(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
2016 年 9 月 15 日 (15.09.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/141783 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/072206

(22) 国际申请日: 2016 年 1 月 26 日 (26.01.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510109267.9 2015 年 3 月 12 日 (12.03.2015) 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 ACCESS CONTROL, POLICY ACQUISITION, ATTRIBUTE ACQUISITION AND RELATED APPARATUS

(54) 发明名称 : 访问控制、策略获取、属性获取方法及相关装置

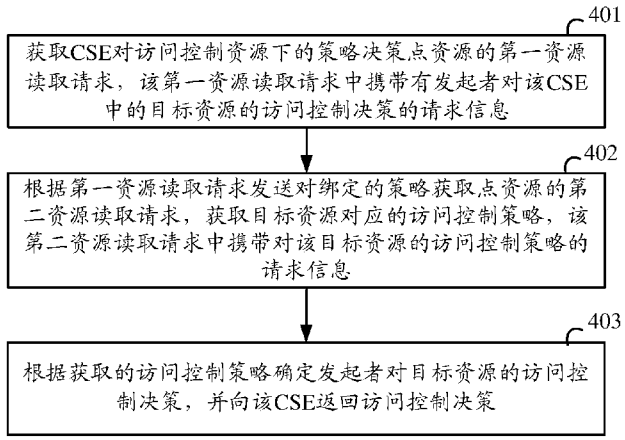

图 4b

401 ACQUIRING A FIRST RESOURCE READ REQUEST OF A CSE FOR A POLICY DECISION POINT RESOURCE UNDER ACCESS CONTROL RESOURCES, WHEREIN THE FIRST RESOURCE READ REQUEST CARRIES INFORMATION ABOUT A REQUEST OF A SPONSOR FOR AN ACCESS CONTROL DECISION FOR A TARGET RESOURCE IN THE CSE
402 ACCORDING TO THE FIRST RESOURCE READ REQUEST, SENDING A SECOND RESOURCE READ REQUEST FOR THE BOUND POLICY ACQUISITION POINT RESOURCE, AND ACQUIRING AN ACCESS CONTROL POLICY CORRESPONDING TO THE TARGET RESOURCE, WHEREIN THE SECOND RESOURCE READ REQUEST CARRIES INFORMATION ABOUT A REQUEST FOR THE ACCESS CONTROL POLICY OF THE TARGET RESOURCE
403 ACCORDING TO THE ACQUIRED ACCESS CONTROL POLICY, DETERMINING THE ACCESS CONTROL DECISION OF THE SPONSOR FOR THE TARGET RESOURCE AND RETURNING THE ACCESS CONTROL DECISION TO THE CSE

(57) Abstract: Disclosed are a method for access control, policy acquisition, attribute acquisition and a related apparatus. The method is used to provide a particular access control mechanism for the oneM2M.The access control method includes: acquiring a first resource read request of a CSE for a policy decision point resource under access control resources, wherein the first resource read request carries information about a request of a sponsor for an access control decision for a target resource in the CSE; according to the first resource read request, sending a second resource read request for the bound policy acquisition point resource, and acquiring an access control policy corresponding to the target resource, wherein the second resource read request carries information about a request for the access control policy of the target resource; and according to the acquired access control policy, determining the access control decision of the sponsor for the target resource and returning the access control decision to the CSE.

(57) 摘要:

[见续页]

WO 2016/141783 A1

本申请公开了一种访问控制、策略获取、属性获取方法及相关装置，用以为 oneM2M 提供具体的访问控制机制。访问控制方法为：获取 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，第一资源读取请求中携带有发起者对 CSE 中的目标资源的访问控制决策的请求信息；根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，获取目标资源对应的访问控制策略，第二资源读取请求中携带对目标资源的访问控制策略的请求信息；根据获取的访问控制策略确定发起者对目标资源的访问控制决策，并向 CSE 返回访问控制决策。

访问控制、策略获取、属性获取方法及相关装置

本申请要求在 2015 年 03 月 12 日提交中国专利局、申请号为 201510109267.9、申请名称为“访问控制、策略获取、属性获取方法及相关装置”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，尤其涉及一种访问控制、策略获取、属性获取方法及相关装置。

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，M2M）服务层（Service Layer）的技术规范。

oneM2M 通过采用对标准的资源树的操作实现服务层资源共享和交互。

根据 oneM2M TS-0001 中关于功能架构的定义，oneM2M 资源树的形式如图 1 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、查询、修改和删除等操作。

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），<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 定义有两种基本实体:

一，应用实体（Application Entity，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，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公共服务实体身份标识（CSE-ID）标识。

资源树存在于 oneM2M 系统定义的 CSE 中。

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。

oneM2M TS-0001 中仅定义了<accessControlPolicy>资源的资源结构及访问控制策略的结构，授权架构和访问控制策略的评估在 oneM2M TS-0003 中提供。

如图 2 所示的授权架构中，各授权组件的功能为:

策略执行点（Policy Enforcement Point，PEP），与需要访问控制的应用系统共存，并由应用系统调用。PEP 根据用户的访问请求生成相应的访问控制决策请求，发送给策略决策点（Policy Decision Point，PDP），并根据 PDP 的访问控制决策应答确定是否执行用户的访问请求。

策略决策点（Policy Decision Point，PDP），负责根据访问控制策略评估是否同意由 PEP 发送来的访问控制决策请求，并将评估结果通过访问控制决策应答返回给 PEP。

策略获取点（Policy Retrieval Point，PRP），根据 PDP 提供的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），根据 PDP 的请求获取与用户、资源或环境相关的属性，例如访问用户的互联网协议（IP）地址、资源的创建者、当前的时间等，然后将获得的各种属性返回给 PDP。

oneM2M 的基本授权流程如下:

1、PEP 根据用户的访问请求生成访问控制决策请求（Access Control Decision Request）发送给 PDP;

2、PDP 根据 PEP 的访问控制决策请求向 PRP 发送访问控制策略请求（Access Control Policy Request）;

3、PDP 分析由 PRP 返回的访问控制策略和 PEP 的访问控制决策请求中提供的内容，若需要其他属性，则向 PIP 发送访问控制属性请求（Access Control Attribute Request），否

则执行步骤 5。

4、PIP 根据 PDP 的访问控制属性请求获取相应的与访问控制相关的属性，并返回给 PDP。

5、PDP 根据确定适用的访问控制策略，并通过该访问控制决策应答（Access Control Attribute Response）返回给 PEP。

6、PEP 根据访问控制决策应答中的访问控制策略决定是否执行用户的访问请求。

oneM2M TS-0003 中仅给出了授权架构的高层描述和基本授权流程，没有给出具体的访问控制机制、实现原理或方法。

发明内容

本申请实施例提供一种访问控制、策略获取、属性获取方法及相关装置，用以为 oneM2M 提供具体的访问控制机制。

本申请实施例提供的具体技术方案如下:

第一方面，提供了一种访问控制方法，包括:

获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，所述第一资源读取请求中携带有发起者对所述 CSE 中的目标资源的访问控制决策的请求信息;

根据所述第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，以获取所述目标资源对应的访问控制策略，所述第二资源读取请求中携带对所述目标资源的访问控制策略的请求信息;

根据获取的所述访问控制策略确定所述发起者对所述目标资源的访问控制决策，并向所述 CSE 返回所述访问控制决策;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略决策点资源以及所述策略获取点资源分别为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，获取所述目标资源对应的访问控制策略后，确定所述发起者对所述目标资源的访问控制决策之前，所述方法还包括:

对绑定的策略信息点资源发送第三资源读取请求，获取所述访问控制策略对应的属性信息，所述第三资源读取请求中携带对所述访问控制策略的访问控制属性的请求信息;

其中，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

可选地，获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之前，所述方法还包括:

根据所述策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略决策点资源。

可选地，根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取所述目标资源对应的访问控制策略之前，所述方法还包括:

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

可选地，对绑定的策略信息点资源发送第三资源读取请求之后，获取所述访问控制策略对应的属性信息之前，所述方法还包括:

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

具体地，确定所述发起者对所述目标资源的访问控制决策，包括:

根据所述访问控制策略以及所述访问控制策略对应的属性信息，确定所述发起者对所述目标资源的访问控制决策。

其中，所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源分别位于不同 CSE 根节点下的访问控制资源下;

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源中的至少两个位于同一 CSE 根节点下的不同访问控制资源下;

