(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106714075 B
(45)授权公告日 2020.06.26

(21)申请号 201510486108.0

(22)申请日 2015.08.10

(65)同一申请的已公布的文献号
申请公布号 CN 106714075 A

(43)申请公布日 2017.05.24

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 张尧烨

(51)Int.Cl.
H04W 4/70(2018.01)
H04L 29/06(2006.01)
H04W 12/06(2009.01)

(56)对比文件
CN 102065430 A,2011.05.18,
CN 104618366 A,2015.05.13,
CN 102835137 A,2012.12.19,
US 2015039896 A1,2015.02.05,
US 9077709 B1,2015.07.07,

审查员 张晨曦

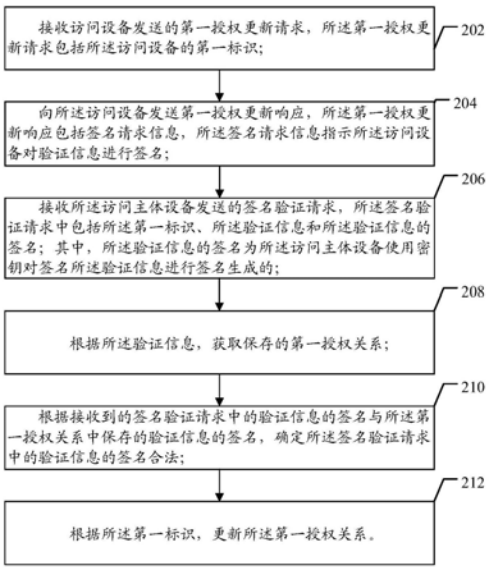
权利要求书6页 说明书39页 附图8页

(54)发明名称

一种处理授权的方法和设备

(57)摘要

本发明涉及一种授权方法和设备。公开了授权服务器接收包括访问设备第一标识的授权更新请求;向访问设备发送包括签名请求信息的授权更新响应,该签名请求信息指示访问设备对验证信息进行签名;接收访问设备发送的签名验证请求,签名验证请求中包括第一标识、验证信息和验证信息的签名;验证信息的签名为访问设备对验证信息进行签名生成;根据验证信息,获取保存的授权关系;确定所述签名验证请求中的验证信息的签名合法;根据第一标识,更新授权关系。通过本发明方法,当访问设备在M2M系统中的标识发生变化时,M2M系统可以通过判断验证信息的签名是否合法,来识别访问设备的身份,进而更新已有的授权关系,使得访问设备能够继续使用已有的授权关系。



CN 106714075 B

1.一种机器通信中处理授权的方法,其特征在于,包括:

授权服务器接收访问设备发送的第一授权更新请求,所述第一授权更新请求包括所述访问设备的第一标识;

所述授权服务器向所述访问设备发送第一授权更新响应,所述第一授权更新响应包括签名请求信息,其中所述签名请求信息用于指示所述访问设备对验证信息进行签名;

所述授权服务器接收所述访问设备发送的签名验证请求,所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名;其中,所述验证信息的签名为所述访问设备使用密钥对所述验证信息进行签名生成的;

所述授权服务器根据所述验证信息,获取保存的第一授权关系;

所述授权服务器根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名,确定所述签名验证请求中的验证信息的签名合法;

所述授权服务器根据所述第一标识,更新所述第一授权关系。

2.如权利要求1所述的方法,其特征在于,在所述接收访问设备发送的第一授权更新请求之前,所述方法还包括:

资源服务器接收所述访问设备发送资源访问请求,所述资源访问请求包括所述第一标识和被访问资源标识;

所述资源服务器根据所述第一标识和所述被访问资源标识,确定所述访问设备没有访问所述被访问资源标识对应的资源的权限;

所述资源服务器拒绝所述访问设备的对所述被访问资源标识对应的资源的访问请求,并向所述访问设备发送包括重定向地址的资源访问响应,其中所述重定向地址为授权服务器的授权更新端口地址,以便于所述访问设备根据所述授权更新端口地址,向所述授权服务器发送所述第一授权更新请求。

3.如权利要求1所述的方法,其特征在于,所述根据所述第一标识,更新所述第一授权关系,具体为:

所述授权服务器将所述第一授权关系中的第二标识更改为所述第一标识,其中,所述第二标识为所述访问设备使用过的标识。

4.如权利要求1-3任一所述方法,其特征在于,在所述接收访问设备发送的第一授权更新请求之前,所述方法还包括:

所述授权服务器对所述访问设备访问所述被访问资源标识对应的资源进行初始授权。

5.如权利要求4所述的方法,其特征在于,所述验证信息为所述访问设备保存的所述第二标识,所述签名验证请求中进一步还包括所述第一标识的签名,其中所述第一标识的签名为所述访问设备使用所述密钥对所述第一标识进行签名生成的;在所述确定所述签名验证请求中的验证信息的签名合法之后,所述方法进一步还包括:

所述授权服务器将所述第一授权关系中保存的验证信息的签名更改为所述第一标识的签名。

6.如权利要求5所述的方法,其特征在于,所述对所述访问设备访问所述被访问资源标识对应的资源进行初始授权,具体为:

所述授权服务器向资源服务器发送资源创建请求,所述资源创建请求包括预设的访问控制策略和所述被访问资源标识,其中,所述预设的访问控制策略包括所述第二标识;

所述授权服务器接收所述资源服务器发送的资源创建响应，所述资源创建响应指示所述资源服务器成功创建所述访问控制策略资源且将所述访问控制策略资源与所述被访问资源标识对应的资源进行绑定；

所述授权服务器向所述访问设备发送签名请求，所述签名请求指示所述访问设备对所述第二标识进行签名；

所述授权服务器接收所述访问设备发送的签名响应，所述签名响应包括所述第二标识的签名；

所述授权服务器保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述第二标识的签名和所述被访问资源标识的对应关系。

7.如权利要求3所述的方法，其特征在于，在所述根据所述第一标识，更新所述第一授权关系之后，所述方法还包括：

所述授权服务器向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述第二标识和所述被访问资源标识。

8.如权利要求4所述的方法，其特征在于，所述验证信息为授权凭证，所述第一授权更新请求还包括所述授权凭证，在所述向所述访问设备发送第一授权更新响应之前，所述方法还包括：

所述授权服务器根据所述授权凭证，确定存在包含所述授权凭证的所述第一授权关系，且所述第一授权关系中绑定的访问设备标识不是所述第一标识。

9.如权利要求8所述的方法，其特征在于，所述对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：

所述授权服务器接收所述访问设备的授权请求，所述授权请求包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；

所述授权服务器当根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限时，生成所述授权凭证；

所述授权服务器向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；

所述授权服务器接收所述资源服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；

所述授权服务器向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；

所述授权服务器接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名为所述访问设备对所述授权凭证使用所述密钥签名生成的；

所述授权服务器保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系。

10.如权利要求8-9任一所述的方法，其特征在于，在所述根据所述第一标识，更新所述第一授权关系之后，所述方法还包括：

所述授权服务器向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述授权凭证和所述被访问资源标识。

11.一种机器通信中处理授权的方法,其特征在于,包括:

接收访问设备发送的第一资源访问请求,所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证;

根据所述授权凭证,确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系,且所述第二授权关系中绑定的访问设备标识不是所述第一标识;

向所述访问设备发送第一资源访问响应,所述第一资源访问响应包括签名请求信息,所述签名请求信息指示所述访问设备对所述授权凭证进行签名;

接收所述访问设备发送的第二资源访问请求,所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识;其中,所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生成的;

向授权服务器发送签名数据请求,所述签名数据请求包含所述授权凭证;

接收所述授权服务器发送的签名数据响应,所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名;

根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名,确定所述第二资源访问请求中的授权凭证的签名合法;

根据所述第一标识,更新所述第二授权关系。

12.如权利要求11所述的方法,其特征在于,在所述根据所述第一标识,更新所述第二授权关系之后,所述方法还包括:

向所述访问设备发送第二资源访问响应,所述第二资源访问响应包括所述被访问资源标识对应的资源。

13.如权利要求11所述的方法,其特征在于,所述根据所述第一标识,更新所述第二授权关系,具体为:

将所述第二授权关系中的第二标识更改为所述第一标识,其中,所述第二标识为所述访问设备使用过的标识。

14.如权利要求13所述的方法,其特征在于,在所述接收访问设备发送的第一资源访问请求之前,所述方法还包括:

所述授权服务器接收所述访问设备发送授权请求,所述授权请求中包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息;

所述授权服务器根据所述认证信息,确定所述用户具有访问所述被访问资源标识对应的资源的权限,生成所述授权凭证,并向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求,所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识;

所述资源服务器将所述第二标识、所述授权凭证和所述被访问资源标识的对应关系保存为第二授权关系,并向所述授权服务器发送的授权绑定响应,所述授权绑定响应包含绑定成功的指示信息;

所述授权服务器向所述访问设备发送授权响应,所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息;

所述授权服务器接收所述访问设备发送的签名绑定请求,所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识,其中,所述授权凭

证的签名是所述访问设备使用所述密钥对所述授权凭证进行签名生成的；

所述授权服务器将所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系保存为第一授权关系。

15.如权利要求11-14任一所述的方法，其特征在于，在所述确定所述第二资源访问请求中的授权凭证的签名合法之后，所述方法还包括：

向所述授权服务器发送第三授权更新请求，所述第三授权更新请求包括所述授权凭证和所述第一标识；

接收所述授权服务器发送的第三授权更新响应，所述第三授权更新响应包括所述授权服务器授权更新成功的指示信息。

16.一种机器通信中的授权服务器，其特征在于，包括：

接收模块，用于接收访问设备发送的第一授权更新请求，所述第一授权更新请求包括所述访问设备的第一标识；

发送模块，用于向所述访问设备发送第一授权更新响应，所述第一授权更新响应包括签名请求信息，其中所述签名请求信息用于指示所述访问设备对验证信息进行签名；

所述接收模块，还用于接收所述访问设备发送的签名验证请求，所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名；其中，所述验证信息的签名为所述访问设备使用密钥对所述验证信息进行签名生成的；

获取模块，用于根据所述接收模块接收到的签名验证请求中的验证信息，获取保存的第一授权关系；

确定模块，用于根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名，确定所述签名验证请求中的验证信息的签名合法；

更新模块，用于根据所述第一标识，更新所述第一授权关系。

17.如权利要求16所述的授权服务器，其特征在于，所述更新模块用于根据所述第一标识，更新所述第一授权关系，具体为：

将所述第一授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

18.如权利要求16或17所述的授权服务器，其特征在于，所述授权服务器还包括：

初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权。

19.如权利要求18所述的授权服务器，其特征在于，所述验证信息为所述访问设备保存的所述第二标识，所述签名验证请求中进一步还包括所述第一标识的签名，其中所述第一标识的签名为所述访问设备使用所述密钥对所述第一标识进行签名生成的；

所述更新模块，还用于将所述第一授权关系中保存的验证信息的签名更改为所述第一标识的签名。

20.如权利要求19所述的授权服务器，其特征在于，其特征在于，所述初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：

向资源服务器发送资源创建请求，所述资源创建请求包括预设的访问控制策略和所述被访问资源标识，其中，所述预设的访问控制策略包括所述第二标识；

接收所述资源服务器发送的资源创建响应，所述资源创建响应指示所述资源服务器成

功创建所述访问控制策略资源且将所述访问控制策略资源与所述被访问资源标识对应的资源进行绑定；

向所述访问设备发送签名请求，所述签名请求指示所述访问设备对所述第二标识进行签名；

接收所述访问设备发送的签名响应，所述签名响应包括所述第二标识的签名；

保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述第二标识的签名和所述被访问资源标识的对应关系。

21.如权利要求17所述的授权服务器，其特征在于，所述发送模块，还用于在根据所述第一标识，更新所述第一授权关系之后，向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识和所述被访问资源标识。

22.如权利要求18所述的授权服务器，其特征在于，所述验证信息为授权凭证，所述第一授权更新请求还包括所述授权凭证，

所述确定模块，还用于在所述向所述访问设备发送第一授权更新响应之前，根据所述授权凭证，确定存在包含所述授权凭证的所述第一授权关系，且所述第一授权关系中绑定的设备标识不是所述第一标识。

23.如权利要求22所述的授权服务器，其特征在于，所述初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：

接收所述访问设备的授权请求，所述授权请求包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；

当根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限时，生成所述授权凭证；

向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；

接收所述资源服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；

向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；

接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名为所述访问设备对所述授权凭证使用所述密钥签名生成的；

保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系。

24.如权利要求22-23任一所述的授权服务器，其特征在于，所述发送模块，还用于在根据所述第一标识，更新所述第一授权关系之后，向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述授权凭证和所述被访问资源标识。

25.一种机器通信中的资源服务器，其特征在于，包括：

接收模块，用于接收访问设备发送的第一资源访问请求，所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证；

确定模块，用于根据所述授权凭证，确定存在包含所述授权凭证与所述被访问资源标

识的第二授权关系，且所述第二授权关系中绑定的设备标识不是所述第一标识；

发送模块，用于向所述访问设备发送第一资源访问响应，所述第一资源访问响应包括签名请求信息，所述签名请求信息指示所述访问设备对所述授权凭证进行签名；

所述接收模块，还用于接收所述访问设备发送的第二资源访问请求，所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识；其中，所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生成的；

所述发送模块，还用于向授权服务器发送签名数据请求，所述签名数据请求包含所述授权凭证；

所述接收模块，还用于接收所述授权服务器发送的签名数据响应，所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名；

所述确定模块，还用于根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名，确定所述第二资源访问请求中的授权凭证的签名合法；

更新模块，用于根据所述第一标识，更新所述第二授权关系。

26.如权利要求25所述的资源服务器，其特征在于，所述发送模块还用于，在根据所述第一标识，更新所述第二授权关系之后，向所述访问设备发送第二资源访问响应，所述第二资源访问响应包括所述被访问资源标识对应的资源。

27.如权利要求25或26所述的资源服务器，其特征在于，所述更新模块，用于根据所述第一标识，更新所述第二授权关系，具体为：

将所述第二授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

28.如权利要求27所述的资源服务器，其特征在于，所述接收模块，还用于接收授权服务器对所述访问设备访问所述被访问资源标识对应的资源进行初始授权后发送的授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；

存储模块，用于将所述第二标识、所述授权凭证和所述被访问资源标识的对应关系保存为第二授权关系。

一种处理授权的方法和设备

技术领域

[0001] 本发明涉及机器通信技术领域,尤其涉及一种处理授权的方法和设备。

背景技术

[0002] 机器通信(Machine-to-Machine Communications,M2M)是一种以机器智能交互为核心的、网络化的应用与服务。它通过在机器内部嵌入无线或有线通信模块以及应用处理逻辑,实现用户对监控、指挥调度、数据采集和测量等方面的信息化需求。M2M系统中,各种M2M设备,如各种传感器,直接经过M2M网关接入到M2M业务平台,从而实现各种M2M业务。例如电力抄表、智能家居等。通过M2M业务平台所提供的业务能力,可以获取M2M设备采集的数据,或对M2M设备进行控制和管理。

[0003] 在现有的M2M规范中,采用RESTful(Representational State Transfer)的架构,任何M2M设备、M2M网关或M2M业务平台以及它们所提供的业务能力,都可以被抽象为资源并且具有唯一的资源标识,即URI(Uniform Resource Identifier)。每个被访问资源都可以设置相应的访问权限,通过引用一个访问控制策略资源,如ACP(accessControlPolicy)资源等来实现系统中对被访问资源的访问控制功能。

[0004] 被访问资源所属的设备收到访问设备对资源的请求消息时,根据该被访问资源的访问控制策略标识accessControlPolicyID去获取相应的访问控制策略资源,访问控制策略资源中的每一条访问控制规则都可以看作一个三元组,<accessControlOriginators、accessControlContexts、accessControlOperations>,其中accessControlOriginator表示具有操作权限的访问设备标识(可能是某个CSE-ID、AE-ID或者是serviceProvider domain,也可能是All);accessControlOperations表示该条规则所允许的操作权限(可能包括Retrieve、Create、Update、Delete、Discovery和Notify中的一个或者多个);accessControlContexts是可选的,定义了accessControlOriginator具有accessControlOperations中规定的操作权限的条件,例如在某个时间范围内,每个地理区域内等等。作为一种可选方式,accessControlContexts的取值可以为空,即不对操作权限的条件进行限制和描述。被访问资源所属的设备根据获取到的访问控制策略资源中的accessControlOriginator属性中是否包含访问设备标识,以及accessControlOperations属性中是否包含访问设备对被访问资源请求的操作 来判断访问设备是否具有对被访问资源的访问权限。只有两个条件都满足时才表示访问设备通过了访问控制权限检查。

[0005] 在oneM2M系统中,访问设备标识用来标识访问设备的身份。具体的,访问设备可以是应用实体(Application Entity,AE)或者公共服务实体(Common Service Entity,CSE)。访问设备标识由访问设备注册的公共服务实体,即Registrar CSE(下文中统称注册服务器),进行分配。现有技术中,当同一个访问设备在不同的注册服务器上注册或者其他原因,导致其被分配的访问设备标识发生变化时,该访问设备将无法使用M2M系统中原先为该访问设备配置的访问控制策略。以AE为例,当某AE在CSE1上注册本地ID时被分配了AE-ID1;当该AE离线后又在CSE2上注册时被分配了AE-ID2。显然此时AE在M2M系统中的标识发生了变

化，原有的与AE-ID1相关联的授权关系(如ACP)都对新的AE-ID2无法适用，需要由管理员为AE-ID2重新设定或添加ACP，这极大地影响了M2M设备的业务连续性和用户体验。例如，在一个M2M系统中，某个资源X对应的ACP资源如下表所示：

[0006]

accessControlOriginators	accessControlContexs	accessControlOperation
AE-ID1	/	Retriseve/Create

[0007] 由该表可知，访问设备标识AE-ID1对应的访问设备对该资源X拥有Retrieve或者Create的访问权限。但是当该访问设备由于某些原因，如在其他注册服务器上注册时，导致M2M系统分配的访问设备标识变为AE-ID2时，该访问设备将无法适用该ACP资源，进而无法获得对该资源X的Retrieve或者Create的访问权限。

发明内容

[0008] 本发明提供了一种处理授权的方法和设备，以解决当访问设备的标识发生变化时，该访问设备无法使用原有授权关系的技术问题。

[0009] 第一方面，本发明提供一种机器通信中处理授权的方法，包括：接收访问设备发送的第一授权更新请求，所述第一授权更新请求包括所述访问设备的第一标识；向所述访问设备发送第一授权更新响应，所述第一授权更新响应包括签名请求信息，所述签名请求信息指示所述访问设备对验证信息进行签名；接收所述访问设备发送的签名验证请求，所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名；其中，所述验证信息的签名为所述访问 设备使用密钥对所述验证信息进行签名生成的；根据所述验证信息，获取保存的第一授权关系；根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名，确定所述签名验证请求中的验证信息的签名合法；根据所述第一标识，更新所述第一授权关系。

[0010] 结合第一方面，在第一方面的第一种可能的实现方式中，在所述接收访问设备发送的第一授权更新请求之前，所述方法还包括：资源服务器接收所述访问设备发送资源访问请求，所述资源访问请求包括所述第一标识和被访问资源标识；所述资源服务器根据所述第一标识和所述被访问资源标识，确定所述访问设备没有访问所述被访问资源标识对应的资源的权限；所述资源服务器拒绝所述访问设备的对所述被访问资源标识对应的资源的访问请求，并向所述访问设备发送包括重定向地址的资源访问响应，其中所述重定向地址为授权服务器的授权更新端口地址，以便于所述访问设备根据所述授权更新端口地址，向所述授权服务器发送所述第一授权更新请求。

[0011] 结合第一方面或第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述根据所述第一标识，更新所述第一授权关系，具体为：将所述第一授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

[0012] 结合第一方面或第一方面的第一种可能的实现方式或第一方面的第二种可能的实现方式，在第一方面的第三种可能的实现方式中，在所述接收访问设备发送的第一授权更新请求之前，所述方法还包括：对所述访问设备访问所述被访问资源标识对应的资源进行初始授权。

[0013] 结合第一方面的第三种可能的实现方式，在第一方面的第四种可能的实现方式中，所述验证信息为所述访问设备保存的所述第二标识，所述签名验证请求中进一步还包

括所述第一标识的签名，其中所述第一标识的签名为所述访问设备使用所述密钥对所述第一标识进行签名生成的；在所述确定所述签名验证请求中的验证信息的签名合法之后，所述方法进一步还包括：将所述第一授权关系中保存的验证信息的签名更改为所述第一标识的签名。

[0014] 结合第一方面的第四种可能的实现方式，在第一方面的第五种可能的实现方式中，所述对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：向资源服务器发送资源创建请求，所述资源创建请求包括预设的 访问控制策略和所述被访问资源标识，其中，所述预设的访问控制策略包括所述第二标识；接收所述资源服务器发送的资源创建响应，所述资源创建响应指示所述资源服务器成功创建所述访问控制策略资源且将所述访问控制策略资源与所述被访问资源标识对应的资源进行绑定；向所述访问设备发送签名请求，所述签名请求指示所述访问设备对所述第二标识进行签名；接收所述访问设备发送的签名响应，所述签名响应包括所述第二标识的签名；保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述第二标识的签名和所述被访问资源标识的对应关系。

