令牌资源,所述访问令牌资源中保存有所述访问令牌;

将所述访问令牌或者所述访问令牌资源的地址信息发送给所述发起实体;

其中,所述访问令牌根资源为公共服务实体 CSE 根资源下的普通资源,所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源,所述访问令牌资源为所述访问令牌根资源下的普通资源。

实施中,所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性,所述公共属性所指定的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

实施中,接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求之后,为所述发起实体生成访问令牌之前,所述方法还包括:

根据所述访问令牌根资源的指定访问控制策略的公共属性,确定允许所述发起实体访问所述访问令牌根资源下的虚拟资源。

实施中,所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性,所述超期时间属性用于指定所述访问令牌资源的有效期,所述签发者属性用于指示生成所述访问令牌的实体,所

述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

实施中，根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌之前，所述方法还包括：

从访问令牌授权策略实体获取所述访问令牌授权策略。

实施中，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、所述发起实体的标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

实施中，根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，包括：

根据所述访问令牌授权策略和所述权限描述信息，生成访问令牌明文；

将生成的所述访问令牌明文发送给安全功能实体，由所述安全功能实体对所述访问令牌明文进行数字签名和/或加密后得到所述访问令牌并返回；

接收所述安全功能实体返回的所述访问令牌。

第二方面，提供了一种访问令牌颁发方法，包括：

向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

接收所述授权实体返回的访问令牌，或者接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息，所述访问令牌资源中保存有访问令牌，所述访问令牌中至少携带授权信息；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌资源为所述访问令牌根资源下的普通资源。

实施中，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定的访问控制策略指示允许访问所述

访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

实施中，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

实施中，接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息后，所述方法还包括：

根据所述地址信息获取所述访问令牌。

实施中，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、请求并持有所述访问令牌的实体标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

实施中，所述方法还包括：

发送资源访问请求，所述资源访问请求中携带所述访问令牌。

第三方面，提供了一种授权实体，包括：

接收模块，用于接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带所述发起实体的标识和请求的访问令牌的权限描述信息；

处理模块，用于根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，所述访问令牌中至少携带授权信息，在所述访问令牌根资源下创建生成的访问令牌的访问令牌资源，所述访问令牌资源中保存有所述访问令牌；

发送模块，用于将所述访问令牌或者所述访问令牌资源的地址信息发送给所述发起实体；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下的普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌

资源为所述访问令牌根资源下的普通资源。

实施中，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

实施中，所述处理模块还用于：

为所述发起实体生成访问令牌之前，根据所述访问令牌根资源的指定访问控制策略的公共属性，确定允许所述发起实体访问所述访问令牌根资源下的虚拟资源。

实施中，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

实施中，所述处理模块还用于：从访问令牌授权策略实体获取所述访问令牌授权策略。

实施中，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、所述发起实体的标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

实施中，所述处理模块具体用于：

根据所述访问令牌授权策略和所述权限描述信息，生成访问令牌明文；

所述发送模块还用于：

将生成的所述访问令牌明文发送给安全功能实体，由所述安全功能实体对所述访问令牌明文进行数字签名和/或加密后得到所述访问令牌并返回；

所述接收模块还用于：

接收所述安全功能实体返回的所述访问令牌。

第四方面，提供了一种发起实体，包括：

发送模块，用于向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

接收模块，用于接收所述授权实体返回的访问令牌，或者接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息，所述访问令牌资源中保存有访问令牌，所述访问令牌中至少携带授权信息；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌资源为所述访问令牌根资源下的普通资源。

实施中，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

实施中，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

实施中，还包括获取模块用于：

在所述接收模块接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息后，根据所述地址信息获取所述访问令牌。

实施中，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、请求并持有所述访问令牌的实体标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

实施中，所述发送模块还用于：

发送资源访问请求，所述资源访问请求中携带所述访问令牌。

第五方面，提供了一种授权实体，包括：处理器、收发机和存储器；

所述处理器，用于读取存储器中的程序，执行下列过程：

通过收发机接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带请求的访问令牌的权限描述信息；

根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，所述访问令牌中至少携带授权信息，在所述访问令牌根资源下创建生成的访问令牌的访问令牌资源，所述访问令牌资源中保存有所述访问令牌；

将所述访问令牌或者所述访问令牌资源的地址信息通过收发机发送给所述发起实体。

第六方面，提供了一种发起实体，包括：处理器、收发机和存储器；

所述处理器，用于读取存储器中的程序，执行下列过程：

通过收发机向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带请求的访问令牌的权限描述信息；

通过收发机接收所述授权实体返回的访问令牌，或者接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息，所述访问令牌资源中保存有访问令牌，所述访问令牌中至少携带授权信息。

基于上述技术方案，本发明实施例中，通过在 CSE 根资源下定义资源类型为普通资源的访问令牌根资源，在访问令牌根资源下定义资源类型为虚拟资源的访问令牌签发资源，以及在访问令牌根资源下定义资源类型为普通资源的访问令牌资源，且定义对访问令牌签发资源的访问令牌资源创建操作触发一个访问令牌颁发过程，从而使得接收到发起实体对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，触发访问令牌颁发过程，根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，并创建访问令牌资源，在 oneM2M 系统中实现了通过访问令牌进行授权的机制。

附图说明

- 图 1 为现有技术中的 oneM2M 功能架构示意图；
- 图 2 为现有技术中的 oneM2M 资源树的结构示意图；
- 图 3 为本发明实施例中定义的三种资源的关系示意图；
- 图 4 为本发明实施例中<accessToken>资源的基本结构示意图；
- 图 5 为本发明实施例中授权实体颁发访问令牌的过程示意图；
- 图 6 为本发明实施例中发起实体请求访问令牌的过程示意图；
- 图 7 为本发明实施例中托管实体使用访问令牌的过程示意图；
- 图 8 为本发明实施例中访问令牌颁发和使用的基本过程示意图；
- 图 9 为本发明实施例中访问令牌颁发以及使用的具体实施过程示意图；
- 图 10 为本发明实施例中访问令牌颁发以及使用的另一具体实施过程示意图；
- 图 11 为本发明实施例中授权实体的结构示意图；
- 图 12 为本发明实施例中另一授权实体的结构示意图；
- 图 13 为本发明实施例中发起实体的结构示意图；
- 图 14 为本发明实施例中另一发起实体的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

本发明实施例中，定义了三种 oneM2M 资源，以实现颁发授权访问令牌（Access Token）。

定义的三种 oneM2M 资源分别为：访问令牌根资源<accessTokens>、访问令牌签发资源<accessTokenIssuing>和访问令牌资源<accessToken>，三者之间的关系如图 3 所示。

其中，<accessTokens>资源定义为 CSE 根资源<CSEBase>下的子资源，资源类型为 oneM2M 普通资源，<CSEBase>资源下可以有 0 个或多个<accessTokens>资源。

<accessTokens>资源除拥有 oneM2M 普通资源所包含的通用属性（Universal Attribute）外，还具有指定访问控制策略的公共属性（Common Attribute）：accessControlPolicyIDs，对<accessTokens>资源下的虚拟资源的访问控制由该公共属性确定，即该公共属性所指定的访问控制策略中定义了允许访问该<accessTokens>资源及其下的虚拟资源的 AE 实体和 CSE 实体。

其中，<accessTokenIssuing>资源为<accessTokens>资源下的子资源，一个<accessTokens>资源下有一个<accessTokenIssuing>资源。<accessTokenIssuing>资源的资源类型为 oneM2M 虚拟资源，因此没有资源属性，也没有子资源。oneM2M 虚拟资源主要用来触发一个处理过程，一个针对<accessTokenIssuing>资源的创建请求（Create Request）将触发一个访问令牌颁发过程。

<accessTokenIssuing>资源的访问控制由其父资源<accessTokens>的 accessControlPolicyIDs 属性指定的访问控制策略确定，accessControlPolicyIDs 属性规定了可以访问<accessTokenIssuing>资源的 AE 实体和 CSE 实体，即申请访问令牌。

其中，<accessToken>资源为<accessTokens>资源下的子资源，一个<accessTokens>资源下可以包含 0 个或多个<accessToken>资源。每个<accessToken>表示一个授权实体所颁发的访问令牌（Access Token），其资源类型为 oneM2M 普通资源（Normal Resource）。

<accessToken>的基本结构如图 4 所示，<accessToken>资源除了包含 oneM2M 普通资源所共有的通用属性（Universal Attribute）外，还包含有公共属性（Common Attribute）：超期时间（expirationTime），还包括新定义的 3 个资源属性。expirationTime 指定该资源的有效期，其与访问令牌的有效期相同。3 个新定义的资源属性为：

issuer: 访问令牌的签发者，具体为生成该访问令牌的 CSE 标识（CSE-ID）。

holder: 访问令牌的持有者, 具体为请求并持有该访问令牌的 AE 标识 (AE-ID) 或 CES 标识 (CSE-ID)。

token: 存储所颁发的访问令牌。

本发明实施例中定义如下:

发起实体 (Originator Entity): 为 oneM2M 系统中访问令牌的拥有者, 具体为 oneM2M 系统中需要对托管实体中的资源进行访问的 AE 实体或 CSE 实体;

授权实体 (Authority Entity): 为 oneM2M 系统中访问令牌的颁发者, 具体为 oneM2M 系统中具有访问令牌颁发能力的 CSE 实体;