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源属于同一 CSE 根节点下的同一访问控制资源下。

第二方面，提供了一种获取访问控制策略的方法，包括:

获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求，所述资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息;

获取所述目标资源对应的访问控制策略，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略获取点资源为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公

共属性。

可选地，获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求之后，获取所述目标资源对应的访问控制策略之前，所述方法还包括:

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

第三方面，提供了一种获取访问控制属性的方法，包括:

获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求，所述资源读取请求中携带对访问控制策略的访问控制属性的请求信息;

获取所述访问控制策略对应的属性信息，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求之后，获取所述访问控制策略对应的属性信息之前，所述方法还包括:

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

第四方面，提供了一种公共服务实体 CSE，包括:

第一获取模块，用于获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，所述第一资源读取请求中携带有发起者对所述 CSE 中的目标资源的访问控制决策的请求信息;

第二获取模块，用于根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，以获取所述目标资源对应的访问控制策略，所述第二资源读取请求中携带对所述目标资源的访问控制策略的请求信息;

处理模块，用于根据获取的所述访问控制策略确定所述发起者对所述目标资源的访问控制决策，并向所述 CSE 返回所述访问控制决策;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略决策点资源以及所述策略获取点资源分别为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，还包括第三获取模块，用于所述第二获取模块获取所述目标资源对应的访问

控制策略后，所述处理模块确定所述发起者对所述目标资源的访问控制决策之前，对绑定的策略信息点资源发送第三资源读取请求，获取所述访问控制策略对应的属性信息，所述第三资源读取请求中携带对所述访问控制策略的访问控制属性的请求信息；

其中，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

可选地，所述处理模块还用于：

在所述第一获取模块获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，在所述第二获取模块根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之前，

根据所述策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略决策点资源。

可选地，所述第二获取模块还用于：

根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

可选地，所述第三获取模块还用于：

对绑定的策略信息点资源发送第三资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

具体地，所述处理模块具体用于：

根据所述访问控制策略以及所述访问控制策略对应的属性信息，确定所述发起者对所述目标资源的访问控制决策。

其中，所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源分别位于不同 CSE 根节点下的访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源中的至少两个位于同一 CSE 根节点下的不同访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源属于同一 CSE 根节点下的同一访问控制资源下。

第五方面，提供了一种公共服务实体 CSE，包括:

获取模块，用于获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求，所述资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息;

处理模块，用于获取所述目标资源对应的访问控制策略，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略获取点资源为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，所述处理模块还用于:

在所述获取模块获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

第六方面，提供了一种公共服务实体 CSE，包括:

获取模块，用于获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求，所述资源读取请求中携带对访问控制策略的访问控制属性的请求信息;

处理模块，用于获取所述访问控制策略对应的属性信息，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，所述处理模块还用于:

在所述获取模块获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

基于上述技术方案，本申请实施例中，通过在 CSE 根资源下定义普通资源访问控制资源，在访问控制资源下定义策略决策点资源和/或策略获取点资源，并且定义策略决策点资源为触发 PDP 处理过程的虚拟资源，定义策略获取点资源为触发 PRP 处理过程的虚拟资源，从而通过对访问控制资源下的策略决策点资源的资源读取请求，触发具备 PDP 功能的

CSE 通过读取绑定的策略获取点资源获取目标资源的访问控制策略，根据获取的访问控制策略对目标资源的访问请求进行访问控制决策。

附图说明

图 1 为 oneM2M 资源树结构示意图；

图 2 为 oneM2M 授权架构示意图；

图 3 为本申请实施例中访问控制资源结构示意图；

图 4a 为本申请实施例中具有 PEP 功能的 CSE 与具有 PDP 功能的 CSE1 交互示意图；

图 4b 为本申请实施例中具有 PDP 功能的 CSE1 进行访问控制的过程示意图；

图 5a 为本申请实施例中具有 PDP 功能的 CSE1 对具有 PRP 功能的 CSE2 交互示意图；

图 5b 为本申请实施例中具有 PRP 的功能 CSE2 获取访问控制策略的过程示意图；

图 6a 为本申请实施例中具有 PDP 功能的 CSE1 与具有 PIP 功能的 CSE3 交互示意图；

图 6b 为本申请实施例中具有 PIP 功能的 CSE3 获取访问控制属性的过程示意图；

图 7 为本申请实施例中 CSE 结构示意图；

图 8 为本申请实施例中另一 CSE 结构示意图；

图 9 为本申请实施例中另一 CSE 结构示意图；

图 10 为本申请实施例中另一 CSE 结构示意图；

图 11 为本申请实施例中另一 CSE 结构示意图；

图 12 为本申请实施例中另一 CSE 结构示意图。

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分实施例，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。

本申请实施例中，定义了四种 oneM2M 资源以实现具体的访问控制机制。

定义的四种 oneM2M 资源分别为：访问控制资源<accessControl>、策略决策点资源<policyDecisionPoint>、策略获取点资源<policyRetrievalPoint>以及策略信息点资源<policyInformationPoint>。

其中，访问控制资源<accessControl>定义为位于 CSE 根资源<CSEBase>下的普通资源，

至少具有 oneM2M 普通资源的通用属性。

策略决策点资源<policyDecisionPoint>、策略获取点资源<policyRetrievalPoint>以及策略信息点资源<policyInformationPoint>定义为位于访问控制资源<accessControl>下的虚拟资源。

具体地，对策略决策点资源<policyDecisionPoint>的读取操作，将触发一个 PDP 处理过程；

对策略获取点资源<policyRetrievalPoint>的读取操作，将触发一个 PRP 处理过程；

对策略信息点资源<policyInformationPoint>的读取操作，将触发一个 PIP 处理过程。

一个 CSE 根节点下可以有 1 个或多个访问控制资源<accessControl>，一个 CSE 根节点下也可以不包含访问控制资源。

其中，访问控制资源<accessControl>与定义的虚拟资源之间的关系如图 3 所示，即一个访问控制资源<accessControl>下可以有策略决策点资源<policyDecisionPoint>、策略获取点资源<policyRetrievalPoint>以及策略信息点资源<policyInformationPoint>中任意一个或多个的组合，也可以不包含任意一个定义的虚拟资源。

可选地，访问控制资源<accessControl>还具有指定访问控制策略的公共属性，该公共属性用于指定适用于该访问控制资源<accessControl>的访问控制策略，对该访问控制资源<accessControl>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访问控制资源<accessControl>及其下的虚拟资源的 CSE。

虚拟资源不具有资源属性，也没有子资源，针对虚拟资源的访问控制由该虚拟资源所属的父资源的指定访问控制策略负责。

基于以上定义的资源，如图 4a 所示，具有 PEP 功能的 CSE 截获发起者对自身的目标资源的访问请求，与具有 PDP 功能的 CSE1 交互的过程如下：

CSE 发送对 CSE1 根资源下的访问控制资源下的策略决策点资源的第一资源读取请求，该第一资源读取请求中携带发起者对 CSE 中的目标资源的访问控制决策的请求信息；

CSE1 根据对访问控制资源下的策略决策点资源的第一资源读取请求，触发策略决策点资源对应的 PDP 处理过程：获取目标资源对应的访问控制策略，可选地，获取该访问控制策略对应的属性信息，根据该访问控制策略或者根据该访问控制策略及其对应的属性信息进行访问控制决策，通过访问控制决策应答将访问控制决策返回给 CSE。

具体地，在第一资源读取请求中的内容（Content）参数携带：发起者对 CSE 中的目标资源的访问控制决策的请求信息，该资源读取请求即为符合 oneM2M 标准的请求。

具体地，在访问控制决策应答中的 Content 参数携带访问控制决策，该访问控制决策

应答为符合 oneM2M 标准的应答。

其中，CSE 与 CSE1 可以为同一 CSE，该 CSE 集成 PEP 和 PDP 的功能，也可以为两个独立的 CSE。

基于以上定义的资源，本申请实施例中，CSE1 的根资源下包含有访问控制资源，该访问控制资源下至少有一个策略决策点资源，如图 4b 所示，该 CSE1 实现访问控制的详细方法流程如下：

步骤 401：获取 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，该第一资源读取请求中携带有发起者对该 CSE 中的目标资源的访问控制决策的请求信息。