[0015] 结合一方面的第二种至第五种可能的实现方式中的任一种实现方式，在第一方面的第六种可能的实现方式中，在所述根据所述第一标识，更新所述第一授权关系之后，所述方法还包括：向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述第二标识和所述被访问资源标识。

[0016] 结合第一方面的第三种可能的实现方式，在第一方面的第七种可能的实现方式中，所述验证信息为授权凭证，所述第一授权更新请求还包括所述授权凭证，在所述向所述访问设备发送第一授权更新响应之前，所述方法还包括：根据所述授权凭证，确定存在包含所述授权凭证的所述第一授权关系，且所述第一授权关系中绑定的访问设备标识不是所述第一标识。

[0017] 结合第一方面的第七种可能的实现方式，在第一方面的第八种可能的实现方式中，所述对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：接收所述访问设备的授权请求，所述授权请求包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；当根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限时，生成所述授权凭证；向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；接收所述资源服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名为所述访问设备对所述授权凭证使用所述密钥签名生成的；保存所 述第一授权关系，所述第一授权关系包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系。

[0018] 结合第一方面的第七种或者第八种可能的实现方式，在第一方面的第九种可能的实现方式中，在所述根据所述第一标识，更新所述第一授权关系之后，所述方法还包括：向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述授权

凭证和所述被访问资源标识。

[0019] 第二方面，提供了一种机器通信中处理授权的方法，包括：接收访问设备发送的第一资源访问请求，所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证；根据所述授权凭证，确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系，且所述第二授权关系中绑定的访问设备标识不是所述第一标识；向所述访问设备发送第一资源访问响应，所述第一资源访问响应包括签名请求信息，所述签名请求信息指示所述访问设备对所述授权凭证进行签名；接收所述访问设备发送的第二资源访问请求，所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识；其中，所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生成的；向授权服务器发送签名数据请求，所述签名数据请求包含所述授权凭证；接收所述授权服务器发送的签名数据响应，所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名；根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名，确定所述第二资源访问请求中的授权凭证的签名合法；根据所述第一标识，更新所述第二授权关系。

[0020] 结合第二方面，在第二方面的第一种可能的实现方式中，在所述根据所述第一标识，更新所述第二授权关系之后，所述方法还包括：向所述访问设备发送第二资源访问响应，所述第二资源访问响应包括所述被访问资源标识对应的资源。

[0021] 结合第二方面或第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述根据所述第一标识，更新所述第二授权关系，具体为：将所述第二授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

[0022] 结合第二方面的第二种可能的实现方式，在第二方面的第三种可能的实现 方式中，在所述接收访问设备发送的第一资源访问请求之前，所述方法还包括：所述授权服务器接收所述访问设备发送授权请求，所述授权请求中包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；所述授权服务器根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限，生成所述授权凭证，并向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；所述资源服务器将所述第二标识、所述授权凭证和所述被访问资源标识的对应关系保存为第二授权关系，并向所述授权服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；所述授权服务器向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；所述授权服务器接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名是所述访问设备使用所述密钥对所述授权凭证进行签名生成的；所述授权服务器将所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系保存为第一授权关系。

[0023] 结合第二方面以及第二方面的第一种至第第三种可能的实现方式中的任一种可能的实现方式，在第二方面的第四种实现方式中，在所述确定所述第二资源访问请求中的授权凭证的签名合法之后，所述方法还包括：向所述授权服务器发送第三授权更新请求，所述第三授权更新请求包括所述授权凭证和所述第一标识；接收所述授权服务器发送的第三

授权更新响应，所述第三授权更新响应包括所述授权服务器授权更新成功的指示信息。

[0024] 第三方面，还提供了一种机器通信中的授权服务器，包括：接收模块，用于接收访问设备发送的第一授权更新请求，所述第一授权更新请求包括所述访问设备的第一标识；发送模块，用于向所述访问设备发送第一授权更新响应，所述第一授权更新响应包括签名请求信息，所述签名请求信息指示所述访问设备对验证信息进行签名；所述接收模块，还用于接收所述访问设备发送的签名验证请求，所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名；其中，所述验证信息的签名为所述访问设备使用密钥对所述验证信息进行签名生成的；获取模块，用于根据所述接收模块接收到的签名验证请 求中的验证信息，获取保存的第一授权关系；确定模块，用于根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名，确定所述签名验证请求中的验证信息的签名合法；更新模块，用于根据所述第一标识，更新所述第一授权关系。

[0025] 结合第三方面，在第三方面的第一种可能的实现方式中，所述更新模块用于根据所述第一标识，更新所述第一授权关系，具体为：将所述第一授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

[0026] 结合第三方面或第三方面的第一种可能的实现方式，在第三方面的第二种可能的实现方式中，所述授权服务器还包括：初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权。

[0027] 结合第三方面的第二种可能的实现方式，在第三方面的第三种可能的实现方式中，所述验证信息为所述访问设备保存的所述第二标识，所述签名验证请求中进一步还包括所述第一标识的签名，其中所述第一标识的签名为所述访问设备使用所述密钥对所述第一标识进行签名生成的；所述更新模块，还用于将所述第一授权关系中保存的验证信息的签名更改为所述第一标识的签名。

[0028] 结合第三方面的第三种可能的实现方式，在第三方面的第四种可能的实现方式中，所述初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：向资源服务器发送资源创建请求，所述资源创建请求包括预设的访问控制策略和所述被访问资源标识，其中，所述预设的访问控制策略包括所述第二标识；接收所述资源服务器发送的资源创建响应，所述资源创建响应指示所述资源服务器成功创建所述访问控制策略资源且将所述访问控制策略资源与所述被访问资源标识对应的资源进行绑定；向所述访问设备发送签名请求，所述签名请求指示所述访问设备对所述第二标识进行签名；接收所述访问设备发送的签名响应，所述签名响应包括所述第二标识的签名；保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述第二标识的签名和所述被访问资源标识的对应关系。

[0029] 结合三方面的第一种至第四种可能的实现方式中的任一种实现方式，在第三方面的第五种可能的实现方式中，所述发送模块，还用于在根据所述第一标识，更新所述第一授权关系之后，向资源服务器发送第二授权更新请求，所述 第二授权更新请求包括所述第一标识和所述被访问资源标识。

[0030] 结合第三方面的第二种可能的实现方式，在第三方面的第六种可能的实现方式中，所述验证信息为授权凭证，所述第一授权更新请求还包括所述授权凭证，所述确定模块，还用于在所述向所述访问设备发送第一授权更新响应之前，根据所述授权凭证，确定存

在包含所述授权凭证的所述第一授权关系，且所述第一授权关系中绑定的设备标识不是所述第一标识。

[0031] 结合第三方面的第六种可能的实现方式，在第三方面的第七种可能的实现方式中，所述初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：接收所述访问设备的授权请求，所述授权请求包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；当根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限时，生成所述授权凭证；向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；接收所述资源服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名为所述访问设备对所述授权凭证使用所述密钥签名生成的；保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系。

[0032] 结合第三方面的第六种或者第七种可能的实现方式，在第三方面的第八种可能的实现方式中，所述发送模块，还用于在根据所述第一标识，更新所述第一授权关系之后，向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述授权凭证和所述被访问资源标识。

[0033] 第四方面，还提供了一种机器通信中的资源服务器，包括：接收模块，用于接收访问设备发送的第一资源访问请求，所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证；确定模块，用于根据所述授权凭证，确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系，且所述第二授权关系中绑定的设备标识不是所述第一标识；发送模块，用于向所述访问设备发送第一资源访问响应，所述第一资源访问响应包括签名请求信 息，所述签名请求信息指示所述访问设备对所述授权凭证进行签名；所述接收模块，还用于接收所述访问设备发送的第二资源访问请求，所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识；其中，所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生成的；所述发送模块，还用于向授权服务器发送签名数据请求，所述签名数据请求包含所述授权凭证；所述接收模块，还用于接收所述授权服务器发送的签名数据响应，所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名；所述确定模块，还用于根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名，确定所述第二资源访问请求中的授权凭证的签名合法；更新模块，用于根据所述第一标识，更新所述第二授权关系。

[0034] 结合第四方面，在第四方面的第一种可能的实现方式中，所述发送模块还用于，在根据所述第一标识，更新所述第二授权关系之后，向所述访问设备发送第二资源访问响应，所述第二资源访问响应包括所述被访问资源标识对应的资源。

[0035] 结合第四方面或第四方面的第一种可能的实现方式，在第四方面的第二种可能的

实现方式中，所述更新模块，用于根据所述第一标识，更新所述第二授权关系，具体为：将所述第二授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

[0036] 结合第四方面的第二种可能的实现方式，在第四方面的第三种可能的实现方式中，所述接收模块，还用于接收授权服务器对所述访问设备访问所述被访问资源标识对应的资源进行初始授权后发送的授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；存储模块，用于将所述第二标识、所述授权凭证和所述被访问资源标识的对应关系保存为第二授权关系。

[0037] 根据本发明提供的技术方案，当访问设备由于某种原因导致自身在M2M系统中的标识发生变化时，M2M系统可以通过判断验证信息的签名是否合法，即通过比较访问设备发送的验证信息的签名和授权服务器保存的第一授权关系中的验证信息签名是否相同，来识别访问设备的身份，进而更新已有的授权关系，使得访问设备能够继续使用已有的授权关系，进而实现无缝的资源访问，保证了M2M系统的业务连续性。

附图说明

[0038] 图1为本本发明一实施例所提供的授权更新的系统框图；

[0039] 图2为本发明一实施例所提供一种机器通信中授权方法的流程图；

[0040] 图3为本发明一实施例提供的又一种处理授权的方法的流程图；

[0041] 图4为本发明一实施例提供的一种基于ACP授权架构的初始授权的流程图；

[0042] 图5为本发明一实施例提供的一种基于ACP授权架构的授权更新的流程图；

[0043] 图6为本发明一实施例提供的一种基于Oauth授权架构的初始授权流程图；

[0044] 图7为本发明一实施例提供的一种基于Oauth授权架构的授权更新流程图；

[0045] 图8为本发明一实施例提供的另一种基于Oauth授权架构的授权更新流程图；

[0046] 图9为本发明一实施例提供的一种授权服务器的结构示意图；

[0047] 图10为本发明一实施例提供的又一种授权服务器的结构示意图；

[0048] 图11为本发明一实施例提供的一种资源服务器的结构示意图；

[0049] 图12为本发明一实施例提供的又一种资源服务器的结构示意图。

具体实施方式

[0050] 为使本发明的目的、技术方案和优点更加清楚，下面结合附图对本发明具体实施例作进一步的详细描述。为了全面理解本发明，在以下详细描述中提到了众多具体细节。但是本领域技术人员应该理解，本发明可以无需这些具体细节实现。在其他实例中，不详细描述公知的方法、过程、组件和电路等，以免造成实施例不必要地模糊。显然，以下所描述的实施例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他实施例，都属于本发明保护的范围。

[0051] 需要说明的是在本发明实施例当中描述的授权服务器和资源服务器的相关功能可以由同一个设备的不同功能模块实现，也可以由不同的设备分别实现，本发明对此不作限定。

[0052] 此外，在下文描述的一些流程中，包含了按照特定顺序出现的多个操作，但是应该清楚了解，这些操作可以不按照其在本文中出现的顺序来执行或并行执行，操作的序号如101、102等，仅仅是用于区分开各个不同的操作，序号本身不代表任何的执行顺序。另外，这些流程可以包括更多或更少的操作，并且这些操作可以按顺序执行或并行执行。需要说明的是，本文中 的“第一”、“第二”等描述，是用于区分不同的消息、设备、模块等，不代表先后顺序，也不限定“第一”和“第二”是不同的类型。

[0053] 图1是依据本发明一实施例所提供的授权更新的系统框图。该系统包含多个通信设备，通过有线或者无线通信网络相互通信。其中，

[0054] 访问设备102：可以为应用实体(Application Entity，AE)，也可以为公共服务实体(Common Service Entity，CSE)，通过注册服务器104接入M2M系统并能访问M2M系统中其他实体所管理的资源。

[0055] 注册服务器104：为M2M系统中的访问设备102提供注册服务的公共服务实体(Registrar CSE，R-CSE)，负责为访问设备102提供注册并为其分配实体标识(Application Entity-Identifier，AE-ID/Common Service Entity-Identifier，CSE-ID)，作为对访问设备的身份标识。

[0056] 授权服务器106：可以是驻留在基础设施节点(Infrastructure Node，IN)中的公共服务主体(Infrastructure Node-CSE，IN-CSE)，也可以是单独运行并与IN-CSE相连的授权服务器(Authorization Server，AS)，负责保存M2M系统中的授权关系，维护访问设备、访问设备的身份验证信息、验证信息的签名以及被访问资源标识之间的对应关系。

[0057] 资源服务器108：一般为被访问资源所在节点的公共服务主体(Hosting CSE，H-CSE)，维护本地资源的对应授权关系，并根据访问设备102发送的资源访问请求执行访问控制决策，根据决策结果向访问设备返回资源访问响应。

[0058] 需要说明的是，本发明中涉及两个授权关系，其中一个由授权服务器维护，称为第一授权关系，另一个由资源服务器维护，称为第二授权关系。此外，本发明还涉及两个访问设备标识，即第一标识和第二标识，其中第二标识为访问设备使用过的标识，并且在授权服务器和资源服务器上维护了与第二标识相关的授权关系，在下面的发明实施例中以AE-ID1标记第二标识；第一标识为访问设备重新注册后获取的标识，在下面的发明实施例中以AE-ID2标记第一标识。当访问设备以第一标识访问资源时，按照现有技术，访问设备的访问请求将被拒绝且访问结束。本发明介绍了一种将所述第一授权关系和第二授权关系中的第二标识更新为第一标识的方法，使得访问设备可以继续使用原有的授权关系获得资源的访问权限。这种方法使得用户通过访问设备可以无缝的访问相应的资源，而不需要重新创建相应的授权关系，这为访问设备访问资源带来很多便利。例如，基于token的授权关系建立，参考 Oauth2.0相关协议可知，需要资源所有者进行在线授权，当资源所有者不在线，则M2M系统将无法对访问设备进行重新授权，进而使得用户无法访问资源。

[0059] 本发明实施例中，在授权服务器106中保存访问设备标识、被访问资源标识、访问设备验证信息以及验证信息的签名对应关系的授权关系。具体的，当为访问设备102初始授权时，该授权服务器106从访问设备102处获取验证信息的签名并与对应的访问设备标识、验证信息、被访问资源标识一起保存于授权关系中。授权服务器106可在收到访问设备102发送的签名验证请求后确认访问设备102的原身份，也可在收到资源服务器108发送的签名

请求时将验证信息的签名发送给资源服务器108，由资源服务器108确认访问设备102的原身份。

[0060] 资源服务器108为资源所在节点的公共服务实体，该资源服务器108可能驻留在M2M系统中的中间节点(Middle Node，MN)、基础设施节点(Infrastructure Node，IN)或者应用服务节点(Application Service Node，ASN)中。本发明在资源服务器108原有的访问控制决策模块中，新增了授权更新处理的判断逻辑，用于当对访问设备102发送的资源访问请求进行访问控制决策，结果为未许可时，启动本地授权更新或将资源访问请求重定向到授权服务器106以进行授权更新。此外，本发明一个实施例中，资源服务器108从授权服务器106获取验证信息的签名，并从访问设备102处获取对应的验证信息的签名以完成访问设备原身份确认。当完成访问设备102原身份确认后授权服务器106主动更新本地授权关系，或在授权服务器106的指令下更新本地授权关系。

[0061] 访问设备102可能是应用实体(AE)也可能是公共服务实体(CSE)，并通过注册服务器104接入M2M系统。本发明在访问设备102中新增签名模块，用于在接收到授权服务器106或资源服务器108的签名请求时使用密钥对相应的信息进行签名，并将该信息的签名返回给授权服务器106或资源服务器108。需要说明的是，访问设备进行签名使用的密钥可以是设备出厂设置的，也可以是其他方式生成的，本发明对该密钥的具体形式不做限定。

[0062] 注册服务器104可能为MN-CSE，也可能为IN-CSE或ASN-CSE，负责给访问设备102分配标识。

[0063] 此外，需要说明的是，在M2M系统中，资源服务器108和授权服务器106可以作为一个设备中的两个功能模块，也可以作为M2M系统中两个单独运行 的设备。当资源服务器108和授权服务器106作为一个设备中的两个功能模块时，资源服务器108和授权服务器106之间的信息交互则作为设备内部信息的交互。本发明对资源服务器108和授权服务器106的具体表现形式不做限定，示范性地，本发明在下面的实施例中将资源服务器108和授权服务器106作为两个单独运行的设备进行介绍。

[0064] 图1的授权架构只是给出了访问设备标识变化的一个例子(AE先后在注册服务器R-CSE1和R-CSE2上注册，被分配了不同的AE-ID)，根据访问设备标识分配方式的不同，访问设备标识在其他情况下也可能发生变化(如在同一个注册服务器上注册，但是访问设备的原标识已被分配给其他实体等)。此外，资源服务器108和注册服务器104可能直连到IN-CSE，也可能经其他CSE多跳转接到IN-CSE，本发明对M2M系统的具体结构不做限定。

[0065] 以下结合附图详细说明本申请涉及的授权方法、装置及系统的实现。

[0066] 图2为本发明提供的一种机器通信中授权方法的流程图，包括：

[0067] 步骤202：接收访问设备发送的第一授权更新请求，所述第一授权更新请求包括所述访问设备的第一标识；

[0068] 可选的，所述第一授权更新请求的目的地址可以为授权服务器的授权更新端口，即所述授权服务器通过所述授权更新端口接收所述访问设备发送的第一授权更新请求。可选的，所述第一授权更新请求还包括被访问资源标识。

[0069] 步骤204：向所述访问设备发送第一授权更新响应，所述第一授权更新响应包括签名请求信息，所述签名请求信息指示所述访问设备对验证信息进行签名；

[0070] 可选的，所述签名请求信息可以是一个签名标志位，当签名标志位取值“1”时，表

示需要所述访问设备对验证信息进行签名;当签名标志位取值“2”时,表示需要所述访问设备对验证信息以及访问设备的当前标识进行签名。

[0071] 步骤206:接收所述访问设备发送的签名验证请求,所述签名验证请求中包括所述第一标识、验证信息和所述验证信息的签名;其中,所述验证信息的签名为所述访问设备使用密钥对所述验证信息进行签名生成的;

[0072] 步骤208:根据所述验证信息,获取保存的第一授权关系;

[0073] 步骤210:根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名,确定所述签名验证请求中的验证信息的签名合法;

[0074] 具体的,授权服务器获取所述第一授权关系中保存的验证信息的签名,并 将所述第一授权关系中保存的验证信息的签名与接收到的签名验证请求中的验证信息的签名进行比较,当两者相同时,则确定所述签名验证请求中的验证信息的签名合法。

[0075] 步骤212:根据所述第一标识,更新所述第一授权关系。

[0076] 具体的,当确定所述签名验证请求中的验证信息的签名合法后,授权服务器确定所述访问设备的标识已经更新为第一标识,所以授权服务器需要对本地保存的与该访问设备相关的授权关系进行更新。

[0077] 可选的,根据所述第一标识,更新所述第一授权关系,具体为:将所述第一授权关系中的第二标识更改为所述第一标识,其中,所述第二标识为所述访问设备使用过的标识;或者删除所述第一授权关系,并创建一个新的授权关系,所述新的授权关系包括所述第一标识、所述第一授权关系中的验证信息和所述第一授权关系中的验证信息的签名。

[0078] 具体的,在步骤202之前,所述方法还包括:资源服务器接收所述访问设备发送资源访问请求,所述资源访问请求包括所述第一标识和被访问资源标识;所述资源服务器根据所述第一标识和所述被访问资源标识,确定所述访问设备没有访问所述被访问资源标识对应的资源的权限;所述资源服务器拒绝所述访问设备的对所述被访问资源标识对应的资源的访问请求,并向所述访问设备发送包括重定向地址的资源访问响应,其中所述重定向地址为授权服务器的授权更新端口地址,以便于所述访问设备根据所述授权更新端口地址,向所述授权服务器发送所述第一授权更新请求。

[0079] 具体的,在所述接收访问设备发送的第一请求消息之前,所述方法还包括:授权服务器对所述访问设备访问所述被访问资源标识对应的资源进行初始授权。

[0080] 当M2M系统采用ACP授权架构时,所述验证信息可以是所述第二标识。当所述验证信息系为第二标识时,在授权服务器上保存有所述第二标识、所述第二标识的签名以及被访问资源标识相对应的第一授权关系。在资源服务器上保存有所述第二标识和所述被访问资源标识相对应的第二授权关系。具体的,当所述验证信息为所述第二标识时,所述签名验证请求中进一步还包括所述第一标识的签名,其中所述第一标识的签名为所述访问设备使用密钥对所述第一标识进行签名生成的;在步骤210所述确定所述签名验证请求中的验证信息的签名合法之后,所述方法进一步还包括:将所述第一授权关系中保存的验证信息的签名更改为所述第一标识的签名。所述授权服务器对所述访问设备访问所 述被访问资源进行初始授权,具体为:向所述资源服务器发送资源创建请求,所述资源创建请求包括预设的访问控制策略和所述被访问资源标识,其中,所述预设的访问控制策略包括所述第二标识,以便于所述资源服务器根据所述预设的访问控制策略设置访问控制策略资源并将所述

