ETSI TR 118 516 V2.0.0 (2016-09)

oneM2M;
Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies
(oneM2M TR-0016 version 2.0.0)

Reference
DTR/oneM2M-000016

Keywords
authorization, IoT, M2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document provides technical solutions for oneM2M authorization architecture, authorization procedures and access control policies. The present document also gives evaluations of these proposed technical solutions.

ETSI TS 118 103 [i.2] only defines a high level authorization architecture that describes its major components and general authorization procedure. The objective of the present document is to provide candidate security solutions related to authorization architecture, authorization procedures and access control policies.

The present document provides security solutions in the following three aspects:

- Detailed design of authorization architecture: This part investigates the interfaces among authorization components (e.g. procedures and parameters), how these components could be distributed in different oneM2M entities (i.e. different CSEs), and how to implement Role Based Access Control (RBAC) and token based access control.
- Supporting user specified access control policies: This part investigates how the oneM2M authorization system could be an extensible system that can support user-defined access control mechanisms and/or access control policy languages.
- Investigating existing access control policy languages: This part investigates if some standardized access control policy languages could become oneM2M recommended access control policy description languages.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[i.2] ETSI TS 118 103: "oneM2M; Security Solutions (oneM2M TS-0003)".

[i.3] ANSI American national standard for information technology - role based access control. ANSI INCITS 359-2004, February 2004.

[i.4] NIST Special Publication 800-162: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations".

[i.5] OASIS Standard: "eXtensible Access Control Markup Language (XACML)", Version 3.0, 22 January 2013.

[i.6] OASIS Standard: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)" V2.0.

[i.7] oneM2M Drafting Rules.

NOTE: Available at http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf.

[i.8] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[i.9] ETSI TR 118 501: "oneM2M; Use Case collection (oneM2M TR-0001)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 118 111 [i.8] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 118 111 [i.8] apply.

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.7].

5 Overview of authorization system

5.1 High level authorization architecture

Figure 5.1-1 provides a high level overview of a generic authorization architecture. This architecture comprises four subcomponents that are described as follows:

- Policy Enforcement Point (PEP):
  - PEP intercepts resource access requests, makes access control decision requests, and enforces access control decisions. The PEP coexists with the entity that needs authorization services.
- Policy Decision Point (PDP):
  - PDP interacts with the PRP and PIP to get applicable authorization polices and attributes needed to evaluate authorization policies respectively, and then evaluates access requests using authorization policies to render an access control decision. The PDP is located in the Authorization service.
- Policy Retrieval Point (PRP):
  - PRP obtains applicable authorization policies according to an access control decision request. These applicable policies should be combined in order to get a finial access control decision. The PRP is located in the Authorization service.

- Policy Information Point (PIP):
  - PIP provides attributes that are needed to evaluate authorization policies, for example the IP address of the requester, creation time of the resource, current time or location information of the requester. The PIP is located in the Authorization service.

The Authorization service may comprise any of the subcomponents: PDP, PRP and/or PIP. This means that the subcomponents PEP, PRP, PDP and PIP could be distributed across different nodes. For example the PEP is located in an ASN/MN and the PDP is located in the IN.

The present release 1 does not support separation of PRP and PIP on different CSE from PDP. The generic procedure described below is provided for information and to support further extensions, while clause 7 provides the details of authorization mechanisms in the current release.