其中，发起者为 AE 或 CSE。

其中，发出对策略决策点资源的第一资源读取请求的 CSE 具有 PEP 的功能；具有访问控制功能的 CSE1 的根资源下包含访问控制资源，且该访问控制资源具有策略决策点资源，即具有访问控制功能的 CSE1 具有 PDP 的功能。

其中，具有 PEP 功能的 CSE 与具有 PDP 功能的 CSE1，可以为同一 CSE，也可以是两个独立的 CSE。

可选地，策略决策点资源所属的访问控制资源还具有指定访问控制策略的公共属性。

相应地，CSE1 在获取 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之前，根据该策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许该 CSE 访问该策略决策点资源。

步骤 402：根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，以获取目标资源对应的访问控制策略，该第二资源读取请求中携带对该目标资源的访问控制策略的请求信息。

可选地，若策略获取点资源所属的访问控制资源还具有指定访问控制策略的公共属性。

相应地，若策略获取点资源所属的访问控制资源位于 CSE1 的根资源下，则 CSE1 根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取目标资源对应的访问控制策略之前，根据该策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许 CSE 访问该策略获取点资源。

步骤 403：根据获取的访问控制策略确定发起者对目标资源的访问控制决策，并向该 CSE 返回访问控制决策。

可选地，CSE1 若根据获取的访问控制策略确定发起者对目标资源的访问控制决策的

过程中，还需要获取该访问控制策略对应的属性信息，则对绑定的策略信息点资源发送第三资源读取请求，获取该访问控制策略对应的属性信息，该第三资源读取请求中携带对该访问控制策略的访问控制属性的请求信息。

其中，CSE1 在获取访问控制策略对应的属性信息后，根据该访问控制策略以及该访问控制策略对应的属性信息，确定该发起者对目标资源的访问控制决策。

可选地，若策略信息点资源所属的访问控制资源还具有指定访问控制策略的公共属性。

相应地，若策略信息点资源所属的访问控制资源位于 CSE1 的根资源下，则 CSE1 对绑定的策略信息点资源发送第三资源读取请求之后，获取访问控制策略对应的属性信息之前，根据策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许 CSE 访问该策略信息点资源。

该实施例中，策略决策点资源、策略获取点资源以及策略信息点资源分别位于不同 CSE 根节点下的访问控制资源下；

或者，

策略决策点资源、策略获取点资源以及策略信息点资源中的至少两个位于同一 CSE 根节点下的不同访问控制资源下；

或者，

策略决策点资源、策略获取点资源以及策略信息点资源属于同一 CSE 根节点下的同一访问控制资源下。

基于以上定义，如图 5a 所示，具有 PDP 功能的 CSE1 对具有 PRP 功能的 CSE2 之间的交互过程如下：

CSE1 对 CSE2 的访问控制资源下的策略获取点资源发送第二资源读取请求，该第二资源读取请求中携带对目标资源的访问控制策略的请求信息；

CSE2 根据对访问控制资源下的策略获取点资源的第二资源读取请求，触发 PRP 的处理过程：获取目标资源的访问控制策略，通过访问控制策略应答将该访问控制策略返回给 CSE1。

具体地，在第二资源读取请求中的内容（Content）参数携带：对目标资源的访问控制策略的请求信息，该资源读取请求为符合 oneM2M 标准的请求。

具体地，在访问控制策略应答中的 Content 参数携带访问控制策略，该访问控制策略应答为符合 oneM2M 标准的应答。

其中，CSE1 和 CSE2 可以是同一 CSE，该 CSE 集成 PDP 和 PRP 的功能，也可以是两

个独立的 CSE。

一个具体实施例中，CSE1 若确定第二资源读取请求中携带的对目标资源的访问控制策略的请求信息中，携带有访问控制令牌，则 CSE1 还可以从该访问控制令牌中获取访问控制策略。

CSE1 按照预设的策略将从 CSE2 获取的访问控制策略与从访问控制令牌中获取的访问控制策略合并，基于合并后的访问控制策略评估发起者对目标资源的访问控制。

基于以上定义的资源，本申请实施例中，CSE2 的根资源下包含有访问控制资源，该访问控制资源下至少有策略获取点资源，即该 CSE2 具有 PRP 的功能，如图 5b 所示，该 CSE2 获取访问控制策略的过程如下：

步骤 501：获取 CSE1 对访问控制资源下的策略获取点资源的第二资源读取请求，该第二资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息。

步骤 502：获取目标资源对应的访问控制策略，并返回给该 CSE1。

可选地，策略获取点资源所属的访问控制资源还具有指定访问控制策略的公共属性。

相应地，CSE2 获取 CSE1 对访问控制资源下的策略获取点资源的第二资源读取请求之后，获取目标资源对应的访问控制策略之前，根据该策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许 CSE1 访问该策略获取点资源。

其中，具有 PRP 功能的 CSE2，与发出资源读取请求的 CSE1，可以同一 CSE，也可以是两个独立的 CSE。

基于以上定义，如图 6a 所示，若具有 PDP 功能的 CSE1 根据获取的访问控制策略，确定发起者对目标资源的访问控制决策的过程中，还需要获取该访问控制策略对应的属性信息，则需要该具有 PDP 功能的 CSE1 与具有 PIP 功能的 CSE3 交互，以获得该属性信息，交互过程如下：

CSE1 对 CSE3 的访问控制资源下的策略信息点资源发送第三资源读取请求，该第三资源读取请求中携带对该访问控制策略的访问控制属性的请求信息；

CSE3 根据对访问控制资源下的策略信息点资源的第三资源读取请求，触发 PIP 的处理过程：获取访问控制策略对应的属性信息，通过访问控制属性应答将该属性信息返回给 CSE1。

具体地，在第三资源读取请求中的内容（Content）参数携带：对访问控制策略的访问控制属性的请求信息，该资源读取请求为符合 oneM2M 标准的请求。

具体地，在访问控制属性应答中的 Content 参数携带该属性信息，该访问控制属性应答为符合 oneM2M 标准的应答。

其中，CSE1 和 CSE3 可以是同一 CSE，该 CSE 集成 PDP 和 PIP 的功能，也可以是两个独立的 CSE。

具体地，访问控制策略的属性信息可以是访问控制策略的创建时间、创建者、访问控制策略的访问者、访问者的签约信息、访问者在访问控制策略中的角色（Role）等。

基于以上定义的资源，本申请实施例中，CSE3 的根资源下包含有访问控制资源，该访问控制资源下至少有策略信息点资源，如图 6b 所示，即该 CSE3 具有 PIP 功能，该 CSE3 获取访问控制属性的过程如下：

步骤 601：获取 CSE1 对访问控制资源下的策略信息点资源的第三资源读取请求，该第三资源读取请求中携带对访问控制策略的访问控制属性的请求信息。

步骤 602：获取访问控制策略对应的属性信息，并返回给该 CSE1。

可选地，策略信息点资源所属的访问控制资源还具有指定访问控制策略的公共属性。

相应地，CSE3 获取 CSE1 对访问控制资源下的策略信息点资源的第三资源读取请求之后，获取访问控制策略对应的属性信息之前，根据该策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许该 CSE1 访问该策略信息点资源。

其中，具有 PIP 功能的 CSE3，与发出资源读取请求的 CSE1，可以同一 CSE，也可以是两个独立的 CSE。

以下通过一个具体实施例对本申请实施例中提供的访问控制过程进行举例说明。

该具体实施例中进行如下假设：

PEP、PDP、PRP 和 PIP 的功能分别集成于不同的 CSE 中，其中 PEP 位于 CSE-0 中，PDP 位于 CSE-1 中，PRP 位于 CSE-2 中，PIP 位于 CSE-3 中；

资源访问的发起者为：AE-1，访问的目标资源为 CSE-1 上的：CSE-1\Group-1\memberIDs;

CSE-3 上存储有适用于 CSE-1\Group-1\memberIDs 资源的访问控制策略：RBAC-Policy;

AE-1 的角色存储在 CSE-4 上的 CSE-4\m2mServiceSubscriptionProfile-1\serviceRoles 资源中，AE-1 的角色为：管理员（Administrator）;

CSE-2 上触发 PDP 功能的虚拟资源为：CSE-2\AccessControl-2\policyDecisionPoint;

CSE-3 上触发 PRP 功能的虚拟资源为：CSE-3\AccessControl-3\policyRetrievalPoint;

CSE-4 上触发 PIP 功能的虚拟资源为：CSE-4\AccessControl-4\policyInformationPoint;