访问控制策略资源与所述被访问资源标识对应的资源进行绑定，其中，所述访问控制策略资源包括所述第二标识；接收所述资源服务器发送的资源创建响应，所述资源创建响应指示所述资源服务器成功创建所述访问控制策略资源且将所述访问控制策略资源与所述被访问资源标识对应的资源进行绑定；向所述访问设备发送签名请求，所述签名请求指示所述访问设备对所述第二标识进行签名；接收所述访问设备发送的签名响应，所述签名响应包括所述第二标识的签名；保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述第二标识的签名和所述被访问资源标识的对应关系。需要说明的是，管理员在授权服务器上创建预设的访问控制策略的一种可能的实现方式是，访问设备102在注册服务器104上进行注册，生成注册信息，所述注册信息包括注册服务器分配的标识，如所述第二标识，和体现所述访问设备特征的信息，如访问设备的IP地址、MAC地址或者设备描述信息等内容，管理员登录授权服务器后获取所述注册信息，并根据所述注册信息创建访问控制策略，即创建一个允许某个访问设备访问某个资源的规则。进一步的，在步骤212之后，所述方法进一步还包括更新资源服务器上保存的第二授权关系，具体的，在所述根据所述第一标识，更新所述第一授权关系之后，所述方法还包括：向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述第二标识和所述被访问资源标识，以便于资源服务器根据所述第二标识和所述被访问资源标识获取保存的第二授权关系，并将保存的第二授权关系中的第二标识更新为所述第一标识，可选的，授权服务器接收所述资源服务器发送的第二授权更新响应，所述第二授权更新响应指示授权关系更新成功。

[0081] 需要说明的是，在基于ACP授权架构时，所述验证信息可以由所述授权服务器在接收到访问设备的第一授权更新请求后，通过第一授权更新响应发送给访问设备，或者所述验证信息也可以是保存在访问设备上。示范性的，在本发明的一个实施例中，所述第二标识作为验证信息是保存在访问设备上的，但是本发明对此不作限定。

[0082] 当M2M系统采用Oauth授权架构时，所述验证信息可以是所述授权凭证。在授权服务器上保存有所述第二标识、所述授权凭证、所述授权凭证的签名以 及被访问资源标识相对应的第一授权关系。在资源服务器上保存有所述第二标识、所述授权凭证和所述被访问资源标识相对应的第二授权关系。具体的，当所述验证信息为授权凭证时，所述第一授权更新请求还包括所述授权凭证，在步骤204向所述访问设备发送第一授权更新响应之前，所述方法还包括：根据所述授权凭证，确定存在包含所述授权凭证的所述第一授权关系，且所述第一授权关系中绑定的设备标识不是所述第一标识。

[0083] 所述对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：接收所述访问设备的授权请求，所述授权请求包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；当根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限时，生成所述授权凭证；向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；接收所述资源服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名为所述访问设备对所

述授权凭证使用所述密钥签名生成的;保存所述第一授权关系,所述第一授权关系包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系。进一步的,在步骤212之后,所述方法进一步还包括更新资源服务器上保存的第二授权关系,具体的,在所述根据所述第一标识,更新所述第一授权关系之后,所述方法还包括:向资源服务器发送第二授权更新请求,所述第二授权更新请求包括所述第一标识、所述授权凭证和所述被访问资源标识。以便于资源服务器根据所述授权凭证和所述被访问资源标识获取保存的第二授权关系,并将所述第二授权关系中的第二标识更新为所述第一标识,可选的,授权服务器接收所述资源服务器发送的第二授权更新响应,所述第二授权更新响应指示授权关系更新成功。

[0084] 当资源服务器将保存的第二授权关系中的第二标识更新为所述第一标识之后,所述访问设备即可使用原有的授权关系,实现资源访问。

[0085] 本发明实施例提供了一种机器通信系统中处理授权的方法,当访问设备由于某种原因导致自身在M2M系统中的标识发生变化时,M2M系统可以通过判断验证信息的签名是否合法,即通过比较访问设备发送的验证信息的签名和授 权服务器保存的第一授权关系中的验证信息签名是否相同,来识别访问设备的身份,进而更新已有的授权关系,使得访问设备能够继续使用已有的授权关系,进而实现无缝的资源访问,保证了M2M系统的业务连续性。

[0086] 图3为本发明一实施例提供的又一种处理授权的方法的流程图,包括;

[0087] 步骤302:接收访问设备发送的第一资源访问请求,所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证;

[0088] 步骤304:根据所述授权凭证,确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系,且所述第二授权关系中绑定的设备标识不是所述第一标识;

[0089] 步骤306:向所述访问设备发送第一资源访问响应,所述第一资源访问响应包括签名请求信息,所述签名请求信息指示所述访问设备对所述授权凭证进行签名;

[0090] 步骤308:接收所述访问设备发送的第二资源访问请求,所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识;其中,所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生成的;

[0091] 步骤310:向授权服务器发送签名数据请求,所述签名数据请求包含所述授权凭证;

[0092] 步骤312:接收所述授权服务器发送的签名数据响应,所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名;

[0093] 步骤314:根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名,确定所述第二资源访问请求中的授权凭证的签名合法;

[0094] 具体的,所述资源服务器比较所述授权服务器发送的授权凭证的签名与所述第二资源访问请求中的授权凭证的签名,当两者相同时,则确定所述第二资源访问请求中的授权凭证的签名合法。

[0095] 步骤316:根据所述第一标识,更新所述第二授权关系。

[0096] 其中,根据所述第一标识,更新所述第二授权关系具体为:将所述第二授权关系中的第二标识更改为所述第一标识,其中,所述第二标识为所述访问设备使用过的标识;或者

删除所述第二授权关系，创建一个新的第二授权关系，其中所述新的第二授权关系包括所述第一标识、所述第二授权关系中的授权凭 证和所述被访问资源标识。

[0097] 具体的，在步骤302之前，还存在初始授权流程：所述授权服务器接收所述访问设备发送授权请求，所述授权请求中包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；所述授权服务器根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限，生成所述授权凭证，并向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；所述资源服务器将所述第二标识、所述授权凭证和所述被访问资源标识的对应关系保存为第二授权关系，并向所述授权服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；所述授权服务器向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；所述授权服务器接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名是所述访问设备使用所述密钥对所述授权凭证进行签名生成的；所述授权服务器将所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系保存为第一授权关系。

[0098] 步骤302中，访问设备向资源服务器发送第一资源访问请求后，资源服务器需要对访问设备的访问请求进行决策。只有资源访问请求中的信息与资源服务器保存的第二授权关系完全匹配时，资源服务器才会允许此次请求，并向访问设备返回请求的资源。具体的，所述资源服务器根据第一资源访问请求，确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系，且所述第二授权关系中绑定的设备标识不是所述第一标识，则资源服务器确定访问设备的标识发生变化或者是授权凭证泄露。进一步的，通过步骤306-步骤314，资源服务器根据从访问设备和授权服务器中获取所述授权凭证的签名，确定所述第一标识和所述第二标识都是所述访问设备的标识，进而主动使用所述第一标识更新保存的第二授权关系。

[0099] 进一步的，在所述根据所述第一标识，更新所述第二授权关系之后，所述方法还包括：向所述访问设备发送第二资源访问响应，所述第二资源访问响应包括所述被访问资源标识对应的资源。从而访问设备利用原有的授权关系，实现了资源访问的目的。

[0100] 可选的，在所述确定所述第二资源访问请求中的授权凭证的签名合法之后， 所述方法还包括：向所述授权服务器发送第三授权更新请求，所述第三授权更新请求包括所述授权凭证和所述第一标识；接收所述授权服务器发送的第三授权更新响应，所述第三授权更新响应包括所述授权服务器授权更新成功的指示信息。

[0101] 本发明实施例提供了一种机器通信系统中处理授权的方法，当访问设备由于某种原因导致自身在M2M系统中的标识发生变化时，M2M系统可以通过判断验证信息的签名是否合法，即通过比较访问设备发送的验证信息的签名和授权服务器保存的第一授权关系中的验证信息签名是否相同，来识别访问设备的身份，进而更新已有的授权关系，使得访问设备能够继续使用已有的授权关系，进而实现无缝的资源访问，保证了M2M系统的业务连续性。

[0102] 以下分别基于ACP授权架构和Oauth授权架构介绍图2、图3所示的授权方法的具体实现过程。

[0103] M2M系统采用ACP授权架构对访问设备访问资源进行授权时，所述验证信息可以是所述访问设备的第二标识。具体的，在图4和图5所述的实施例中，将提供一种M2M系统中基于ACP授权架构的授权流程，包括初始授权和授权更新两个子流程，其中所述初始授权是指访问设备标识变化前，授权服务器为访问设备获取验证信息的签名并生成授权关系的过程。

[0104] 参阅图4，图4为本发明提供的一种基于ACP授权架构的初始授权的流程图，在本实施例中访问设备为一个应用实体AE，但是本发明实施例对访问设备的具体形式并不做限定，所述方法包括：

[0105] 步骤402-步骤404：AE向注册服务器1(R-CSE1)发送注册请求，注册服务器1为AE分配标识AE-ID1；

[0106] 步骤406：系统管理员(Admin)在授权服务器(AS)上为AE创建ACP；

[0107] 具体的，在基于ACP授权架构下，通常Admin手动为AE设置ACP。在M2M系统中，ACP作为资源被创建并与对应的资源进行绑定。所述绑定方式为在对应资源的访问控制策略标识accessControlPolicyIDs属性值中添加该ACP资源标识(ACP ID)。正如背景技术中所介绍，在M2M系统中ACP资源的每一个规则都是一个三元组<accessControlOriginators、accessControlContexts、accessControlOperations>。在本发明实施例中，Admin为AE创建ACP，具体可以为：设置accessControlOriginators参数为“/CSE0005/CAE0001”，其中，/CSE0005/CAE0001即为AE-ID1。其他参数与本发明方案无关，因此本发明实施例不做限定。

[0108] 步骤408：授权服务器向资源服务器(H-CSE)发送ACP资源创建请求；

[0109] 所述ACP资源创建请求包含Admin为AE创建的ACP的所有属性数据和对应绑定的资源标识。例如，授权服务器向资源服务器发送的ACP资源创建请求可以为：

[0110] POST http://m2m.things.com/CSE0003 HTTP/1.1

[0111] From:http://authzserver.things.com

[0112] Content-type:application/onem2m-resource+json

[0113] {“ResourceType”:“accessControlPolicy”,

[0114] “privileges.accessControlOriginators”:“/CSE0005/CAE0001”,

[0115] “res_uri”:“/CSE0003/resource1”}

[0116] 其中，“http://m2m.things.com/CSE0003”为该H-CSE的URL(Uniform Resoure Locator)，也是AS想要创建ACP资源的父节点，即该ACP资源是创建在H-CSE的根节点下，在具体实现中AS也可在POST请求的URL中限定所需创建ACP资源的父资源ID，该ACP资源具体创建于哪个资源之下对本发明方案没有影响，本发明不做限定。“From”部分描述资源创建请求的发起者ID，在本实施例中即授权服务器的URL地址“http://authzserver.things.com”。HTTP消息体中包含所述被创建的ACP资源的所有属性，

[0117] ““ResourceType”:“accessControlPolicy””部分表示本次请求所创建的资源类型为ACP，““privileges.accessControlOriginators”:“/CSE0005/CAE0001””部分表示所创建ACP资源适用的访问设备为“/CSE0005/CAE0001”；HTTP消息体中还应包含被创建ACP资源的其他属性，但由于与本发明方案无关因此在本实施例中并未描述。此外，““res_uri”:“/CSE0003/resource1””部分表示该ACP资源所需绑定的资源URI为“/CSE0003/resource1”，具体实现中所需绑定的资源URI也可以通过其他方式描述(如包含在POST请求

的URL中作为查询字符串形式描述),但其具体描述方式并不影响ACP资源的创建和绑定过程。

[0118] 步骤410:资源服务器创建ACP资源,并将创建的ACP资源与对应的资源进行绑定;

[0119] 具体的,在H-CSE收到AS的ACP资源创建请求后,首先从资源创建请求中解析得到该ACP资源的创建位置或父资源ID,然后从HTTP消息体中解析得到所述被创建的ACP资源的各属性取值。例如,本发明实施例中该ACP资源的创建位置是“http://m2m.things.com/CSE0003”,即在H-CSE的根节点下创建该资源;此外,HTTP消息体中的““ResourceType”:“accessControlPolicy””部分表 示所创建资源的类型为ACP,

[0120] ““accessControlOriginators”:“/CSE0005/CAE0001””部分则表示该ACP的一个访问控制规则的accessControlOriginators参数取值为“/CSE0005/CAE0001”;在具体实现中ACP资源创建请求的HTTP消息体中可能还包含该ACP资源的其他属性值,H-CSE在创建ACP资源的时候需要一并获取并为所创建的ACP资源的对应属性值赋值。

[0121] 具体的,在H-CSE完成ACP资源的创建后,H-CSE为该ACP资源分配一个ACP ID并将其设置为ACP资源的资源标识(即resourceID属性),例如“ACP0001”,该ACP ID在H-CSE范围内唯一标识该ACP资源。然后H-CSE根据ACP资源创建请求中的被绑定资源标识找到对应的资源,即“/CSE0003/resource1”,并在该资源的accessControlPolicyIDs属性值列表中添加所创建ACP资源的ACP ID,即“ACP0001”。

[0122] 步骤412:资源服务器向授权服务器返回ACP资源创建响应;

[0123] 具体的,H-CSE向AS返回ACP资源创建响应,该响应包含HTTP 200响应码。例如,所述H-CSE向AS返回的ACP资源创建响应为:

[0124] HTTP/1.1 200 OK

[0125] Content-type:application/onem2m-resource+json

[0126] {“resourceID”:“/CSE0003/ACP0001”}

[0127] 其中,HTTP响应的状态码为“200”,表示H-CSE已完成对应ACP资源的创建和绑定。HTTP消息体中的““resourceID”:“/CSE0003/ACP0001””部分则表示H-CSE为所创建的ACP分配的ACP ID为“/CSE0003/ACP0001”,该ACP ID前添加了H-CSE的CSE ID,以在oneM2M系统中唯一标识该ACP资源。

[0128] 步骤414:授权服务器确定保存的授权关系映射表中是否存在AE-ID1对应的验证信息的签名;

[0129] 具体的,AS在保存的授权关系映射表中查询访问设备标识等于AE-ID1的授权关系,若能找到相应的授权关系,并且在该授权关系中保存有相应的验证信息的签名,则完成初始授权;否则进入步骤316,向AE发起签名请求,请求AE对相应的验证信息进行签名。

[0130] 具体的,所述授权关系映射表中的每一条授权关系,用于保存一个访问设备标识、被访问资源标识、访问设备验证信息以及验证信息的签名。例如,表1记录了一种可能的授权关系映射表的结构:

[0131] 表1授权关系映射表

[0132]

subjectID	signature	res_uris
/CSE0003/CAE0002	94R3JDFSF0	/CSE0002/resource3,/CSE0004/resource2
/CSE0005/CAE0004	FSAF9432J3	/CSE0002/resource5

[0133] 如表1所示，表中的每一行都表示一个访问设备所对应的授权关系，包含访问设备标识(subjectID)、签名(signature)和被访问资源URI列表(res_uris)。需要说明是，在该授权关系映射表中，访问设备标识同时也作为访问设备的验证信息。所述“签名”栏取值为访问设备使用密钥对相应访问设备标识的签名。从表1的第一行可知，res_uris一栏有两个被访问资源URI，事实上，授权关系映射表中的每一条授权关系都记录保存了一个访问设备的授权情况，显然，同一个访问设备可以获得多个资源的访问权限。

[0134] 在具体实现中也可对每个访问设备使用其他形式的验证信息，如将随机生成的字符串作为验证信息，并保存各访问设备对该验证信息的签名数值，如表2所示：

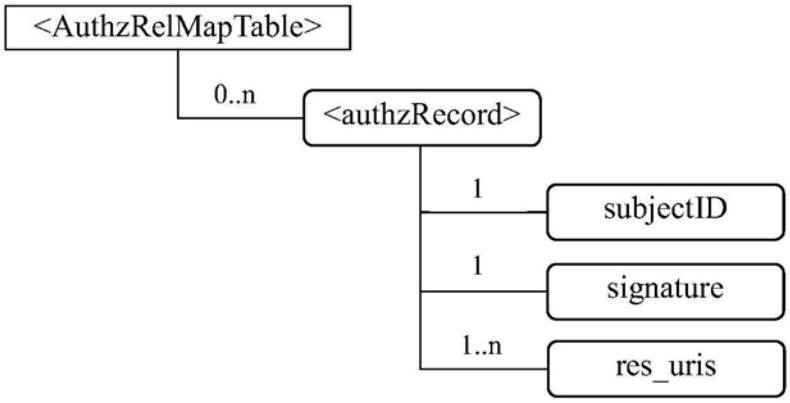
[0135] 表2授权关系映射表(另一例子)

[0136]

subjectID	challenge	signature	res_uris
/CSE0003/CAE0002	8A43RJNKFE984TJK35	94R3JDFSF0	/CSE0002/resource3, /CSE0004/resource2
/CSE0005/CAE0004	MNXCVDFS4I3SDAF832	FSAF9432J3	/CSE0002/resource5

[0137] 如表2所述是对每个访问设备保存随机生成的验证信息(challenge)及其签名的授权关系映射表结构。在具体实现时采用何种信息作为验证信息并不影响本发明的具体方案。在本实施例中假设M2M系统使用如表1所述的授权关系映射表结构，即将访问设备标识作为验证信息。该授权关系映射表在具体实施时，可通过AS内部的一般数据库来进行维护，或者作为一种RESTful资源AuthzRelMapTable进行表述。在基于ACP的授权架构下，该AuthzRelMapTable资源可以表示为如下表3所示的形式：

[0138]



[0139] 表3授权关系映射表资源及属性

[0140] 其中，AuthzRelMapTable为授权关系映射表资源，该资源包含若干条授权记录属性，即authzRecord资源，每一个authzRecord资源记录一个访问设备的授权关系，authzRecord资源包含以下属性：

[0141] subjectID:对应表1中的访问设备标识属性；

[0142] signature:对应表1中的签名属性；

[0143] res_uris:对应表1中的被访问资源URI列表属性。

[0144] 以表1为例，具体的，AS在收到H-CSE的资源创建响应后，首先在授权关系映射表中查找访问设备标识等于AE-ID1的授权关系，即查找“subjectID”栏取值等于“/CSE0005/CAE0001”的授权关系。如果在授权关系映射表中能够找到符合条件的授权关系，且该授权

关系的signature属性值不为空，则AS直接结束初始授权流程；否则，AS发起签名请求流程，执行步骤416。

[0145] 步骤416：授权服务器向AE发送签名请求；

[0146] 具体的，AS向AE发起的签名请求可以为：

[0147] POST http://m2m.things.com/CSE0005/CAE0001 HTTP/1.1

[0148] Content-type:application/onem2m-resource+json

[0149] {“SigReq”:“1”}

[0150] 其中，POST部分请求的URL为AE在R-CSE上的URI，R-CSE收到该请求后会将签名请求转发给AE。HTTP消息体中的““SigReq”:“1””部分为一个签名请求标志位，表示需要AE对验证信息进行签名。在本实施例中验证信息即AE-ID1，由于AE本身会保存自己的标识，所以此时不需要在上述签名请求的 HTTP消息体中包含验证信息参数；当具体实现时采用其他形式的验证信息时，可在上述签名请求的HTTP消息体中包含对应的验证信息参数。

[0151] 步骤418：AE使用设备出厂密钥对验证信息进行签名；

[0152] 具体的，在AE收到AS的签名请求后，首先检测HTTP消息体中是否包含签名请求标志位“SigReq”，当资源访问响应中包含“SigReq”参数且其取值为“1”时，AE使用某种预设的签名算法和设备的出厂密钥对相应的验证信息进行签名。本实施例中，对AE-ID1计算所得的签名为“JYUI7BZO92”。

[0153] 具体的，AE将此时的AE-ID1与M2M SP ID(M2M Service Provider Identifier)绑定保存在本地，该保存方法可以使用访问设备标识映射表实现，或使用其他的方式保存。具体实现中使用何种保存方法不影响本发明的方案，在本实施例中假设AE端使用一个访问设备标识映射表保存AE-ID和M2M SP ID的对应关系，如表4所示：

[0154] 表4：访问设备标识映射表

[0155]

访问设备标识	M2M SP ID
/CSE0005/CAE0001	http://m2m.things.com
SAE2002	http://m2m.example.com

[0156] 在M2M系统中AE会保存当前被分配的标识，需要说明的是，AE保存当前被分配的标识与这里保存的访问设备标识映射表并不相关。例如，由于某种原因，访问设备重新在新的注册服务器注册获得标识AE-ID11，则访问设备会保存AE-ID11为当前设备标识。但是如果访问设备不以AE-ID11重新申请授权，则访问设备标识映射表中的访问设备标识不会更新。