托管实体 (Hosting Entity): 为 oneM2M 系统中访问令牌的使用者, 具体为 oneM2M 系统中提供资源访问的 CSE 实体, 其根据访问令牌中描述的访问权限为发起实体提供资源访问服务;

访问令牌授权策略实体 (Access Token Authorization Policy Entity): 为授权实体提供访问令牌授权策略, 该访问令牌授权策略用于确定写入访问令牌的权限;

安全功能实体 (Security Function Entity): 可对访问令牌明文进行数字签名和/或加密以生成访问令牌, 或对访问令牌进行解密和/或验证数字签名以获得访问令牌明文。

本发明实施例中的访问令牌定义为: 用于携带应用于 oneM2M 环境中的授权信息, 主要包括服务角色和/或访问控制策略。访问令牌中携带的服务角色用于基于角色的访问控制 (Role Based Access Control, 简称 RBAC); 还用于携带认证信息, 所述认证信息包括生成访问令牌的 CSE 标识 (即签发者标识)、请求并持有访问令牌的实体标识 (将持有者标识) 和超期时间。

若访问令牌的授权信息中仅携带角色, 托管实体利用访问令牌中携带的角色和托管实体本地存储的基于角色的访问控制策略评估发起实体的资源访问请求, 以确定是否同意发起实体的资源访问请求。

若访问令牌的授权信息中仅携带访问控制策略, 该访问控制策略为访问

令牌持有者的专用授权策略，托管实体使用访问令牌中携带的访问控制策略评估发起实体的资源访问请求，以确定是否同意该资源访问请求。

若访问令牌的授权信息中携带角色和访问控制策略，托管实体利用访问令牌中携带的角色和访问控制策略评估发起实体的资源访问请求，以确定是否同意发起实体的资源访问请求。

需要说明的是，本发明实施例对访问令牌的具体格式不作限制。授权实体、发起实体和托管实体之间约定访问令牌的格式即可正确使用访问令牌，本发明的保护范围并不受访问令牌具体格式的限制。

基于以上定义，本发明实施例中，如图 5 所示，授权实体颁发访问令牌的详细方法流程如下：

步骤 501: 接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带所述发起实体的标识和请求的访问令牌的权限描述信息。

其中，访问令牌根资源为 CSE 根资源下的普通资源，访问令牌签发资源为访问令牌根资源下的虚拟资源。

实施中，由于访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，公共属性所指定的访问控制策略指示允许访问访问令牌根资源及访问令牌根资源下的虚拟资源的实体，因此授权实体在接收发起实体向访问令牌根资源下的访问令牌签发资源发送的访问令牌资源创建请求之后，为发起实体生成访问令牌之前，根据访问令牌根资源的指定访问控制策略的公共属性，确定允许发起实体访问该访问令牌根资源下的虚拟资源。

对访问令牌签发资源的资源创建操作，将触发一个访问令牌颁发过程。

步骤 502: 根据访问令牌授权策略和访问令牌资源创建请求中携带的权限描述信息，为发起实体生成访问令牌，所述访问令牌中至少携带授权信息，在访问令牌根资源下创建生成的访问令牌的访问令牌资源，访问令牌资源中保存有访问令牌。

其中，访问令牌资源具有普通资源的通用属性以及超期时间属性、签发

者属性、持有者属性和令牌属性，超期时间属性用于指定访问令牌资源的有效期，签发者属性用于指示生成访问令牌的实体，即授权实体的标识，持有者属性用于指示请求并获得访问令牌的实体，即发起实体的标识，令牌属性用于存储访问令牌。

授权实体生成的访问令牌以及令牌属性存储的访问令牌除包含授权信息外，还包括认证信息。其中，认证信息包括生成访问令牌的授权实体的标识（即签发者标识）、请求并持有访问令牌的发起实体的标识（将持有者标识）和超期时间，超期时间定义了访问令牌的有效期。其中，授权信息包括发起实体的服务角色和/或访问控制策略。

可选地，访问令牌授权策略保存在访问令牌授权策略实体；授权实体根据访问令牌授权策略和权限描述信息，为发起实体生成访问令牌之前，从访问令牌授权策略实体获取访问令牌授权策略。

一个具体实施中，访问令牌授权策略实体中保存访问令牌授权策略与发起实体以及授权实体的对应关系，例如，访问令牌授权策略实体中包含各授权实体资源树，分别对应不同的授权实体，授权实体资源数下包含不同的发起实体的访问令牌授权策略资源。

其中，权限描述信息用于描述发起实体请求的权限，该权限可以是请求的服务角色，或者是请求的访问控制策略，也可以是服务角色和访问控制策略。

实施中，授权信息中颁发给发起实体的服务角色为：授权描述信息中请求的服务角色且访问令牌授权策略允许颁发给发起实体的服务角色。授权信息中颁发给发起实体的访问控制策略为：授权描述信息中所请求的权限且访问令牌授权策略允许发起实体使用的权限所对应的访问控制策略。

需要说明的是，访问令牌授权策略用于确定是否为发起实体颁发访问令牌，以及确定写入访问令牌的权限，即颁发给访问令牌的发起和持有者的权限，具体的策略根据具体应用进行设计，本领域技术人员可以将已有的授权策略结合应用于本发明，本发明的保护范围不以此为限制。

实施中，授权实体若根据访问令牌授权策略和权限描述信息，确定不允许为发起实体颁发访问令牌，不再执行步骤 503，向发起实体返回错误信息。

步骤 503：将访问令牌或者访问令牌资源的地址信息发送给发起实体。

其中，访问令牌资源为访问令牌根资源下的普通资源。

一个可选地实施方式中，授权实体根据访问令牌授权策略和权限描述信息生成访问令牌明文，将生成的访问令牌明文发送给安全功能实体，由安全功能实体对访问令牌进行数字签名和/或加密后得到访问令牌并返回；授权实体接收安全功能实体返回的访问令牌，并将访问令牌发送给发起实体。

需要说明的是，安全功能实体具体采用的数字签名算法和加密算法不受限制，已有的数字签名算法和加密算法均可用于本发明，具体的数字签名算法和加密算法不受限制，本发明的保护范围不受此限制。

基于以上定义，本发明实施例中，如图 6 所示，发起实体请求访问令牌的详细方法流程如下：

步骤 601：向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息。

其中，访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，公共属性所指定的访问控制策略指示允许访问访问令牌根资源及访问令牌根资源下的虚拟资源的实体。

其中，权限描述信息用于描述发起实体请求的权限，该权限可以是请求的服务角色，或者是请求的访问控制策略，也可以是服务角色和访问控制策略。

步骤 602：接收授权实体返回的访问令牌，或者接收授权实体在访问令牌根资源下创建的访问令牌资源的地址信息，访问令牌资源中保存有访问令牌，访问令牌中至少携带授权信息。

其中，访问令牌根资源为 CSE 根资源下的普通资源，访问令牌签发资源为访问令牌根资源下的虚拟资源，访问令牌资源为访问令牌根资源下的普通

资源。

访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，超期时间属性用于指定访问令牌资源的有效期，签发者属性用于指示生成访问令牌的实体，持有者属性用于指示请求并获得访问令牌的实体，令牌属性用于存储访问令牌。

实施中，若发起实体接收授权实体在访问令牌根资源下创建的访问令牌资源的地址信息后，根据地址信息获取访问令牌。

其中，访问令牌中除携带授权信息之外还携带认证信息，认证信息包括生成访问令牌的实体标识、请求并持有访问令牌的实体标识和超期时间，授权信息包括发起实体的服务角色和/或访问控制策略。

实施中，授权信息中颁发给发起实体的服务角色为：授权描述信息中请求的服务角色且访问令牌授权策略允许颁发给发起实体的服务角色。授权信息中颁发给发起实体的访问控制策略为：授权描述信息中所请求的权限且访问令牌授权策略允许发起实体使用的权限所对应的访问控制策略。

实施中，发起实体在获得访问令牌后，向授权实体发送资源访问请求，该资源访问请求中携带访问令牌。

基于同一发明构思，本发明实施例中，如图 7 所示，托管实体使用访问令牌的详细方法流程如下：

步骤 701：接收发起实体发送的资源访问请求，资源访问请求中携带访问令牌。

其中，访问令牌中至少携带授权信息，授权信息包括发起实体的服务角色和/或访问控制策略。

实施中，访问令牌中除携带授权信息之外还携带认证信息，认证信息包括生成访问令牌的实体标识、请求并持有访问令牌的实体标识和超期时间。

实施中，托管实体获取资源访问请求中的访问令牌后，判断该访问令牌是否有效，具体如下：

若满足预设条件，则确定该访问令牌有效，否则，确定访问令牌无效；

预设条件可以包括以下条件：

若确定访问令牌中携带的生成访问令牌的实体标识与预设的 CSE 标识相同；和/或，

访问令牌中携带的请求并持有访问令牌的实体标识与发起实体的标识相同；和/或，

访问令牌的使用时间未超过访问令牌中携带的超期时间，则确定该访问令牌有效。

实施中，托管实体若确定访问令牌无效，不再执行步骤 702，向发起实体返回错误信息。

步骤 702：根据访问令牌中的授权信息，确定发起实体的资源访问请求在授权范围内，执行发起实体的资源访问请求。

实施中，若授权信息中仅包括服务角色，根据访问令牌中的服务角色，获取本地保存的基于服务角色的访问控制策略，根据基于服务角色的访问控制策略确定发起实体的资源访问请求在授权范围内；若授权信息中仅包括访问控制策略，根据访问令牌中的访问控制策略确定发起实体的资源访问请求在授权范围内；若授权信息中包括服务角色和访问控制策略，根据访问令牌中的服务角色和访问控制策略确定发起实体的资源访问请求在授权范围内。