在 CSE-2 上，CSE-2\AccessControl-2 的访问控制策略允许来自于 CSE-1 的资源读取请求；

在 CSE-3 上，CSE-3\AccessControl-3 的访问控制策略允许来自于 CSE-2 的资源读取请求；

在 CSE-4 上，CSE-4\AccessControl-4 的访问控制策略允许来自于 CSE-2 的资源读取请求。

第一步，AE-1 向 CSE-1 中的目标资源发送读取请求，具体为：发起者为 AE-1，目标资源为 CSE-1\Group-1\memberIDs，动作为读取（Retrieve）。

第二步，CSE-1 中的 PEP 截取到该请求，并向预先配置的 PDP 发送访问控制决策请求，具体为：

发起者为 CSE-1，目标资源为 CSE-2\AccessControl-2\policyDecisionPoint，动作为读取，参数 Content 的内容为访问控制决策请求的内容：

{发起者=AE-1，目标资源=CSE-1\Group-1\memberIDs，动作= 读取}。

第三步，CSE-2 接收到 CSE-1 的访问控制决策请求。

首先检查 CSE-2\AccessControl-2 指定的访问控制策略，确定该指定的访问控制策略允许来自 CSE-1 的访问，然后向预先配置的 PRP 发送访问控制策略请求，具体为：

发起者为 CSE-2，目标资源为 CSE-3\AccessControl-3\policyRetrievalPoint，动作为读取，参数 Content 的内容为访问控制决策请求的内容：

{To=CSE-1\Group-1\memberIDs}。

第四步，CSE-3 接收到 CSE-2 的访问控制策略请求。

首先检查 CSE-3\AccessControl-3 指定的访问控制策略，确定该指定的访问控制策略允许来自 CSE-2 的访问请求，然后根据 AE-1 访问的目标资源获取适用的访问控制策略。

第五步，CSE-3 将获取的访问控制策略通过 oneM2M 响应返回给 CSE-2，该 oneM2M 响应即为访问控制策略响应，具体为：响应代码（Response Code）为成功获取，参数 Content 的内容为获取的访问控制策略：

{访问控制策略= RBAC-Policy}。

第六步，CSE-2 接收到 CSE-3 的访问控制策略响应，分析获得的基于角色的访问控制策略：RBAC-Policy，得知需要获取 AE-1 的角色（Role）才能进行策略评估，则 CSE-2 向预先配置的 PIP 发送访问控制属性请求，具体为：

发起者为 CSE-2，目标资源为 CSE-4\AccessControl-4\policyInformationPoint，动作为读取，参数 Content 的内容为：{用户=AE-1，请求的属性信息=Role}。

第七步，CSE-4 接收到 CSE-2 的访问控制属性请求。首先检查 CSE-4\AccessControl-4 指定的访问控制策略，确定该指定的访问控制策略允许来自 CSE-2 的访问请求，然后根据

用户信息从该用户的签约信息中获取该用户的角色为：管理员（Administrator）。

第八步，CSE-4 将获取的属性信息通过 oneM2M 响应返回给 CSE-2，该 oneM2M 响应即为访问控制属性响应，具体为：响应代码为成功获取，参数 Content 的内容为获取的属性信息：

{角色=Administrator}。

第九步，CSE-2 接收到 CSE-4 的访问控制属性响应，获取 AE-1 的角色，然后利用获得的基于角色的访问控制策略和 AE-1 的角色评估用户 AE-1 的资源访问请求，确定评估结果，即访问控制决策为：允许 AE-1 的资源访问请求。

第十步，CSE-2 将访问控制决策通过 oneM2M 响应返回给 CSE-1，该 oneM2M 响应即为访问控制决策响应，具体为：

响应代码为成功获取，参数 Content 的内容为访问控制决策：

{访问控制决策=允许}。

基于同一发明构思，本申请实施例还提供了一种 CSE，该 CSE 的具体实施可参见上述关于具有 PDP 功能的 CSE1 的描述，重复之处不再赘述，如图 7 所示，该 CSE 主要包括：

第一获取模块 701，用于获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，所述第一资源读取请求中携带有发起者对所述 CSE 中的目标资源的访问控制决策的请求信息；

第二获取模块 702，用于根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，以获取所述目标资源对应的访问控制策略，所述第二资源读取请求中携带对所述目标资源的访问控制策略的请求信息；

处理模块 703，用于根据获取的所述访问控制策略确定所述发起者对所述目标资源的访问控制决策，并向所述 CSE 返回所述访问控制决策；

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略决策点资源以及所述策略获取点资源分别为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，还包括第三获取模块 704，用于所述第二获取模块 702 获取所述目标资源对应的访问控制策略后，所述处理模块 703 确定所述发起者对所述目标资源的访问控制决策之前，对绑定的策略信息点资源发送第三资源读取请求，获取所述访问控制策略对应的属性信息，所述第三资源读取请求中携带对所述访问控制策略的访问控制属性的请求信息；

其中，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

具体地，所述处理模块 703 还用于：

在所述第一获取模块获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，在所述第二获取模块根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之前，

根据所述策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略决策点资源。

具体地，所述第二获取模块还用于：

根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

具体地，所述第三获取模块还用于：

对绑定的策略信息点资源发送第三资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

具体地，若获取到访问控制策略对应的属性信息，则所述处理模块具体用于：

根据所述访问控制策略以及所述访问控制策略对应的属性信息，确定所述发起者对所述目标资源的访问控制决策。

具体地，所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源分别位于不同 CSE 根节点下的访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源中的至少两个位于同一 CSE 根节点下的不同访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源属于同一 CSE 根节点下的同一访问控制资源下。

基于同一发明构思，本申请实施例还提供了一种 CSE，该 CSE 的具体实施可参见上述关于具有 PDP 功能的 CSE1 的描述，重复之处不再赘述，如图 8 所示，该 CSE 主要包括处理器 801 和存储器 802，其中，存储器 802 中保存有预设程序，处理器 801 用于读取存储器 802 中的预设程序，按照该程序执行以下过程：

获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，所述第一资源读取请求中携带有发起者对所述 CSE 中的目标资源的访问控制决策的请求信息；

根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，以获取所述目标资源对应的访问控制策略，所述第二资源读取请求中携带对所述目标资源的访问控制策略的请求信息；

根据获取的所述访问控制策略确定所述发起者对所述目标资源的访问控制决策，并向所述 CSE 返回所述访问控制决策；

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略决策点资源以及所述策略获取点资源分别为对应的访问控制资源下的虚拟资源。

可选地，处理器 801 获取所述目标资源对应的访问控制策略后，确定所述发起者对所述目标资源的访问控制决策之前，对绑定的策略信息点资源发送第三资源读取请求，获取所述访问控制策略对应的属性信息，所述第三资源读取请求中携带对所述访问控制策略的访问控制属性的请求信息；

其中，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

可选地，访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

具体地，处理器 801 在获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之前，

根据所述策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略决策点资源。

具体地，处理器 801 根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

具体地，处理器 801 对绑定的策略信息点资源发送第三资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

具体地，处理器 801 若获取访问控制策略对应的属性信息，则根据所述访问控制策略

以及所述访问控制策略对应的属性信息，确定所述发起者对所述目标资源的访问控制决策。

其中，所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源分别位于不同 CSE 根节点下的访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源中的至少两个位于同一 CSE 根节点下的不同访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源属于同一 CSE 根节点下的同一访问控制资源下。

基于同一发明构思，本申请实施例还提供了一种 CSE，该 CSE 的具体实施可参见上述关于具有 PRP 功能的 CSE2 的描述，重复之处不再赘述，如图 9 所示，该 CSE2 主要包括：

获取模块 901，用于获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求，所述资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息；

处理模块 902，用于获取所述目标资源对应的访问控制策略，并返回给所述 CSE；

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略获取点资源为对应的访问控制资源下的虚拟资源。

其中，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

可选地，所述处理模块 902 还用于：

在所述获取模块获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

基于同一发明构思，本申请实施例还提供了一种 CSE，该 CSE 的具体实施可参见上述关于具有 PRP 功能的 CSE2 的描述，重复之处不再赘述，如图 10 所示，该 CSE 主要包括处理器 1001 和存储器 1002，其中，存储器 1002 中保存有预设程序，处理器 1001 用于读取存储器 1002 中的预设程序，按照该程序执行以下过程：

获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求，所述资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息；