[0157] 步骤420：AE向AS返回签名响应。

[0158] 具体的，AE向AS返回签名响应。例如，AE向AS返回的签名响应为：

[0159] HTTP/1.1 200 OK

[0160] Content-type:application/onem2m-resource+json

[0161] {“signature”:“JYUI7BZO92”}

[0162] 其中，HTTP响应的状态码为“200”，表示AE已对验证信息进行签名。HTTP消息体中的““signature”:“JYUI7BZO92””部分表示验证信息的签名为 “JYUI7BZO92”。

[0163] 步骤422：授权服务器收到AE的签名响应后，从签名响应中解析得到验证信息的签名，并在授权关系映射表中添加对应的授权关系。

[0164] 具体的，在AS收到AE的签名响应时，AS首先从所述签名响应的HTTP消息体中解析

得到验证信息的签名,即“JYUI7BZO92”;然后AS在授权关系映射表中查找与该AE对应的授权关系,即查找subjectID属性值等于AE-ID1,即“/CSE0005/CAE0001”的授权关系:若找到该授权关系,则将该授权关系的signature属性值赋值为“JYUI7BZO92”;若未找到该授权关系,则构造新的授权关系,并将该授权关系添加到授权关系映射表中。在本发明实施例中,如表1所示,AS的授权关系映射表中不存在与该AE对应的授权关系,所以AS生成新的授权关系,并更新到授权关系映射表中,更新后的授权关系映射表如表5所示,表中第三行数据即是新生成的授权关系。

[0165] 表5授权关系映射表

[0166]

subjectID	signature	res_uris
/CSE0003/CAE0002	94R3JDFSF0	/CSE0002/resource3,/CSE0004/resource2
/CSE0005/CAE0004	FSAF9432J3	/CSE0002/resource5
/CSE0005/CAE0001	JYUI7BZO92	/CSE0003/resource1

[0167] 参阅图5,图5为本发明提供的一种基于ACP授权架构的授权更新的流程图。当图4所述实施例中的AE由于更改接入地点等原因,导致在不同的注册服务器(如R-CSE2)上注册时,新的注册服务器R-CSE2可能会为AE分配新的标识AE-ID2,从而导致M2M系统中现有的授权关系失效。图5所述的方法提供了一种当访问标识发生变化后,更新授权关系的方法,包括:

[0168] 步骤502-步骤504:AE向注册服务器2(R-CSE2)发送注册请求,注册服务器2为AE分配标识AE-ID2;

[0169] 步骤506:AE向资源服务器(H-CSE)发起资源访问请求,所述资源访问请求中包含AE-ID2和被访问资源的URI。

[0170] 具体的,AE向H-CSE发送资源访问请求。例如,AE向H-CSE发起的初次资源访问请求为:

[0171] GET http://m2m.things.com/CSE0003/resource1?from＝/CSE0005/CAE0001HTTP/1.1

[0172] 其中,“http://m2m.things.com/CSE0003/resource1”为被访问资源的URI,“from＝/CSE0006/CAE0003”表示访问设备标识,即该AE的AE-ID2。

[0173] 步骤508:资源服务器(H-CSE)根据访问请求中携带的信息进行访问控制决策;

[0174] 具体的,在H-CSE收到AE的资源访问请求后,H-CSE首先解析资源访问请求中的被访问资源的URI,即GET请求中的URL地址“/CSE0003/resource1”,并在本地查找对应的资源resource1。然后,H-CSE在资源访问请求中解析得到AE-ID2,即GET请求中的URL查询字符串部分“/CSE0006/CAE0003”;最后,在对应资源resource1的accessControlPolicyIDs属性值中找到与该资源绑定的ACP ID列表,并根据背景技术中所介绍的访问控制决策过程来决策AE是否具有访问资源的权限。本实施例中假设相对于初始授权情况下只有AE的访问设备标识由AE-ID1变为AE-ID2,而其他资源访问相关的属性(如操作、上下文环境等)均与初始授权限定的条件一致。由于Admin在初始授权时为AE预设的ACP中,privileges.accessControlOriginators属性值仅包含AE-ID1,即/CSE0005/CAE0001,因此在访问决策过程中,H-CSE找不到符合AE-ID2,即/CSE0006/CAE0003的ACP,因此访问控制决策的结果是不允许本次资源访问。现有技术中,资源服务器将直接拒绝访问设备的访问请求。从而导致同一个访问设

备由于设备标识发生变化，而出现访问资源失败的情况。

[0175] 步骤510：资源服务器向AE返回资源访问响应，该响应包含HTTP 302响应码以及一个重定向URL，所述重定向URL指向授权服务器的授权更新端口。

[0176] 具体的，当H-CSE的访问控制决策为不允许本次资源访问时，H-CSE向AE返回的资源访问响应为：

[0177] HTTP/1.1 302 Move temporarily

[0178] Location:http://authzserver.things.com/authzupdate#from＝/CSE0006/CAE0003&res_uri＝/CSE0003/resource1

[0179] 其中，HTTP响应的状态码为“302”，表示该AE的资源访问请求需要被重定向到新的URL。“Location:http://authzserver.things.com/authzupdate”表示重定向URL，该重定向URL指向该M2M系统授权服务器的授权更新端口，例如http://authzserver.things.com/authzupdate即为该授权服务器的授权更新端口地址。“#from＝/CSE0006/CAE0003&res_uri＝/CSE0003/resource1”为重定向后的资源访问请求所需要附带的参数信息，包括AE-ID2(即/CSE0006/CAE0003)和被访问资源的URI(即/CSE0003/resource1)，以查询字符串的形式表示。

[0180] 步骤512：AE收到资源服务器的资源访问响应后，向授权服务器发送授权更新请求，该授权更新请求包括AE-ID2和被访问资源的URI。

[0181] 具体的，AE收到H-CSE的资源访问响应并检测HTTP状态码，当状态码为“302”时，AE向AS发送授权更新请求。例如，AE向AS发送的授权更新请求可以为：

[0182] GET /authzupdate?from＝/CSE0006/CAE0003&res_uri＝CSE0003/resource1 HTTP/1.1

[0183] Host:http://authzserver.things.com

[0184] 其中，GET请求的URL地址“/authzupdate?from＝/CSE0006/CAE0003&res_uri＝CSE0003/resource1HTTP/1.1”表示授权服务器的授权更新端口地址以及附带的参数信息，该附带的参数信息包括AE-ID2(即/CSE0006/CAE0003)和被访问资源标识(即/CSE0003/resource1)，“Host”部分则描述了授权服务器地址”。

[0185] 步骤514：授权服务器收到AE授权更新请求后，向AE返回授权更新响应，该响应包含HTTP 202响应码和签名请求标志位。

[0186] 具体的，当AS收到AE授权更新请求后，AS向AE返回的授权更新响应为：

[0187] HTTP/1.1 202 Accepted

[0188] Content-type:application/onem2m-resource+json

[0189] {“SigReq”:“2”}

[0190] 其中，HTTP响应的状态码为“202”，表示AS已接受了AE的授权更新请求，但需要进一步的信息并等待后续处理。HTTP消息体中的““SigReq”:“2””部分为一个签名请求标志位，表示需要AE对验证信息和访问设备的当前标识进行签名。在本实施例中，所述验证信息即AE在初始授权时的访问设备标识AE-ID1，即/CSE0005/CAE0001，访问设备的当前标识即AE-ID2，/CSE0006/CAE0003。

[0191] 步骤516：AE使用设备出厂密钥对验证信息进行签名，并对访问设备的当前标识AE-ID2进行签名；

[0192] 具体的，在AE收到H-CSE的授权更新响应后，当检测得到HTTP响应的状态码为“202”和HTTP消息体中包含“SigReq”参数且取值为“2”时，AE对本地保存的AE-ID1进行签名。本实施例中，所述AE-ID1在本地以访问设备标识映射表的形式保存，如表4所述，AE根据当前接入的M2M系统标识(即 M2M SP ID，本实施例中为“http://m2m.things.com”)在该访问设备标识映射表中找到对应的访问设备标识AE-ID1：/CSE0005/CAE0001，在实施例中，AE-ID1/CSE0005/CAE0001即为相应的验证信息。

[0193] 具体的，在AE查找到本地保存的AE-ID1后，AE对AE-ID1和AE-ID2进行签名。本实施例中，对AE-ID1进行签名得到“JYUI7BZO92”，对AE-ID2进行签名得到“M6UI7B2OKQ”。然后，将AE-ID2更新到本地保存的访问设备标识映射表中，代替原来AE-ID1，即在表4中用“/CSE0006/CAE0003”替换“/CSE0005/CAE0001”，得到如表5所示的更新的访问设备标识映射表。

[0194] 表5：访问设备标识映射表

[0195]

访问设备标识	M2M SP ID
/CSE0006/CAE0003	http://m2m.things.com
SAE2002	http://m2m.example.com

[0196] 步骤518：AE向授权服务器发送签名验证请求；

[0197] 在AE完成签名后，AE向AS发起签名验证请求，该请求包含AE-ID1、AE-ID1的签名、AE-ID2、AE-ID2的签名。

[0198] 具体的，AE向AS发起的签名验证请求为：

[0199] PUT http://authzserver.things.com/authzupdate HTTP/1.1

[0200] Content-type:application/onem2m-resource+json

[0201] {“aeid_ori”:“/CSE0005/CAE0001”,“sig_ori”:“JYUI7BZO92”

[0202] “aeid_now”:“/CSE0006/CAE0003”,“sig_now”:“M6UI7B2OKQ”}

[0203] 其中，HTTP响应的状态码为“200”，表示AE已对验证信息进行签名。HTTP消息体中的““aeid_ori”:“/CSE0005/CAE0001””表示初始授权时的访问设备标识AE-ID1为“/CSE0005/CAE0001”，““sig_ori”:“JYUI7BZO92””表示初始授权时的访问设备标识AE-ID1的签名为“JYUI7BZO92”；““aeid_now”:“/CSE0006/CAE0003””部分表示当前该AE的访问设备标识AE-ID2为“/CSE0006/CAE0003”，““sig_now”:“M6UI7B2OKQ””部分表示当前该AE的访问设备标识AE-ID2的签名为“M6UI7B2OKQ”。

[0204] 步骤520：AS验证签名验证请求中的签名，确定是否更新授权关系映射表；

[0205] 在AS收到AE的签名验证请求后，AS在授权关系映射表中查找访问设备标识为AE-ID1的授权关系，比较签名验证请求中的AE-ID1签名和该授权关系中的签名是否一致，并进一步为AE进行授权更新或拒绝授权更新请求。

[0206] 具体的，在AS收到AE的签名验证请求后，AS首先从签名验证请求中解 析得到AE-ID1、AE-ID1签名、AE-ID2和AE-ID2签名，然后，AS在授权关系映射表中查找subjectID属性值为AE-ID1(即“/CSE0005/CAE0001”)的授权关系，并验证该授权关系中的signature属性值是否与AE-ID1签名(即“JYUI7BZO92”)相同。如果对应授权关系中的signature属性值与AE-ID1的签名不相同，则授权服务器拒绝AE的签名验证请求并返回签名验证响应，例如：HTTP/1.1 403Forbidden，授权更新流程结束；如果对应授权关系中的signature属性值与

AE-ID1的签名相同，则允许AE此次授权更新并将该授权关系中的subjectID属性值更新为AE-ID2(即“/CSE0006/CAE0003”)，同时将signature属性值更新为AE-ID2的签名(即“M6UI7B2OKQ”)，本发明实施中，显然签名验证通过，AS更新授权关系映射表，如表6所示：

[0207] 表6授权关系映射表

[0208]

subjectID	signature	res_uris
/CSE0003/CAE0002	94R3JDFSF0	/CSE0002/resource3,/CSE0004/resource2
/CSE0005/CAE0004	FSAF9432J3	/CSE0002/resource5
/CSE0006/CAE0003	M6UI7B2OKQ	/CSE0003/resource1

[0209] 步骤522:授权服务器向资源服务器发送授权更新请求；

[0210] 当AS允许AE的授权更新后，AS向H-CSE发起授权更新请求，该请求包含被访问资源URI、AE-ID1和AE-ID2。

[0211] 具体的，授权更新请求可以为：

[0212] PUT http://m2m.things.com/CSE0003/resource1 HTTP/1.1

[0213] From:http://authzserver.things.com

[0214] Content-type:application/onem2m-resource+json

[0215] {“aeid_ori”:“/CSE0005/CAE0001”,

[0216] “aeid_now”:“/CSE0006/CAE0001”}

[0217] 其中，“/CSE0003/resource1”为被访问资源的URI，HTTP消息体中的““aeid_ori”:“/CSE0005/CAE0001””表示原访问设备标识AE-ID1为“/CSE0005/CAE0001”，““aeid_now”:“/CSE0006/CAE0001””表示访问设备的当前标识AE-ID2为“/CSE0006/CAE0003”。

[0218] 步骤524:资源服务器更新授权关系；

[0219] 在H-CSE收到AS的授权更新请求后，H-CSE根据被访问资源的URI找到的对应资源，并更新该资源关联的授权关系。

[0220] 具体的，在H-CSE收到AS的授权更新请求后，首先从授权更新请求中解析得到被访问资源的URI，即“/CSE0003/resource1”，并在本地查找到对应资源；其次，从授权更新请求的HTTP消息体中解析得到AE-ID1(即“/CSE0005/CAE0001”)和AE-ID2(即“/CSE0006/CAE0003”)；然后，在对应资源resource1的accessControlPolicyIDs属性中找到所有与该资源关联的ACP ID列表，并在这些ACP中查找privileges.accessControlOriginators属性值包含“/CSE0005/CAE0001”的ACP资源，并将所述ACP资源中的privileges.accessControlOriginators属性值更新为“/CSE0006/CAE0003”。

[0221] 步骤526:资源服务器向授权服务器发送授权更新响应；

[0222] 在H-CSE完成授权更新后，H-CSE向AS返回授权更新响应。具体的，在H-CSE完成授权更新后，H-CSE向AS返回的授权更新响应为：

[0223] HTTP/1.1 200OK

[0224] 其中，HTTP响应的状态码为“200”，表示H-CSE已完成对应ACP资源的更新。

[0225] 步骤528:授权服务器向AE发送签名验证响应；

[0226] 在AS收到H-CSE的授权更新响应后，AS向AE返回签名验证响应。

[0227] 具体的，在AS收到H-CSE的授权更新响应后，AS向AE返回的签名验证响应为：

[0228] HTTP/1.1 200OK

[0229] 其中,HTTP响应的状态码为“200”,表示AS已完成AE所请求的授权更新。

[0230] 当AE接收到授权服务器发送的签名验证响应后,表明M2M系统已经完成授权关系的更新,此时AE可以使用AE-ID2的访问设备标识对被访问资源/CSE0003/resource1进行访问。

[0231] 本实施例中,当M2M系统中的M2M设备,如AE,在标识发生变化后,访问被访问资源时,资源服务器触发授权关系更新流程,M2M系统通过验证访问设备对验证信息的签名来确定访问设备的身份,并更新已有的授权关系, 使得M2M设备能够实现无缝的资源访问,保证了M2M系统的业务连续性。

[0232] M2M系统采用Oauth授权架构对访问设备访问资源进行授权时,所述验证信息可以授权服务器生成的访问令牌。具体的,在图6和图7所述的实施例中,将提供一种M2M系统中基于Oauth授权架构的授权流程,包括初始授权和授权更新两个流程,其中所述初始授权是指访问设备标识变化前,授权服务器为访问设备获取身份验证信息并生成授权关系的过程。

[0233] 参阅图6,图6为本发明提供的一种基于Oauth授权架构的初始授权的流程图,在本实施例中访问设备为一个应用实体AE,但是本发明实施例对访问设备的具体形式并不做限定,所述方法包括:

[0234] 步骤602-步骤604:AE向注册服务器1(R-CSE1)发送注册请求,注册服务器1为AE分配身份标识AE-ID1;

[0235] 步骤606:AE向资源服务器(H-CSE)发起初次资源访问请求,所述资源访问请求中包含AE-ID1和被访问资源的URI。

[0236] 具体的,AE向H-CSE发送初次资源访问请求。例如,AE向H-CSE发起的资源访问请求为:

[0237] GET http://m2m.things.com/CSE0003/resource1?from＝/CSE0005/CAE0001 HTTP/1.1

[0238] 其中,“CSE0003/resource1”为被访问资源的URI,“from＝/CSE0005/CAE0001”部分表示访问设备的应用标识,即该AE的AE-ID1。由于该AE是初次访问该被访问资源,在AE本地并没有保存与该资源绑定的访问令牌,因此在初次访问请求中并不包含访问令牌参数。

[0239] 步骤608:资源服务器(H-CSE)接收AE发送的资源访问请求,并进行访问控制决策。

[0240] 具体的,当H-CSE接收资源访问请求时,首先根据资源访问请求中的被访问资源的URI在本地查找对应的资源,若在本地不能找到该资源,则H-CSE向AE返回资源访问拒绝响应,例如:HTTP/1.1 404 Not Found;若在本地能找到被访问的资源,则H-CSE根据资源访问请求中访问设备标识和访问令牌在资源属性中查找对应的授权关系。当AE所发送的资源访问请求为初次资源访问请求时,如步骤606所述,该请求中并不包含访问令牌参数,则H-CSE确定该AE是首次访问资源,H-CSE发起授权流程。

[0241] 步骤610:资源服务器向AE返回资源访问响应;

[0242] 该响应包含重定向响应码和重定向URL,该重定向URL指向该M2M系统授权服务器的动态授权端口。

[0243] 具体的,H-CSE向请求资源访问的AE返回资源访问响应。例如,H-CSE向AE返回的资源访问响应可以为:

[0244] HTTP/1.1 302 Move temporarily

[0245] Location:http://authzserver.things.com/dynamicauthz#from＝/CSE0005/CAE0001&res_uri＝/CSE0003/resource1

[0246] 其中,HTTP响应的状态码为“302”,表示该AE的资源访问请求需要被重定向到新的URL。“Location”部分表示重定向URL,该重定向URL指向该M2M系统授权服务器的动态授权端口,例如http://authzserver.things.com/dynamicauthz即为该授权服务器的动态授权端口地址。“#from＝/CSE0005/CAE0001&res_uri＝/CSE0003/resource1”部分为重定向后的资源访问请求所需要附带的参数信息,以查询字符串的形式表示,该例子中所述附带的参数信息为:访问设备标识为“/CSE0005/CAE0001”,被访问资源的URI为“/CSE0003/resource1”。

[0247] 步骤612:AE向资源服务器发送授权请求,该授权请求包括AE-ID1和被访问资源的URI;

[0248] AE收到H-CSE的资源访问响应,向AS发送授权请求,该授权请求的地址使用步骤610中资源访问响应的Location参数所提供的重定向URL。

[0249] 具体的,AE收到H-CSE的资源访问响应并检测HTTP状态码,当状态码为“302”时,AE向AS发送授权请求。例如,AE向AS发送的授权请求为:

[0250] GET http://authzserver.things.com/dynamicauthz?from＝/CSE0005/CAE0001&res_uri＝CSE0003/resource1HTTP/1.1

[0251] 其中,“/dynamicauthz?from＝/CSE0005/CAE0001&res_uri＝CSE0003/resource1”表示授权服务器的动态授权端口地址以及附带的参数信息,附带的参数信息包括AE-ID1和被访问资源的URI,“Host”部分则描述了授权服务器地址,本实施例中为“http://authzserver.thnings.com”。AE在向AS发送授权请求时也可以直接使用GET请求访问资源访问响应中Location参数所提供的重定向URL,而不使用Host参数,例如该授权请求可以为:

[0252] GET http://authzserver.things.com/dynamicauthz?from＝/CSE0005/CAE0001

[0253] &res_uri＝/CSE0003/resource1HTTP/1.1

[0254] 其中第一行末的换行符仅为文档表述清晰的需要,具体实现时上述两行消 息中间并无换行符。

[0255] 步骤614:授权服务器向AE返回授权响应,该授权响应中包括请求用户认证的标志位;

[0256] 具体的,AS在收到AE的授权请求后,首先检测该授权请求中是否包含用户认证相关的参数,当该授权请求中不包含用户认证信息时,AS向AE返回的授权响应为:

[0257] HTTP/1.1 202 Accepted

[0258] Content-type:application/onem2m-resource+json

[0259] {“NeedUserAuthN”:“1”}

[0260] 其中,HTTP响应的状态码为“202”,表示该授权请求已被接收,但需要进一步的信息并等待后续处理。HTTP消息体中的““NeedUserAuthN”:“1””参数表示一个请求用户认证的标志位,该参数指示AE在下一次授权请求中需要携带用户认证信息。

[0261] 步骤616:AE授权服务器发送的授权响应,当检测到响应中包含请求用户认证的标

志位时，令用户在AE中输入用户认证信息。

[0262] 具体的，AE收到AS发送的授权响应并检测HTTP状态码，当状态码为“202”时，AE继续检测HTTP消息体，当检测到消息体内包含“NeedUserAuthN”参数且参数值为“1”时，令用户在AE中输入用户认证信息。此处用户可根据AE所驻留设备的用户交互能力选择合适的输入方法，例如，当该设备拥有用户交互接口(如键盘、触摸屏等)时，用户可使用该交互接口输入其账号密码；当该设备不支持用户交互操作时，用户可以利用其它交互设备完成用户信息的输入；此外，用户也可以通过身份卡等能够证明其身份的对象完成身份信息的输入。具体的用户认证信息输入方式不在本发明的讨论范围内，对本发明的方案也没有影响，为简便起见，本发明方案中假设该设备拥有用户交互接口，用户通过该交互接口向AE输入其账号user1和密码password1。