一个可选地实施方式中，托管实体在获得资源访问请求中的访问令牌后，将该访问令牌发送给安全认证实体，由该安全认证实体对该访问令牌进行解密和/或数字签名验证获得访问令牌明文并返回；托管实体接收安全认证实体返回的访问令牌明文，获得访问令牌明文中的授权信息，根据获得的授权信息，判断发起实体的资源访问请求是否在授权范围内。

以上实施例，授权实体和托管实体可以部署在同一个实体设备中，也可以部署在不同的实体设备中。

以上实施例，发起实体和授权实体之间通信之前，发起实体和托管实体之间通信之前，分别采用 oneM2M 提供的方法通过双向认证建立安全关联，以确保相互通信的两个实体之间通信的完整性和机密性，具体的通过双向认

证建立安全关联的方式参见 oneM2M 的规定，此处不再详述。

以上实施例中所涉及的访问令牌颁发和使用的基本过程可参见图 8 所示，具体过程可参见以上实施例的描述，此处不再重复。

以下通过两个具体实施例对本发明所提供的访问令牌颁发以及使用过程进行举例说明。

第一具体实施例，作为授权实体的 oneM2M 基础设施节点（IN-CSE）向发起实体（AE-1）颁发包含有服务角色（Service Role）的访问令牌；发起实体（AE-1）利用该访问令牌访问托管实体（CSE-1）中的设备管理资源；CSE-1 所在的节点为 Node-1。

该具体实施例中假设：IN-CSE 可访问的安全功能实体和 CSE-1 可访问的安全功能实体拥有用于访问令牌加密和解密的对称密钥 K_s ；IN-CSE 可访问的安全功能实体拥有用于对访问令牌明文进行签名的私钥 K_{priv} ；CSE-1 可访问的安全功能实体拥有用于验证 IN-CSE 数字签名的公钥证书 IN_{cert} ，其中包含有与 K_{priv} 匹配的公钥 K_{pub} 。

并且，假设 oneM2M 应用服务提供商的应用实体 AE-1 注册至 oneM2M 服务提供商的基础设施节点 IN-CSE 上。在 IN-CSE 资源树的根资源 $\langle CSEBase \rangle$ 下创建有负责颁发访问令牌的 $\langle accessTokens-1 \rangle$ 资源；在 IN-CSE 资源树中定义有 $\langle m2mServiceSubscriptionProfile \rangle$ ， $\langle serviceSubscribedNode \rangle$ 和 $\langle serviceSubscribedAppRule \rangle$ 等资源，其中描述了该应用服务提供商的应用实体所能拥有的角色和管理的 M2M 节点（M2M Node）

如图 9 所示，访问令牌颁发以及使用的过程具体如下：

步骤 901：AE-1 与 IN-CSE 通过双向认证建立安全关联；

步骤 902：AE-1 向 IN-CSE 发送对 IN-CSE 资源树下的 $\langle accessTokens-1 \rangle$ 资源的子资源 $\langle accessTokenIssuing \rangle$ 的 $\langle accessToken \rangle$ 资源创建请求，该请求要求对 CSE-1 所在的节点 Node-1 执行设备诊断功能，也即 AE-1 想要获取包含有“设备诊断和管理（Device Diagnostics and Management）”角色的访问令牌；

步骤 903：IN-CSE 接收到 AE-1 的请求后，该请求所激活的访问令牌创建

过程将做如下操作:

1、检查与<accessTokenIssuing>资源相关联的访问控制策略, 确定 AE-1 是否拥有创建<accessToken>资源的权限, 若允许则继续进行下一步的操作;

2、从作为访问令牌授权策略实体的 IN-CSE 资源树中获取所需的访问令牌授权策略, 也即与 AE-1 相关的 <m2mServiceSubscriptionProfile>, <serviceSubscribedNode>和<serviceSubscribedAppRule>等资源;

3、检查属于该应用服务提供商的<m2mServiceSubscriptionProfile>资源中的 serviceRoles 属性以确定是否拥有所请求的“设备诊断和管理 (Device Diagnostics and Management)”角色, 若有则继续进行下一步的操作;

4、检查 <m2mServiceSubscriptionProfile> 资源下的 <serviceSubscribedNode>子资源, 以确定该应用服务商是否拥有对节点 Node-1 的管理权限, 也即是否某个<serviceSubscribedNode>子资源的 node-ID 属性的值为 Node-1, 若有则继续进行下一步的操作;

5、检查上一步匹配的<serviceSubscribedNode>资源下的 ruleLinks 属性所指定的<serviceSubscribedAppRule>资源, 以确定该 AE-1 可以注册至节点 Node-1, 也即 AE-1 是否在该<serviceSubscribedAppRule>资源 allowedAEs 属性的 AE 列表中, 若有则继续进行下一步的操作;

6、生成一个访问令牌明文, 其中包含有“设备诊断和管理 (Device Diagnostics and Management)”角色, 并设定了访问令牌的有效期;

7、要求安全功能实体利用私钥 Kpriv 对访问令牌明文进行数字签名, 然后利用对称密钥 Ks 对访问令牌明文和签名结果进行加密, 从而生成访问令牌 AE-Token-1。

步骤 904: IN-CSE 将生成的访问令牌 AE-Token-1 发送给 AE-1;

步骤 905: AE-1 与 CSE-1 通过双向认证建立安全关联;

步骤 906: AE-1 向 Node-1 所包含的 CSE-1 发送设备诊断请求, 该请求中包含有访问令牌 AE-Token-1;

步骤 907: CSE-1 接收到来自 AE-1 的设备诊断请求, 并从设备诊断请求

中提取出访问令牌 AE-Token-1，然后做如下操作：

- 1、要求安全功能实体利用 K_s 对访问令牌进行解密，然后利用 INcert 中的公钥 K_{pub} 验证访问令牌的数字签名，若正确则继续进行下一步的操作；
- 2、检查访问令牌中的有效期，以确定令牌是否已经失效，若有效则继续进行下一步的操作；
- 3、提取出令牌中包含的角色，并利用基于角色的访问控制策略评估是否同意 AE-1 的设备诊断请求，若同意则继续进行下一步的操作；
- 4、执行 AE-1 所要求的设备诊断功能。

步骤 908：CSE-1 将执行结果返回给 AE-1。

第二具体实施例中，如图 10 所示，该具体实施例中授权实体与托管实体为同一个实体，即为 CSE-1，该具体实施例中访问令牌颁发与使用过程与第一具体实施例的过程类似，不同之处在于：

因为授权实体与托管实体为同一实体，安全功能实体中保护访问令牌的安全机制可以采用单纯的对称密钥机制，也即利用对称密钥实现访问令牌的完整性和机密性保护。

并且，由于 CSE-1 的类型不是 IN-CSE，即基础设施节点，也不是基础设施节点信任和授权的节点，所以 CSE-1 不能颁发包含有服务角色（Service Role）的访问令牌。

基于同一发明构思，本发明实施例中提供了一种授权实体，该授权实体的具体实施可参见上述方法部分的描述，重复之处不再赘述，如图 11 所示，该授权实体主要包括：

接收模块 1101，用于接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

处理模块 1102，用于根据访问令牌授权策略和权限描述信息，为发起实体生成访问令牌，访问令牌中至少携带授权信息，在访问令牌根资源下创建生成的访问令牌的访问令牌资源，访问令牌资源中保存有访问令牌；

发送模块 1103, 用于将访问令牌或者访问令牌资源的地址信息发送给发起实体。

其中, 访问令牌根资源为 CSE 根资源下的普通资源, 访问令牌签发资源为访问令牌根资源下的虚拟资源, 访问令牌资源为访问令牌根资源下的普通资源。

实施中, 访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性, 公共属性所指定的访问控制策略指示允许访问访问令牌根资源及访问令牌根资源下的虚拟资源的实体。

实施中, 处理模块 1102 还用于:

为发起实体生成访问令牌之前, 根据访问令牌根资源的指定访问控制策略的公共属性, 确定允许发起实体访问访问令牌根资源下的虚拟资源。

实施中, 访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性, 超期时间属性用于指定访问令牌资源的有效期, 签发者属性用于指示生成访问令牌的实体, 持有者属性用于指示请求并获得访问令牌的实体, 令牌属性用于存储访问令牌。

实施中, 处理模块 1102 还用于: 从访问令牌授权策略实体获取访问令牌授权策略。

实施中, 访问令牌中还携带认证信息, 认证信息包括生成访问令牌的实体标识、发起实体的标识和超期时间;

访问令牌的授权信息包括发起实体的服务角色和/或访问控制策略。

实施中, 处理模块 1102 具体用于:

根据访问令牌授权策略和权限描述信息, 生成访问令牌明文;

发送模块 1103 还用于:

将生成的访问令牌明文发送给安全功能实体, 由安全功能实体对访问令牌明文进行数字签名和/或加密后得到访问令牌并返回;

接收模块 1101 还用于:

接收安全功能实体返回的访问令牌。

实施中，授权实体为 CSE 实体。

基于同一发明构思，本发明实施例中提供了一种授权实体，该授权实体的具体实施可参见上述方法部分的描述，重复之处不再赘述，如图 12 所示，该授权实体主要包括处理器 1201、存储器 1202 和收发机 1203，收发机 1203 用于在处理器 1201 的控制下接收和发送数据，存储器 1202 中保存预设的程序，处理器 1201 用于读取存储器中保存的程序，按照该程序执行以下过程：

通过收发机 1203 接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

根据访问令牌授权策略和权限描述信息，为发起实体生成访问令牌，访问令牌中至少携带授权信息，在访问令牌根资源下创建生成的访问令牌的访问令牌资源，访问令牌资源中保存有访问令牌；

通过收发机 1203 将访问令牌或者访问令牌资源的地址信息发送给发起实体。

其中，访问令牌根资源为 CSE 根资源下的普通资源，访问令牌签发资源为访问令牌根资源下的虚拟资源，访问令牌资源为访问令牌根资源下的普通资源。

实施中，访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，公共属性所指定的访问控制策略指示允许访问访问令牌根资源及访问令牌根资源下的虚拟资源的实体。

实施中，处理器 1201 为发起实体生成访问令牌之前，根据访问令牌根资源的指定访问控制策略的公共属性，确定允许发起实体访问访问令牌根资源下的虚拟资源。

实施中，访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，超期时间属性用于指定访问令牌资源的有效期，签发者属性用于指示生成访问令牌的实体，持有者属性用于指示请求并获得访问令牌的实体，令牌属性用于存储访问令牌。

实施中，处理器 1201 从访问令牌授权策略实体获取访问令牌授权策略。

实施中，访问令牌中还携带认证信息，认证信息包括生成访问令牌的实体标识、发起实体的标识和超期时间；

访问令牌的授权信息包括发起实体的服务角色和/或访问控制策略。

实施中，处理器 1201 根据访问令牌授权策略和权限描述信息，生成访问令牌明文；通过收发机 1203 将生成的访问令牌明文发送给安全功能实体，由安全功能实体对访问令牌明文进行数字签名和/或加密后得到访问令牌并返回；通过收发机 1203 接收安全功能实体返回的访问令牌。

实施中，授权实体为 CSE 实体。

其中，总线架构可以包括任意数量的互联的总线和桥，具体由处理器代表的一个或多个处理器和存储器代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机可以是多个元件，即包括发送机和收发机，提供用于在传输介质上与各种其他装置通信的单元。处理器负责管理总线架构和通常的处理，存储器可以存储处理器在执行操作时所使用的数据。

基于同一发明构思，本发明实施例提供了一种发起实体，该发起实体的具体实施可参见上述方法部分的描述，如图 13 所示，该发起实体主要包括：

发送模块 1301，用于向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

接收模块 1302，用于接收授权实体返回的访问令牌，或者接收授权实体在访问令牌根资源下创建的访问令牌资源的地址信息，访问令牌资源中保存有访问令牌，访问令牌中至少携带授权信息；

其中，访问令牌根资源为公共服务实体 CSE 根资源下普通资源，访问令牌签发资源为访问令牌根资源下的虚拟资源，访问令牌资源为访问令牌根资源下的普通资源。

其中，访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，公共属性所指定的访问控制策略指示允许访问访问令牌根资源及访问令牌根资源下的虚拟资源的实体。

其中，访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，超期时间属性用于指定访问令牌资源的有效期，签发者属性用于指示生成访问令牌的实体，持有者属性用于指示请求并获得访问令牌的实体，令牌属性用于存储访问令牌。

实施中，还包括获取模块 1303 用于：

在接收模块 1302 接收授权实体在访问令牌根资源下创建的访问令牌资源的地址信息后，根据地址信息获取访问令牌。

其中，访问令牌中还携带认证信息，认证信息包括生成访问令牌的实体标识、请求并持有访问令牌的实体标识和超期时间；

访问令牌的授权信息包括发起实体的服务角色和/或访问控制策略。

实施中，发送模块 1301 还用于：

发送资源访问请求，资源访问请求中携带访问令牌。

实施中，发起实体为 AE 实体或 CSE 实体。

基于同一发明构思，本发明实施例还提供了另一发起实体，该发起实体的具体实施可参见上述方法部分的描述，重复之处不再赘述，如图 14 所示，该发起实体主要包括处理器 1401、存储器 1402 和收发机 1403，收发机 1403 用于在处理器 1401 的控制下接收和发送数据，存储器 1402 中保存预设的程序，处理器 1401 用于读取存储器中保存的程序，按照该程序执行以下过程：

指示收发机 1403 向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

通过收发机 1403 接收授权实体返回的访问令牌，或者接收授权实体在访问令牌根资源下创建的访问令牌资源的地址信息，访问令牌资源中保存有访问令牌，访问令牌中至少携带授权信息；

其中，访问令牌根资源为公共服务实体 CSE 根资源下普通资源，访问令牌签发资源为访问令牌根资源下的虚拟资源，访问令牌资源为访问令牌根资源下的普通资源。

其中，访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，公共属性所指定的访问控制策略指示允许访问访问令牌根资源及访问令牌根资源下的虚拟资源的实体。

其中，访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，超期时间属性用于指定访问令牌资源的有效期，签发者属性用于指示生成访问令牌的实体，持有者属性用于指示请求并获得访问令牌的实体，令牌属性用于存储访问令牌。

实施中，处理器 1401 在通过收发机 1403 接收授权实体在访问令牌根资源下创建的访问令牌资源的地址信息后，根据地址信息获取访问令牌。

其中，访问令牌中还携带认证信息，认证信息包括生成访问令牌的实体标识、请求并持有访问令牌的实体标识和超期时间；

访问令牌的授权信息包括发起实体的服务角色和/或访问控制策略。

实施中，处理器 1401 指示收发机 1403 发送资源访问请求，资源访问请求中携带访问令牌。

实施中，发起实体为 AE 实体或 CSE 实体。

其中，总线架构可以包括任意数量的互联的总线和桥，具体由处理器代表的一个或多个处理器和存储器代表的存储器的各种电路链接在一起。总线架构还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起，这些都是本领域所公知的，因此，本文不再对其进行进一步描述。总线接口提供接口。收发机可以是多个元件，即包括发送机和收发机，提供用于在传输介质上与各种其他装置通信的单元。处理器负责管理总线架构和通常的处理，存储器可以存储处理器在执行操作时所使用的数据。

基于上述技术方案，本发明实施例中，通过在 CSE 根资源下定义资源类型为普通资源的访问令牌根资源，在访问令牌根资源下定义资源类型为虚拟

资源的访问令牌签发资源，以及在访问令牌根资源下定义资源类型为普通资源的访问令牌资源，且定义对访问令牌签发资源的访问令牌资源创建操作触发一个访问令牌颁发过程，从而使得接收到发起实体对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，触发访问令牌颁发过程，根据访问令牌授权策略和权限描述信息，为发起实体生成访问令牌，并创建访问令牌资源，在 oneM2M 系统中实现了通过访问令牌进行授权的机制。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步

骤。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种访问令牌颁发方法，其特征在于，包括：

接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带所述发起实体的标识和请求的访问令牌的权限描述信息；

根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，所述访问令牌中至少携带授权信息，在所述访问令牌根资源下创建生成的访问令牌的访问令牌资源，所述访问令牌资源中保存有所述访问令牌；

将所述访问令牌或者所述访问令牌资源的地址信息发送给所述发起实体；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下的普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌资源为所述访问令牌根资源下的普通资源。

2、如权利要求 1 所述的方法，其特征在于，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

3、如权利要求 2 所述的方法，其特征在于，接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求之后，为所述发起实体生成访问令牌之前，所述方法还包括：

根据所述访问令牌根资源的指定访问控制策略的公共属性，确定允许所述发起实体访问所述访问令牌根资源下的虚拟资源。

4、如权利要求 1 所述的方法，其特征在于，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述

访问令牌的实体，所述令牌属性用于存储所述访问令牌。

5、如权利要求 1 所述的方法，其特征在于，根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌之前，所述方法还包括：

从访问令牌授权策略实体获取所述访问令牌授权策略。

6、如权利要求 1-5 任一项所述的方法，其特征在于，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、所述发起实体的标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

7、如权利要求 6 所述的方法，其特征在于，根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，包括：

根据所述访问令牌授权策略和所述权限描述信息，生成访问令牌明文；

将生成的所述访问令牌明文发送给安全功能实体，由所述安全功能实体对所述访问令牌明文进行数字签名和/或加密后得到所述访问令牌并返回；

接收所述安全功能实体返回的所述访问令牌。

8、一种访问令牌颁发方法，其特征在于，包括：

向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

接收所述授权实体返回的访问令牌，或者接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息，所述访问令牌资源中保存有访问令牌，所述访问令牌中至少携带授权信息；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌资源为所述访问令牌根资源下的普通资源。

9、如权利要求 8 所述的方法，其特征在于，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定

的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

10、如权利要求 8 所述的方法，其特征在于，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

11、如权利要求 10 所述的方法，其特征在于，接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息后，所述方法还包括：

根据所述地址信息获取所述访问令牌。

12、如权利要求 8-11 任一项所述的方法，其特征在于，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、请求并持有所述访问令牌的实体标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