获取所述目标资源对应的访问控制策略，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略获取点资源为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

具体地，处理器 1001 在获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

基于同一发明构思，本申请实施例还提供了一种 CSE，该 CSE 的具体实施可参见上述关于具有 PIP 功能的 CSE3 的描述，重复之处不再赘述，如图 11 所示，该 CSE3 主要包括:

获取模块 1101，用于获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求，所述资源读取请求中携带对访问控制策略的访问控制属性的请求信息;

处理模块 1102，用于获取所述访问控制策略对应的属性信息，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

具体地，所述处理模块还用于:

在所述获取模块获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

基于同一发明构思，本申请实施例还提供了一种 CSE，该 CSE 的具体实施可参见上述关于具有 PIP 功能的 CSE3 的描述，重复之处不再赘述，如图 12 所示，该 CSE 主要包括处理器 1201 和存储器 1202，其中，存储器 1202 中保存有预设程序，处理器 1201 用于读取存储器 1202 中的预设程序，按照该程序执行以下过程:

获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求，所述资源读取请求中携带对访问控制策略的访问控制属性的请求信息;

获取所述访问控制策略对应的属性信息，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略信息点资源为

对应的访问控制资源下的虚拟资源。

可选地，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

具体地，处理器 1201 在获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

基于上述技术方案，本申请实施例中，通过在 CSE 根资源下定义普通资源访问控制资源，在访问控制资源下定义策略决策点资源和/或策略获取点资源，并且定义策略决策点资源为触发 PDP 处理过程的虚拟资源，定义策略获取点资源为触发 PRP 处理过程的虚拟资源，从而通过对访问控制资源下的策略决策点资源的资源读取请求，触发具备 PDP 功能的 CSE 通过读取绑定的策略获取点资源获取目标资源的访问控制策略，根据获取的访问控制策略对目标资源的访问请求进行访问控制决策。

进一步地，在访问控制资源下定义策略信息点资源，并定义策略信息点资源为触发 PIP 处理过程的虚拟资源，具备 PDP 功能的 CSE 通过对绑定的策略信息点资源的读取请求，触发访问控制策略的属性信息的获取过程，使得能够结合访问控制策略及其属性信息进行访问控制决策。

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、一种访问控制方法，其特征在于，包括:

获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，所述第一资源读取请求中携带有发起者对所述 CSE 中的目标资源的访问控制决策的请求信息;

根据所述第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，以获取所述目标资源对应的访问控制策略，所述第二资源读取请求中携带对所述目标资源的访问控制策略的请求信息;

根据获取的所述访问控制策略，确定所述发起者对所述目标资源的访问控制决策，并向所述 CSE 返回所述访问控制决策;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略决策点资源以及所述策略获取点资源分别为对应的访问控制资源下的虚拟资源。

2、如权利要求 1 所述的方法，其特征在于，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

3、如权利要求 2 所述的访问控制方法，其特征在于，所述获取所述目标资源对应的访问控制策略后，确定所述发起者对所述目标资源的访问控制决策之前，所述方法还包括:

对绑定的策略信息点资源发送第三资源读取请求，获取所述访问控制策略对应的属性信息，所述第三资源读取请求中携带对所述访问控制策略的访问控制属性的请求信息;

其中，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

4、如权利要求 2 所述的方法，其特征在于，所述获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之前，所述方法还包括:

根据所述策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略决策点资源。

5、如权利要求 2 所述的方法，其特征在于，所述根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取所述目标资源对应的访问控制策略之前，所述方法还包括:

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

6、如权利要求 3 所述的方法，其特征在于，所述对绑定的策略信息点资源发送第三资源读取请求之后，获取所述访问控制策略对应的属性信息之前，所述方法还包括:

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述CSE访问所述策略信息点资源。

7、如权利要求 3 所述的方法，其特征在于，所述确定所述发起者对所述目标资源的访问控制决策，包括:

根据所述访问控制策略以及所述访问控制策略对应的属性信息，确定所述发起者对所述目标资源的访问控制决策。

8、如权利要求 3 所述的方法，其特征在于，所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源分别位于不同 CSE 根节点下的访问控制资源下;

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源中的至少两个位于同一 CSE 根节点下的不同访问控制资源下;

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源属于同一 CSE 根节点下的同一访问控制资源下。

9、一种获取访问控制策略的方法，其特征在于，包括:

获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求，所述资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息;

获取所述目标资源对应的访问控制策略，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略获取点资源为对应的访问控制资源下的虚拟资源。

10、如权利要求 9 所述的方法，其特征在于，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

11、如权利要求 10 所述的方法，其特征在于，所示获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求之后，获取所述目标资源对应的访问控制策略之前，所述方法还包括:

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述CSE访问所述策略获取点资源。

12、一种获取访问控制属性的方法，其特征在于，包括:

获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求，所述资源读取请求中携带对访问控制策略的访问控制属性的请求信息;

获取所述访问控制策略对应的属性信息，并返回给所述 CSE;

其中，所述访问控制资源为所属的CSE根资源下的普通资源，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

13、如权利要求 12 所述的方法，其特征在于，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

14、如权利要求 13 所述的方法，其特征在于，所述获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求之后，获取所述访问控制策略对应的属性信息之前，所述方法还包括:

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述CSE 访问所述策略信息点资源。

15、一种公共服务实体 CSE，其特征在于，包括:

第一获取模块，用于获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求，所述第一资源读取请求中携带有发起者对所述 CSE 中的目标资源的访问控制决策的请求信息;

第二获取模块，用于根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，获取所述目标资源对应的访问控制策略，所述第二资源读取请求中携带对所述目标资源的访问控制策略的请求信息;

处理模块，用于根据获取的所述访问控制策略确定所述发起者对所述目标资源的访问控制决策，并向所述 CSE 返回所述访问控制决策;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略决策点资源以及所述策略获取点资源分别为对应的访问控制资源下的虚拟资源。

16、如权利要求 15 所述的 CSE，其特征在于，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

17、如权利要求 16 所述的 CSE，其特征在于，还包括第三获取模块，用于所述第二获取模块获取所述目标资源对应的访问控制策略后，所述处理模块确定所述发起者对所述目标资源的访问控制决策之前，对绑定的策略信息点资源发送第三资源读取请求，获取所述访问控制策略对应的属性信息，所述第三资源读取请求中携带对所述访问控制策略的访问控制属性的请求信息;

其中，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

18、如权利要求 16 所述的 CSE，其特征在于，所述处理模块还用于:

在所述第一获取模块获取公共服务实体 CSE 对访问控制资源下的策略决策点资源的第一资源读取请求之后，在所述第二获取模块根据第一资源读取请求发送对绑定的策略获

取点资源的第二资源读取请求之前，

根据所述策略决策点资源所属的访问控制资源指定的访问控制策略，确定允许所述CSE访问所述策略决策点资源。

19、如权利要求16所述的CSE，其特征在于，所述第二获取模块还用于：

根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述CSE访问所述策略获取点资源。

20、如权利要求17所述的CSE，其特征在于，所述第三获取模块还用于：

对绑定的策略信息点资源发送第三资源读取请求之后，获取所述访问控制策略对应的属性信息之前，

根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述CSE访问所述策略信息点资源。

21、如权利要求17所述的CSE，其特征在于，所述处理模块具体用于：

根据所述访问控制策略以及所述访问控制策略对应的属性信息，确定所述发起者对所述目标资源的访问控制决策。

22、如权利要求17所述的CSE，其特征在于，所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源分别位于不同CSE根节点下的访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源中的至少两个位于同一CSE根节点下的不同访问控制资源下；

或者，

所述策略决策点资源、所述策略获取点资源以及所述策略信息点资源属于同一CSE根节点下的同一访问控制资源下。

23、一种公共服务实体CSE，其特征在于，包括：

获取模块，用于获取公共服务实体CSE对访问控制资源下的策略获取点资源的资源读取请求，所述资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息；

处理模块，用于获取所述目标资源对应的访问控制策略，并返回给所述CSE；

其中，所述访问控制资源为所属的CSE根资源下的普通资源，所述策略获取点资源为对应的访问控制资源下的虚拟资源。

24、如权利要求 23 所述的 CSE，其特征在于，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

25、如权利要求 24 所述的 CSE，其特征在于，所述处理模块还用于:

在所述获取模块获取公共服务实体 CSE 对访问控制资源下的策略获取点资源的资源读取请求之后，获取所述目标资源对应的访问控制策略之前，

根据所述策略获取点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略获取点资源。

26、一种公共服务实体 CSE，其特征在于，包括:

获取模块，用于获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求，所述资源读取请求中携带对访问控制策略的访问控制属性的请求信息;

处理模块，用于获取所述访问控制策略对应的属性信息，并返回给所述 CSE;

其中，所述访问控制资源为所属的 CSE 根资源下的普通资源，所述策略信息点资源为对应的访问控制资源下的虚拟资源。

27、如权利要求 26 所述的 CSE，其特征在于，所述访问控制资源具有普通资源的通用属性，还具有指定访问控制策略的公共属性。

28、如权利要求 27 所述的 CSE，其特征在于，所述处理模块还用于:

在所述获取模块获取公共服务实体 CSE 对访问控制资源下的策略信息点资源的资源读取请求之后，获取所述访问控制策略对应的属性信息之前，根据所述策略信息点资源所属的访问控制资源指定的访问控制策略，确定允许所述 CSE 访问所述策略信息点资源。

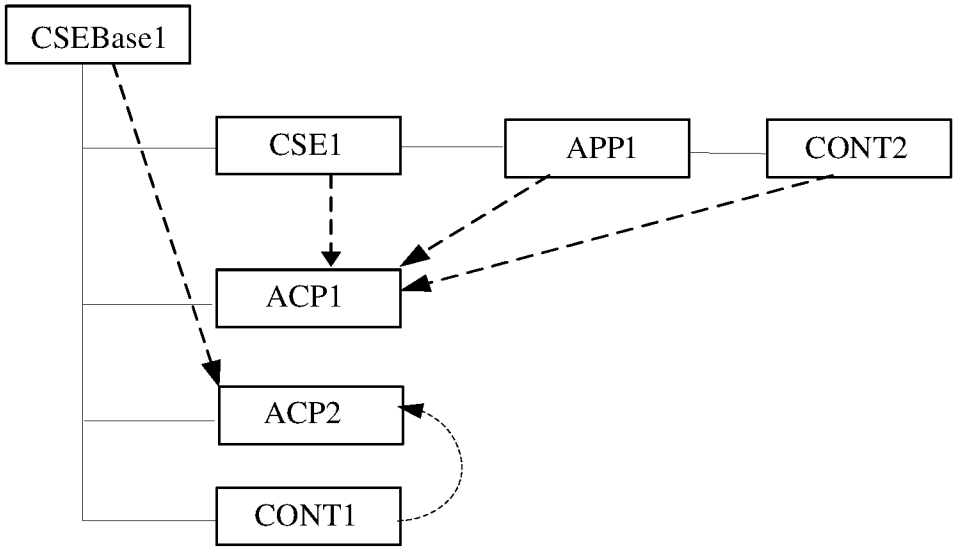
CSEBase1
CSE1
APP1
CONT2
ACP1
ACP2
CONT1

图 1

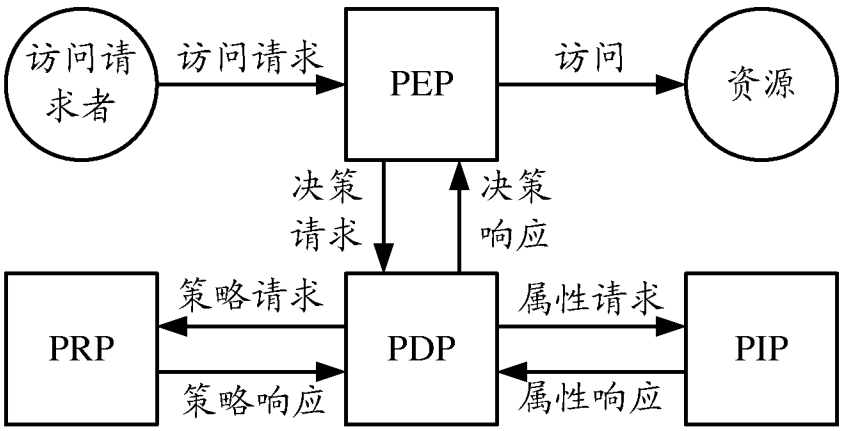
访问请求者
访问请求
PEP
访问
资源
决策请求
决策响应
PRP
策略请求
策略响应
PDP
属性请求
属性响应
PIP

图 2

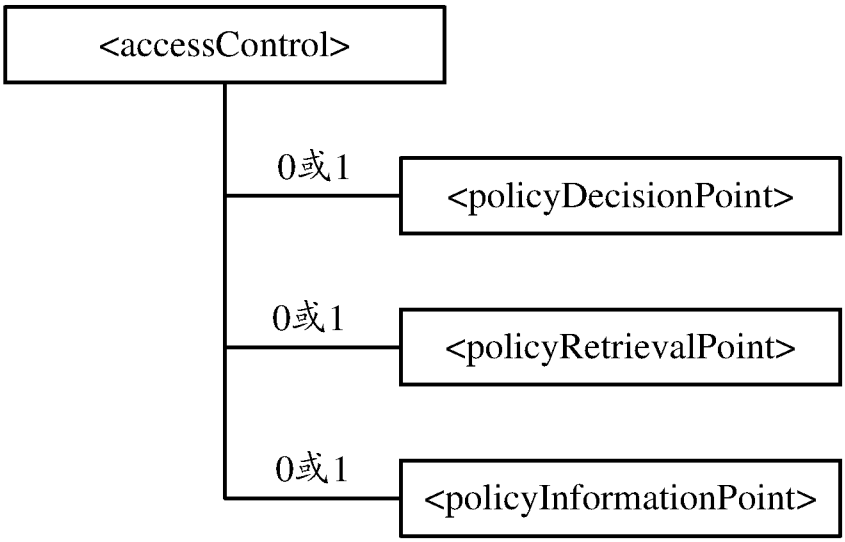
<accessControl>
0或1
<policyDecisionPoint>
0或1
<policyRetrievalPoint>
0或1
<policyInformationPoint>

图 3

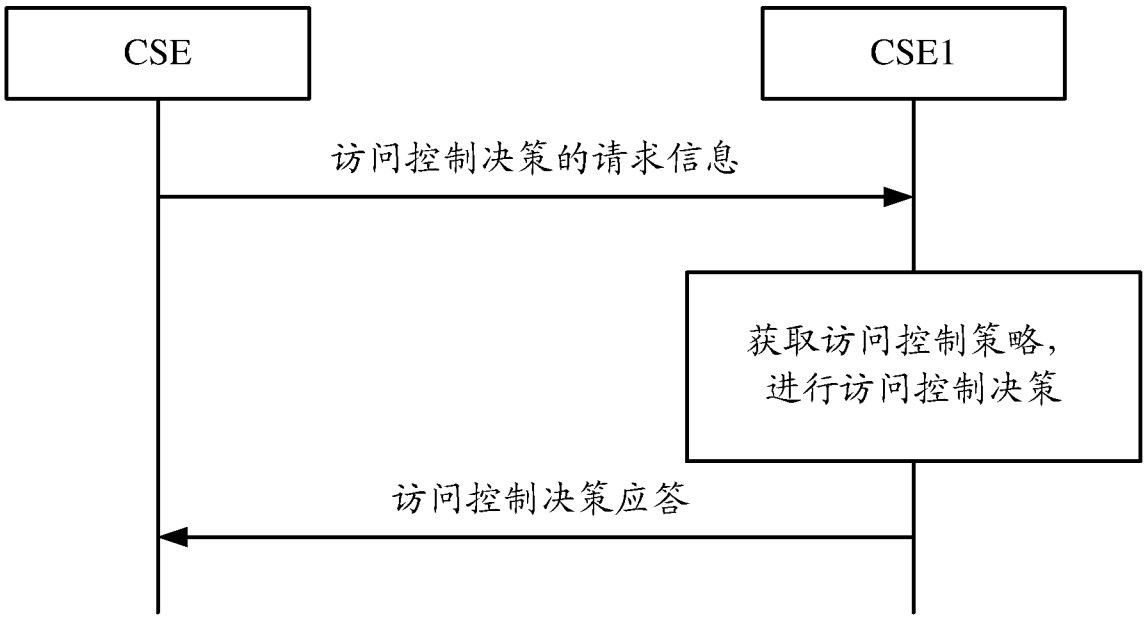
CSE
CSE1
访问控制决策的请求信息
获取访问控制策略，
进行访问控制决策
访问控制决策应答