[0263] 步骤618：用户输入用户认证信息；

[0264] 步骤620：AE向资源服务器发送授权请求，该授权请求包括AE-ID1、被访问资源的URI和用户认证信息；

[0265] 具体的，当用户在AE端输入其用户认证信息后，AE向AS发送的授权请求为：

[0266] GET /dynamicauthz?from＝/CSE0005/CAE0001&res_uri＝/CSE0003/resource1HTTP/1.1

[0267] Host:http://authzserver.things.com

[0268] Content-type:application/onem2m-resource+json

[0269] {“user”:“user1”,

[0270] “password”:“password1”}

[0271] 该授权请求与步骤612所述授权请求相比，增加了用户认证信息相关的参数。其中，““user”:“user1””部分表示用户的账号名，““password”:“password1””部分表示用户账号名对应的密码。本实施例中，用户的认证信息包含在HTTP消息体中并采用JSON格式编码，实际实现中，该用户认证信息也可以查询字符串的形式包含在GET请求的URL中，本发明对此不作限定。

[0272] 步骤622：授权服务器根据用户认证信息确定用户身份和权限，生成访问令牌(token)；

[0273] AS收到AE的授权请求并检测到用户认证信息后，AS从所述授权请求中获取用户认证信息，并在用户信息数据库中对用户认证信息进行验证，并确认该用户是否具有访问该资源的权限；当用户身份和权限得到确认后，AS为本次授权生成token。

[0274] 具体的，AS在收到AE的授权请求后，首先检测该授权请求中是否包含用户认证相关的参数，当所述授权请求的消息体中包含“user”和“password”参数时，表示该AE想要进行用户认证；然后，AS从所述授权请求的消息体中获取“user”的参数值“user1”以及“password”的参数值“password1”，并在用户信息数据库中查找账号名为“user1”的用户，并验证其密码是否等于“password1”。所述用户信息数据库为保存M2M系统中所有用户认证信息和访问权限的数据库，所述用户信息数据库中保存的用户认证信息与AS所使用的认证方法相关，在本实施例中，AS使用传统的账号名和密码进行用户认证，因此用户信息数据库中保存的用户认证信息至少应包含用户的账号名和密码，此外可能还包含该用户能够访问资源的权限。

[0275] 当AS在用户信息数据库中找到账号名为“user1”且密码等于“password1”的用户记录时，进一步判断被访问资源的URI，即“/CSE0003/resource1”是否在该用户的访问权限内中，具体的权限表示形式与M2M系统权限管理方式相关，本实施例中假设用户权限信息在用户信息数据库中表现为一个可访问资源列表，所述可访问资源列表包含了该用户有权限访问的所有资源的URI。当用户信息数据库中该用户记录的可访问资源列表中包含被访问资源的URI时，AS即许可本次授权请求，并为本次授权请求生成对应的访问令牌(token)，所述 token的生成方式由AS自行决定。采用何种token生成方法对本发明的方案没有影响，在本实施例中，假设所述token采用一个由AS随机生成的固定长度的字符串表示，例如“2YotnFZFEjr1zCsicMWpAA”。

[0276] 步骤624：授权服务器向资源服务器发送授权绑定请求，该授权绑定请求中包含AE-ID1、token和被访问资源的URI。

[0277] 在AS为AE的授权请求生成token后，AS向H-CSE发送授权绑定请求，令H-CSE将授权信息与对应资源绑定保存，所述授权绑定请求中包含AE-ID1、token和被访问资源的URI。

[0278] 具体的，在AS为AE的授权请求生成token后，AS向H-CSE发送的授权绑定请求可以为：

[0279] PUT http://m2m.things.com/CSE0003/resource1 HTTP/1.1

[0280] From:/CSE0005/CAE0001

[0281] Content-type:application/onem2m-resource+json

[0282] {“token”:“2YotnFZFEjr1zCsicMWpAA”}

[0283] 其中，PUT请求的URL表示需要更新的被访问资源URI，即“/CSE0003/resource1”，“From”部分表示访问设备的标识，即“/CSE0005/CAE0001”，HTTP消息体中的““token”:“2YotnFZFEjr1zCsicMWpAA””部分表示与该访问设备和被访问资源URI对应的访问令牌具体数值为“2YotnFZFEjr1zCsicMWpAA”。

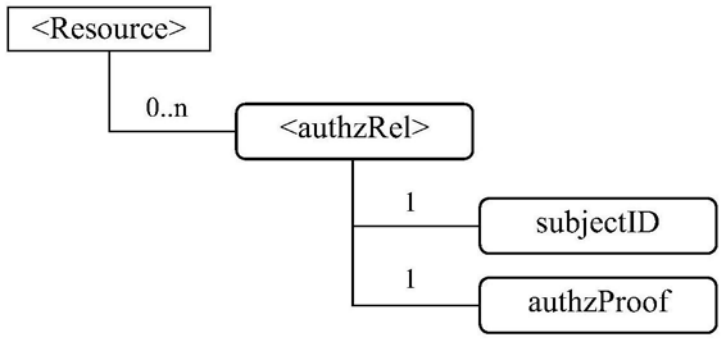
[0284] 步骤626：资源服务器将根据授权服务器发送的授权绑定请求，进行授权关系的绑定；

[0285] H-CSE根据AS的授权绑定请求中被访问资源URI找到H-CSE上保存的被访问资源，然后AS从授权绑定请求中获取访问设备标识和访问令牌，并将其保存在被访问资源对应的资源属性中。

[0286] 具体的，当H-CSE收到AS的授权绑定请求后，H-CSE从所述授权绑定请求中获取被访问资源的URI，例如从PUT请求的URL中获取被访问资源的URI即“/CSE0003/resource1”，并在H-CSE本地保存的资源中找到该被访问资源。然后，H-CSE从授权绑定请求中获取访问设备的AE-ID1和对应的token，例如，从PUT请求的HTTP头域的“From”参数中获取AE-ID1即“/CSE0005/CAE0001”，并从HTTP消息体的“token”参数中获取访问令牌即“2YotnFZFEjr1zCsicMWpAA”。然后，H-CSE将上述AE-ID和token保存到被访问资源对应的资源属性中。

[0287] 现有oneM2M标准中仅为资源对象定义了与访问控制策略(ACP)对应的属性accessControlPolicyIDs，而并没有为基于token的授权架构定义对应的资源属性。表7提供了一种可能的授权关系绑定方法：在资源的通用属性中增加授权关系属性authzRel，用于表示与该资源绑定的一条授权关系。

[0288]



[0289] 表7资源新增授权关系属性

[0290] 如表7所示,每个资源的属性中都可能包含若干个authzRel属性,表示与该资源绑定的若干条授权关系,而每个authzRel资源又表示为一个二元组资源,其中包含subjectID(访问设备标识)和authzProof(访问令牌)两个属性。

[0291] 当H-CSE获取授权绑定请求中的AE-ID1和token参数后,则构造一个<authzRel>资源实例authzRel1,令authzRel1的subjectID属性值等于“/CSE0005/CAE0001”,authzProof属性值等于“2YotnFZFEjr1zCsicMWpAA”,然后将该authzRel1资源添加到Resource1的属性中,从而完成授权关系的绑定。

[0292] 步骤628:当资源服务器完成授权关系绑定后,向AS返回授权绑定响应。

[0293] 具体的,当H-CSE完成授权关系绑定后,H-CSE向AS返回的授权绑定响应可以为:

[0294] HTTP/1.1 200 OK

[0295] 其中,HTTP响应的状态码为“200”,表示本次授权关系绑定成功。

[0296] 步骤630:当授权服务器接收到资源服务器发送的授权绑定响应后,授权服务器向AE返回授权响应,所述授权响应包含token、被访问资源的URI和签名请求标志位。

[0297] 具体的,当AS收到H-CSE的授权绑定响应后,AS向AE返回的授权响应可以为:

[0298] HTTP/1.1 202 Accepted

[0299] Content-type:application/onem2m-resource+json

[0300] {“token”:“2YotnFZFEjr1zCsicMWpAA”,

[0301] “res_uri”:“/CSE0003/resource1”,

[0302] “SigReq”:“1”}

[0303] 其中,HTTP响应的状态码为“202”,表示本次授权请求已被许可,但需要进一步的信息并等待后续处理。HTTP消息体中,““token”:“2YotnFZFEjr1zCsicMWpAA””部分表示本次授权中生成的访问令牌,AE下次可使用该token访问对应资源;““res_uri”:“/CSE0003/resource1””部分表示本次授权响应是针对“/CSE0003/resource1”的,所述token也是针对该资源访问所使用的,该res_uri参数主要是针对AS同时处理多个由该AE发起的授权请求的情况,res_uri参数用于让AE能区分不同授权响应消息;““SigReq”:“1””部分为一个签名请求标志位,表示需要AE进一步提供token签名数据以在AS端保存与本次授权关联的验证信息的签名。

[0304] 步骤632:AE保存访问令牌,并使用设备出厂密钥对访问令牌进行签名;

[0305] 当AE收到AS的授权响应后,AE首先从所述授权响应中获取token和被访问资源的URI,并将其绑定保存在本地;然后,AE检测到所述授权响应包含了签名请求标志位,则使用

设备出厂密钥对所收到的token进行签名。

[0306] 具体的，当AE收到AS的授权响应后，AE首先从所述授权响应中获取token和被访问资源的URI，即从HTTP响应消息体的“token”参数中获取访问令牌“2YotnFZFEjr1zCsicMWpAA”，从“res_uri”参数中获取被访问资源的URI即“/CSE0003/resource1”，并将上述两者绑定保存在本地，该保存方法可以使用访问令牌映射表实现，或使用其他的方式保存。具体实现中使用何种保存方法不影响本发明的方案，在本实施例中假设AE端使用一个访问令牌映射表保存被访问资源URI和token的对应关系，如下表8所示，表8中每一行都表示该AE已获取的一项授权：

[0307] 表8：访问令牌映射表

[0308]

被访问资源的URI	Token
/CSE0003/resource1	2YotnFZFEjr1zCsicMWpAA
/CSE0004/resource2	tGzv3JOkF0XG5Qx2TlKWIA

[0309] 然后，AE检测授权响应中是否包含签名请求标志位“SigReq”，当授权响应中包含“SigReq”参数且其取值为“1”时，AE使用某种预算的签名算法和设备的出厂密钥对token进行签名，所述签名算法可以为MAC、HMAC等通用的签名算法。具体实现中使用何种签名算法对本发明的方案没有影响，在本实施例中假定AE采用了MAC签名算法，对上述token计算所得的签名为“8456B1CD”。

[0310] 步骤634：当AE完成token签名后，AE向授权服务器发起签名绑定请求，该请求包含AE-ID1、token、token签名和被访问资源的URI。

[0311] 具体的，当AE完成token签名后，AE向AS发起的签名绑定请求可以为：

[0312] PUT http://authzserver.things.com/dynamicauthz HTTP/1.1

[0313] From:/CSE0005/CAE0001

[0314] Content-type:application/onem2m-resource+json

[0315] {“token”:“2YotnFZFEjr1zCsicMWpAA”,

[0316] “token_sig”:“8456B1CD”,

[0317] “res_uri”:“/CSE0003/resource1”}

[0318] 其中，PUT请求的URL地址，即“http://authzserver.things.com/dynamicauthz”为AS的动态授权端口，“From”部分表示发起签名绑定请求的访问设备标识，HTTP消息体中的“token”和“token_sig”参数分别表示需要进行签名绑定的token和token签名。

[0319] 步骤636：当收到AE的签名绑定请求后，授权服务器生成对应的授权关系并保存在授权关系映射表中。

[0320] 具体的，当AS收到AE的签名绑定请求后，首先为本次授权生成一个授权关系，该授权关系至少应包含访问设备标识、token、token签名和被访问资源URI，然后AS将所述生成的授权关系添加到授权关系映射表中。所述授权关系映射表结构可以如表9所示：

[0321] 表9授权关系映射表

[0322]

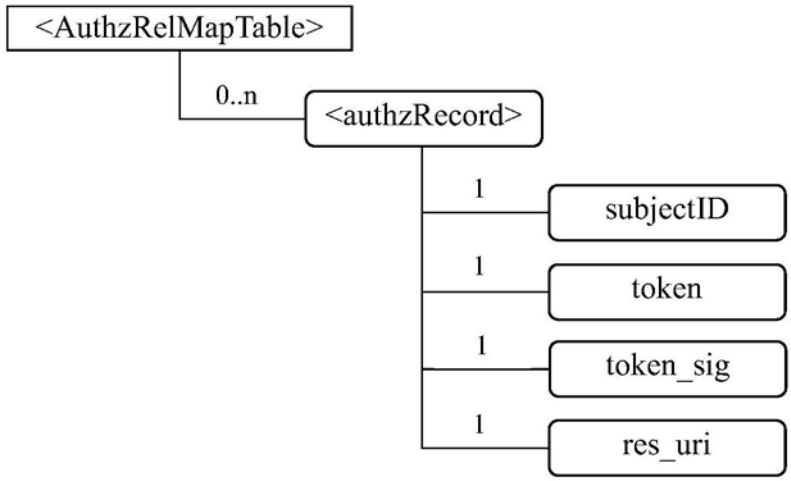
访问设备标识	Token	Token签名	被访问资源URI
/CSE0003/CAE0002	czZCaGRSa3FOMzpnWDFmQmFOM2JW	7432A8D9	/CSE0002/resource3
/CSE0005/CAE0001	2YotnFZFEjr1zCsicMWpAA	8456B1CD	/CSE0003/resource1

[0323] 如表9所示，表中的每一行都表示一条授权关系。当AS收到AE的签名绑定请求后，

AS从AE的签名绑定请求中获取对应参数的数值并添加到对应的授权关系中。在本实施例中，AS生成对应的授权关系并将其添加到授权关系映射表中，如表9中第2条记录所示。

[0324] 上述授权关系映射表在具体实施时，可通过AS内部的一般数据库来进行维护，或者作为一种RESTful资源AuthzRelMapTable进行表述。在基于token 的授权架构下，该AuthzRelMapTable资源可以表示为如下的形式：

[0325]



[0326] 表10授权关系映射表资源及属性

[0327] 其中，AuthzRelMapTable为授权关系映射表资源，该资源包含若干条授权关系属性，即authzRecord资源；authzRecord为授权关系资源，该资源包含以下的一些属性：

[0328] subjectID：对应表9中的访问设备标识；

[0329] token：对应表9中的token属性；

[0330] token_sig：对应表9中的token签名属性；

[0331] res_uri：对应表9中的被访问资源URI属性。

[0332] 需要说明的是，本发明对授权关系映射表的具体表现形式不做限定。

[0333] 步骤538：授权服务器向AE返回签名绑定响应；

[0334] 具体的，当AS完成授权关系保存后，AS向AE返回的签名绑定响应可以为：

[0335] HTTP/1.1 200 OK

[0336] 其中，HTTP响应的状态码为“200”，表示本次签名绑定请求已经完成，AE可以使用token访问对应的资源。

[0337] 本发明实施例中，当资源服务器确定接收到的资源访问请求中，没有访问令牌时，资源服务器向访问设备返回的资源访问响应中携带授权服务器的URI，使得访问设备向授权服务器申请认证授权。授权服务器验证用户认证信息合法，生成访问令牌。授权服务器将访问设备标识、被访问资源URI以及生成的访问令牌发送资源服务器，以便于资源服务器生成相应的授权关系。授权服务器将 生成的访问令牌以及被访问资源URI发送给AE，并且请求AE对访问令牌进行签名。AE保存被访问资源URI和访问令牌的对应关系。授权服务器将访问设备标识、被访问资源URI、访问令牌以及访问令牌的签名的对应关系保存进授权关系映射表中。

[0338] 后续需要访问该被访问资源时，需要在资源访问请求中携带对应的访问令牌。当后续AE访问该被访问资源时，如果访问设备标识发生变化，则资源服务器可以根据本地存

在该被访问资源URI和该访问令牌对应的授权关系，但是该授权关系中的访问设备标识不符合，确定访问设备标识可能发生变化，从而触发授权更新流程。

[0339] 参阅图7，图7为本发明提供的一种基于Oauth授权架构的授权更新的流程图。当图6所述实施例中的AE由于更改接入地点等原因，导致在不同的注册服务器(如R-CSE2)上注册时，新的注册服务器R-CSE2可能会为AE分配新的标识AE-ID2，从而导致M2M系统中现有的授权关系失效。图7所述的方法提供了一种当访问标识发生变化后，更新授权关系的方法，包括：

[0340] 步骤702-步骤704：AE向注册服务器2(R-CSE2)发起注册请求，注册服务器2为AE分配标识AE-ID2。

[0341] 步骤706：AE根据被访问资源URI在本地找到该资源对应的token，并向资源服务器(H-CSE)发送资源访问请求，该资源访问请求中包括AE-ID2、该被访问资源URI以及与该被访问资源URI对应的token。

[0342] 具体的，如图6所述方法中的步骤632所描述，AE经过初始授权后，会保存被访问资源URI和访问令牌的对应关系。AE首先从本地保存的授权信息中，根据被访问资源URI查找到对应的token，然后AE向H-CSE发送资源访问请求。

[0343] 步骤708：资源服务器接收AE所发送的资源访问请求，并进行访问控制决策。

[0344] 具体的，如步骤626所述资源服务器保存有被访问资源URI、AE-ID1以及相应的访问令牌的授权关系。H-CSE解析资源访问请求，获取被访问资源URI、AE-ID2和token。当H-CSE确定本地存在被访问资源，且H-CSE在该被访问资源的授权关系属性(authzRel)中查找authzProof属性值与token相同，而subjectID属性值与AE-ID2不相同的授权记录，则资源服务器启动授权更新流程。

[0345] 步骤710：资源服务器向AE返回资源访问响应，该响应包含重定向响应码 和一个重定向URL，该重定向URL指向该M2M系统授权服务器的授权更新端口。

[0346] 具体的，H-CSE向AE返回资源访问响应。例如，H-CSE向AE返回的资源访问响应可以为：

[0347] HTTP/1.1 302Move temporarily

[0348] Location:http://authzserver.things.com/authzupdate#from＝/CSE0006/CAE0003&res_uri＝/CSE0003/resource1&token＝2YotnFZFEjr1zCsicMWpAA

[0349] 其中，HTTP响应的状态码为“302”，表示该AE的资源访问请求需要被重定向到新的URL。“Location”部分表示重定向URL，该重定向URL指向该M2M系统授权服务器的授权更新端口，例如http://authzserver.things.com/authzupdate即为该授权服务器的动态授权端口地址。“#from＝/CSE0006/CAE0003&res_uri＝/CSE0003/resource1&token＝2YotnFZFEjr1 zCsic MWpAA”部分为重定向后的资源访问请求所需要附带的参数信息，以查询字符串的形式表示，上述附带参数信息的具体内容参见步骤510的描述，本发明实施例在此不再详述。

[0350] 步骤712：AE收到资源服务器的资源访问响应，向授权服务器(AS)发送授权更新请求，该授权更新请求的地址使用响应的Location参数所提供的URL。

[0351] 具体的，AE收到H-CSE的资源访问响应并检测HTTP状态码，当状态码为“302”时，AE向AS发送授权更新请求。例如，AE向AS发送的授权更新请求为：

[0352] GET /authzupdate?from＝/CSE0006/CAE0001&res_uri＝CSE0003/resource1

[0353] &token＝2YotnFZFEjr1zCsicMWpAA HTTP/1.1

[0354] Host:http://authzserver.things.com

[0355] 其中，重定向响应中的Location参数被分解为两部分，GET请求的URL地址“/authzupdate?from＝/CSE0006/CAE0001&res_uri＝CSE0003/resource1&token＝2YotnFZFEjr1zCsicMWpAA”表示授权服务器本地的授权更新端口地址以及附带的参数信息，“Host”部分则描述了授权服务器地址，本实施例中为“http://authzserver.thnings.com”。AE在向AS发送授权更新请求时也可以直接 使用GET请求访问重定向响应中Location参数所提供的重定向URL，而不使用Host参数，例如该授权更新请求可以为：

[0356] GET http://authzserver.things.com/authzupdate?from＝/CSE0006/CAE0001

[0357] &res_uri＝/CSE0003/resource1&token＝2YotnFZFEjr1zCsicMWpAA HTTP/1.1

[0358] 步骤714：当收到AE的授权更新请求后，授权服务器确定本地存在与所述授权更新请求中的token对应的授权关系。

[0359] 具体的，当AS收到AE的授权更新请求后，AS首先从所述授权更新请求的查询字符串中解析得到token和被访问资源的URI，例如token为“2YotnFZFEjr1zCsicMWpAA”，被访问资源的URI为“/CSE0003/resource1”。然后AS在本地保存的授权关系映射表中查找“Token”栏数值为“2YotnFZFEjr1zCsicMWpAA”且“被访问资源URI”栏数值为“/CSE0003/resource1”的授权关系；当授权关系映射表采用如步骤536中表10所述的RESTful资源AuthzRelMapTable实现时，即在AuthzRelMapTable的属性中，查找token取值等于“2YotnFZFEjr1zCsicMWpAA”且res_uri等于“/CSE0003/resource1”的authzRecord授权关系。若不存在符合上述条件的授权记录则AS拒绝AE的授权更新请求，向AE返回授权更新失败响应：HTTP/1.1 404 Not Found，其中，HTTP响应的状态码为“404”，表示AS没有找到对应的授权记录；若存在符合条件的授权关系，则AS向AE返回的授权更新响应，请求AE对该token进行签名。

