(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 10 月 26 日 (26.10.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/181775 A1

(51) 国际专利分类号:
H04W 12/08 (2009.01)

(21) 国际申请号: PCT/CN2017/075429

(22) 国际申请日: 2017 年 3 月 2 日 (02.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610242998.5 2016年4月18日 (18.04.2016) 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, DJ, 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, 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, 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)。

(54) **Title:** DISTRIBUTED AUTHORIZATION MANAGEMENT METHOD AND DEVICE

(54) **发明名称**: 分布式授权管理方法及装置

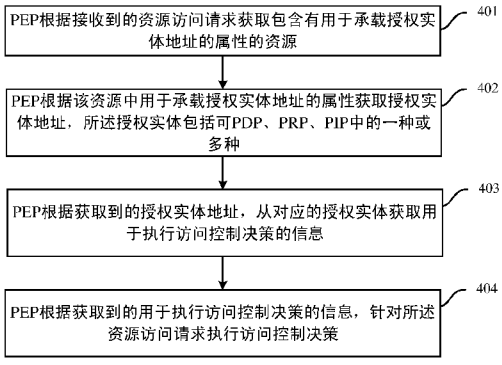

图 4

401 A PEP obtains, according to a received resource access request, a resource comprising an attribute for bearing addresses of authorized entities

402 The PEP obtains, from the resource, an address of an authorized entity according to the attribute for bearing addresses of authorized entities, the authorized entities comprising one or more of a PDP, a PRP, and a PIP

403 The PEP obtains, according to the obtained address of the authorized entity, information for executing an access control decision from the corresponding authorized entity

404 The PEP executes the access control decision with regard to the resource access request according to the obtained information for executing the access control decision

(57) Abstract: Disclosed are a distributed authorization management method and device. In the present application, an authorized entity obtains, from a resource comprising an attribute for bearing addresses of authorized entities, an address of another authorized entity according to the attribute for bearing addresses of authorized entities, thereby obtaining information from the another authorized entity on the basis of the address, and providing a distributed authorization management solution on the resource structural level.

(57) 摘要: 本申请公开了分布式授权管理方法及装置。本申请中，授权实体根据包含有用于承载授权实体地址的属性的资源中用于承载授权实体地址的属性获取其他授权实体的地址，从而基于该地址从其他授权实体获取相应信息，在资源结构层面给出了分布式授权管理方案。

WO 2017/181775 A1

[见续页]

本国际公布:

— 包括国际检索报告(条约第21条(3))。

分布式授权管理方法及装置

本申请要求在2016年4月18日提交中国专利局、申请号为201610242998.5、发明名称为“分布式授权管理方法及装置”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

本申请涉及通信技术领域，尤其涉及分布式授权管理方法及装置。

背景技术

物联网标准化组织 oneM2M 致力于开发一系列用于构造公共的 M2M（Machine-To-Machine，机器对机器通信）服务层的技术规范。oneM2M 的核心是数据共享，具体是通过 oneM2M CSE（Common Services Entity，公共服务实体）内定义的资源树上的数据项的共享实现的。

oneM2M 通过对标准化的资源树进行操作来实现服务层资源的共享和交互，oneM2M 资源树存在于 oneM2M 系统所定义的 CSE 中。根据 oneM2M 功能架构规范（oneM2M TS-0001:"Functional Architecture"）中的定义，oneM2M 资源树的形式如图 1 所示。对 oneM2M 资源可进行创建（Create)、查询（Retrieve）、修改（Update）和删除（Delete）等操作。

oneM2M 所定义的资源中与授权相关的资源是访问控制策略资源 <accessControlPolicy>，其中定义有 ACP（Access Control Policy，访问控制策略）。<accessControlPolicy>资源由资源 ID 唯一标识，其他资源通过 accessControlPolicyIDs 属性指定所适用的访问控制策略。

目前，oneM2M 系列规范中的安全规范（oneM2M TS-0003: "Security Solutions"）给出了 oneM2M 授权架构的高层描述，具体给出了授权架构的主要组成部分和基本流程，但尚未在资源结构层面给出具体的分布式授权管理方案。

发明内容

本申请实施例提供了分布式授权管理方法及装置，在资源结构层面给出了分布式授权管理方案。

本申请实施例提供的分布式授权管理方法，包括:

PEP 根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性;

所述 PEP 根据所述资源中用于承载授权实体地址的属性获取授权实体地址，所述授权实体包括 PDP、PRP、PIP 中的一种或多种;

所述 PEP 根据获取到的授权实体地址，从该授权实体地址对应的授权实体获取用于执行访问控制决策的信息;

所述 PEP 根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求执行访问控制决策。

优选地，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源;

PEP 根据所述资源中用于承载授权实体地址的属性获取 PDP 地址，包括:

若所述 PEP 未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PDP 地址。

优选地，PEP 根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性，包括:

所述 PEP 根据接收到的资源访问请求，获取所请求访问的目标资源适用的访问控制策略资源;

若所述 PEP 未从所述访问控制策略资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括: PDP 接入点属性，所述 PDP 接入点属性用于承载一个或多个 PDP 地址。

其中，若 PDP 接入点属性中承载有多个 PDP 地址，则所述 PEP 根据所述资源中用于承载授权实体地址的属性获取 PDP 地址，包括: 所述 PEP 根据所述资源中的 PDP 接入点属性获取 PDP 地址，并从获取到的 PDP 地址中选择一个 PDP 地址。

本申请另一实施例提供的分布式授权管理方法，包括:

PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性;

所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PRP 地址;

所述 PDP 根据获取到的 PRP 地址，从该 PRP 地址对应的 PRP 获取访问控制策略;

所述 PDP 根据获取到的访问控制策略进行访问控制决策。

优选地，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源;

所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PRP 地址，包括:

若所述 PDP 未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PRP 地址。

优选地，所述 PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性，包括:

所述 PDP 根据接收到的访问控制决策请求，获取所请求访问的目标资源适用的访问控制策略资源;

若所述 PEP 未从所述访问控制策略资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括: PRP 接入点属性，所述 PRP 接入点属性用于承载一个或多个 PRP 地址。

其中，若 PRP 接入点属性中承载有多个 PRP 地址，则所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PRP 地址，包括: 所述 PDP 根据所述资源中的 PRP 接入点属性获取多个 PRP 地址，并从获取到的 PRP 地址中选择一个 PRP 地址。

本申请另一实施例提供的分布式授权管理方法，包括:

PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性;

所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PIP 地址;

所述 PDP 根据获取到的 PIP 地址，从对应的 PIP 获取访问控制信息;

所述 PDP 根据获取到的访问控制信息进行访问控制决策。

优选地，所述 PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性，包括: 所述 PDP 根据接收到的访问控制决策请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括: PIP 接入点属性，所述 PIP 接入点属性用于承载一个或多个 PIP 地址。

其中，若 PIP 接入点属性中承载有多个 PIP 地址，则所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PIP 地址，包括: 所述 PDP 根据所述资源中的 PIP 接入点属性获取 PIP 地址，并从获取到的 PIP 地址中选择一个 PIP 地址。

本申请实施例提供的 PEP 设备，包括:

第一获取模块，用于根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性;

第二获取模块，用于根据所述资源中用于承载授权实体地址的属性获取授权实体地址，所述授权实体包括 PDP、PRP、PIP 中的一种或多种;

第三获取模块，用于根据获取到的授权实体地址，从该授权实体地址对应的授权实体获取用于执行访问控制决策的信息;

决策执行模块，用于根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求执行访问控制决策。

优选地，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源；所述第二获取模块具体用于：若未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PDP 地址；或者，

所述第一获取模块具体用于：根据接收到的资源访问请求，获取所请求访问的目标资源适用的访问控制策略资源，若未从该资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括：PDP 接入点属性，所述 PDP 接入点属性用于承载一个或多个 PDP 地址。

本申请实施例提供的 PDP 设备，包括：

第一获取模块，用于根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性；

第二获取模块，用于根据所述资源中用于承载授权实体地址的属性获取 PRP 地址；

第三获取模块，用于根据获取到的 PRP 地址，从该 PRP 地址对应的 PRP 获取访问控制策略；

决策模块，用于根据获取到的访问控制策略进行访问控制决策。

优选地，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源；所述第二获取模块具体用于：若未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PRP 地址；或者，

所述第一获取模块具体用于：根据接收到的访问控制决策请求，获取所请求访问的目标资源适用的访问控制策略资源，若未从该资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括：PRP 接入点属性，所述 PRP 接入点属性用于承载一个或多个 PRP 地址。

本申请另一实施例提供的 PDP 设备，包括：

第一获取模块，用于根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性；

第二获取模块，用于根据所述第一资源中用于承载授权实体地址的属性获取 PIP 地址；

所述第三获取模块，用于根据获取到的 PIP 地址，从对应的 PIP 获取访问控制信息；

决策模块，用于根据获取到的访问控制信息进行访问控制决策。

优选地，所述第一获取模块具体用于：根据接收到的访问控制决策请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括：PIP 接入点属性，所述 PIP 接入点属性用于承载一个或多个 PIP 地址。

本申请的上述实施例中，授权实体根据包含有用于承载授权实体地址的属性的资源中用于承载授权实体地址的属性获取其他授权实体的地址，从而基于该地址从其他授权实体获取相应信息，在资源结构层面给出了分布式授权管理方案。