13、如权利要求 12 所述的方法，其特征在于，所述方法还包括：

发送资源访问请求，所述资源访问请求中携带所述访问令牌。

14、一种授权实体，其特征在于，包括：

接收模块，用于接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带所述发起实体的标识和请求的访问令牌的权限描述信息；

处理模块，用于根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，所述访问令牌中至少携带授权信息，在所述访问令牌根资源下创建生成的访问令牌的访问令牌资源，所述访问令牌资源中保存有所述访问令牌；

发送模块，用于将所述访问令牌或者所述访问令牌资源的地址信息发送给所述发起实体；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下的普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌资源为所述访问令牌根资源下的普通资源。

15、如权利要求 14 所述的授权实体，其特征在于，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

16、如权利要求 15 所述的授权实体，其特征在于，所述处理模块还用于：为所述发起实体生成访问令牌之前，根据所述访问令牌根资源的指定访问控制策略的公共属性，确定允许所述发起实体访问所述访问令牌根资源下的虚拟资源。

17、如权利要求 14 所述的授权实体，其特征在于，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

18、如权利要求 14 所述的授权实体，其特征在于，所述处理模块还用于：从访问令牌授权策略实体获取所述访问令牌授权策略。

19、如权利要求 14-18 任一项所述的授权实体，其特征在于，所述访问令牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、所述发起实体的标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

20、如权利要求 19 所述的授权实体，其特征在于，所述处理模块具体用于：

根据所述访问令牌授权策略和所述权限描述信息，生成访问令牌明文；
所述发送模块还用于：

将生成的所述访问令牌明文发送给安全功能实体，由所述安全功能实体对所述访问令牌明文进行数字签名和/或加密后得到所述访问令牌并返回；

所述接收模块还用于：

接收所述安全功能实体返回的所述访问令牌。

21、一种发起实体，其特征在于，包括：

发送模块，用于向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带发起实体的标识和请求的访问令牌的权限描述信息；

接收模块，用于接收所述授权实体返回的访问令牌，或者接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息，所述访问令牌资源中保存有访问令牌，所述访问令牌中至少携带授权信息；

其中，所述访问令牌根资源为公共服务实体 CSE 根资源下普通资源，所述访问令牌签发资源为所述访问令牌根资源下的虚拟资源，所述访问令牌资源为所述访问令牌根资源下的普通资源。

22、如权利要求 21 所述的发起实体，其特征在于，所述访问令牌根资源具有普通资源的通用属性以及指定访问控制策略的公共属性，所述公共属性所指定的访问控制策略指示允许访问所述访问令牌根资源及所述访问令牌根资源下的虚拟资源的实体。

23、如权利要求 21 所述的发起实体，其特征在于，所述访问令牌资源具有普通资源的通用属性以及超期时间属性、签发者属性、持有者属性和令牌属性，所述超期时间属性用于指定所述访问令牌资源的有效期，所述签发者属性用于指示生成所述访问令牌的实体，所述持有者属性用于指示请求并获得所述访问令牌的实体，所述令牌属性用于存储所述访问令牌。

24、如权利要求 23 所述的发起实体，其特征在于，还包括获取模块用于：在所述接收模块接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息后，根据所述地址信息获取所述访问令牌。

25、如权利要求 21-24 任一项所述的发起实体，其特征在于，所述访问令

牌中还携带认证信息，所述认证信息包括生成所述访问令牌的实体标识、请求并持有所述访问令牌的实体标识和超期时间；

所述访问令牌的授权信息包括所述发起实体的服务角色和/或访问控制策略。

26、如权利要求 25 所述的发起实体，其特征在于，所述发送模块还用于：发送资源访问请求，所述资源访问请求中携带所述访问令牌。

27、一种授权实体，其特征在于，包括：处理器、收发机和存储器；所述处理器，用于读取存储器中的程序，执行下列过程：

通过收发机接收发起实体发送的对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带请求的访问令牌的权限描述信息；

根据访问令牌授权策略和所述权限描述信息，为所述发起实体生成访问令牌，所述访问令牌中至少携带授权信息，在所述访问令牌根资源下创建生成的访问令牌的访问令牌资源，所述访问令牌资源中保存有所述访问令牌；

将所述访问令牌或者所述访问令牌资源的地址信息通过收发机发送给所述发起实体。

28、一种发起实体，其特征在于，包括：处理器、收发机和存储器；所述处理器，用于读取存储器中的程序，执行下列过程：

通过收发机向授权实体发送对访问令牌根资源下的访问令牌签发资源的访问令牌资源创建请求，所述访问令牌资源创建请求中携带请求的访问令牌的权限描述信息；

通过收发机接收所述授权实体返回的访问令牌，或者接收所述授权实体在所述访问令牌根资源下创建的访问令牌资源的地址信息，所述访问令牌资源中保存有访问令牌，所述访问令牌中至少携带授权信息。