[0360] 步骤716：授权服务器向AE返回授权更新响应，该响应包含HTTP 202响应码、token和一个签名请求标志位。

[0361] 具体的，当AS启动授权更新流程后，AS向AE返回的授权更新响应为：

[0362] HTTP/1.1 202 Accepted

[0363] Content-type:application/onem2m-resource+json

[0364] {“token”:“2YotnFZFEjr1zCsicMWpAA”,

[0365] “SigReq”:“1”}

[0366] 其中，HTTP响应的状态码为“202”，表示AS已接受了AE的授权更新请求，但需要进一步的信息并等待后续处理。HTTP消息体中的““token”:“2YotnFZFEjr1zCsicMWpAA””表示与该token对应的授权关系在请求签名，AE 需要对该授权关系对应的验证信息进行签名，在本实施例中该验证信息即token本身，在具体实现时也可以使用其他信息(如原AE-ID等)作为验证信息，取决于AS授权更新端口的具体实现方式而定。HTTP消息体中的““SigReq”:“1””部分为一个签名请求标志位，表示需要AE进一步提供token签名数据以使AS能确认AE的身份。

[0367] 需要说明的是,具体实现中授权更新响应中的验证信息token并不是必须的。

[0368] 步骤718:当AE检测所收到资源访问响应中包含签名请求标志位时,则使用设备出厂密钥对所收到的token进行签名。

[0369] 具体的,在AE收到H-CSE的资源访问响应后,当检测得到HTTP响应的状态码为“202”和HTTP消息体中包含“SigReq”参数且取值为“1”时,AE对token进行签名。。

[0370] 步骤720:当AE完成token签名后,AE向授权服务器发起签名验证请求,该请求包含AE-ID2、token和token签名。

[0371] 具体的,当AE完成token签名后,AE向AS发起签名验证请求为:

[0372] PUT http://authzserver.things.com/authzupdate HTTP/1.1

[0373] From:/CSE0006/CAE0001

[0374] Content-type:application/onem2m-resource+json

[0375] {“token”:“2YotnFZFEjr1zCsicMWpAA”,

[0376] “token_sig”:“8456B1CD”,

[0377] “res_uri”:“/CSE0003/resource1”}

[0378] 其中,各参数解释可参见步骤534的描述,本发明实施例在此不再详述。

[0379] 步骤722:授权服务器从AE的签名验证请求中获取token和token签名,然后在授权关系映射表中查找与token对应的授权关系,并验证签名验证请求中的token签名是否与该授权关系中的token签名一致。

[0380] 具体的,当AS收到AE的签名验证请求时,AS首先从AE的签名验证请求中解析得到token数值“2YotnFZFEjr1zCsicMWpAA”和token签名数值“8456B1CD”,然后AS在本地保存的授权关系映射表中查找“Token”栏取值 等于“2YotnFZFEjr1zCsicMWpAA”的授权关系,并比较该授权关系的“Token签名”栏是否等于“8456B1CD”。若对应授权记录的“Token签名”栏不等于“8456B1CD”,AS向AE返回签名验证失败响应,该响应包含HTTP 403响应码,例如:HTTP/1.1 403 Forbidden;若“Token签名”栏等于“8456B1CD”,则AS对该授权关系进行更新,即将该token对应的授权关系中的访问设备标识AE-ID1更改为当前访问设备标识AE-ID2。

[0381] 步骤724:授权服务器向资源服务器发送第二授权更新请求,该请求中包括被访问资源URI、token和AE-ID2。

[0382] 具体的,在AS对授权记录进行更新时,AS向H-CSE发起的授权更新请求可以为:

[0383] PUT http://m2m.things.com/CSE0003/resource1 HTTP/1.1

[0384] From:/CSE0006/CAE0003

[0385] Content-type:application/onem2m-resource+json

[0386] {“token”:“2YotnFZFEjr1zCsicMWpAA”}

[0387] 其中,PUT请求的URL表示需要更新的被访问资源的URI,即“/CSE0003/resource1”,“From”部分表示访问设备的新的应用标识AE-ID2,即“/CSE0006/CAE0003”,HTTP消息体中的““token”:“2YotnFZFEjr1zCsicMWpAA””部分表示与该访问设备和被访问资源URI对应的访问令牌具体数值为“2YotnFZFEjr1zCsicMWpAA”。

[0388] 步骤726:在收到授权服务器的第二授权更新请求后,资源服务器根据被访问资源URI找到本地保存的被访问资源resource1,并在resource1的授权关系属性中查找访问令牌为token的授权记录,并将该授权记录的访问设备标识更新为AE-ID2。

[0389] 具体的，在H-CSE收到AS的授权更新请求后，H-CSE首先从所述授权更新请求的URL部分获取被访问资源URI，即“/CSE0003/resource1”，并在本地找到该资源resource1。然后，H-CSE分别从授权更新请求的“From”头域和HTTP消息体中解析得到token和AE-ID2数值，即token为“2YotnFZFEjr1zCsicMWpAA”和AE-ID2为“/CSE0006/CAE0001”，在resource1的授权关系属性中查找访问令牌为token的授权记录，并将该授权记录的访问设 备应用标识更新为AE-ID2。具体的，H-CSE在resource1的authzRel属性中查找authzProof属性值等于“2YotnFZFEjr1zCsicMWpAA”的授权记录，然后将该授权记录对应的subjectID属性值改为“/CSE0006/CAE0003”。

[0390] 步骤728：在完成本地授权更新后，资源服务器向授权服务器返回第二授权更新响应，该响应包含HTTP 200状态码。

[0391] 具体的，在H-CSE完成本地授权更新后，H-CSE向AS返回的授权更新响应为：

[0392] HTTP/1.1 200OK

[0393] 其中，HTTP响应的状态码为“200”，表示H-CSE已完成对应资源的授权更新。

[0394] 步骤730：授权服务器向AE返回签名验证响应，该响应中包含HTTP 200响应码。

[0395] 具体的，在AS收到H-CSE的授权更新响应后，AS向AE返回的签名验证响应为：

[0396] HTTP/1.1 200 OK

[0397] 其中，HTTP响应的状态码为“200”，表示AS已完成签名验证并M2M系统已完成授权更新。

[0398] 步骤732：在AE确定M2M系统已完成授权更新后，AE即可按照已有的资源访问流程向H-CSE发起资源访问请求，并获取到对应的资源。

[0399] 本发明实施例中，当M2M系统中的M2M设备，如AE，在标识发生变化后，访问被访问资源时，资源服务器触发授权关系更新流程，M2M系统通过验证访问设备对验证信息的签名(token的签名)来确定访问设备的身份，并更新已有的授权关系，使得M2M设备能够实现无缝的资源访问，保证了M2M系统的业务连续性。

[0400] 由图6所述授权方法可知，M2M系统采用Oauth授权架构对访问设备访问资源进行授权时，授权服务器上保存有访问设备标识、token、token签名和被访问资源URI相对应的授权关系；而资源服务器上保存有访问设备标识、token以及被访问资源URI相对应的授权关系。当访问设备标识发生变化后，再去资源服务器上请求访问所述被访问资源时，资源服务器拒绝访问，并将访问设备的 资源访问请求重定向到授权服务器上进行授权更新，由授权服务器根据验证信息的签名，即token的签名，来确定访问设备的身份，进而更新M2M系统的授权关系。实际上，也可以由资源服务器来验证访问设备的身份，进而更新M2M系统的授权关系。

[0401] 参阅图8，图8为本发明提供的另一种基于Oauth授权架构的授权更新的流程图。

[0402] 步骤802-步骤808同图7所述的实施例中的步骤702-708，相关描述请参见图7所述实施例的相关步骤，这里不再详述。

[0403] 步骤810：资源服务器向授权服务器(AS)发送签名数据请求，该请求中包含token。

[0404] 具体的，当H-CSE发起授权更新流程时，H-CSE向授权服务器发送的签名数据请求为：

[0405] GET http://authzserver.things.com/sigquery?token=

2YotnFZFEjr1zCsicMWpAA HTTP/1.1

[0406] 其中,“http://authzserver.things.com/sigquery”即为该授权服务器的签名数据请求端口地址,“?token＝2YotnFZFEjr1zCsicMWpAA”为所请求签名对应的访问令牌,以查询字符串的形式表示。

[0407] 步骤812:授权服务器在本地的授权关系映射表中获取与签名数据请求中的token对应的授权关系中的签名。

[0408] 具体的,当AS收到H-CSE的签名数据请求后,首先从所述签名数据请求的查询字符串中解析得到token数值,例如“2YotnFZFEjr1zCsicMWpAA”。然后,AS在本地保存的授权关系映射表中进行查找,在“Token”栏中查找与签名数据请求中的token相同的授权关系,并获取对应授权关系的“Token签名”数值。例如在步骤636中描述的授权关系映射表(表9)中,在“Token”栏中查找数值等于“2YotnFZFEjr1zCsicMWpAA”的授权关系,然后提取该授权关系的“Token签名”,即“8456B1CD”。

[0409] 步骤814:授权服务器向资源服务器返回签名数据响应,所述签名数据响应包括token的签名;

[0410] 具体的,AS向H-CSE返回的签名数据响应为:

[0411] HTTP/1.1 200 OK

[0412] Content-type:application/onem2m-resource+json

[0413] {“token_sig”:“8456B1CD”}

[0414] 其中,HTTP响应的状态码为“200”,表示本次签名数据请求已被许可。HTTP消息体中,““token_sig”:“8456B1CD””部分表示所请求的token签名数值为“8456B1CD”。

[0415] 步骤816:资源服务器向AE返回资源访问响应,该响应中包括签名请求标志位。

[0416] 具体的,当H-CSE收到AS的签名数据响应后,H-CSE向AE返回的资源访问响应可以为:

[0417] HTTP/1.1 202 Accepted

[0418] Content-type:application/onem2m-resource+json

[0419] {“token”:“2YotnFZFEjr1zCsicMWpAA”,

[0420] “SigReq”:“1”}

[0421] 其中,HTTP响应的状态码为“202”,表示本次资源访问请求已被处理,但需要进一步的信息并等待后续处理。HTTP消息体中,““token”:“2YotnFZFEjr1zCsicMWpAA””部分表示AE需要提供的签名数据是与该token对应的,该参数主要是针对H-CSE同时处理多个由该AE发起的资源访问请求的情况,该参数用于让AE区分不同资源访问响应消息;““SigReq”:“1””部分为一个签名请求标志位,表示需要AE进一步提供token签名数据以使H-CSE能确认AE的身份。

[0422] 步骤818:当AE检测所收到资源访问响应中包含签名请求标志位时,则使用设备出厂密钥对所收到的token进行签名。

[0423] 该步骤同步骤718,请参与步骤718的相关的描述,这里不再赘述。

[0424] 步骤820:当AE完成token签名后,AE向H-CSE再次发起资源访问请求,该请求中包含AE-ID2、初始授权得到的token、token签名和资源URI。

[0425] 具体的,当AE完成token签名后,AE向H-CSE发起的资源访问请求可以为:

[0426] GET http://m2m.things.com/CSE0003/resource1?from＝/CSE0006/CAE0001

[0427] &token＝2YotnFZFEjr1zCsicMWpAA&token_sig＝8456B1CD HTTP/1.1

[0428] 其中，相比于步骤806中描述的资源访问请求，本步骤中资源访问请求所携带的信息增加了访问令牌签名参数，即“token_sig＝8456B1CD”，该部分表示本次资源访问请求不仅携带了访问令牌，还携带了访问令牌对应的签名数据。

[0429] 步骤822：在收到AE的资源访问请求后，H-CSE从资源访问请求中获取token签名，确定该token签名与步骤814中从授权服务器获取的token签名是否相同。

[0430] 具体的，在H-CSE收到AE的资源访问请求后，H-CSE首先从资源访问请求的HTTP消息体中解析得到token签名，即获取“token_sig”参数对应的取值“8456B1CD”。然后，将资源访问请求中的token签名与步骤814中所述的签名数据响应中的token签名进行比较，例如本实施例中上述两者取值均为“8456B1CD”，当两者相同时即确认该资源访问请求的访问设备AE与初始授权时的AE是同一个访问设备；如果两者不同，则资源服务器拒绝访问设备的访问，流程结束。

[0431] 步骤824：在资源服务器确认签名合法后，H-CSE向AS发起授权更新请求，该请求包含token和AE-ID2。

[0432] 具体的，在H-CSE确认AE与初始授权的访问设备的对应关系后，H-CSE向AS发起的授权更新请求可以为：

[0433] PUT http://authzserver.things.com/authzupdate HTTP/1.1

[0434] From:/CSE0006/CAE0001

[0435] Content-type:application/onem2m-resource+json

[0436] {“token”:“2YotnFZFEjr1zCsicMWpAA”}

[0437] 其中，PUT请求的URL地址，即“http://authzserver.things.com/authzupdate”为AS的授权更新端口地址，“From”部分表示需要授权更新的访问设备的新标识AE-ID2，即“/CSE0006/CAE0003”，HTTP消息体中的“token”表示需要更新的授权关系中对应token的取值，即需要更新的授权关系中token取值为“2YotnFZFEjr1zCsicMWpAA”，该参数用于让AS找到需要更新的授权关系。

[0438] 步骤828：授权服务器对本地保存的授权关系映射表进行更新。

[0439] 具体的，当AS收到H-CSE的授权更新请求后，首先从授权更新请求中解析得到访问设备的新标识“/CSE0006/CAE0003”，以及与本次资源访问请求所对应授权关系的token取值“2YotnFZFEjr1zCsicMWpAA”；然后，AS在本地保存的授权关系映射表中查找“Token”栏取值为“2YotnFZFEjr1zCsicMWpAA”的授权关系，所述授权关系映射表如步骤609中表9的描述。当AS找到对应的授权关系后，即将所述授权关系的“访问设备标识”栏的原数值“/CSE0005/CAE0001”替换为授权更新请求中的新标识“/CSE0006/CAE0003”。当授权关系映射表采用如步骤609所述的RESTful资源AuthzRelMapTable实现时，该授权更新即在AuthzRelMapTable的属性中，查找token取值等于“2YotnFZFEjr1zCsicMWpAA”的authzRecord授权关系，并将该授权记录的subjectID更新为“/CSE0006/CAE0003”。

[0440] 步骤828：当授权服务器完成授权关系映射表的更新后，向资源服务器返回授权更新响应。

[0441] 具体的，当AS完成授权关系映射表的更新后，AS向H-CSE返回的授权更新响应为：

[0442] HTTP/1.1 200 OK

[0443] 其中,HTTP响应的状态码为“200”,表示AS已成功更新授权关系映射表。

[0444] 步骤830:当资源服务器收到授权服务器的授权更新响应后,对被访问资源关联的授权关系进行更新。

[0445] 具体的,当H-CSE收到AS的授权更新响应后,即在被访问资源的authzRel属性中查找authzProof等于token(“2YotnFZFEjr1zCsicMWpAA”)的授权关系,并将该授权关系中的subjectID取值更新为“/CSE0006/CAE0003”。

[0446] 步骤832:当资源服务器完成被访问资源关联的授权关系更新后,按照正常的资源访问流程向AE返回资源访问响应。

[0447] 具体的,当H-CSE完成被访问资源关联的授权关系更新后,H-CSE向AE返回的资源访问响应可以为:

[0448] HTTP/1.1 200 OK

[0449] Content-type:application/onem2m-resource+json

[0450] {“content”:“xxxxxxxxxxxx”}

[0451] 其中,HTTP响应的状态码为“200”,表示H-CSE已许可AE本次资源访问请求,HTTP消息体中则包含了AE所请求的资源内容,本实施例中““content”:“xxxxxxxxxxxx””仅示意资源内容包含在HTTP消息体中返回给AE,具体返回格式和内容根据被访问资源的类型确定,本发明不做限定。

[0452] 本发明实施例中,当M2M系统中的M2M设备,如AE,在标识发生变化后,访问被访问资源时,资源服务器触发授权关系更新流程,M2M系统通过验证访问设备对验证信息的签名(token的签名)来确定访问设备的身份,并更新已有的授权关系,使得M2M设备能够实现无缝的资源访问,保证了M2M系统的业务连续性。

[0453] 本发明实施例还描述了与图2所示实施例属于同一发明构思下的一种授权服务器,如图9所示,图9为本发明实施例提供的授权服务器的结构示意图,该授权服务器可以包括:接收模块901、发送模块902、获取模块903、确定模块904和更新模块905,其中:

[0454] 接收模块901,用于接收访问设备发送的第一授权更新请求,所述第一授权更新请求包括所述访问设备的第一标识;

[0455] 发送模块902,用于向所述访问设备发送第一授权更新响应,所述第一授权更新响应包括签名请求信息,所述签名请求信息指示所述访问设备对验证信息进行签名;

[0456] 所述接收模块901,还用于接收所述访问设备发送的签名验证请求,所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名;其中,所述验证信息的签名为所述访问设备使用密钥对所述验证信息进行签名生成的;

[0457] 获取模块903,用于根据所述接收模块接收到的签名验证请求中的验证信息,获取保存的第一授权关系;

[0458] 确定模块904,用于根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名,确定所述签名验证请求中的验证信息的签名合法;

[0459] 更新模块905,用于根据所述第一标识,更新所述第一授权关系。

[0460] 其中,所述更新模块用于根据所述第一标识,更新所述第一授权关系,具 体为:将所述第一授权关系中的第二标识更改为所述第一标识,其中,所述第二标识为所述访问设

备使用过的标识。

[0461] 具体的，所述授权服务器还包括初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权。

[0462] 可选的，当所述验证信息为所述访问设备保存的所述第二标识时，所述签名验证请求中进一步还包括所述第一标识的签名，其中所述第一标识的签名为所述访问设备使用所述密钥对所述第一标识进行签名生成的；所述更新模块905，还用于将所述第一授权关系中保存的验证信息的签名更改为所述第一标识的签名。所述初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：向资源服务器发送资源创建请求，所述资源创建请求包括预设的访问控制策略和所述被访问资源标识，其中，所述预设的访问控制策略包括所述第二标识；接收所述资源服务器发送的资源创建响应，所述资源创建响应指示所述资源服务器成功创建所述访问控制策略资源且将所述访问控制策略资源与所述被访问资源标识对应的资源进行绑定；向所述访问设备发送签名请求，所述签名请求指示所述访问设备对所述第二标识进行签名；接收所述访问设备发送的签名响应，所述签名响应包括所述第二标识的签名；保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述第二标识的签名和所述被访问资源标识的对应关系。可选的，所述发送模块902，还用于在根据所述第一标识，更新所述第一授权关系之后，向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述第二标识和所述被访问资源标识，以便于所述资源服务器根据所述所述第二标识和所述被访问资源标识获取本地保存第二授权关系，并将所述第二授权关系中的第二标识更新为所述第一标识。

[0463] 可选的，当所述验证信息为授权凭证，所述第一授权更新请求还包括所述授权凭证，所述确定模块904，还用于在所述向所述访问设备发送第一授权更新响应之前，根据所述授权凭证，确定存在包含所述授权凭证的所述第一授权关系，且所述第一授权关系中绑定的设备标识不是所述第一标识。所述初始授权模块，用于对所述访问设备访问所述被访问资源标识对应的资源进行初始授权，具体为：接收所述访问设备的授权请求，所述授权请求包括所述第二标识、所述被访问资源标识和用户同意所述访问设备访问资源的认证信息；当根据所述认证信息，确定所述用户具有访问所述被访问资源标识对应的资源的权限时， 生成所述授权凭证；向所述被访问资源标识对应的资源所在的资源服务器发送授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；接收所述资源服务器发送的授权绑定响应，所述授权绑定响应包含绑定成功的指示信息；向所述访问设备发送授权响应，所述授权响应包括所述授权凭证、所述被访问资源标识和对所述授权凭证进行签名的指示信息；接收所述访问设备发送的签名绑定请求，所述签名绑定请求包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识，其中，所述授权凭证的签名为所述访问设备对所述授权凭证使用所述密钥签名生成的；保存所述第一授权关系，所述第一授权关系包括所述第二标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识的对应关系。可选的，所述发送模块902，还用于在根据所述第一标识，更新所述第一授权关系之后，向资源服务器发送第二授权更新请求，所述第二授权更新请求包括所述第一标识、所述授权凭证和所述被访问资源标识，以便于所述资源服务器根据所述授权凭证和所述被访问资源标识获取所述第二授权关系，并将所述第二授权关系中的第二标识更新为所述第一标识。