附图说明

图 1 为现有技术中的 oneM2M 资源树示意图；

图 2 为现有技术中的 oneM2M 授权架构示意图；

图 3 为本申请实施例中定义的<accessControlPolicy>资源的结构示意图；

图 4 和图 5 分别为本申请实施例提供的基于 PDP-PoAs 属性实现的 PEP 与 PDP 之间的交互过程示意图；

图 6 和图 7 分别为本申请实施例提供的基于 PRP-PoAs 属性实现的 PDP 与 PRP 之间的交互过程示意图；

图 8 和图 9 分别为本申请实施例提供的基于 PIP-PoAs 属性实现的 PDP 与 PIP 之间的交互过程示意图；

图 10 为本申请实施例提供的具体应用场景示意图；

图 11 为本申请实施例提供的 PEP 结构示意图；

图 12 为本申请实施例提供的 PDP 结构示意图之一；

图 13 为本申请实施例提供的 PDP 结构示意图之二。

具体实施方式

为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述，显然，所描述的实施例仅仅是本申请一部份实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

oneM2M 定义了两种基本实体：应用实体（Application Entity，AE）和公共服务实体（Common Services Entity，CSE）。

AE 位于应用层，可实现一个 M2M 应用逻辑。一个应用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。应用逻辑的每个执行实例被称为一个

AE，每个 AE 由唯一的 AE-ID 所标识。

CSE 由一组 M2M 环境中的“公共服务功能（common service functions）”构成。每个 CSE 由唯一的 CSE-ID 所标识。oneM2M 资源树存在于 CSE 中。

oneM2M 定义了 3 种类型的资源:

普通资源（Normal Resource）：具有具体的资源结构及资源属性。

虚拟资源（Virtual Resource）：不具有具体的资源结构及资源属性，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属性，该资源为其他实体上普通资源某些内容的拷贝，主要目的是为资源发现提供便利。

oneM2M 安全解决方案技术规范（oneM2M TS-0003: Security Solutions）中给出的授权架构如图 2 所示，该架构中可包括如下组件:

- 策略执行点（Policy Enforcement Point，PEP）：PEP 与需要访问控制的应用系统共存，并由应用系统调用，PEP 将根据资源访问发起方的资源访问请求生成访问控制决策请求，并发送给 PDP，然后根据 PDP 返回的访问控制决策响应确定是否执行该资源访问请求。

- 策略决策点（Policy Decision Point，PDP）：PDP 负责根据访问控制策略判决是否同意对由 PEP 发送来的访问控制决策请求所请求的目标资源进行访问，并将判决结果通过访问控制决策响应返回给 PEP。

- 策略获取点（Policy Retrieval Point，PRP）：PRP 根据 PDP 提供的访问控制策略请求获取适用的访问控制策略，并将获取的访问控制策略返回给 PDP。

- 策略信息点（Policy Information Point，PIP）：PIP 根据 PDP 的访问控制信息请求获取与用户、资源或环境相关的属性，例如访问用户的 IP 地址，资源的创建者，当前的时间等，然后将获得的属性返回给 PDP。

oneM2M 的基本资源访问控制流程可包括:

资源访问发起方向 PEP 发送资源访问请求（Access Request），PEP 根据该资源访问请求向 PDP 发送访问控制决策请求（Decision Request）。

PDP 根据 PEP 发送的访问控制决策请求向 PRP 发送访问控制策略请求（Policy Request），PRP 向 PDP 返回访问控制策略响应（Policy Response），该访问控制策略响应中包含有访问控制策略。

PDP 对访问控制决策请求和访问控制策略中包含的内容进行分析、判决；在进行分析、判决时，若需要其他属性，则向 PIP 发送访问控制信息请求（Attribute Request），PIP 向 PDP 发送访问控制信息响应，该访问控制信息响应中包括根据访问控制信息请求获取到的与访问控制相关的属性。

PDP 向 PEP 发送访问控制决策响应（Decision Response），该问控制决策响应中包括访问控制决策结果。PEP 根据访问控制决策响应中的访问控制决策结果，决定是否执行资源访问发起方的资源访问请求。

为了在资源结构层面给出分布式授权管理方案，本申请实施例中对 oneM2M 中已定义的<accessControlPolicy>资源类型进行了重新定义，以便其能为分布式授权系统提供授权实体的地址信息。新定义的<accessControlPolicy>资源除能完成原有的功能外，还能在分布式授权的情况下，根据新定义的<accessControlPolicy>资源确定应该向哪个或哪些授权相关的实体发送相应的与授权相关的请求，也即向访问控制系统提供有关 PDP、PRP 或 PIP 的地址信息。

重新定义的<accessControlPolicy>资源的基本结构如图 3 所示。图 3 中用“0..n”表示属性或子资源可能的数量，n 为大于等于 1 的整数；用“L”表示属性值可以是列表（List）形式。

本申请实施例在<accessControlPolicy>资源中新增加了三个资源属性：

PDP 接入点属性：用于承载一组（即一个或多个）可实现 PDP 功能的实体的地址；该属性的属性名称可表示为可表示为 PDP-PoAs 或 pdpAddresses，属性值为；一组可实现 PDP 功能的实体的地址，比如一个 PDP 地址列表；PDP-PoAs 属性为可选属性。其中，PoA 为 Point of Access 的缩略语，意为接入点；

PRP 接入点属性：用于承载一组（即一个或多个）可实现 PRP 功能的实体的地址；该属性的属性名称可表示为 PRP-PoAs 或 prpAddresses，属性值为一组可实现 PRP 功能的实体的地址，比如一个 PRP 地址列表；PRP-PoAs 属性为可选属性；

PIP 接入点属性：用于承载一组（即一个或多个）可实现 PIP 功能的实体的地址；该属性的属性名称可表示为 PIP-PoAs 或 pipAddresses，属性值为一组可实现 PIP 功能的实体的地址，比如一个 PIP 地址列表；PIP-PoAs 属性为可选属性。

进一步地，<accessControlPolicy>资源中还可包括以下已定义的属性中的一种或多种：

privileges 属性：用于承载访问控制策略；

selfPrivileges 属性：用于承载访问控制策略。

进一步地，可将上述 privileges 属性从原来的“必选”调整为“可选”。进一步地，如果<accessControlPolicy>资源中包含 privileges 属性，则其数量可以是一个或多个。

进一步地，<accessControlPolicy>资源中还可包含子资源，表示为<subscription>。<accessControlPolicy>资源中所包含的<subscription>资源的数量可以是一个或多个。<subscription>可以是 oneM2M 已定义的子资源。

上述实施例中，通过对<accessControlPolicy>资源重新定义，用新增加的资源属性承载授权实体的地址，进而可根据<accessControlPolicy>资源实现分布式授权管理。与此类似地，

在其他一些实施例中，也可保持现有技术中已定义的<accessControlPolicy>资源不变，而将上述 3 种资源属性（如 PDP-PoAs 属性、PRP-PoAs 属性和 PIP-PoAs 属性）中的一种或多种组织在一个单独定义的新资源中，例如，该新定义的资源可命名为<authorizationEntity>。与<accessControlPolicy>资源处理方式类似，对于不能直接拥有<authorizationEntity>子资源类型的资源，可以通过公共资源属性（Common attribute）<authorizationEntityID>与某个<authorizationEntity>资源相关联。<authorizationEntity>资源中的资源属性的使用与其在<accessControlPolicy>资源类型中的方式相同。

可选地，现有技术中已定义的<accessControlPolicy>资源和本申请实施例定义的<authorizationEntity>资源使用的优先级顺序可以是：<accessControlPolicy>资源的优先级高于<authorizationEntity>资源的优先级。

下面以重新定义的<accessControlPolicy>资源为例，对本申请实施例提供的分布式授权管理流程进行说明。上述原理和处理方式同样适用于根据新定义的<authorizationEntity>资源实现分布式授权管理的过程。

参见图 4，为本申请实施例提供的基于新定义的用于承载授权实体地址的属性实现 PEP 与 PDP 之间的交互的过程，如图所示，该流程可包括如下步骤：

步骤 401：PEP 根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性（以下为描述方便将该资源称为第一资源）。

步骤 402：PEP 根据第一资源中用于承载授权实体地址的属性获取授权实体地址。所述授权实体包括可 PDP、PRP、PIP 中的一种或多种。具体地，PEP 可根据第一资源中的 PDP-PoAs 属性获取 PDP 地址，根据第一资源中的 PRP-PoAs 属性获取 PRP 地址，根据第一资源中的 PIP-PoAs 属性获取 PIP 地址。

步骤 403：PEP 根据获取到的授权实体地址，从该授权实体地址对应的授权实体获取用于执行访问控制决策的信息。

该步骤中，PEP 根据获取到的 PDP 地址，向对应的 PDP 发送访问控制决策请求；PDP 接收到该访问控制决策请求后，根据目标资源采用相应的访问控制策略进行访问控制决策，并将访问控制决策信息（即决策结果）携带于访问控制决策响应中发送给该 PEP。

PEP 可根据获取到的 PRP 地址，向对应的 PRP 发送访问控制策略请求；PRP 接收到该访问控制策略请求后，获取访问控制策略，并将访问控制策略携带于访问控制策略响应中发送给该 PEP。