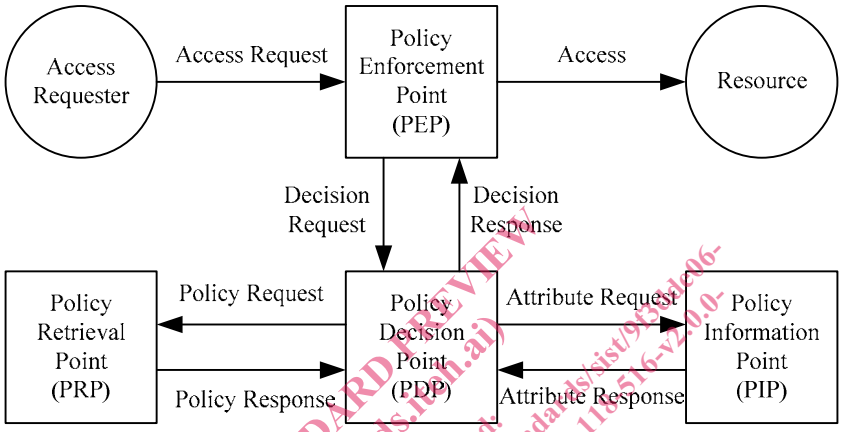

Figure 5.1-1: Overview of the authorization architecture

5.2 Generic authorization procedure

The generic authorization procedure is shown in figure 5.2-1.

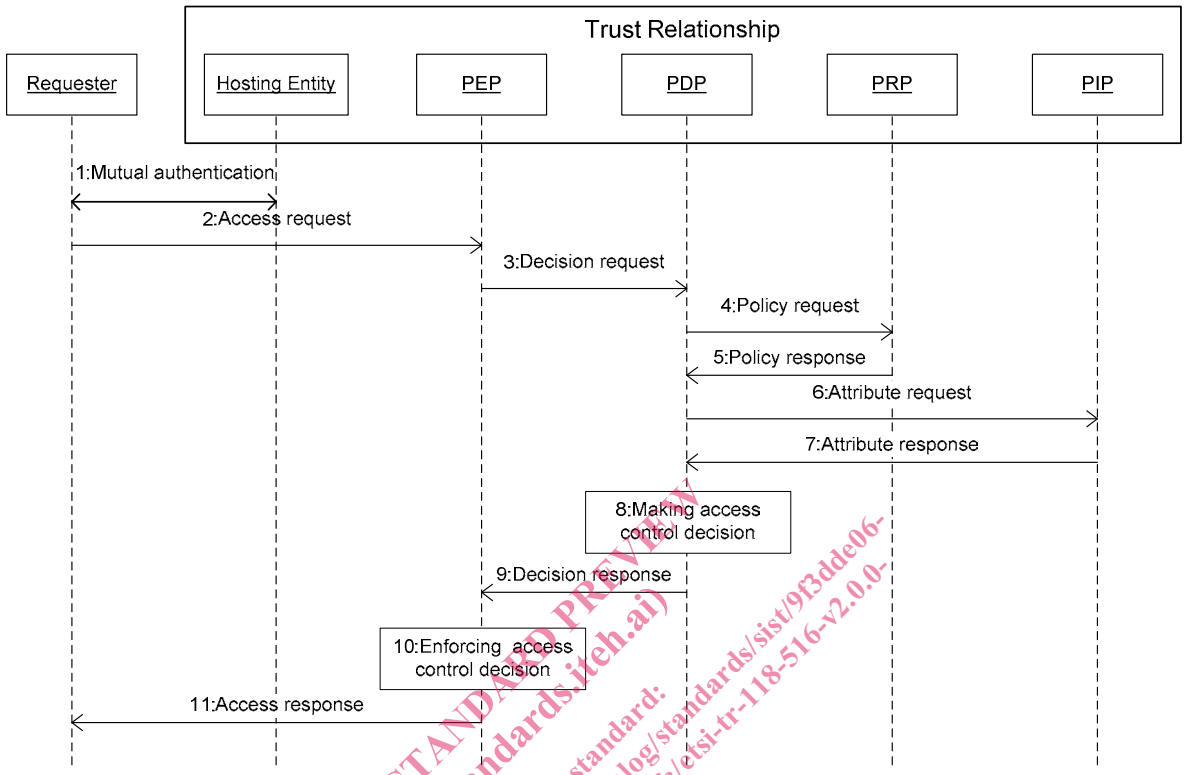

Figure 5.2-1: Authorization Procedure

Step 001: Mutual authentication (Pre-requisite).

Step 002: Access Requester sends an Access Request to the PEP.