[0464] 图10描述了本发明另一个实施例提供的授权服务器的结构，用于执行前述图2、图4、图5、图6和图7所述实施例的授权服务器实施的授权方法，包括至少一个处理器1001(例如CPU)，至少一个网络接口1002或者其他通信接口，存储器1003，和至少一个通信总线1004，用于实现这些装置之间的连接通信。处理器1001用于执行存储器1003中存储的可执行程序，例如计算机程序。存储器1003可能包含高速随机存取存储器(RAM:Random Access Memory)，也可能还包括非不稳定的存储器(non-volatile memory)，例如至少一个磁盘存储器。通过至少一个网络接口1002(可以是有线或者无线)实现该系统网关与至少一个其他网元之间的通信连接，可以使用互联网，广域网，本地网，城域网等。

[0465] 在一些实施方式中，存储器1003存储了程序10031，程序10031可以被处理器1001执行，这个程序包括：接收访问设备发送的第一授权更新请求，所述第一授权更新请求包括所述访问设备的第一标识；向所述访问设备发送第一授权更新响应，所述第一授权更新响应包括签名请求信息，所述签名请求信息指示所述访问设备对验证信息进行签名；接收所述访问设备发送的签名验证请求，所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名；其中，所述验证信息的签名为所述访问设备使用密钥对所述验证信 息进行签名生成的；根据所述验证信息，获取保存的第一授权关系；根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名，确定所述签名验证请求中的验证信息的签名合法；根据所述第一标识，更新所述第一授权关系。

[0466] 本发明实施例还描述了与图3所示实施例属于同一发明构思下的一种资源服务器，如图11所示，图11为本发明实施例提供的资源服务器的结构示意图，该授权服务器可以包括：接收模块1101、确定模块1102、发送模块1103、和更新模块1104，其中：

[0467] 接收模块1101，用于接收访问设备发送的第一资源访问请求，所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证；

[0468] 确定模块1102，用于根据所述授权凭证，确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系，且所述第二授权关系中绑定的设备标识不是所述第一标识；

[0469] 发送模块1103，用于向所述访问设备发送第一资源访问响应，所述第一资源访问响应包括签名请求信息，所述签名请求信息指示所述访问设备对所述授权凭证进行签名；

[0470] 所述接收模块1101，还用于接收所述访问设备发送的第二资源访问请求，所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识；其中，所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生成的；

[0471] 所述发送模块1103，还用于向授权服务器发送签名数据请求，所述签名数据请求包含所述授权凭证；

[0472] 所述接收模块1101，还用于接收所述授权服务器发送的签名数据响应，所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名；

[0473] 所述确定模块1102，还用于根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名，确定所述第二资源访问请求中的授权凭证的签名合法；

[0474] 更新模块1104，用于根据所述第一标识，更新所述第二授权关系。

[0475] 可选的，所述更新模块，用于根据所述第一标识，更新所述第二授权关系，具体为：将所述第二授权关系中的第二标识更改为所述第一标识，其中，所述第二标识为所述访问设备使用过的标识。

[0476] 其中，所述发送模块1103还用于，在根据所述第一标识，更新所述第二授权关系之后，向所述访问设备发送第二资源访问响应，所述第二资源访问响应包括所述被访问资源标识对应的资源。

[0477] 具体的，所述接收模块1101，还用于接收授权服务器对所述访问设备访问所述被访问资源标识对应的资源进行初始授权后发送的授权绑定请求，所述授权绑定请求包括所述第二标识、所述授权凭证和所述被访问资源标识；所述资源服务器进一步还包括存储模块，用于将所述第二标识、所述授权凭证和所述被访问资源标识的对应关系保存为第二授权关系。

[0478] 图12描述了本发明另一个实施例提供的资源服务器的结构，用于执行前述图3、图6和图8所述实施例中资源服务器实施的授权方法，包括至少一个处理器1201(例如CPU)，至少一个网络接口1202或者其他通信接口，存储器1203，和至少一个通信总线1204，用于实现这些装置之间的连接通信。处理器1201用于执行存储器1203中存储的可执行程序，例如计算机程序。存储器1203可能包含高速随机存取存储器(RAM:Random Access Memory)，也可能还包括非不稳定的存储器(non-volatile memory)，例如至少一个磁盘存储器。通过至少一个网络接口1202(可以是有线或者无线)实现该系统网关与至少一个其他网元之间的通信连接，可以使用互联网，广域网，本地网，城域网等。

[0479] 在一些实施方式中，存储器1203存储了程序12031，程序12031可以被处理器1201执行，这个程序包括：接收访问设备发送的第一资源访问请求，所述第一资源访问请求包括所述访问设备的第一标识、被访问资源标识以及授权凭证；根据所述授权凭证，确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系，且所述第二授权关系中绑定的访问设备标识不是所述第一标识；向所述访问设备发送第一资源访问响应，所述第一资源访问响应包括签名请求信息，所述签名请求信息指示所述访问设备对所述授权凭证进行签名；接收所述访问设备发送的第二资源访问请求，所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识；其中，所述授权凭证的签名为所述访问设备使用密钥对所述授权凭证进行签名生 成的；向授权服务器发送签名数据请求，所述签名数据请求包含所述授权凭证；接收所述授权服务器发送的签名数据响应，所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名；根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名，确定所述第二资源访问请求中的授权凭证的签名合法；根据所述第一标识，更新所述第二授权关系。

[0480] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0481] 上述装置和系统内的各模块之间的信息交互、执行过程等内容，由于与本发明方

法实施例基于同一构思,具体内容可参见本发明方法实施例中的叙述,此处不再赘述。

[0482] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,上述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,上述的存储介质可为磁碟、光盘、只读存储记忆体(ROM:Read-Only Memory)或随机存储记忆体(RAM:Random Access Memory)等。

[0483] 本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

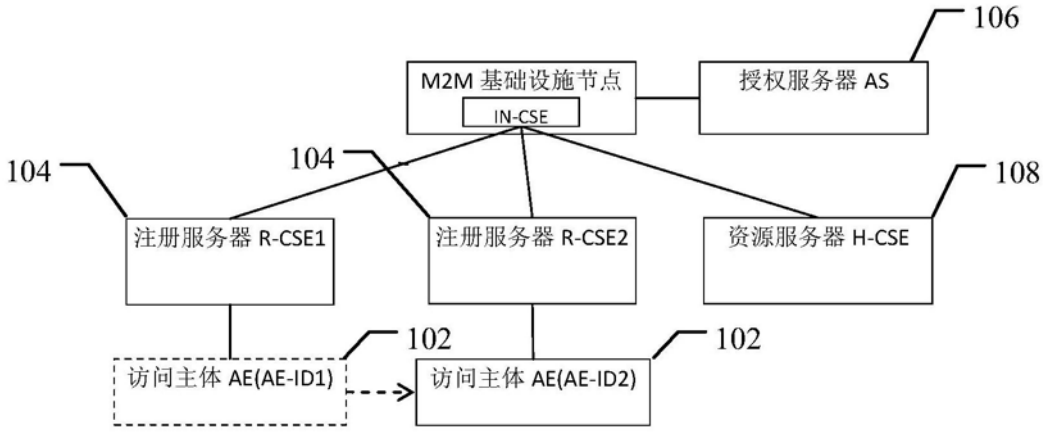

106
M2M 基础设施节点
IN-CSE
授权服务器 AS
104
104
108
注册服务器 R-CSE1
注册服务器 R-CSE2
资源服务器 H-CSE
102
102
访问主体 AE(AE-ID1)
访问主体 AE(AE-ID2)

图1

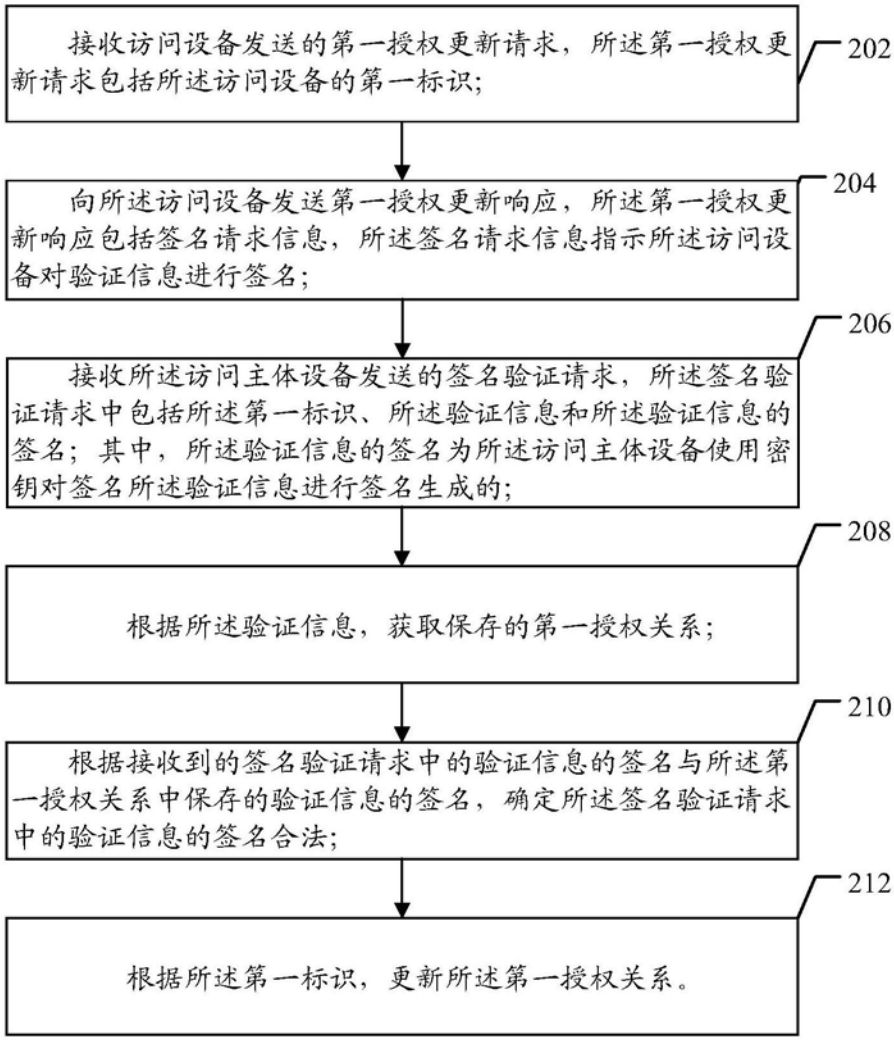

接收访问设备发送的第一授权更新请求，所述第一授权更新请求包括所述访问设备的第一标识；
202
向所述访问设备发送第一授权更新响应，所述第一授权更新响应包括签名请求信息，所述签名请求信息指示所述访问设备对验证信息进行签名；
204
接收所述访问主体设备发送的签名验证请求，所述签名验证请求中包括所述第一标识、所述验证信息和所述验证信息的签名；其中，所述验证信息的签名为所述访问主体设备使用密钥对签名所述验证信息进行签名生成的；
206
根据所述验证信息，获取保存的第一授权关系；
208
根据接收到的签名验证请求中的验证信息的签名与所述第一授权关系中保存的验证信息的签名，确定所述签名验证请求中的验证信息的签名合法；
210
根据所述第一标识，更新所述第一授权关系。
212

图2

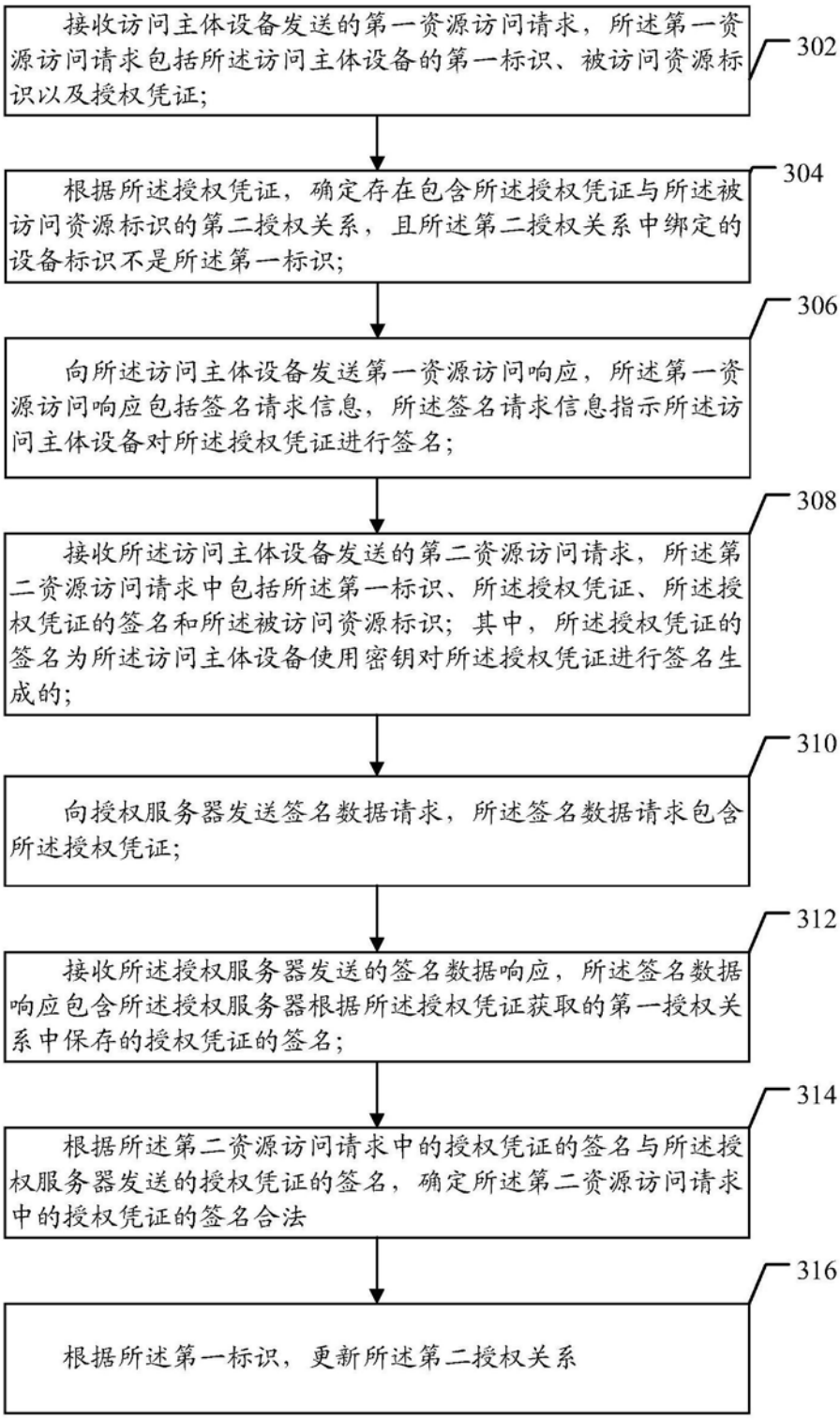

接收访问主体设备发送的第一资源访问请求，所述第一资源访问请求包括所述访问主体设备的第一标识、被访问资源标识以及授权凭证；
302
根据所述授权凭证，确定存在包含所述授权凭证与所述被访问资源标识的第二授权关系，且所述第二授权关系中绑定的设备标识不是所述第一标识；
304
向所述访问主体设备发送第一资源访问响应，所述第一资源访问响应包括签名请求信息，所述签名请求信息指示所述访问主体设备对所述授权凭证进行签名；
306
接收所述访问主体设备发送的第二资源访问请求，所述第二资源访问请求中包括所述第一标识、所述授权凭证、所述授权凭证的签名和所述被访问资源标识；其中，所述授权凭证的签名为所述访问主体设备使用密钥对所述授权凭证进行签名生成的；
308
向授权服务器发送签名数据请求，所述签名数据请求包含所述授权凭证；
310
接收所述授权服务器发送的签名数据响应，所述签名数据响应包含所述授权服务器根据所述授权凭证获取的第一授权关系中保存的授权凭证的签名；
312
根据所述第二资源访问请求中的授权凭证的签名与所述授权服务器发送的授权凭证的签名，确定所述第二资源访问请求中的授权凭证的签名合法
314
根据所述第一标识，更新所述第二授权关系
316

图3

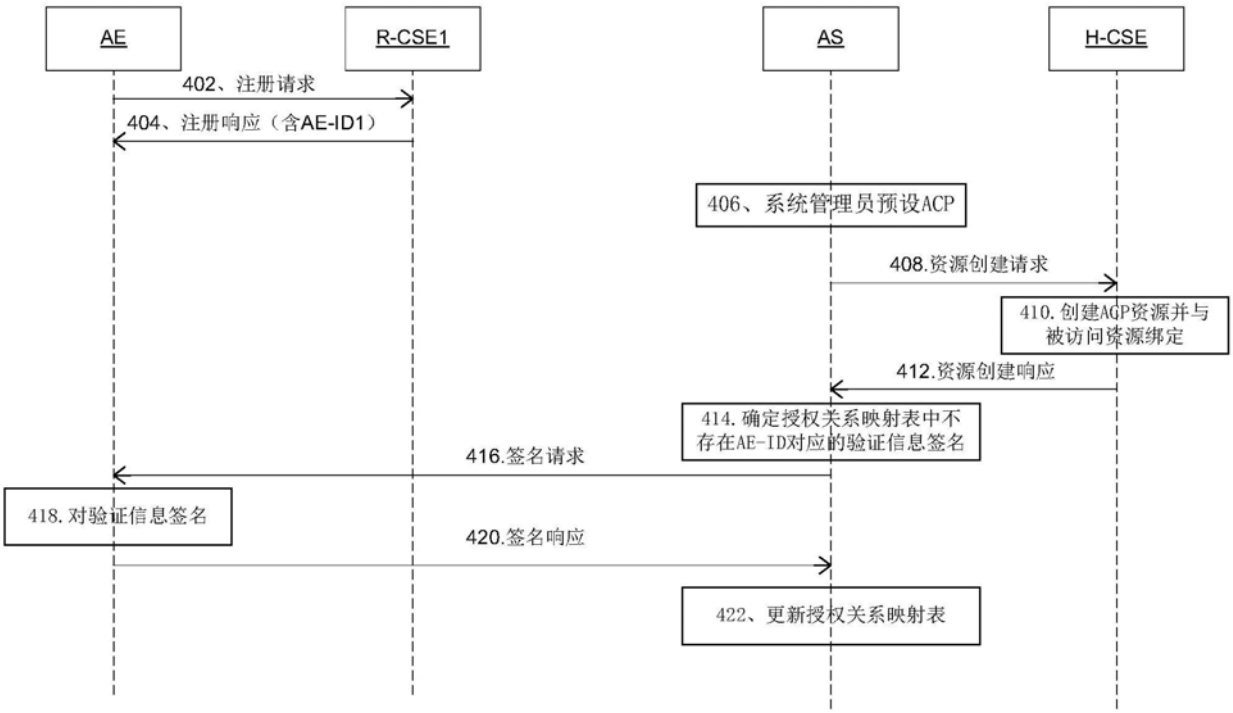

AE
R-CSE1
AS
H-CSE
402、注册请求
404、注册响应（含AE-ID1）
406、系统管理员预设ACP
408.资源创建请求
410.创建AGP资源并与被访问资源绑定
412.资源创建响应
414.确定授权关系映射表中不存在AE-ID对应的验证信息签名
416.签名请求
418.对验证信息签名
420.签名响应
422、更新授权关系映射表

图4

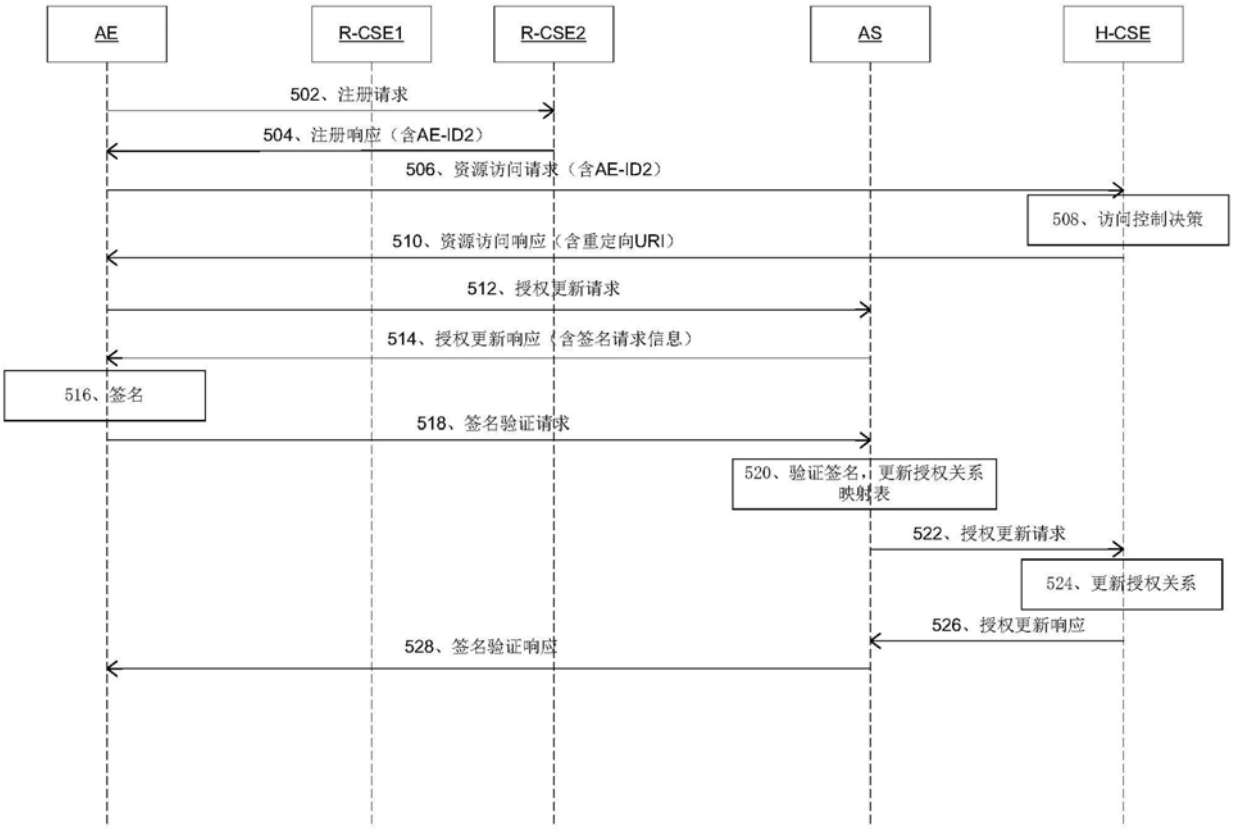

AE
R-CSE1
R-CSE2
AS
H-CSE
502、注册请求
504、注册响应（含AE-ID2）
506、资源访问请求（含AE-ID2）
508、访问控制决策
510、资源访问响应（含重定向URI）
512、授权更新请求
514、授权更新响应（含签名请求信息）
516、签名
518、签名验证请求
520、验证签名，更新授权关系映射表
522、授权更新请求
524、更新授权关系
526、授权更新响应
528、签名验证响应