PEP 可根据获取到的 PIP 地址，向对应的 PIP 发送访问控制信息请求；PIP 接收到该访问控制信息请求后，获取访问控制信息，并将访问控制信息携带于访问控制信息响应中发送给该 PEP。

步骤 404：PEP 根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求

执行访问控制决策。

作为一个例子，上述流程中的第一资源为上述重新定义的<accessControlPolicy>资源。步骤 401 中，PEP 根据接收到的资源访问请求，获取所请求访问的目标资源适用的<accessControlPolicy>资源；步骤 402 中，PEP 获取<accessControlPolicy>资源的 privileges 属性值，该属性值即为访问控制策略，若 PEP 未从<accessControlPolicy>资源中获取到访问控制策略（比如在<accessControlPolicy>资源中未包含 privileges 属性的情况下，或者在<accessControlPolicy>资源中包含 privileges 属性但该属性的值为空的情况下，PEP 无法从<accessControlPolicy>资源中获取到访问控制策略），则根据<accessControlPolicy>资源中的 PDP-PoAs 属性获取 PDP 地址。

作为另一个例子，上述流程中的第一资源为上述重新定义的<authorizationEntity>资源，第二资源为现有技术中的<accessControlPolicy>资源。步骤 401 中，PEP 根据接收到的资源访问请求，获取所请求访问的目标资源适用的<accessControlPolicy>资源，PEP 获取<accessControlPolicy>资源的 privileges 属性值，该属性值即为访问控制策略，若 PEP 未从<accessControlPolicy>资源中获取到访问控制策略（比如在<accessControlPolicy>资源中未包含 privileges 属性的情况下，或者在<accessControlPolicy>资源中包含 privileges 属性但该属性的值为空的情况下，PEP 无法从<accessControlPolicy>资源中获取到访问控制策略），则获取<authorizationEntity>资源。如上所述，<authorizationEntity>资源中可包含上述的 PDP-PoAs 属性、PRP-PoAs 属性和 PIP-PoAs 属性，这三种属性均为可选属性。

下面以基于新定义的<accessControlPolicy>资源为例，结合图 5 描述图 4 的一种具体实现过程。如图 5 所述，该流程可包括如下步骤：

步骤 501：位于宿主 CSE（Hosting CSE）中的 PEP 截取到来自于资源访问发起方（Originator）的资源访问请求后，按 oneM2M 系统的规定检索到目标资源适用的<accessControlPolicy>资源。

步骤 502: PEP 检查<accessControlPolicy>资源中是否包含有 privileges 属性且属性值不为空。若不包含有 privileges 属性或属性值为空，则转入步骤 503；若包含有 privileges 属性且属性值不为空，则转入步骤 506;

步骤 503：PEP 检查<accessControlPolicy>资源中是否包含有 PDP-PoAs 属性且属性值不为空。若包含有 PDP-PoAs 属性且属性值不为空，则转入步骤 504; 若不包含有 PDP-PoAs 属性或属性值为空，则转入步骤 507;

步骤 504：PEP 读取 PDP-PoAs 属性中的 PDP 地址列表，并获得一个 PDP 地址（即 PoA），然后转入步骤 505;

步骤 505：PEP 生成访问控制决策请求（Access Control Decision Request），并将其发送给该 PDP 地址对应的 PDP，从该 PDP 接收返回的访问控制决策响应（Access Control

Decision Response），该访问控制决策响应中包含访问控制决策信息，然后转入步骤 508;

步骤 506: PEP 读取 privileges 属性中的访问控制策略，并利用其评估发起方的资源访问请求，进而获得访问控制决策，然后转入步骤 508;

步骤 507: PEP 进行出错处理，然后转入步骤 508;

步骤 508: PEP 执行访问控制决策，并结束本次访问控制过程。其中，如果是从步骤 507 转入到步骤 508 的，则由于步骤 507 中进行了出错处理，则在步骤 508 中，PEP 可拒绝资源访问发起方（Originator）的资源访问请求，或者按照预先约定进行处理。

参见图 6，为本申请实施例提供的基于新定义的 PRP 接入点属性（以下称为 PRP-PoAs 属性）实现 PDP 与 PRP 之间的交互的过程，如图所示，该流程可包括如下步骤:

步骤 601: PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性（以下为描述方便将该资源称为第一资源）;

步骤 602: PDP 根据第一资源中用于承载授权实体地址的属性获取 PRP 地址。具体地，PEP 根据第一资源中的 PRP-PoAs 属性获取 PRP 地址。

步骤 603: PDP 根据获取到的 PRP 地址，从该 PRP 地址对应的 PRP 获取访问控制策略。

该步骤中，PDP 根据获取到的 PRP 地址，向对应的 PRP 发送访问控制策略请求；PRP 接收到该访问控制策略请求后，获取访问控制策略，并将访问控制策略携带于访问控制策略响应中发送给该 PDP。

步骤 604: PDP 根据获取到的访问控制策略进行访问控制决策。

作为一个例子，上述流程中的第一资源为上述重新定义的<accessControlPolicy>资源。步骤 601 中，PDP 根据接收到的访问控制策略请求，获取所请求访问的目标资源适用的<accessControlPolicy>资源；步骤 602 中，PDP 获取<accessControlPolicy>资源的 privileges 属性值，该属性值即为访问控制策略，若 PDP 未从<accessControlPolicy>资源中获取到访问控制策略（比如在<accessControlPolicy>资源中未包含 privileges 属性的情况下，或者在<accessControlPolicy>资源中包含 privileges 属性但该属性的值为空的情况下，PDP 无法从<accessControlPolicy>资源中获取到访问控制策略），则根据<accessControlPolicy>资源中的 PRP-PoAs 属性获取 PRP 地址。

作为另一个例子，上述流程中的第一资源为上述重新定义的<authorizationEntity>资源，第二资源为现有技术中的<accessControlPolicy>资源。步骤 601 中，PDP 根据接收到的访问控制策略请求，获取所请求访问的目标资源适用的<accessControlPolicy>资源，PDP 获取<accessControlPolicy>资源的 privileges 属性值，该属性值即为访问控制策略，若 PDP 未从<accessControlPolicy>资源中获取到访问控制策略（比如在<accessControlPolicy>资源中未包含 privileges 属性的情况下，或者在<accessControlPolicy>资源中包含 privileges 属性但该

属性的值为空的情况下，PDP 无法从<accessControlPolicy>资源中获取到访问控制策略），则获取<authorizationEntity>资源。如上所述，<authorizationEntity>资源中可包含上述的 PDP-PoAs 属性、PRP-PoAs 属性和 PIP-PoAs 属性，这三种属性均为可选属性。

下面以基于新定义的<accessControlPolicy>资源为例，结合图 7 描述图 6 的一种具体实现过程。如图 7 所述，该流程可包括如下步骤：

步骤 701：PDP 收到来自于 PEP 的访问控制决策请求后，利用访问控制决策请求中的目标资源地址检索适用的<accessControlPolicy>资源。

步骤 702：PDP 检查<accessControlPolicy>资源中是否包含有 privileges 属性且属性值不为空。若不包含有 privileges 属性或属性值为空，则转入步骤 703；若包含有 privileges 属性且属性值不为空，则转入步骤 706；

步骤 703：PDP 检查<accessControlPolicy>资源中是否包含有 PRP-PoAs 属性且属性值不为空。若包含 PRP-PoAs 属性且属性值不为空，则转入步骤 704；若不包含有 PRP-PoAs 属性或属性值为空，则转入步骤 707；

步骤 704：PDP 读取 PRP-PoAs 属性中的 PRP 地址列表，并获得一个 PRP 地址，然后转入步骤 705；

步骤 705：PDP 生成访问控制策略请求（Access Control Policy Request），并将其发送给该 PRP 地址对应的 PRP，从该 PRP 接收返回的访问控制策略响应（Access Control Policy Response），获取响应中的访问控制策略，然后转入步骤 708；

步骤 706：PDP 读取 privileges 属性中的访问控制策略，然后转入步骤 708；

步骤 707：PDP 进行出错处理，然后转入步骤 708；

步骤 708：PDP 结束本次获取访问控制策略的过程。进一步地，PDP 可根据获取到的访问控制策略进行访问控制决策。

参见图 8，为本申请实施例提供的基于新定义的 PIP 接入点属性（以下称为 PIP-PoAs 属性）实现 PDP 与 PIP 之间的交互的过程，如图所示，该流程可包括如下步骤：

步骤 801：PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性（以下为描述方便将该资源称为第一资源）；

步骤 802：PDP 根据第一资源中用于承载授权实体地址的属性获取 PIP 地址。具体地，PEP 根据第一资源中的 PIP-PoAs 属性获取 PIP 地址。

步骤 803：PDP 根据获取到的 PIP 地址，从对应的 PIP 获取访问控制信息。

该步骤中，PDP 根据获取到的 PIP 地址，向对应的 PIP 发送访问控制信息请求；PIP 接收到该访问控制信息请求后，获取访问控制信息，并将访问控制信息携带于访问控制信息响应中发送给该 PDP。

步骤 804：PDP 根据获取到的访问控制信息进行访问控制决策。

作为一个例子，上述流程中的第一资源为上述重新定义的<accessControlPolicy>资源。步骤 801 中，PDP 根据接收到的访问控制策略请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的<accessControlPolicy>资源。