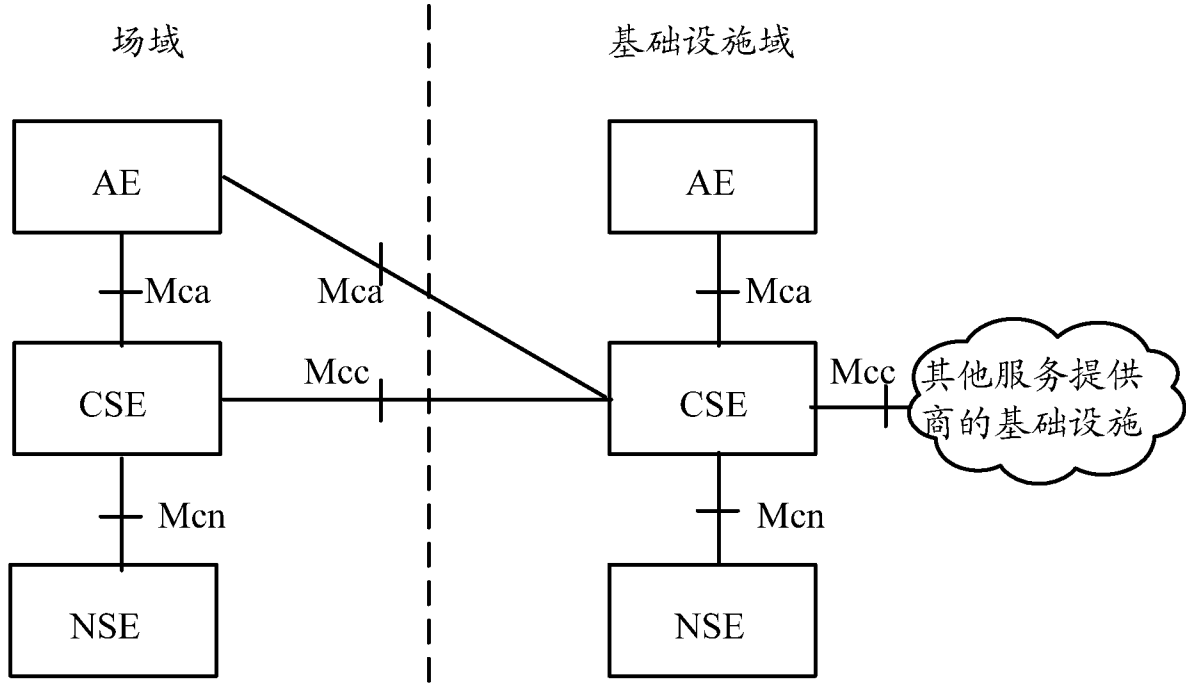


图 1

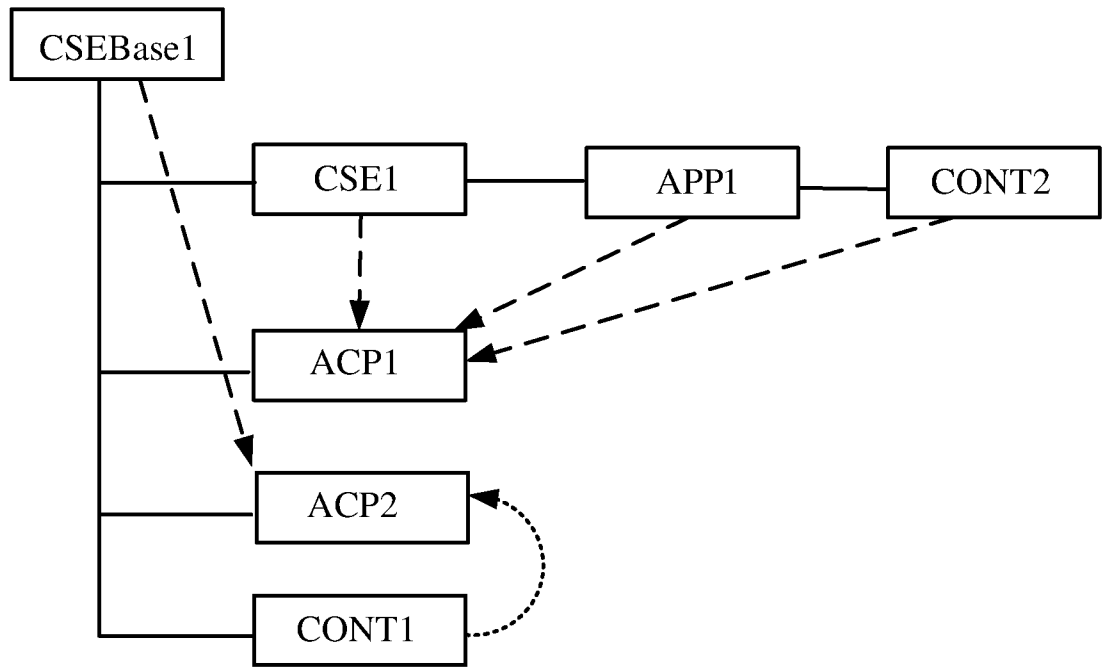


图 2

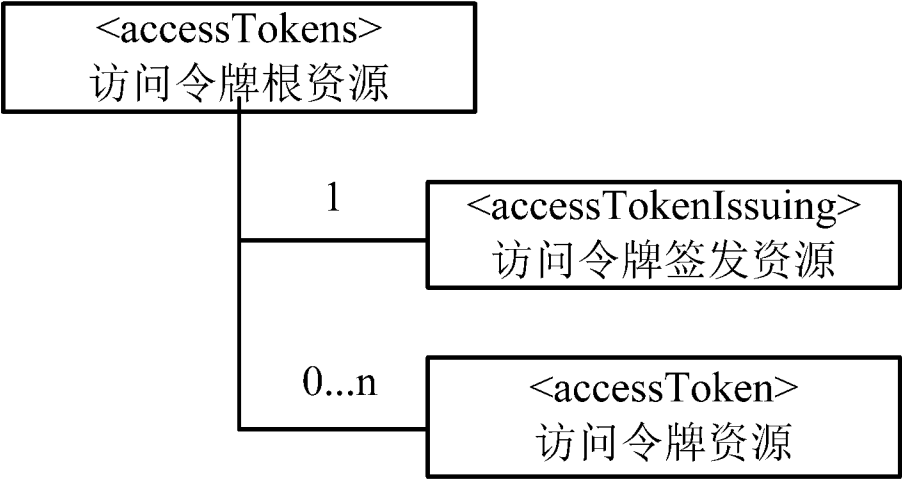


图 3

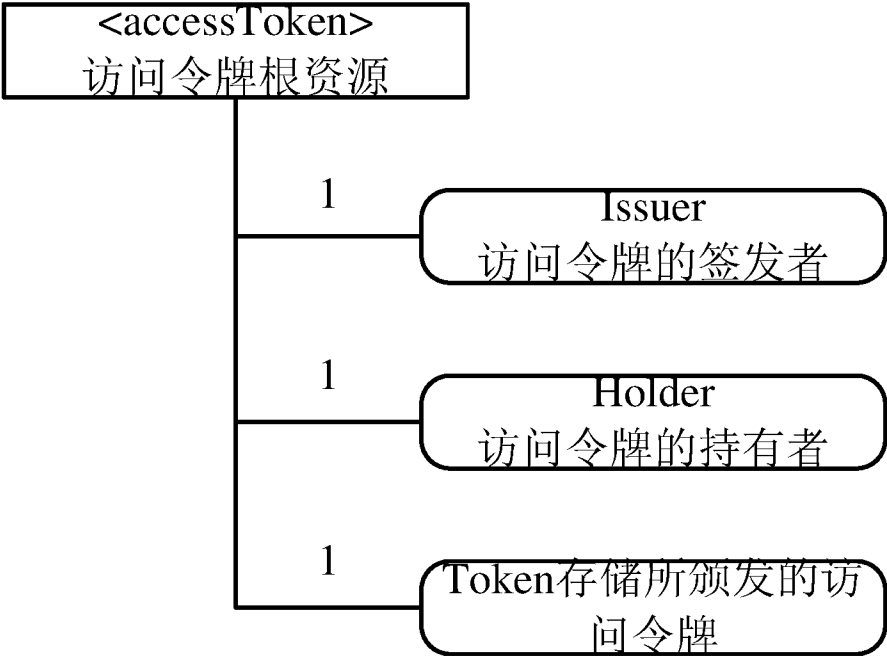


图 4

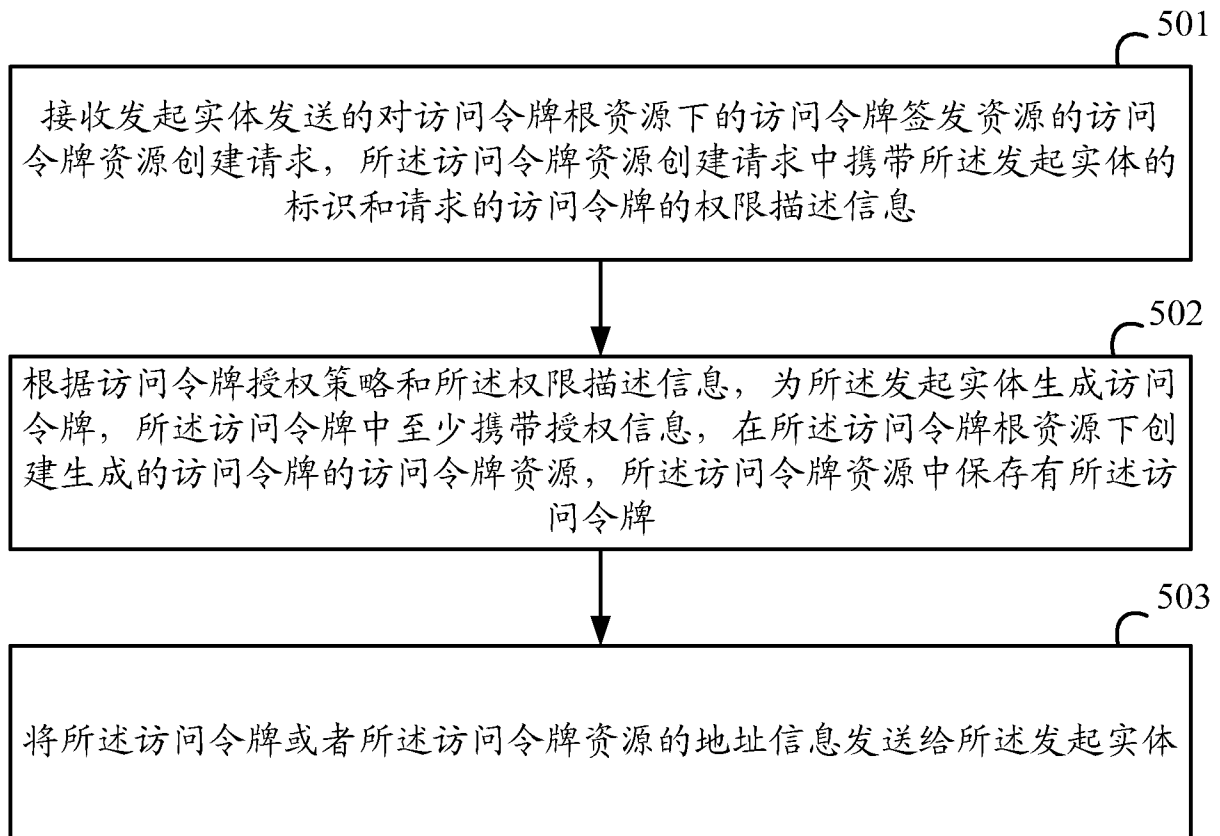


图 5

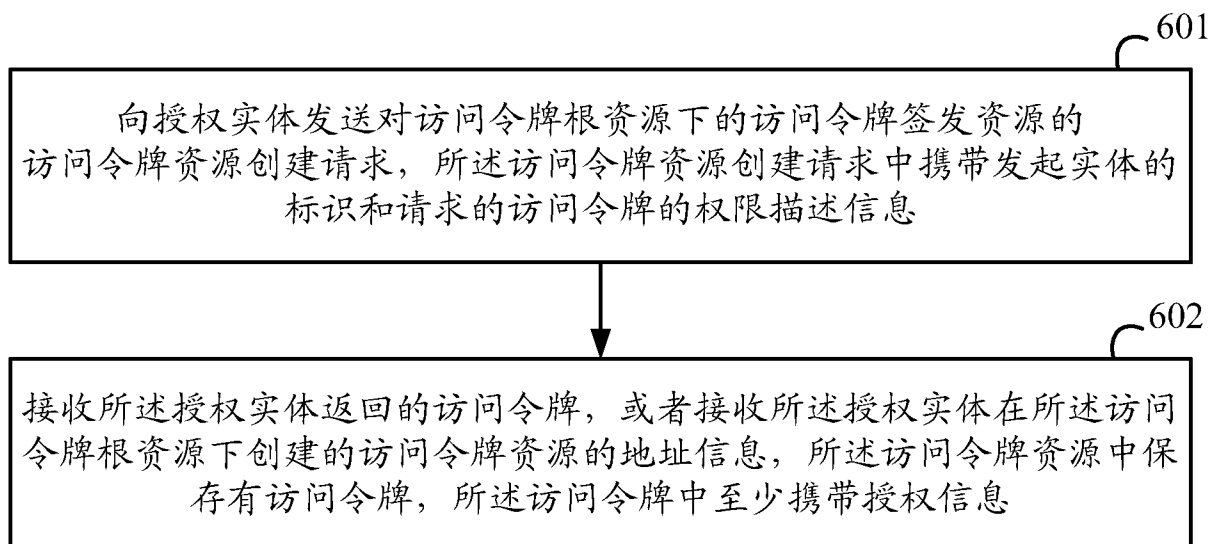


图 6

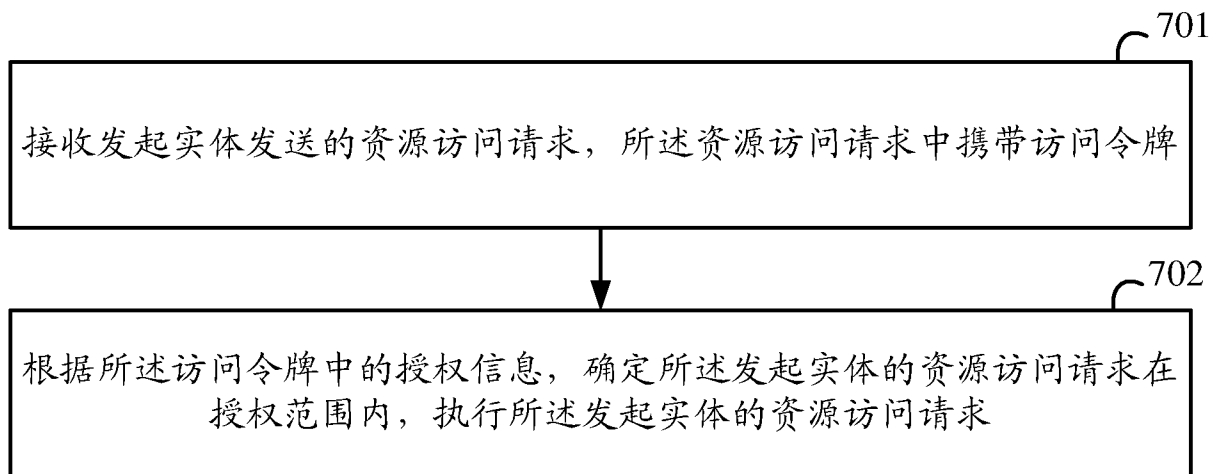


图 7

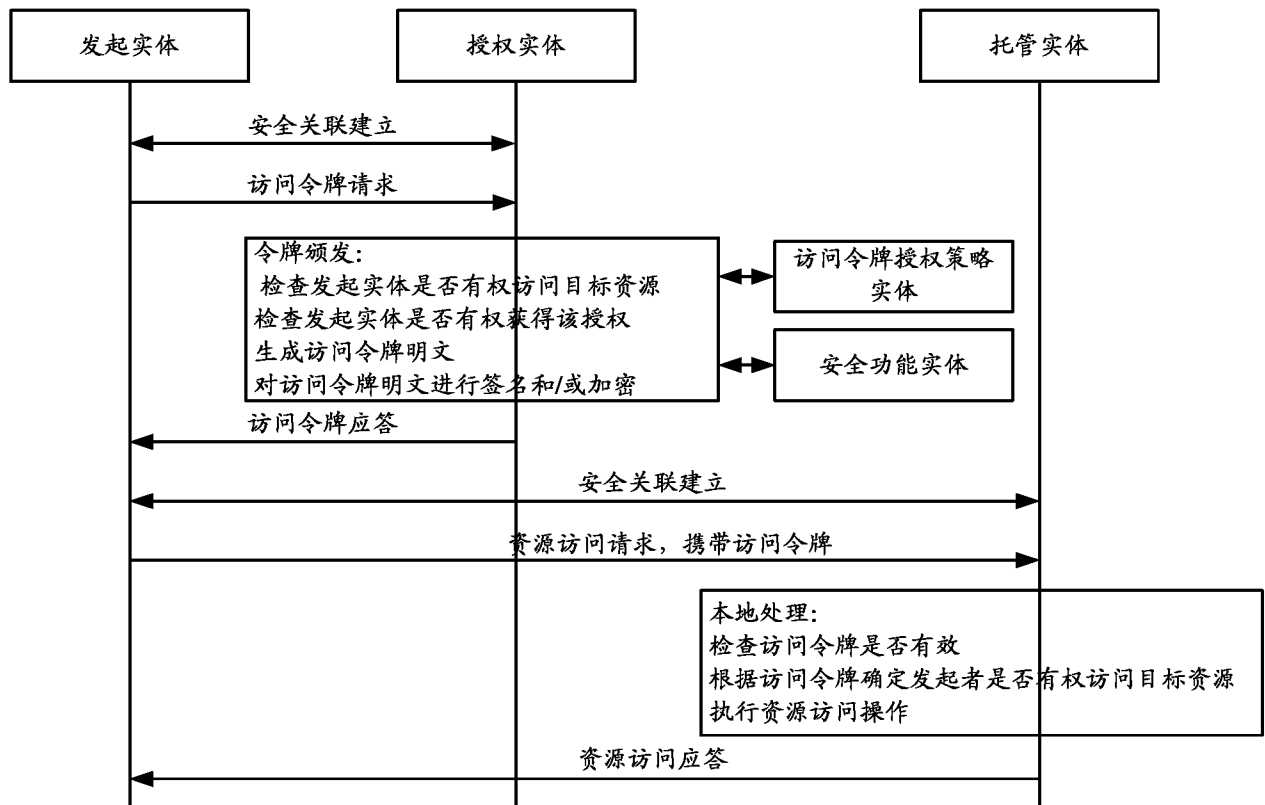


图 8

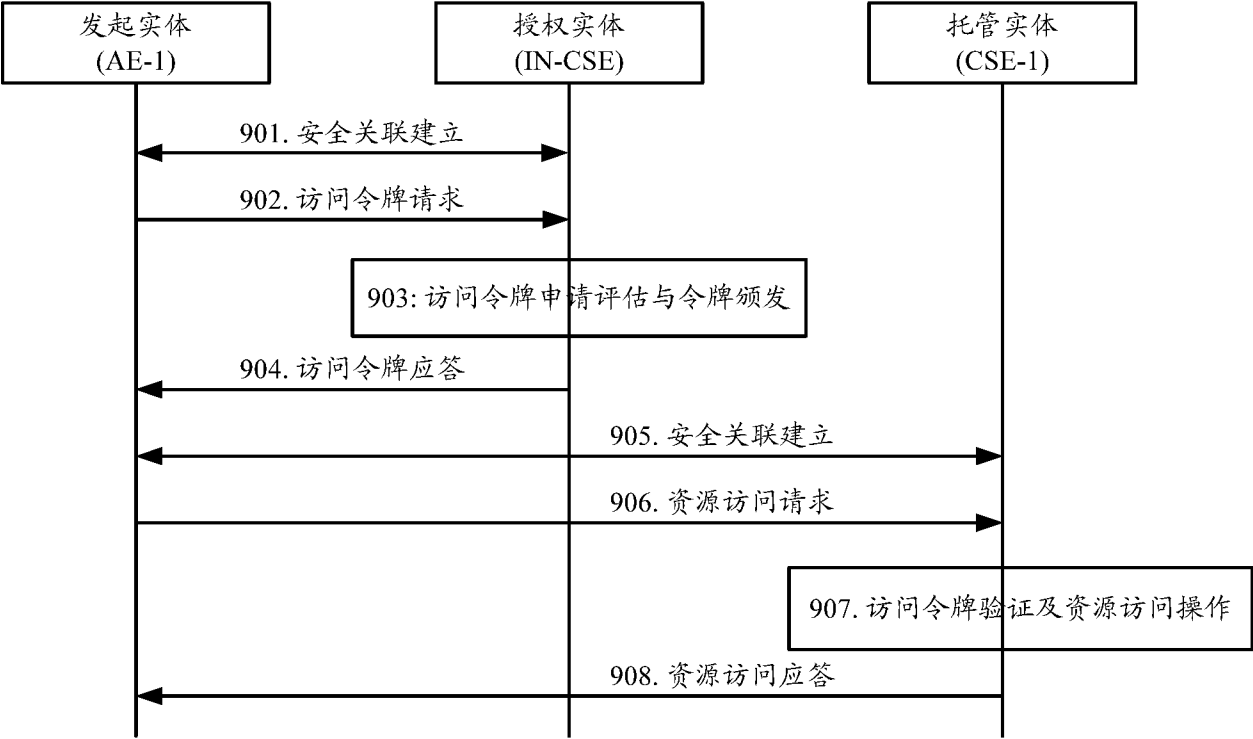


图 9

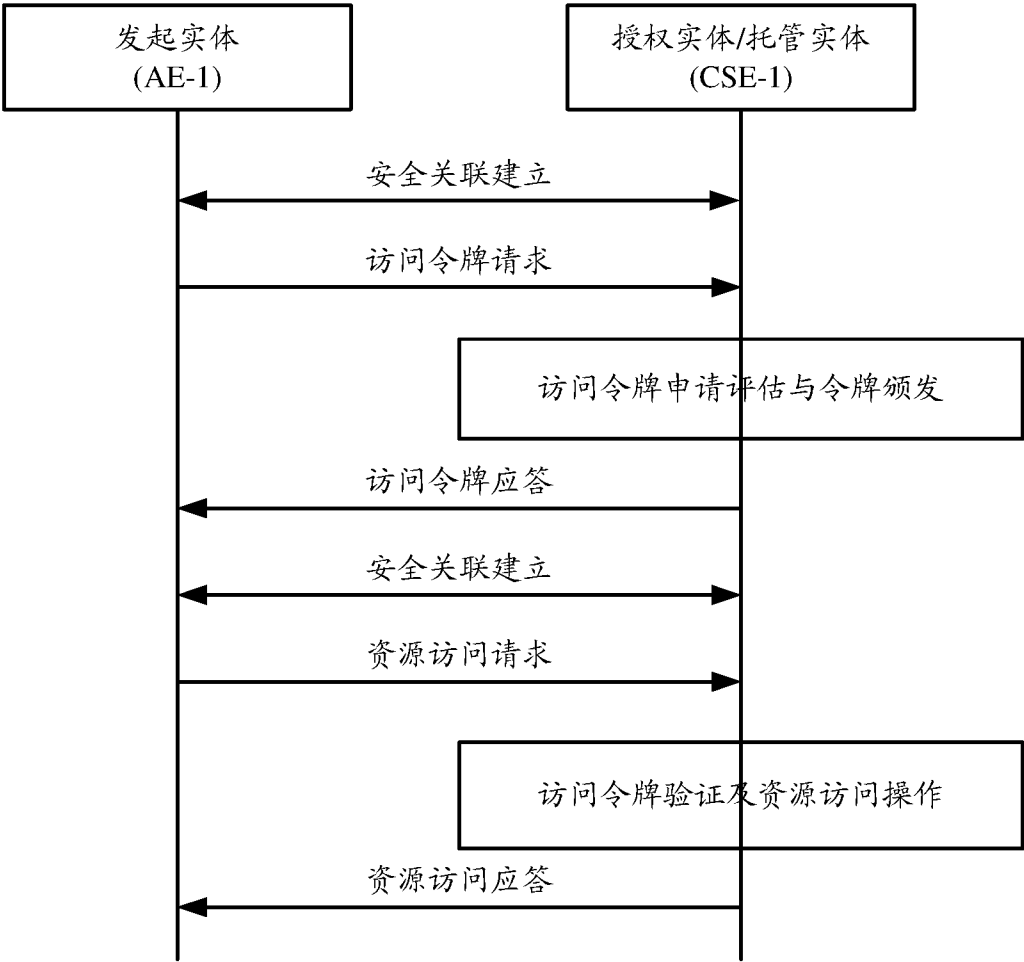


图 10

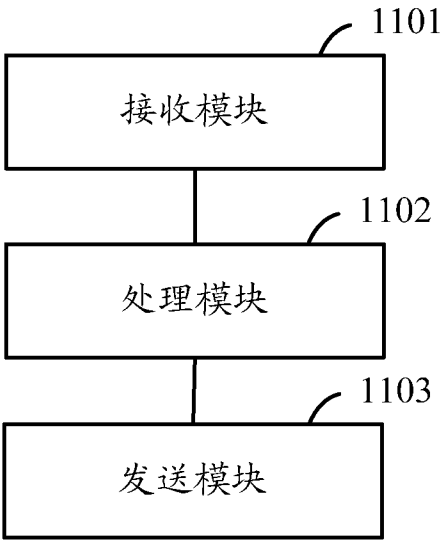


图 11

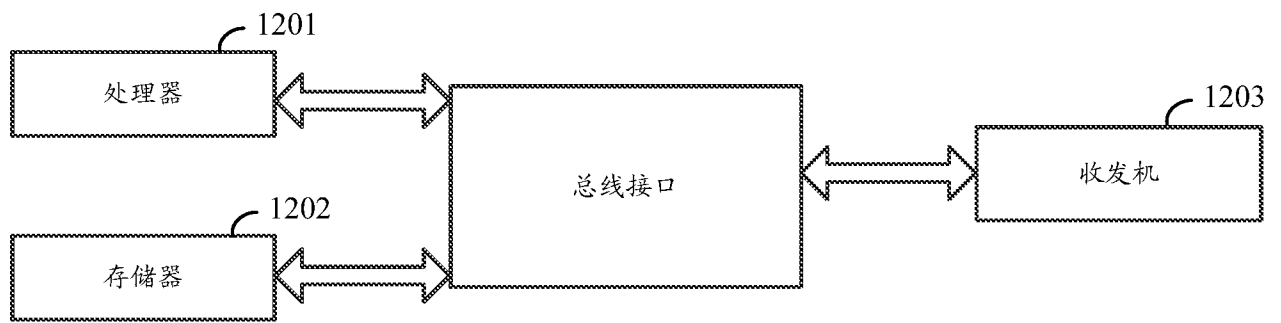


图 12

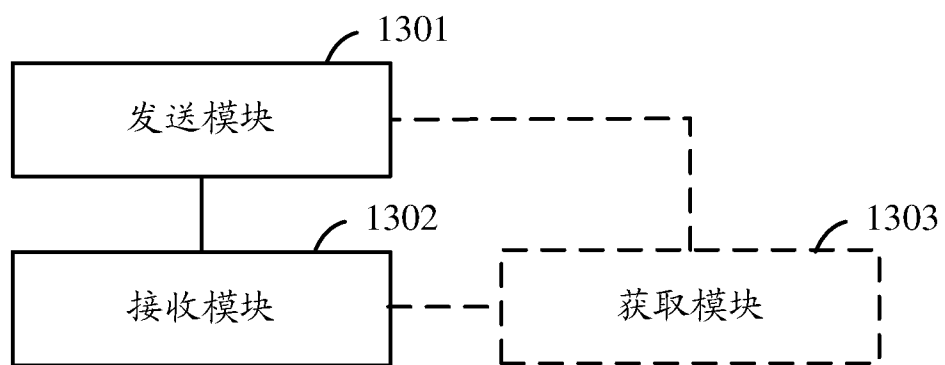


图 13



图 14

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/087973**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 28/16 (2009.01) 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)

H04W; H04L; H04Q

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, CNKI, WPI, EPODOC: machine, access, token, resource, request, authority, authorization, M2M, oneM2M

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2890073 A1 (GEMALTO SA), 01 July 2015 (01.07.2015), description, paragraphs [0015]-[0045], [0051] and [0076]-[0100]	1-28
A	CN 102546648 A (UTSTARCOM INC.), 04 July 2012 (04.07.2012), the whole document	1-28
A	CN 103188229 A (ALCATEL-LUCENT SHANGHAI BELL CO., LTD.), 03 July 2013 (03.07.2013), the whole document	1-28