图 4a

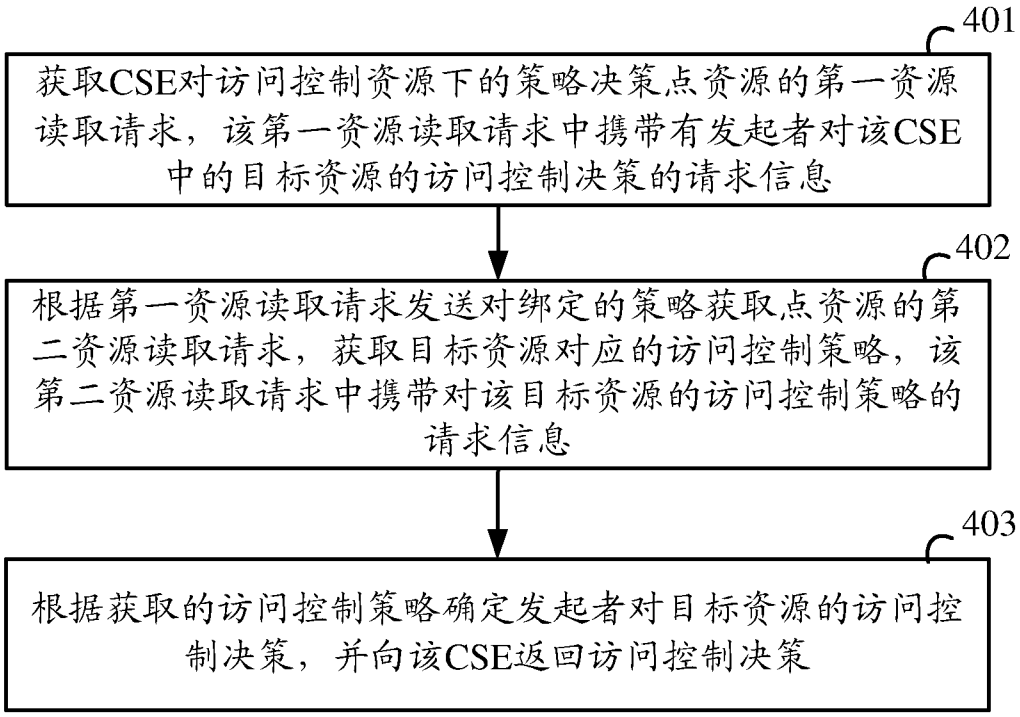
401
获取CSE对访问控制资源下的策略决策点资源的第一资源读取请求，该第一资源读取请求中携带有发起者对该CSE中的目标资源的访问控制决策的请求信息
402
根据第一资源读取请求发送对绑定的策略获取点资源的第二资源读取请求，获取目标资源对应的访问控制策略，该第二资源读取请求中携带对该目标资源的访问控制策略的请求信息
403
根据获取的访问控制策略确定发起者对目标资源的访问控制决策，并向该CSE返回访问控制决策

图 4b

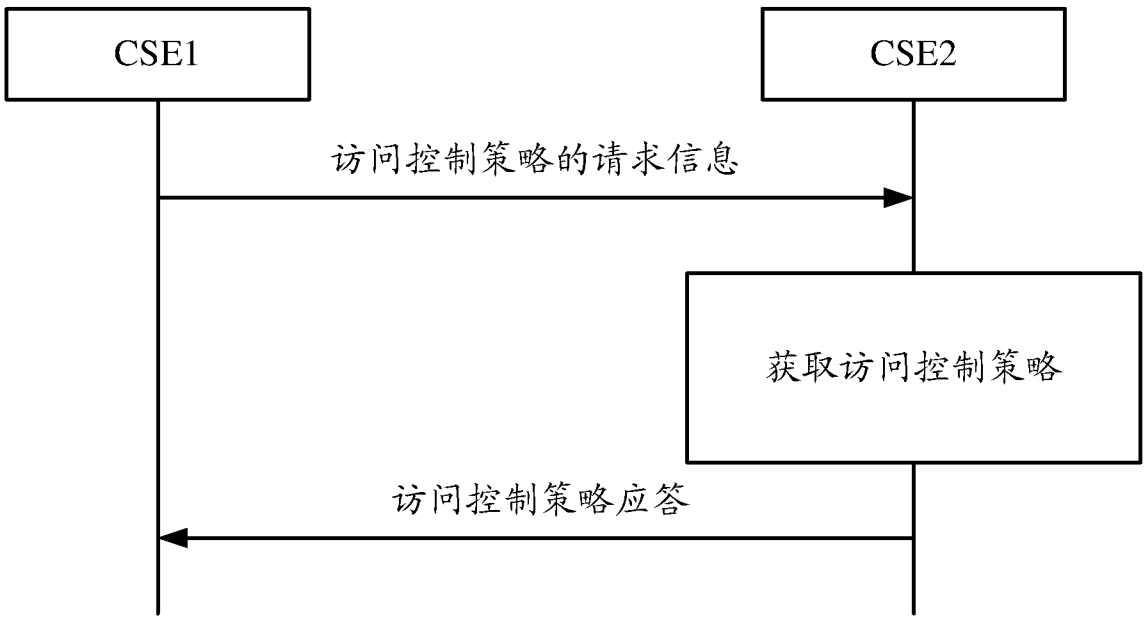
CSE1
CSE2
访问控制策略的请求信息
获取访问控制策略
访问控制策略应答

图 5a

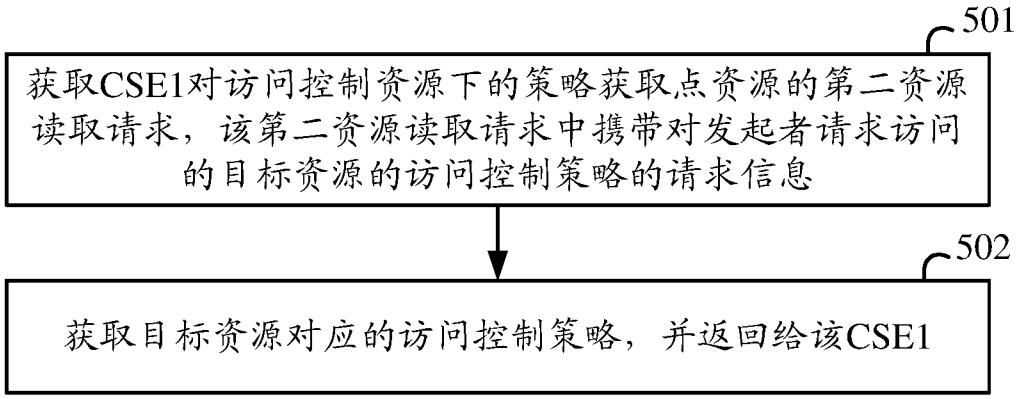
501
获取CSE1对访问控制资源下的策略获取点资源的第二资源读取请求，该第二资源读取请求中携带对发起者请求访问的目标资源的访问控制策略的请求信息
502
获取目标资源对应的访问控制策略，并返回给该CSE1