Step 003: PEP makes an Access Control Decision Request according to the requester's Access Request, and sends the Access Control Decision Request to the PDP.

Step 004: PDP sends an Access Control Policy Request that is generated based on the Access Control Decision Request to the PRP.

Step 005: PRP finds all access control policies applicable to the access request and sends them back to the PDP. When multiple access control polices are involved, the PRP also provides a policy combination algorithm to combine multiple evaluation results into one finial result.

Step 006 PDP sends Attribute Request to the PIP, if any attributes are needed to evaluate these access control policies.

Step 007: PIP gets requested attributes and sends them back to the PDP.

Step 008: PDP evaluates Access Request using access control policies. When there are multiple applicable access control policies, the PEP needs to calculate a final Access Control Decision using the policy combination algorithm.

Step 009: PDP returns the Access Control Decision to the PEP.

Step 010: PEP enforces the access control decision, i.e. either forwards the Access Request to the resource or denies this access.

Step 011: PEP returns access result back to the Access Requester.

6 Detailed design of authorization architecture

6.1 Self-contained authorization

In a self-contained authorization system the PEP, PDP, PRP and PIP are all in the same CSE, and the messages exchanged between these authorization components are not crossing the oneM2M reference points Mca, Mcc and Mcn. So there is no specific standardization requirement about how to implement PEP, PDP, PRP and PIP, and the interactions between them.

6.2 Distributed authorization

6.2.1 Distributed authorization use cases

6.2.1.1 M2M gateway make access control decisions on behalf of m2m devices

Some constrained M2M Devices may be unable to evaluate the complex access control policy languages, such as those investigated in clause 8 "Investigating existing access control policy languages". These M2M Devices may be configured to request an M2M Gateway to assist with making access control decisions.

Here consider a scenario with two M2M Devices, Device 1 and Device 2, registered to a common M2M Gateway. Device 1 often interacts with M2M Devices that it has not encountered before, and so it frequently encounters situations where the Originator of the request cannot have been configured into the <accessControlPolicies> resources resident on Device 1. In this case, Device 1 has not encountered Device 2 previously, and so Device 1 requests the M2M Gateway to make an access control decision on behalf of Device 1. The relevant access control policies for Device 1 are not present on the M2M Gateway, so the M2M Gateway requests the relevant access control policies from M2M Server 1. When the M2M Gateway receives the access control policies, it realizes that it needs additional information about Device 2, so the M2M Gateway requests the relevant information from M2M Server 2. The M2M Gateway makes the access control decision and returns the decision result to Device 1. Figure 6.2.1.1-1 illustrates this process, which can be seen to map onto figure 5.1-1 "Overview of the authorization architecture".

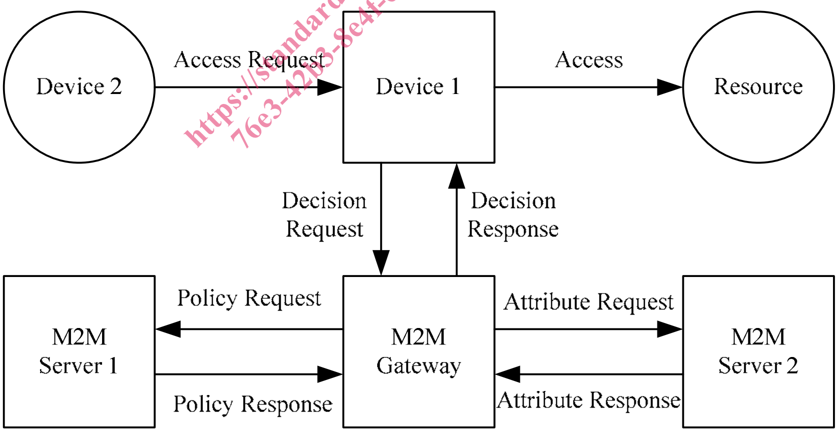

Figure 6.2.1.1-1: Use case scenario where an M2M Gateway makes authorization decisions on behalf of an M2M Device

Table 6.2.1.1-1 provides the mapping from the actors in the present use case scenario to functions in figure 5.1-1. Each authorization component (PEP, PDP, PRP and PIP) is on a distinct entity in this scenario. This motivates defining mechanisms for using oneM2M primitives enabling the following:

- a PEP entity requesting an access control decision from a distinct PDP entity;
- a PDP entity requesting relevant access control policies from a distinct PRP entity; and
- a PDP entity requesting relevant access control information from a distinct PIP entity.