A	oneM2M, "Functional Architecture, TS-001-V1.6.1", ONEM2M TECHNICAL SPECIFICATION, 30 January 2015 (30.01.2015), sections 9.4 and 9.6	1-28

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 18 August 2016 (18.08.2016)	Date of mailing of the international search report 21 September 2016 (21.09.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer FENG, Ji Telephone No.: (86-10) 62413333

International application No.
PCT/CN2016/087973

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 H04W 28/16 (2009.01) 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) H04W; H04L; H04Q 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, CNKI, WPI, EPDOC: 访问, 令牌, 资源, 请求, 权限, 授权, 机器, access, token, resource, request, authority, authorization, M2M, oneM2M																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>EP 2890073 A1 (GEMALTO SA) 2015年 7月 1日 (2015 - 07 - 01) 说明书第[0015]-[0045], [0051], [0076]-[0100]段</td> <td>1-28</td> </tr> <tr> <td>A</td> <td>CN 102546648 A (UT斯达康通讯有限公司) 2012年 7月 4日 (2012 - 07 - 04) 全文</td> <td>1-28</td> </tr> <tr> <td>A</td> <td>CN 103188229 A (上海贝尔股份有限公司) 2013年 7月 3日 (2013 - 07 - 03) 全文</td> <td>1-28</td> </tr> <tr> <td>A</td> <td>oneM2M. "Functional Architecture, TS-001-V1.6.1" oneM2M TECHNICAL SPECIFICATION, 2015年 1月 30日 (2015 - 01 - 30), 第9.4, 9.6节</td> <td>1-28</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	