图5

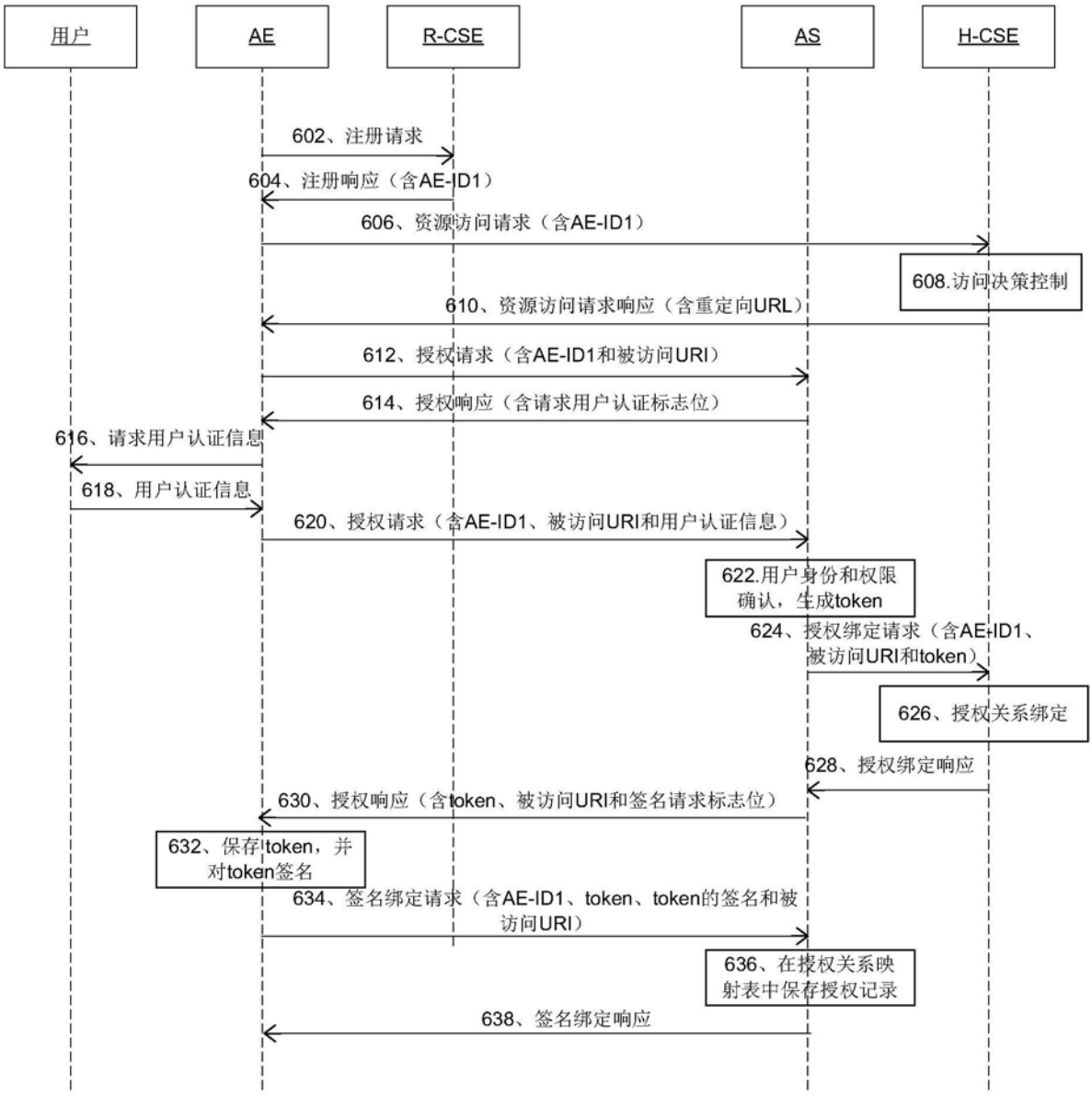

用户
AE
R-CSE
AS
H-CSE
602、注册请求
604、注册响应（含AE-ID1）
606、资源访问请求（含AE-ID1）
608.访问决策控制
610、资源访问请求响应（含重定向URL）
612、授权请求（含AE-ID1和被访问URI）
614、授权响应（含请求用户认证标志位）
616、请求用户认证信息
618、用户认证信息
620、授权请求（含AE-ID1、被访问URI和用户认证信息）
622.用户身份和权限确认，生成token
624、授权绑定请求（含AE-ID1、被访问URI和token）
626、授权关系绑定
628、授权绑定响应
630、授权响应（含token、被访问URI和签名请求标志位）
632、保存token，并对token签名
634、签名绑定请求（含AE-ID1、token、token的签名和被访问URI）
636、在授权关系映射表中保存授权记录
638、签名绑定响应

图6

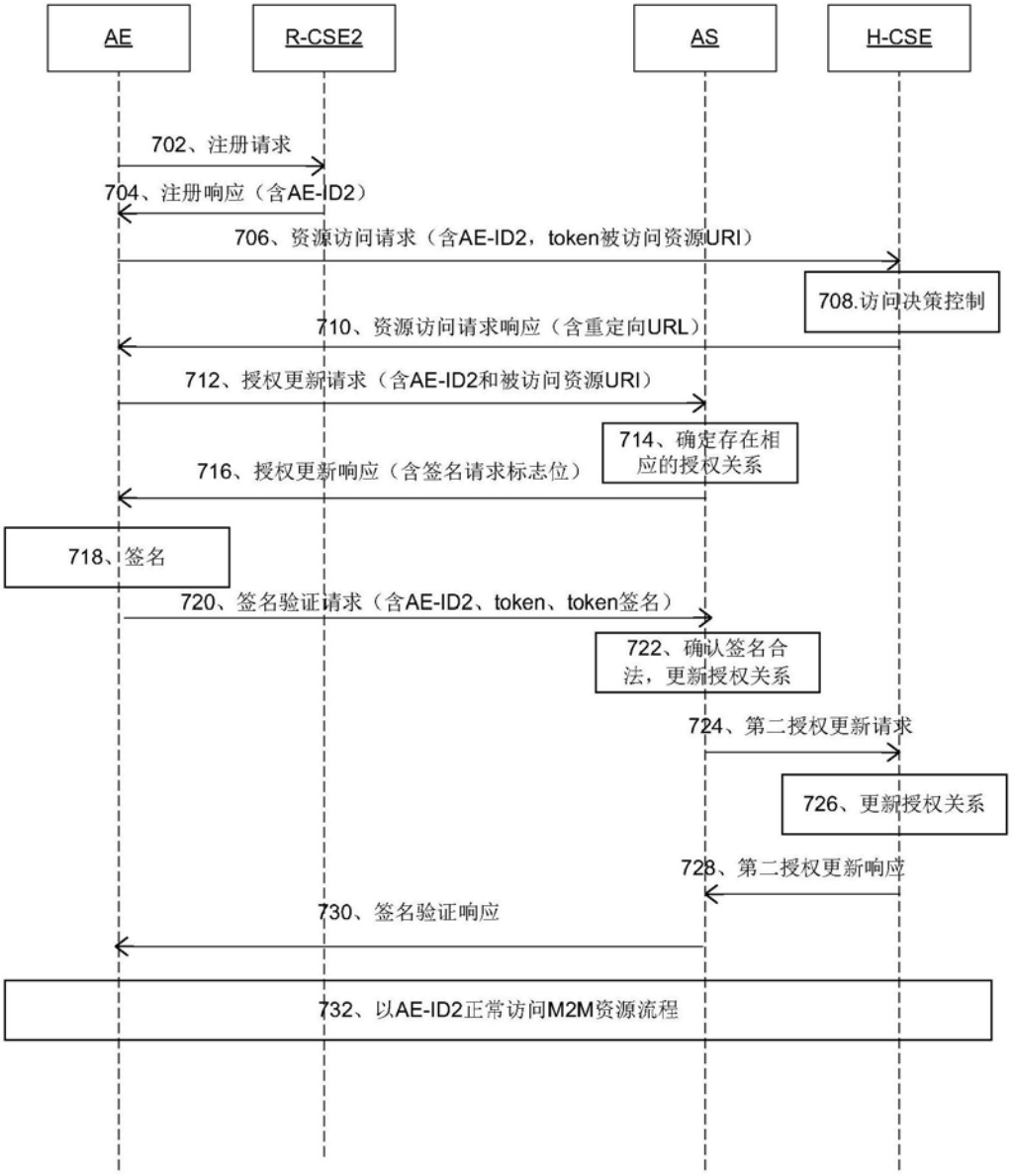

AE
R-CSE2
AS
H-CSE
702、注册请求
704、注册响应（含AE-ID2）
706、资源访问请求（含AE-ID2，token被访问资源URI）
708.访问决策控制
710、资源访问请求响应（含重定向URL）
712、授权更新请求（含AE-ID2和被访问资源URI）
714、确定存在相应的授权关系
716、授权更新响应（含签名请求标志位）
718、签名
720、签名验证请求（含AE-ID2、token、token签名）
722、确认签名合法，更新授权关系
724、第二授权更新请求
726、更新授权关系
728、第二授权更新响应
730、签名验证响应
732、以AE-ID2正常访问M2M资源流程

图7

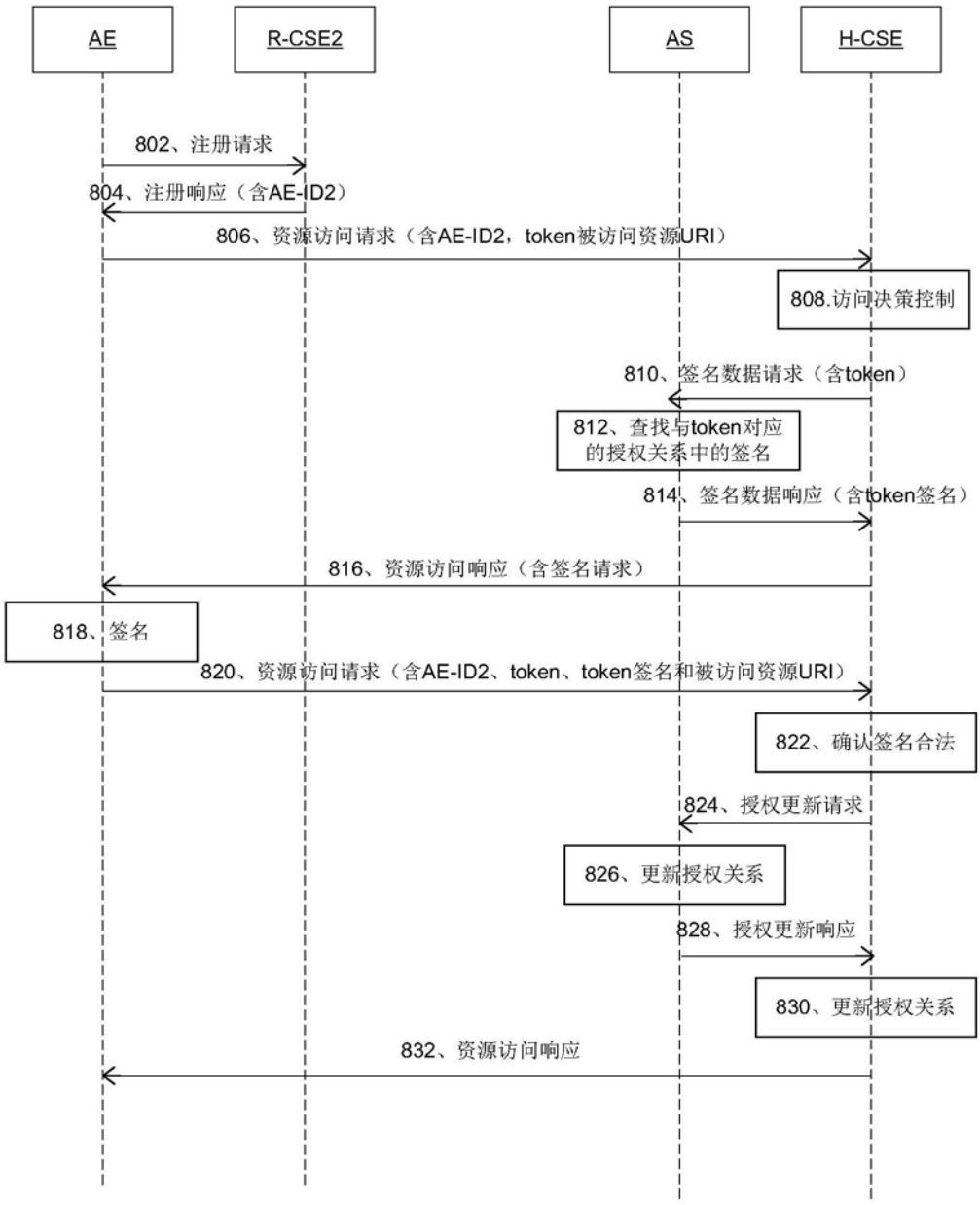

AE
R-CSE2
AS
H-CSE
802、注册请求
804、注册响应（含AE-ID2）
806、资源访问请求（含AE-ID2，token被访问资源URI）
808.访问决策控制
810、签名数据请求（含token）
812、查找与token对应的授权关系中的签名
814、签名数据响应（含token签名）
816、资源访问响应（含签名请求）
818、签名
820、资源访问请求（含AE-ID2、token、token签名和被访问资源URI）
822、确认签名合法
824、授权更新请求
826、更新授权关系
828、授权更新响应
830、更新授权关系
832、资源访问响应

图8

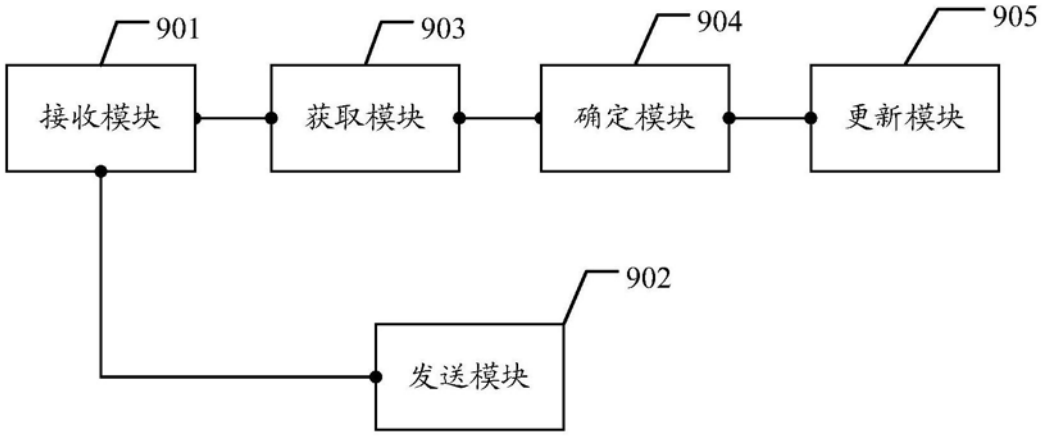

901
903
904
905
接收模块
获取模块
确定模块
更新模块
902
发送模块

图9

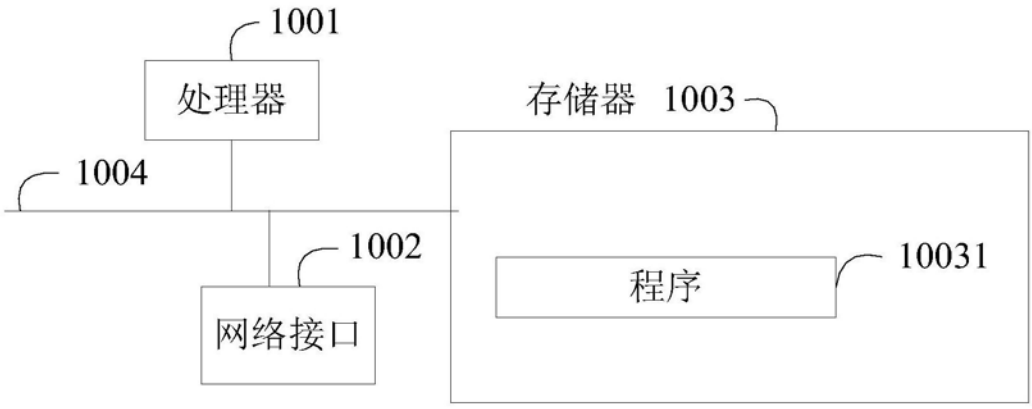

1001
处理器
存储器 1003
1004
1002
网络接口
程序
10031

图10

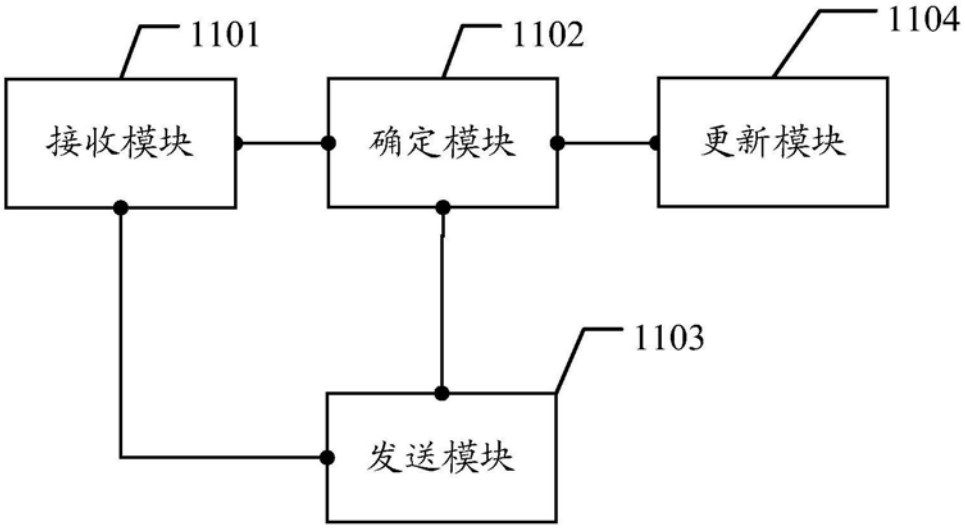

1101
1102
1104
接收模块
确定模块
更新模块
1103
发送模块

图11

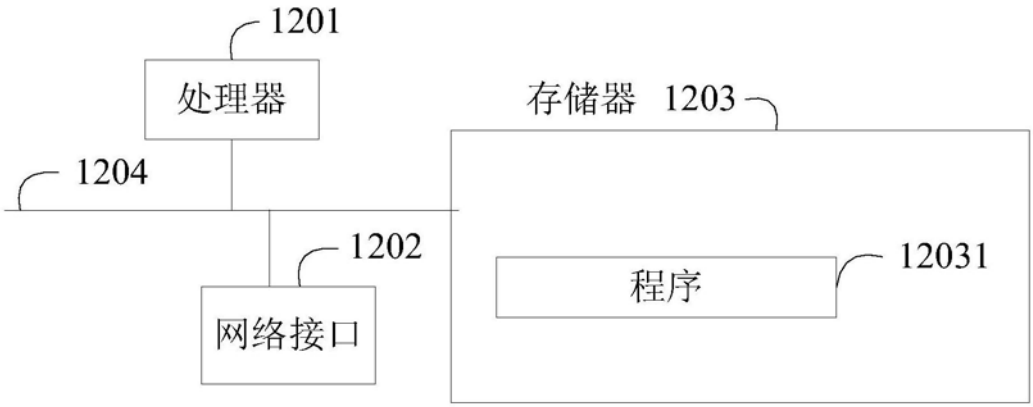


图12