作为另一个例子，上述流程中的第一资源为上述重新定义的<authorizationEntity>资源，第二资源为现有技术中的<accessControlPolicy>资源。步骤 801 中，PDP 根据接收到的访问控制策略请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的<authorizationEntity>资源。如上所述，<authorizationEntity>资源中可包含上述的 PDP-PoAs 属性、PRP-PoAs 属性和 PIP-PoAs 属性，这三种属性均为可选属性。

下面以基于新定义的<accessControlPolicy>资源为例，结合图 9 描述图 8 的一种具体实现过程。如图 9 所述，该流程可包括如下步骤：

步骤 901：PDP 收到来自于 PEP 的访问控制决策请求后，检查访问控制决策请求中的参数，确定是否有本地不能提供的访问控制信息，例如角色标识或令牌标识等。若有，则转入步骤 902；否则转入步骤 907；

步骤 902：PDP 利用访问控制决策请求中的目标资源地址检索适用的<accessControlPolicy>资源。

步骤 903：PDP 检查<accessControlPolicy>资源中是否包含有 PIP-PoAs 属性且属性值不为空。若包含有 PIP-PoAs 属性且属性值不为空，则转入步骤 904；若不包含有 PIP-PoAs 属性或属性值为空，则转入步骤 906；

步骤 904：PDP 读取有 PIP-PoAs 属性中的 PIP 地址列表，并获得一个 PIP 地址，然后转入步骤 905；

步骤 905：PDP 生成访问控制信息请求（Access Control Information Request），并将其发送给该 PIP，并从该 PIP 接收返回的访问控制信息响应（Access Control Information Response），获取该响应中的访问控制信息，然后转入步骤 907；

步骤 906：PDP 进行出错处理，然后执行步骤 907；

步骤 907：PDP 结束本次获取访问控制信息过程。进一步地，PDP 可根据获取到的访问控制信息进行访问控制决策。

为了更清楚地理解本申请实施例，下面以一个具体应用场景为例对本申请实施例提供的分布式授权管理方案进行说明。

该场景中，oneM2M 应用服务提供商（oneM2M Application Service Provider）通过 oneM2M 服务商（oneM2M Service Provider）提供的 oneM2M 平台读取安装在用户家中的物联网设备。具体场景如图 10 所示。其中，CSE0 为 oneM2M 服务商的基础设施节点；CSE1 为用户的家庭网关；CSE2、CSE3 和 CSE4 为用户家中的物联网设备；AE1 为 oneM2M 应用服务提供商注册至 CSE0 的应用服务实体；其中，CSE2、CSE3 和 CSE4 的访问控制策

略和访问控制决策点均设置在 CSE1 中；AE1 通过角色访问 CSE2、CSE3 和 CSE4 中的资源。

系统资源及参数配置如下：

CSE2、CSE3 和 CSE4 中的访问控制策略资源（<accessControlPolicy>资源）中的 privileges 属性均为空，但 PDP-PoAs 属性设置为指向 CSE1（即 PDP-PoAs 属性的属性值中包含 CSE1 的地址）；

CSE1 中的访问控制策略资源（<accessControlPolicy>资源）中的 PIP-PoAs 属性设置为指向 CSE0（即 PDP-PoAs 属性的属性值中包含 CSE0 的地址）；

CSE0 中存储有 AE1 的角色信息。

基于上述架构以及系统配置，分布式授权访问控制的过程可包括：

AE1 向 CSE2 资源树发送数据读取指令，其中包含有角色标识；

CSE2 检查本地的访问控制策略，发现与该资源相关联的访问控制资源的 privileges 属性为空，但 PDP-PoAs 不为空，且指向 CSE1，于是生成一个访问控制决策请求，并发送给 CSE1；

CSE1 检查存储在本地的针对目标资源的访问控制策略资源，并获得访问控制策略；

CSE1 检查 CSE2 发送来的访问控制决策请求，发现其中包含有角色标识；其检查存储在本地的针对目标资源的访问控制策略资源，发现 PIP-PoAs 不为空且指向 CSE0，于是生成一个访问控制信息请求，并发送给 CSE0；

CSE0 根据 CSE1 的访问控制信息请求检索到相关的角色信息，并将其通过访问控制信息响应返回给 CSE1；

CSE1 根据访问控制策略和 AE1 的角色信息评估 AE1 的资源访问请求，并将访问控制决策通过访问控制决策响应返回给 CSE2；

CSE2 根据访问控制决策决定是否执行 AE1 的资源访问请求。

通过以上描述可以看出，授权实体根据本申请实施例定义的资源（该资源中包含用于承载授权实体地址的资源属性）中用于承载授权实体地址的属性获取其他授权实体的地址，从而基于该地址从其他授权实体获取相应信息，在资源结构层面给出了分布式授权管理方案。

基于相同的技术构思，本申请实施例还提供了一种 PEP。

参见图 11，为本申请实施例提供的 PEP 的结构示意图，该 PEP 可实现本申请上述实施例提供的相关流程。如图所示，该 PEP 可包括：第一获取模块 1101、第二获取模块 1102、第三获取模块 1103、决策执行模块 1104，其中：

第一获取模块 1101，用于根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性；

第二获取模块 1102，用于根据所述资源中用于承载授权实体地址的属性获取授权实体地址，所述授权实体包括 PDP、PRP、PIP 中的一种或多种；

第三获取模块 1103，用于根据获取到的授权实体地址，从该授权实体地址对应的授权实体获取用于执行访问控制决策的信息；

决策执行模块 1104，用于根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求执行访问控制决策。

优选地，在一些实施例中，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源；；第二获取模块 1102 可具体用于：若未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PDP 地址。

优选地，在另一些实施例中，第一获取模块 1101 可具体用于：根据接收到的资源访问请求，获取所请求访问的目标资源适用的访问控制策略资源；若未从该资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括：PDP 接入点属性，所述 PDP 接入点属性用于承载一个或多个 PDP 地址。

基于相同的技术构思，本申请实施例还提供了一种 PDP。

参见图 12，为本申请实施例提供的 PDP 的结构示意图，该 PDP 可实现本申请上述实施例提供的相关流程。如图所示，该 PDP 可包括：第一获取模块 1201、第二获取模块 1202、第三获取模块 1203、决策模块 1204，其中：

第一获取模块 1201，用于根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性；

第二获取模块 1202，用于根据所述资源中用于承载授权实体地址的属性获取 PRP 地址；

第三获取模块 1203，用于根据获取到的 PRP 地址，从该 PRP 地址对应的 PRP 获取访问控制策略；

决策模块 1204，用于根据获取到的访问控制策略进行访问控制决策。

优选地，在一些实施例中，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源；第二获取模块 1202 具体用于：若未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PRP 地址.

优选地，在另一些实施例中，第一获取模块 1201 具体用于：根据接收到的访问控制决策请求，获取所请求访问的目标资源适用的访问控制策略资源；若所述 PEP 未从该资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括：PRP 接入点属性，所述 PRP 接入点属性用于承载一个或多个 PRP 地址。

基于相同的技术构思，本申请实施例还提供了一种 PDP。

参见图 13，为本申请实施例提供的 PDP 的结构示意图，该 PDP 可实现本申请上述实施例提供的相关流程。如图所示，该 PDP 可包括：第一获取模块 1301、第二获取模块 1302、第三获取模块 1303、决策模块 1304，其中：

第一获取模块 1301，用于根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性；

第二获取模块 1302，用于根据所述资源中用于承载授权实体地址的属性获取策略信息点 PIP 地址；

所述第三获取模块 1303，用于根据获取到的 PIP 地址，从对应的 PIP 获取访问控制信息；

决策模块 1304，用于根据获取到的访问控制信息进行访问控制决策。

优选地，第一获取模块 1301 具体用于：根据接收到的访问控制决策请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的包含有用于承载授权实体地址的属性的资源。

优选地，所述用于承载授权实体地址的属性包括：PIP 接入点属性，所述 PIP 接入点属性用于承载一个或多个 PIP 地址。

本申请实施例中上述任一模块，均可以由处理器或具有收发功能的处理器等实体模块实现。

综上所述，目前 oneM2M 只定义了授权系统的高层架构，并未提供具体的解决方案。本申请实施例提供了一种在 oneM2M 系统中实现分布式授权系统管理的方案。本申请实施例通过重新定义 oneM2M <accessControlPolicy>资源类型，将所需的功能加入其中，避免新建资源类型以及对 TS 的大量修改。

本申请是参照根据本申请实施例的方法、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。

尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

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

权 利 要 求

1、一种分布式授权管理方法，其特征在于，包括:

策略执行点 PEP 根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性;

所述 PEP 根据所述资源中用于承载授权实体地址的属性获取授权实体地址;

所述 PEP 根据获取到的授权实体地址，从该授权实体地址对应的授权实体获取用于执行访问控制决策的信息;

所述 PEP 根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求执行访问控制决策。

2、如权利要求 1 所述的方法，其特征在于，所述授权实体包括策略决策点 PDP、策略获取点 PRP、策略信息点 PIP 中的一种或多种。

3、如权利要求 2 所述的方法，其特征在于，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源;

若所述授权实体包括 PDP，则所述 PEP 根据所述资源中用于承载授权实体地址的属性获取 PDP 地址，是在所述 PEP 未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略的情况下执行的。