EP 2890073 A1 (GEMALTO SA) 2015年 7月 1日 (2015 - 07 - 01) 说明书第[0015]-[0045], [0051], [0076]-[0100]段	1-28	A	CN 102546648 A (UT斯达康通讯有限公司) 2012年 7月 4日 (2012 - 07 - 04) 全文	1-28	A	CN 103188229 A (上海贝尔股份有限公司) 2013年 7月 3日 (2013 - 07 - 03) 全文	1-28	A	oneM2M. "Functional Architecture, TS-001-V1.6.1" oneM2M TECHNICAL SPECIFICATION, 2015年 1月 30日 (2015 - 01 - 30), 第9.4, 9.6节	1-28
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
X	EP 2890073 A1 (GEMALTO SA) 2015年 7月 1日 (2015 - 07 - 01) 说明书第[0015]-[0045], [0051], [0076]-[0100]段	1-28															
A	CN 102546648 A (UT斯达康通讯有限公司) 2012年 7月 4日 (2012 - 07 - 04) 全文	1-28															
A	CN 103188229 A (上海贝尔股份有限公司) 2013年 7月 3日 (2013 - 07 - 03) 全文	1-28															
A	oneM2M. "Functional Architecture, TS-001-V1.6.1" oneM2M TECHNICAL SPECIFICATION, 2015年 1月 30日 (2015 - 01 - 30), 第9.4, 9.6节	1-28															
☐ 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 2016年 8月 18日		国际检索报告邮寄日期 2016年 9月 21日															
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (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		授权官员 冯骥 电话号码 (86-10)62413333															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/087973

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)
EP	2890073	A1	2015年 7月 1日	WO	2015101451	A1 2015年 7月 9日
CN	102546648	A	2012年 7月 4日	无		
CN	103188229	A	2013年 7月 3日	无		