Table 6.2.1.1-1: Mapping from actors in the use case scenario to the functions in figure 5.1-1

Actor	Function in figure 5.1-1
Device 1	Policy Enforcement Point (PEP)
Device 2	Access Requestor
M2M Gateway	Policy Decision Point (PDP)
M2M Server 1	Policy Retrieval Point (PRP)
M2M Server 2	Policy Information Point (PIP)

6.2.2 Proposal 1: Using resource-based approach to implement distributed authorization

6.2.2.1 Introduction

According to the description in clause 8 of ETSI TS 118 101 [i.1], the general flow that governs the information exchange within a procedure is based on the use of Request and Response messages. The message applies to communications between an AE and a CSE which should cross the Mca reference point and among CSEs which should cross the Mcc reference point. Requests over the Mca and Mcc reference points, from an Originator to a Receiver should address the target resource or target attribute for the operation.

In the distributed authorization system the PEP, PDP, PRP and PIP might be located in different CSEs, so the communication between PEP, PDP, PRP and PIP should cross the Mcc reference point. The method of message exchange among these authorization components should conform to the ETSI TS 118 101 [i.1], i.e. the request message sent from one authoriztion component in one CSE to another authorization component in another CSE should address a resource.

According to the description in clause 9.2.2 of ETSI TS 118 101 [i.1], a virtual resource or a virtual attribute does not have a permanent representation in a CSE, they are used to trigger processing and/or retrieve results. So we can use virtual resources to exchange authorization messages among different CSEs, and at the same time, trigger a corresponding authorization process.

This clause describes a solution for distributed authorization using a newly defined <*authorization*> resource and its child resources over the Mcc and Mcc' reference points. The child resources of the <*authorization*> resource are <policyDecisionPoint>, <policyRetrievalPoint> and <policyInformationPoint>. These child resources are virtual resources that are used to trigger PDP process, PRP process and PIP process defined in ETSI TS 118 103 [i.2] respectively.

This clause also describes the management procedures for the <*authorization*> resource and its child resources.

6.2.2.2 Resources

6.2.2.2.1 Resource type *authorization*

The <*authorization*> resource represents the method for providing authorization related services. The <*authorization*> resource contains three child resources, they are <*policyDecisionPoint*>, <*policyRetrievalPoint*> and <*policyInformationPoint*>. These child resources are virtual resources that provide authorization functions of PDP, PRP and PIP defined in ETSI TS 118 103 [i.2] respectively. The <*authorization*> resource should be located directly under <*CSEBase*>.