4、如权利要求 1 所述的方法，其特征在于，所述 PEP 根据接收到的资源访问请求获取资源，包括:

所述 PEP 根据接收到的资源访问请求，获取所请求访问的目标资源适用的访问控制策略资源;

若所述 PEP 未从所述访问控制策略资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

5、如权利要求 2 至 4 中任一项所述的方法，其特征在于，若所述授权实体包括 PDP，则所述用于承载授权实体地址的属性包括: PDP 接入点属性，所述 PDP 接入点属性用于承载一个或多个 PDP 地址。

6、如权利要求 5 所述的方法，其特征在于，若所述 PDP 接入点属性中承载有多个 PDP 地址，则所述 PEP 根据所述资源中用于承载授权实体地址的属性获取 PDP 地址，包括:

所述 PEP 根据所述资源中的 PDP 接入点属性获取多个 PDP 地址，并从获取到的多个 PDP 地址中选择一个 PDP 地址。

7、一种分布式授权管理方法，其特征在于，包括:

策略决策点 PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性;

所述 PDP 根据所述资源中用于承载授权实体地址的属性获取策略获取点 PRP 地址;

所述 PDP 根据获取到的 PRP 地址，从该 PRP 地址对应的 PRP 获取访问控制策略;

所述 PDP 根据获取到的访问控制策略进行访问控制决策。

8、如权利要求 7 所述的方法，其特征在于，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源;

所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PRP 地址是在所述 PDP 未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略的情况下执行的。

9、如权利要求 7 所述的方法，其特征在于，所述 PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性，包括:

所述 PDP 根据接收到的访问控制决策请求，获取所请求访问的目标资源适用的访问控制策略资源;

若所述 PEP 未从所述访问控制策略资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

10、如权利要求 7 至 9 中任一项所述的方法，其特征在于，所述用于承载授权实体地址的属性包括: PRP 接入点属性，所述 PRP 接入点属性用于承载一个或多个 PRP 地址。

11、如权利要求 10 所述的方法，其特征在于，若 PRP 接入点属性中承载有多个 PRP 地址，则所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PRP 地址，包括:

所述 PDP 根据所述资源中的 PRP 接入点属性获取多个 PRP 地址，并从获取到的多个 PRP 地址中选择一个 PRP 地址。

12、一种分布式授权管理方法，其特征在于，包括:

策略决策点 PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性;

所述 PDP 根据所述资源中用于承载授权实体地址的属性获取策略信息点 PIP 地址;

所述 PDP 根据获取到的 PIP 地址，从对应的 PIP 获取访问控制信息;

所述 PDP 根据获取到的访问控制信息进行访问控制决策。

13、如权利要求 12 所述的方法，其特征在于，所述 PDP 根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性，包括:

所述 PDP 根据接收到的访问控制决策请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的包含有用于承载授权实体地址的属性的资源。

14、如权利要求 12 或 13 所述的方法，其特征在于，所述用于承载授权实体地址的属性包括: PIP 接入点属性，所述 PIP 接入点属性用于承载一个或多个 PIP 地址。

15、如权利要求 14 所述的方法，其特征在于，若 PIP 接入点属性中承载有多个 PIP 地址，则所述 PDP 根据所述资源中用于承载授权实体地址的属性获取 PIP 地址，包括:

所述 PDP 根据所述资源中的 PIP 接入点属性获取多个 PIP 地址，并从获取到的多个 PIP 地址中选择一个 PIP 地址。

16、一种策略执行点 PEP 设备，其特征在于，包括:

第一获取模块，用于根据接收到的资源访问请求获取资源，该资源中包含用于承载授权实体地址的属性;

第二获取模块，用于根据所述资源中用于承载授权实体地址的属性获取授权实体地址;

第三获取模块，用于根据获取到的授权实体地址，从该授权实体地址对应的授权实体获取用于执行访问控制决策的信息;

决策执行模块，用于根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求执行访问控制决策。

17、如权利要求 16 所述的设备，其特征在于，所述授权实体包括策略决策点 PDP、策略获取点 PRP、策略信息点 PIP 中的一种或多种。

18、如权利要求 16 所述的设备，其特征在于，所述包含有用于承载授权实体地址的属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源；所述第二获取模块具体用于：若未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PDP 地址；或者，

所述第一获取模块具体用于：根据接收到的资源访问请求，获取所请求访问的目标资源适用的访问控制策略资源，若未从该资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

19、如权利要求 16 或 17 或 18 所述的设备，其特征在于，所述用于承载授权实体地址的属性包括：PDP 接入点属性，所述 PDP 接入点属性用于承载一个或多个 PDP 地址。

20、一种策略决策点 PDP 设备，其特征在于，包括:

第一获取模块，用于根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性;

第二获取模块，用于根据所述资源中用于承载授权实体地址的属性获取策略获取点 PRP 地址;

第三获取模块，用于根据获取到的 PRP 地址，从该 PRP 地址对应的 PRP 获取访问控制策略;

决策模块，用于根据获取到的访问控制策略进行访问控制决策。

21、如权利要求 20 所述的设备，其特征在于，所述包含有用于承载授权实体地址的

属性的资源，为包含有用于承载授权实体地址的属性的访问控制策略资源；所述第二获取模块具体用于：若未从所述包含有用于承载授权实体地址的属性的访问控制策略资源中获取到访问控制策略，则根据该资源中用于承载授权实体地址的属性获取 PRP 地址；或者，

所述第一获取模块具体用于：根据接收到的访问控制决策请求，获取所请求访问的目标资源适用的访问控制策略资源，若未从该资源中获取到访问控制策略，则获取所述包含有用于承载授权实体地址的属性的资源。

22、如权利要求 20 或 21 所述的设备，其特征在于，所述用于承载授权实体地址的属性包括：PRP 接入点属性，所述 PRP 接入点属性用于承载一个或多个 PRP 地址。

23、一种策略决策点 PDP 设备，其特征在于，包括：

第一获取模块，用于根据接收到的访问控制决策请求获取资源，该资源中包含用于承载授权实体地址的属性；

第二获取模块，用于根据所述第一资源中用于承载授权实体地址的属性获取策略信息点 PIP 地址；

所述第三获取模块，用于根据获取到的 PIP 地址，从对应的 PIP 获取访问控制信息；

决策模块，用于根据获取到的访问控制信息进行访问控制决策。

24、如权利要求 23 所述的设备，其特征在于，所述第一获取模块具体用于：根据接收到的访问控制决策请求，在所述 PDP 本地未获取到所需的访问控制信息，则获取所请求访问的目标资源适用的包含有用于承载授权实体地址的属性的资源。

25、如权利要求 23 或 24 所述的设备，其特征在于，所述用于承载授权实体地址的属性包括：PIP 接入点属性，所述 PIP 接入点属性用于承载一个或多个 PIP 地址。

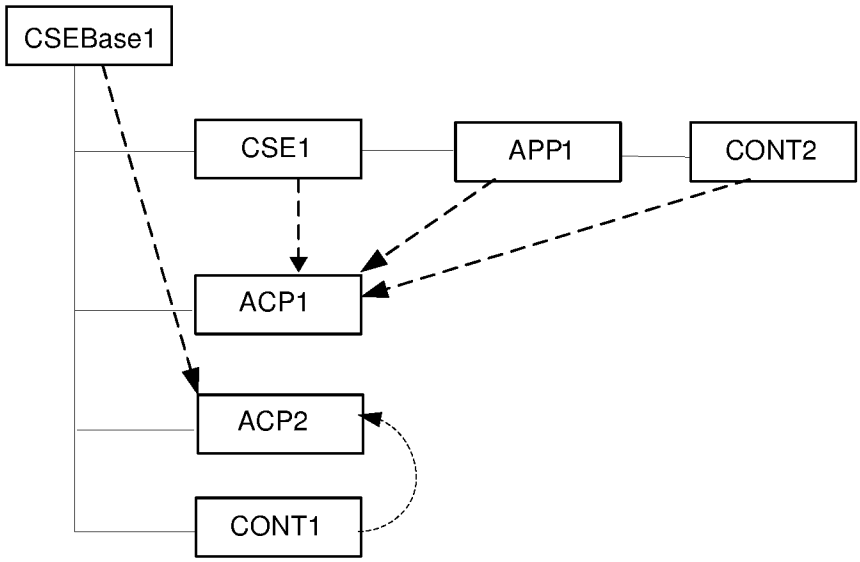
CSEBase1
CSE1
APP1
CONT2
ACP1
ACP2
CONT1