图 5b

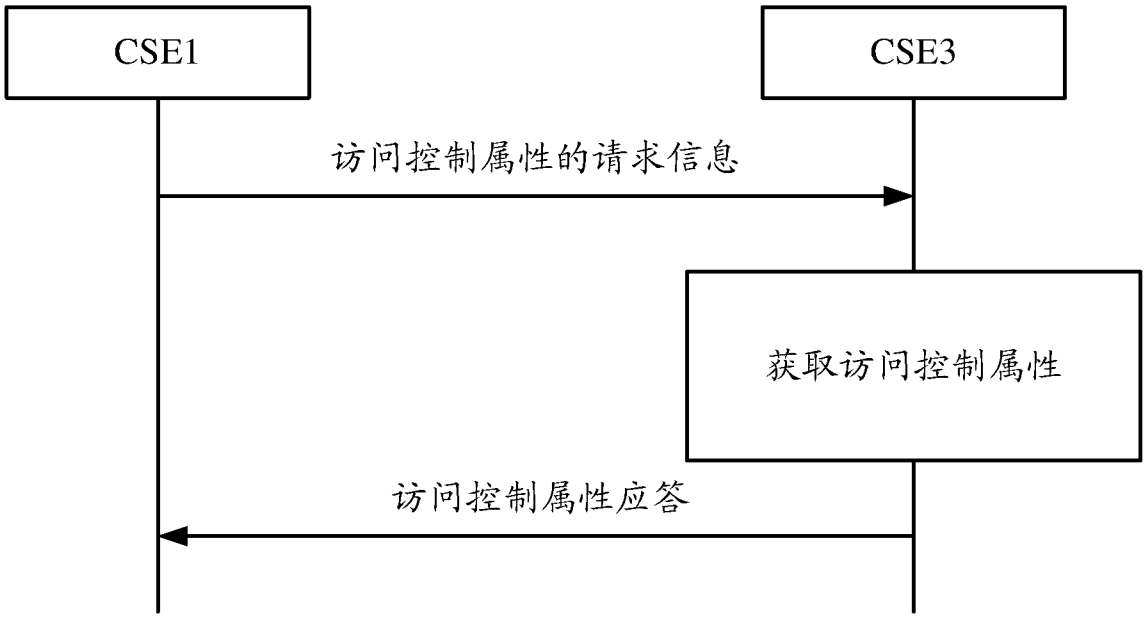
CSE1
CSE3
访问控制属性的请求信息
获取访问控制属性
访问控制属性应答

图 6a

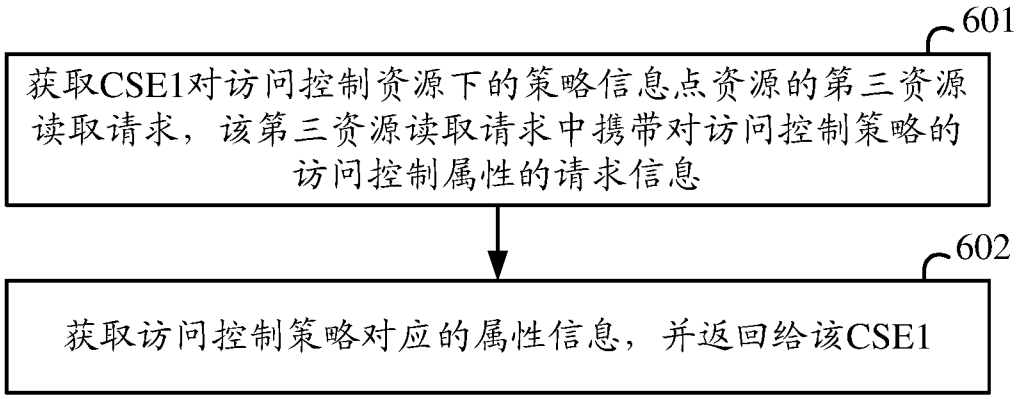
601
获取CSE1对访问控制资源下的策略信息点资源的第三资源读取请求，该第三资源读取请求中携带对访问控制策略的访问控制属性的请求信息
602
获取访问控制策略对应的属性信息，并返回给该CSE1

图 6b

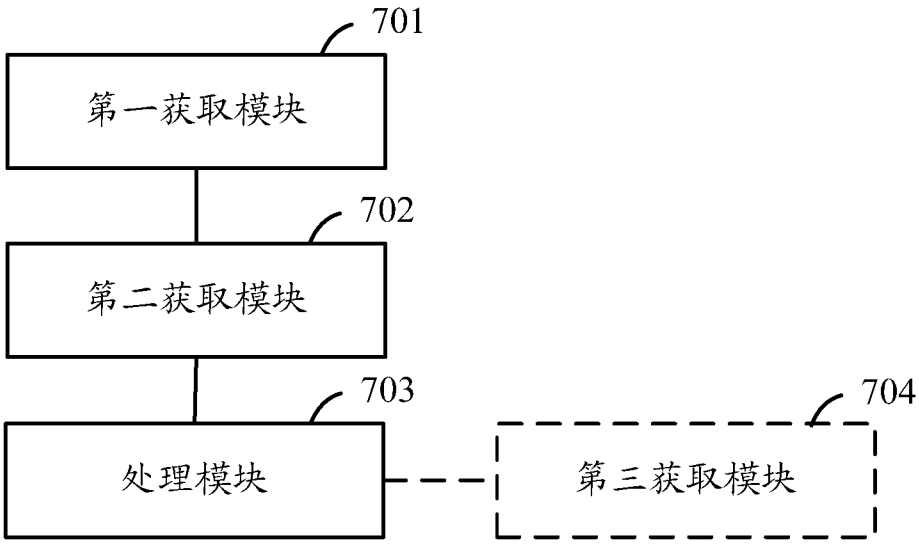
701
第一获取模块
702
第二获取模块
703
处理模块
704
第三获取模块

图 7



图 8

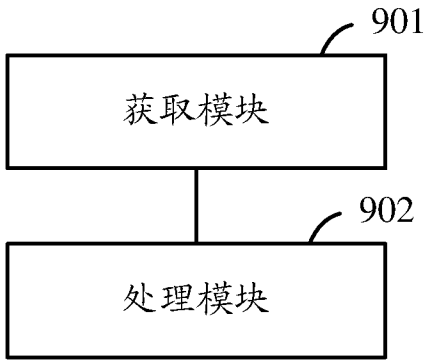

图 9



图 10

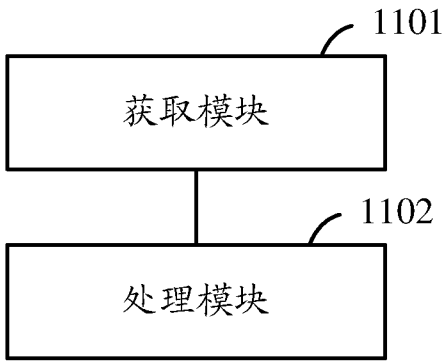

图 11



图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/072206

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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; H04Q; H04W; G06F

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)

CPRSABS, CNABS, CNTXT, CNKI, VEN, USTXT: oneM2M, access control, machine to machine, M2M, policy, decision, resource request, attribute, PEP, PDP, PRP, PIP, CSE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	OneM2M., "Security solutions", OneM2M technical specification, TS-0003-v1.0.1, 30 January 2015 (30.01.2015), section 6.2.2, figures 6.2.2-1 and 6.2.2-2, and page 88, paragraph 1	1-28
A	OneM2M., "Functional Architecture", OneM2M technical specification, TS-0001-v1.6.1, 30 January 2015 (30.01.2015), section 9.2	1-28
A	US 2015033311 A1 (CONVIDA WIRELESS LLC.), 29 January 2015 (29.01.2015), the whole document	1-28

☐ 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
17 March 2016 (17.03.2016)	**15 April 2016 (15.04.2016)**
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 **ZHANG, Xin** Telephone No.: (86-10) **62089567**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/072206

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US 2015033311 A1	29 January 2015	WO 2015013645 A1	29 January 2015
		WO 2015013685 A1	29 January 2015
		US 2015033312 A1	29 January 2015

国际检索报告

国际申请号
PCT/CN2016/072206

A. 主题的分类

H04L 29/06(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; H04Q; H04W; G06F

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）)

CPRSABS,CNABS,CNTXT,CNKI,VEN,USTXT:访问控制，接入控制，机器对机器，策略，决策，资源请求，属性，oneM2M，access control，machine to machine，M2M，policy，decision，resource request，attribute，PEP，PDP，PRP，PIP，CSE

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
A	OneM2M. ″“Security solutions”″ OneM2M technical specification， TS-0003-v1.0.1，2015年 1月 30日 (2015-01-30)， 第6.2.2节，图6.2.2-1，6.2.2-2，第88页第1段	1-28
A	OneM2M. ″“Functional Architecture”″ OneM2M technical specification， TS-0001-v1.6.1，2015年 1月 30日 (2015-01-30)， 第9.2节	1-28
A	US 2015033311 A1 (CONVIDA WIRELESS LLC.) 2015年 1月 29日 (2015-01-29) 全文	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	国际检索报告邮寄日期
2016年 3月 17日	2016年 4月 15日

ISA/CN的名称和邮寄地址	受权官员
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	张鑫
传真号 (86-10)62019451	电话号码 (86-10)62089567

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/072206

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)
US 2015033311 A1	2015年 1月 29日	WO 2015013645 A1	2015年 1月 29日
		WO 2015013685 A1	2015年 1月 29日
		US 2015033312 A1	2015年 1月 29日