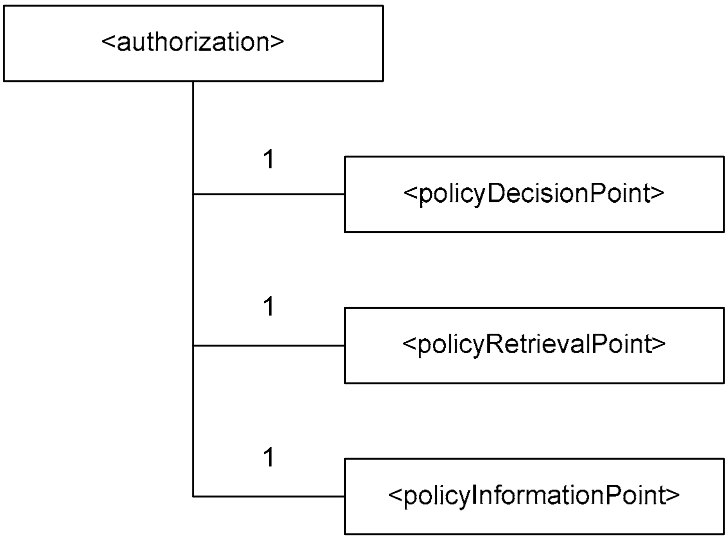

Figure 6.2.2.2.1-1: Structure of <*authorization*> resource

The <*authorization*> resource should contain the child resources specified in table 6.2.2.2.1-1.

Table 6.2.2.2.1-1: Child resources of <*authorization*> resource

Child Resources of <*authorization*>	Child Resource Type	Multiplicity	Description	<*authorizationAnnc*> Child Resource Types
[variable]	<*policyDecisionPoint*>	1	See clause 6.2.2.2.2	none
[variable]	<*policyRetrievalPoint*>	1	See clause 6.2.2.2.3	none
[variable]	<*policyInformationPoint*>	1	See clause 6.2.2.2.4	none

The <*authorization*> resource should contain the attributes specified in table 6.2.2.2.1-2.

Table 6.2.2.2.1-2: Attributes of <*authorization*> resource

Attributes of <*statsConfig*>	Multiplicity	RW/ RO/ WO	Description
resourceType	1	RO	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described
resourceID	1	RO	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described.
resourceName	1	WO	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described.
parentID	1	RO	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described.
authorizationPolicyIDs	1 (L)	RW	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described
creationTime	1	RO	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described
expirationTime	1	RW	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described
lastModifiedTime	1	RO	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described
labels	0..1 (L)	RW	See clause 9.6.1.3 of ETSI TS 118 101 [i.1] where this common attribute is described

6.2.2.2.2 Resource type *policyDecisionPoint*

The <*policyDecisionPoint*> resource is a virtual resource because it does not have a representation. It is the child resource of the <*authorization*> resource. When a RETRIEVE Request addresses the <*policyDecisionPoint*> resource, a PDP process is triggered. The access control decision request should be included in the Content parameter of the RETRIEVE Request, and the access control decision response should be included in the Content parameter of the RETRIEVE Response.

The <*policyDecisionPoint*> resource inherits access control policies that apply to the parent <*authorization*> resource.

6.2.2.2.3 Resource type *policyRetrievalPoint*

The <*policyRetrievalPoint*> resource is a virtual resource because it does not have a representation. It is the child resource of the <*authorization*> resource. When a RETRIEVE Request addresses the <*policyRetrievalPoint*> resource, a PRP process is triggered. The access control policy request should be included in the Content parameter of the RETRIEVE Request, and the access control policy response should be included in the Content parameter of the RETRIEVE Response.

The <*policyRetrievalPoint*> resource inherits access control policies that apply to the parent <*authorization*> resource.

6.2.2.2.4 Resource type *policyInformationPoint*

The <*policyInformationPoint*> resource is a virtual resource because it does not have a representation. It is the child resource of the <*authorization*> resource. When a RETRIEVE Request addresses the <*policyInformationPoint*> resource, a PIP process is triggered. The access control attribute request should be included in the Content parameter of the RETRIEVE Request, and the access control attribute response should be included in the Content parameter of the RETRIEVE Response.

The <*policyInformationPoint*> resource inherits access control policies that apply to the parent <*authorization*> resource.

6.2.2.3 Procedures

6.2.2.3.1 Introduction

This clause describes the management procedures for the <*authorization*> resource and its virtual child resources. These virtual child resources are <*policyDecisionPoint*>, <*policyRetrievalPoint*> and <*policyInformationPoint*> that are used to trigger a PDP process, a PRP process and a PIP process defined in ETSI TS 118 103 [i.2] respectively. Only Retrieve operation should be allowed on these virtual resources.

6.2.2.3.2 Create <*authorization*>

This procedure should be used to create a <*authorization*> resource.