图 1

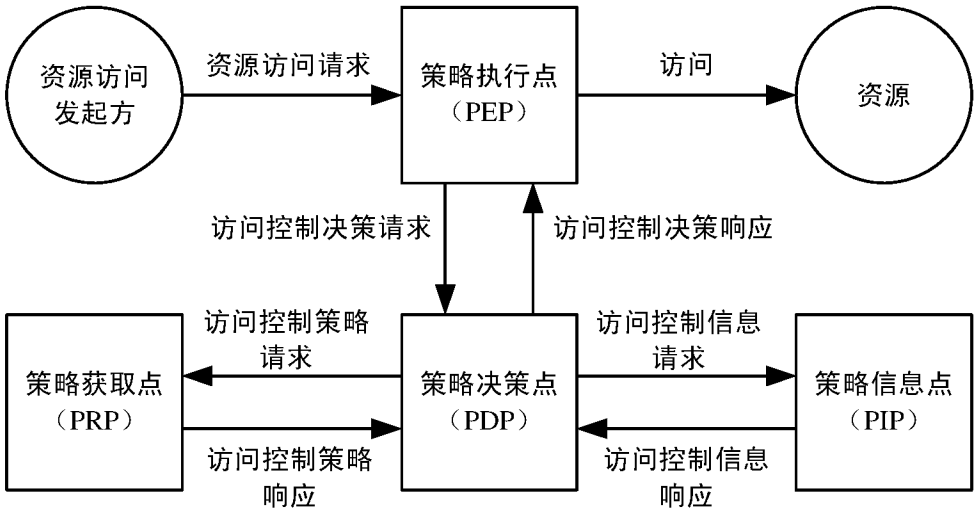
资源访问
发起方
资源访问请求
策略执行点
（PEP）
访问
资源
访问控制决策请求
访问控制决策响应
访问控制策略
请求
访问控制信息
请求
策略获取点
（PRP）
策略决策点
（PDP）
策略信息点
（PIP）
访问控制策略
响应
访问控制信息
响应

图 2

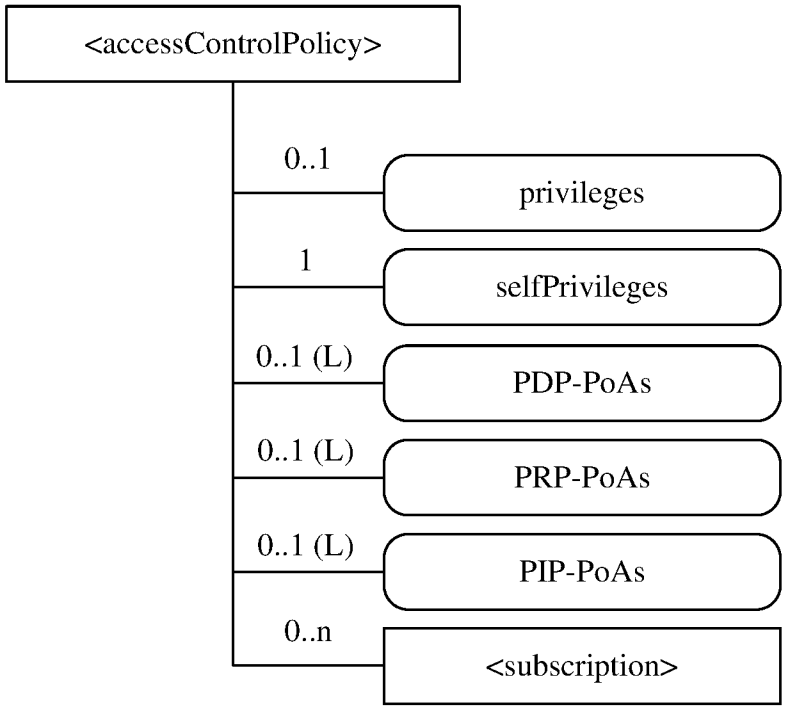
<accessControlPolicy>
0..1
privileges
1
selfPrivileges
0..1 (L)
PDP-PoAs
0..1 (L)
PRP-PoAs
0..1 (L)
PIP-PoAs
0..n
<subscription>

图 3

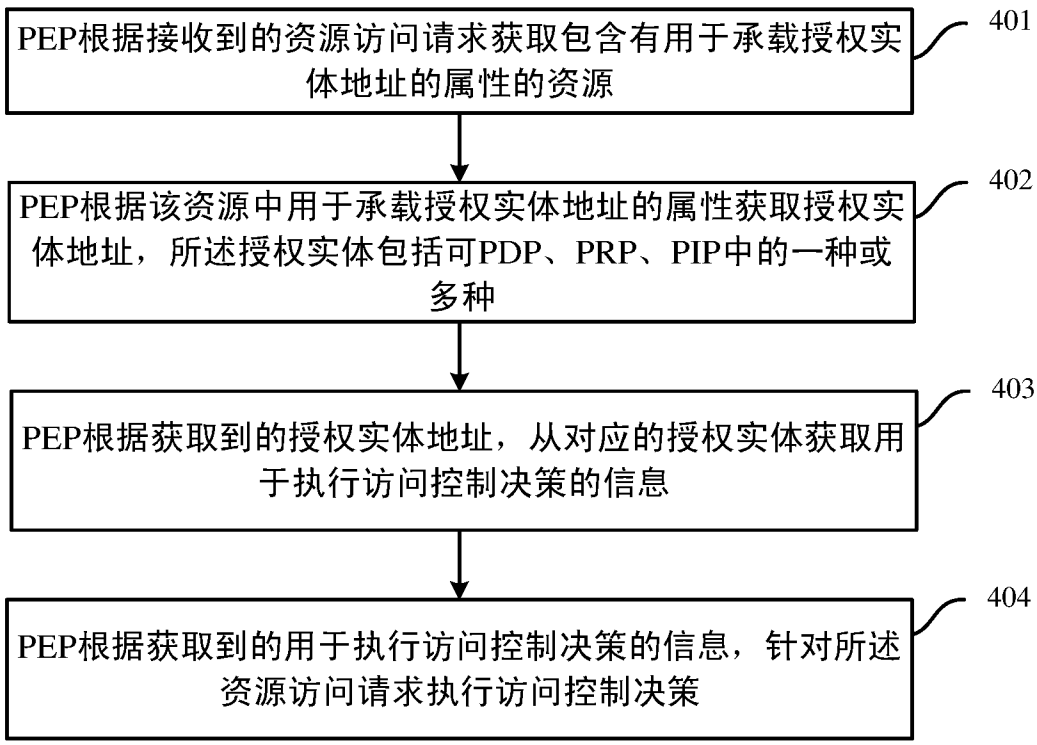
PEP根据接收到的资源访问请求获取包含有用于承载授权实体地址的属性的资源
401
PEP根据该资源中用于承载授权实体地址的属性获取授权实体地址，所述授权实体包括可PDP、PRP、PIP中的一种或多种
402
PEP根据获取到的授权实体地址，从对应的授权实体获取用于执行访问控制决策的信息
403
PEP根据获取到的用于执行访问控制决策的信息，针对所述资源访问请求执行访问控制决策
404

图 4

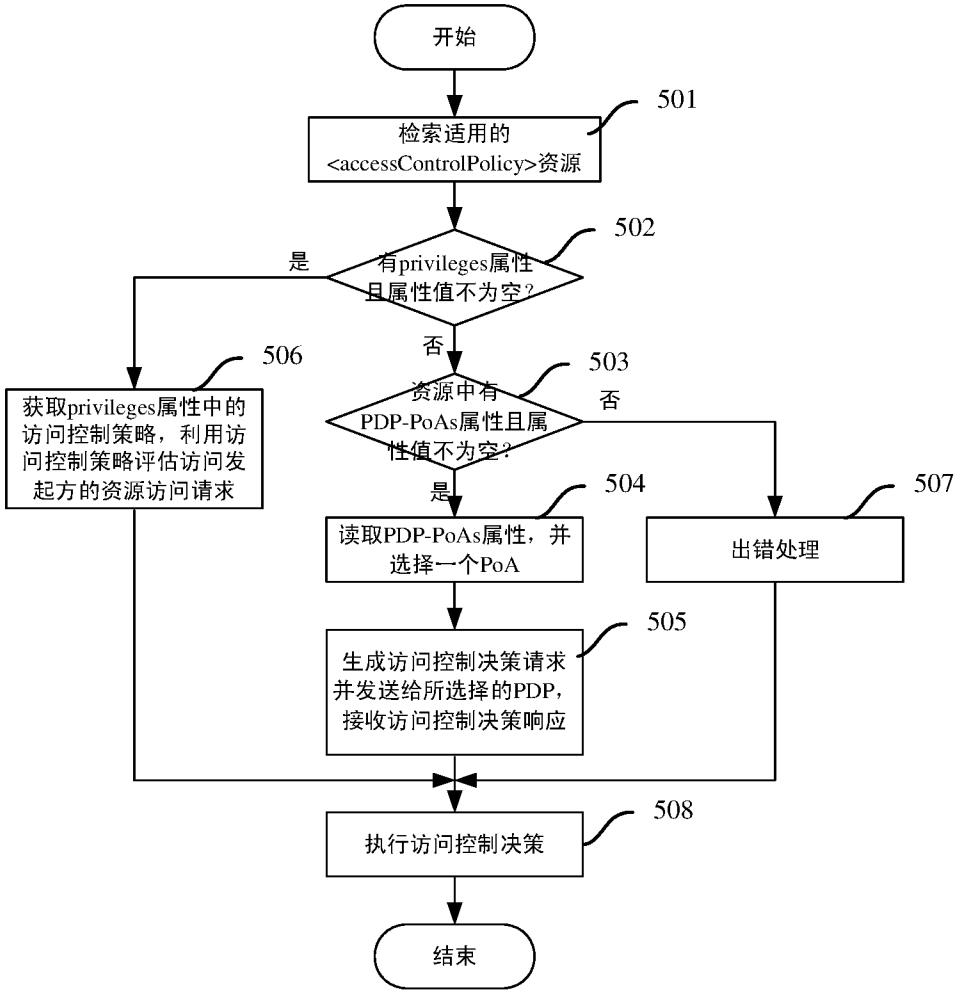
开始
检索适用的<accessControlPolicy>资源
501
有privileges属性且属性值不为空?
502
是
否
获取privileges属性中的访问控制策略，利用访问控制策略评估访问发起方的资源访问请求
506
资源中有PDP-PoAs属性且属性值不为空?
503
否
是
读取PDP-PoAs属性，并选择一个PoA
504
出错处理
507
生成访问控制决策请求并发送给所选择的PDP，接收访问控制决策响应
505
执行访问控制决策
508
结束

图 5

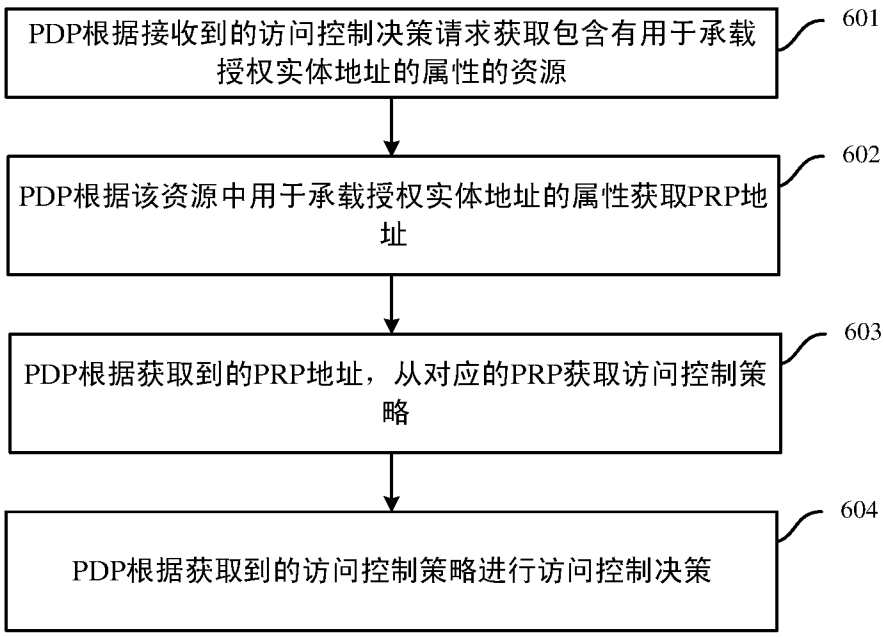
PDP根据接收到的访问控制决策请求获取包含有用于承载授权实体地址的属性的资源
601
PDP根据该资源中用于承载授权实体地址的属性获取PRP地址
602
PDP根据获取到的PRP地址，从对应的PRP获取访问控制策略
603
PDP根据获取到的访问控制策略进行访问控制决策
604

图 6

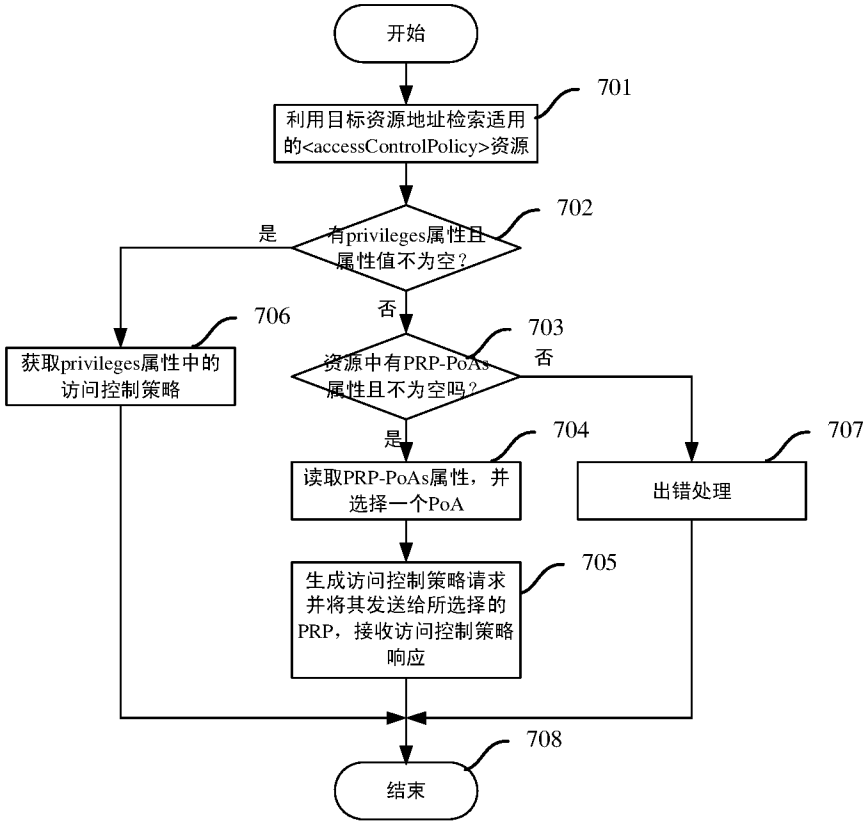
开始
701
利用目标资源地址检索适用的<accessControlPolicy>资源
702
有privileges属性且属性值不为空？
是
否
706
获取privileges属性中的访问控制策略
703
资源中有PRP-PoAs属性且不为空吗？
否
是
704
读取PRP-PoAs属性，并选择一个PoA
707
出错处理
705
生成访问控制策略请求并将其发送给所选择的PRP，接收访问控制策略响应
708
结束

图 7

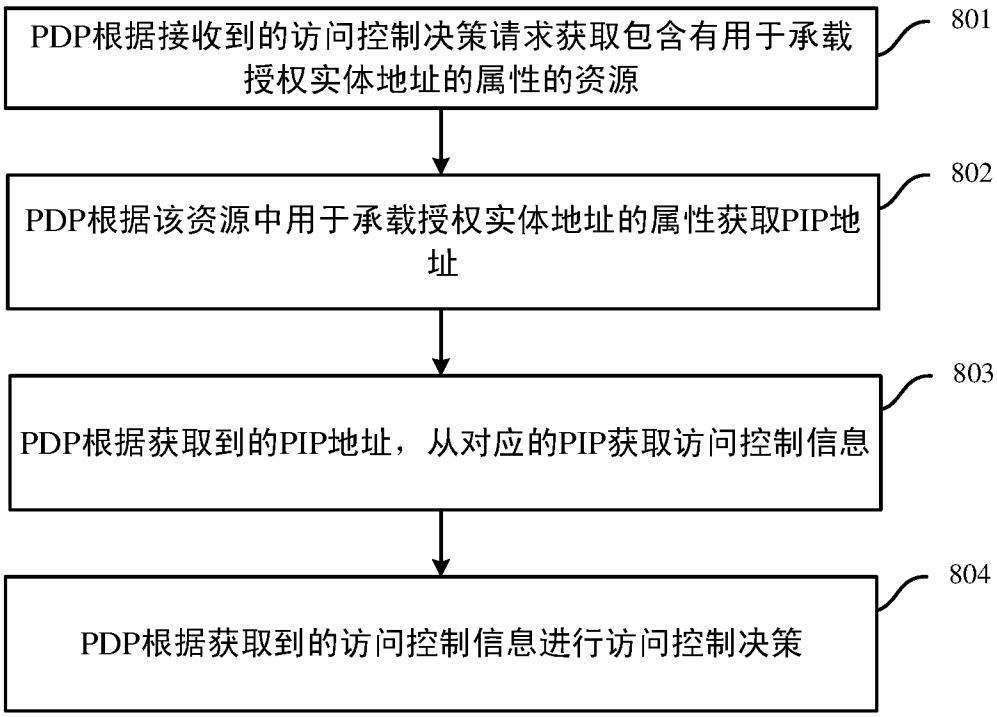
PDP根据接收到的访问控制决策请求获取包含有用于承载授权实体地址的属性的资源
801
PDP根据该资源中用于承载授权实体地址的属性获取PIP地址
802
PDP根据获取到的PIP地址，从对应的PIP获取访问控制信息
803
PDP根据获取到的访问控制信息进行访问控制决策
804

图 8

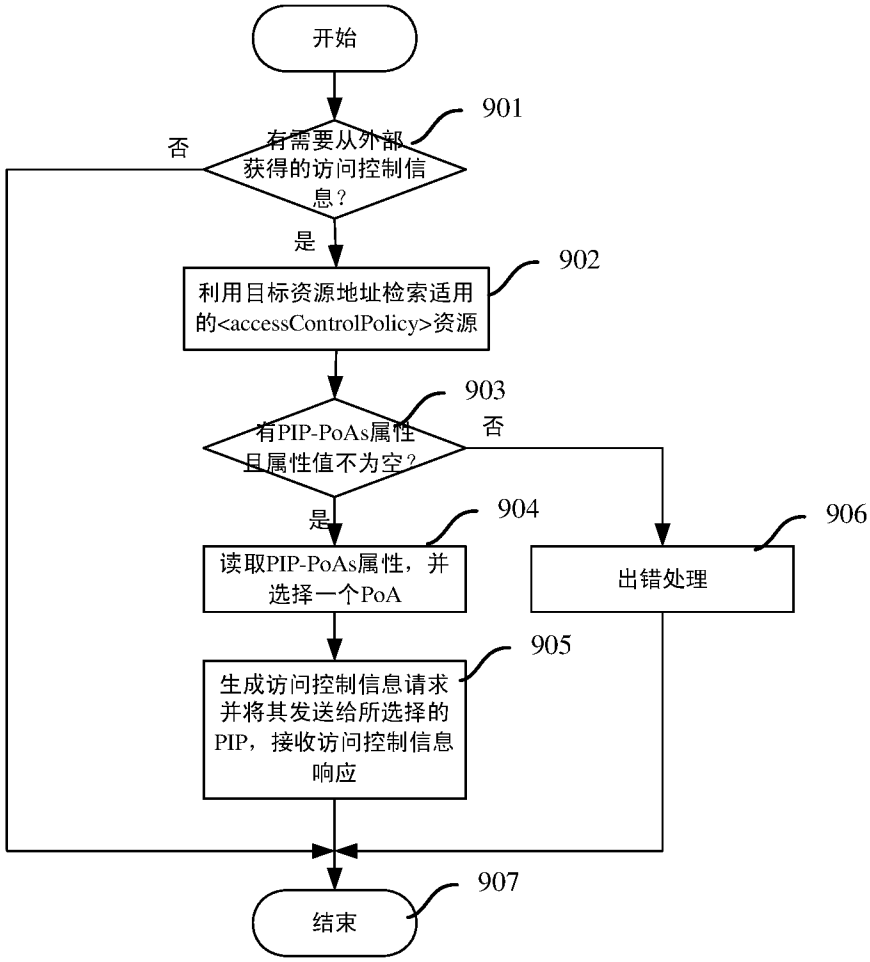
开始
901
有需要从外部获得的访问控制信息？
否
是
902
利用目标资源地址检索适用的<accessControlPolicy>资源
903
有PIP-PoAs属性且属性值不为空？
否
是
904
读取PIP-PoAs属性，并选择一个PoA
906
出错处理
905
生成访问控制信息请求并将其发送给所选择的PIP，接收访问控制信息响应
907
结束

图 9

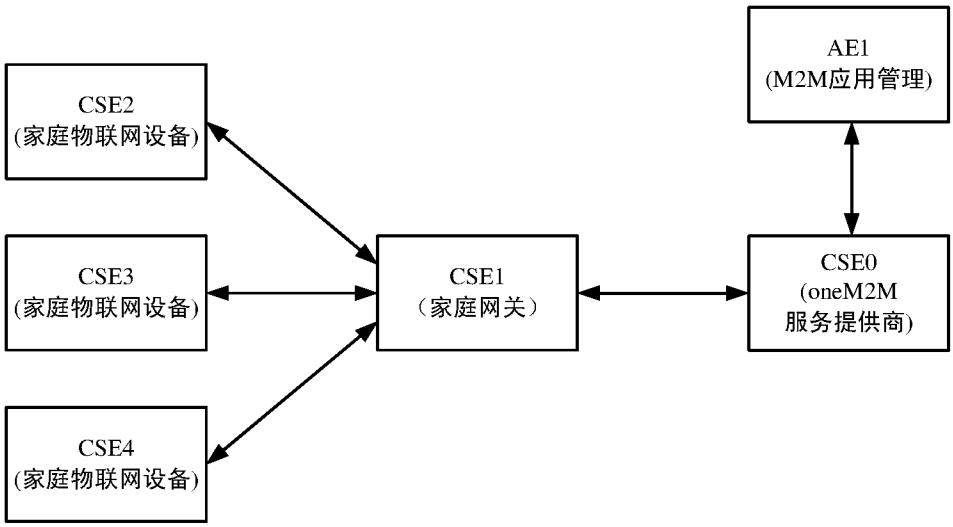
AE1
(M2M应用管理)
CSE2
(家庭物联网设备)
CSE3
(家庭物联网设备)
CSE1
（家庭网关）
CSE0
(oneM2M
服务提供商)
CSE4
(家庭物联网设备)

图 10

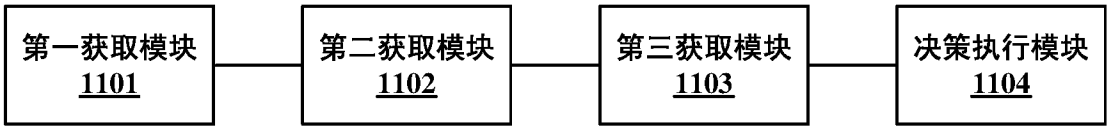
第一获取模块
1101
第二获取模块
1102
第三获取模块
1103
决策执行模块
1104

图 11

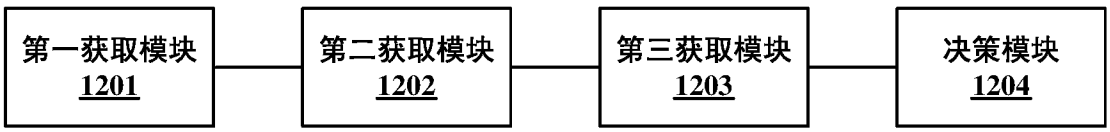
第一获取模块
1201
第二获取模块
1202
第三获取模块
1203
决策模块
1204

图 12

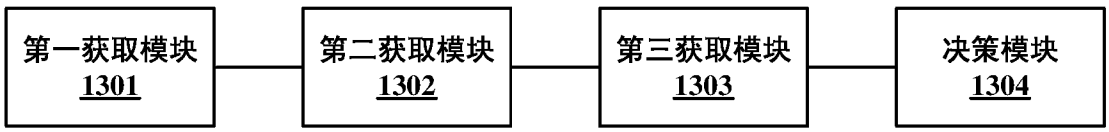
第一获取模块
1301
第二获取模块
1302
第三获取模块
1303
决策模块
1304

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/075429

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08 (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

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)

USTXT; CPRSABS; EPTXT; CNTXT; CNABS; WOTXT; DWPI; TWTXT; VEN; CNKI; PTSN.NET.CN: authorization entity, decision, attribute, oneM2M, PEP, PDP, PRP, PIP, policy, authoriz+, address+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ETSI, "oneM2M; Security solutions (oneM2M TS-0003 version 1.4.2 Release 1)", ETSI TS 118 103 v1.1.0, 31 March 2016 (31.03.2016), pages 21-25, section 6.2, and figures 6.2.2-1 and 6.2.2-2	1-25
A	WO 2013161212 A1 (IBM et al.), 31 October 2013 (31.10.2013), the whole document	1-25
A	US 2005166260 A1 (BETTS, C. et al.), 28 July 2005 (28.07.2005), the whole document	1-25
A	CN 103378987 A (INTERNATIONAL BUSINESS MACHINES CORPORATION), 30 October 2013 (30.10.2013), the whole document	1-25

☐ 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
25 April 2017 (25.04.2017)	**04 May 2017 (04.05.2017)**
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 **WENG, Xiaojun** Telephone No.: (86-10) **62411510**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/075429

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2013161212 A1	31 October 2013	US 9253210 B2	02 February 2016
		US 2013291055 A1	31 October 2013
		US 9253209 B2	02 February 2016
		US 2013290709 A1	31 October 2013
US 2005166260 A1	28 July 2005	WO 2005009003 A1	27 January 2005
		EP 1649668 A1	26 April 2006
CN 103378987 A	30 October 2013	US 2013283338 A1	24 October 2013
		CN 103378987 B	03 August 2016
		US 9054971 B2	09 June 2015

国际检索报告

国际申请号
PCT/CN2017/075429

A. 主题的分类

H04W 12/08(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

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））

USTXT;CPRSABS;EPTXT;CNTXT;CNABS;WOTXT;DWPI;TWTXT;VEN;CNKI;通标网:授权实体，地址，策略，决策，属性，oneM2M,PEP,PDP,PRP,PIP,policy,authoriz+,address+

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
X	ETSI. "oneM2M; Security solutions(oneM2M TS-0003 version 1.4.2 Release 1)" ETSI TS 118 103 v1.1.0, 2016年 3月 31日 (2016-03-31)，第21-25页第6.2节以及附图6.2.2-1、6.2.2-2	1-25
A	WO 2013161212 A1 (IBM等) 2013年 10月 31日 (2013-10-31) 全文	1-25
A	US 2005166260 A1 (CHRISTOPHER BETTS等) 2005年 7月 28日 (2005-07-28) 全文	1-25
A	CN 103378987 A (国际商业机器公司) 2013年 10月 30日 (2013-10-30) 全文	1-25

☐ 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
2017年 4月 25日	2017年 5月 4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	受权官员 翁晓君 电话号码 (86-10)62411510

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/075429

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)
WO	2013161212	A1	2013年 10月 31日	US	9253210	B2	2016年 2月 2日
				US	2013291055	A1	2013年 10月 31日
				US	9253209	B2	2016年 2月 2日
				US	2013290709	A1	2013年 10月 31日
US	2005166260	A1	2005年 7月 28日	WO	2005009003	A1	2005年 1月 27日
				EP	1649668	A1	2006年 4月 26日
CN	103378987	A	2013年 10月 30日	US	2013283338	A1	2013年 10月 24日
				CN	103378987	B	2016年 8月 3日
				US	9054971	B2	2015年 6月 9日