|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting:\* | ARC#25 |
| Source:\* | C-DOT |
| Date:\* | 2016-10-20 |
| Contact:\* | Poornima ([poornima@cdot.in](mailto:poornima@cdot.in)), Chaitan([chaitan.yadav@cdot.in](mailto:chaitan.yadav@cdot.in)),  Suman([ssheoran@cdot.in](mailto:ssheoran@cdot.in) ) |
| Reason for Change/s:\* | See the introduction |
| CR against: Release\* | Release 1 |
| CR against: WI\* | Active <Work Item number>  MNT maintenace / < Work Item number(optional)>  STE Small Technical Enhancements / < Work Item number (optional)>  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0001 v1.13.8 |
| Clauses/Sub Clauses\* | Section 9.6.2 |
| Type of change: \* | Editorial change  Bug Fix or Correction  Change to existing feature or functionality  New feature or functionality  Only ONE of the above shall be ticked |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES  NO  This CR may break backwards compatibility with the last approved version of the TS? YES  NO  This CR is a mirror CR? YES  if YES, please indicate the document number of the original CR: ARC-2016-0472R01 : NO |
| Template Version:27 May 2015 (Dot not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

GUIDELINES for Change Requests:

Provide an informative introduction containing the problem(s) being solved, and a summary list of proposals.

Each CR should contain changes related to only one particular issue/problem.

In case of a correction, and the change apply to previous releases, a separated “mirror CR” should be posted at the same time of this CR

Follow the principle of completeness, where all changes related to the issue or problem within a deliverable are simultaneously proposed to be made E.g. A change impacting 5 tables should not only include a proposal to change only 3 tables. Includes any changes to references, definitions, and acronyms in the same deliverable.

Follow the drafting rules.

All pictures must be editable.

Check spelling and grammar to the extent practicable.

Use Change bars for modifications.

The change should include the current and surrounding clauses to clearly show where a change is located and to provide technical context of the proposed change. Additions of complete sections need not show surrounding clauses as long as the proposed section number clearly shows where the new section is proposed to be located.

Multiple changes in a single CR shall be clearly separated by horizontal lines with embedded text such as, start of change 1, end of change 1, start of new clause, end of new clause.

When subsequent changes are made to content of a CR, then the accepted version should not show changes over changes. The accepted version of the CR should only show changes relative to the baseline approved text.

## Introduction

### During the discussion of CR ARC-2016-0462 (TP 25) , it was discussed that for updation of acpId attribute of any resource , permission in selfPrivileges is being checked by Hosting CSE, while for updation of other attributes of a resource, permission in Privileges is being checked .

In TS-0001, section 9.6.1.3.2 , accessControlPolicyIDs description, it is mentioned as highlighted below:

**Table 9.6.1.3.2-1: Common Attributes**

| Attribute Name | Description |
| --- | --- |
| *accessControlPolicyIDs* | The attribute contains a list of identifiers of an *<accessControlPolicy>* resource. The privileges defined in the *<accessControlPolicy>* resource that are referenced determine who is allowed to access the resource containing this attribute for a specific purpose (e.g. Retrieve, Update, Delete, etc.).  If a resource type does not have an *accessControlPolicyIDs* attribute definition, then the *accessControlPolicyIDs* for that resource is governed in a different way, for example, the *accessControlPolicy* associated with the parent may apply to a child resource that does not have an *accessControlPolicyIDs* attribute definition, or the privileges for access are fixed by the system. Refer to the corresponding resource type definitions and procedures to see how access control is handled in such cases.  If a resource type does have an *accessControlPolicyIDs* attribute definition, but the (optional) *accessControlPolicyIDs* attribute is not set, or it is set to a value that does not correspond to valid*<accessControlPolicy>* resource(s), or it refers to an *<accessControlPolicy>* resource(s) that is not reachable (e.g. because it is located on a remote CSE that is offline or not reachable), then the system default access privileges shall apply.  All resources are accessible if and only if the privileges(i.e. stored as *privileges* or *selfPrivileges* attribute of <accessControlPolicy> resource) allow it, therefore all resources shall have an associated *accessControlPolicyIDs* attribute, either explicitly (setting the attribute in the resource itself) or implicitly (either by using the parent privileges or the system default policies). Which means that the system shall provide a default access privileges in case that the Originator does not provide a specific accessControlPolicyIDs during the creation of the resource.  To update this attribute, a Hosting CSE shall check whether an Originator has Update permission in any *selfPrivileges* of the *<accessControlPolicy>* resources which this attribute originally indicates. |

### But this information is missing in description of selfPrivileges in section 9.6.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *selfPrivileges* | 1 | RW | A set of access control rules that apply to the *<accessControlPolicy>* resource itself. | MA |

### So this CR proposes to modify the description of selfPrivileges attribute in section 9.6.2 to give the correct understanding.

### -----------------------Start of change 1----------------------------------------------

### 9.6.2 Resource Type *accessControlPolicy*

#### 9.6.2.0 Introduction

The Access Control Policies (ACPs) shall be used by the CSE to control access to the resources as specified in the present document and in oneM2M TS-0003 [3].

The ACP is designed to fit different access control models such as access control lists, role or attribute based access control.

The *<accessControlPolicy>* resource is comprised *privileges* and *selfPrivileges* attributes which represent a set of access control rules defining which entities (defined as *accessControlOriginators*) have the privilege to perform certain operations (defined as *accessContolOperations*) within specified contexts (defined as *accessControlContexts*) and are used by the CSEs in making Access Decision to specific resources.

In a privilege, each access control rule defines which AE/CSE is allowed for which operation. So for sets of access control rules an operation is permitted if it is permitted by one or more access control rules in the set.

For a resource that is not of *<accessControlPolicy>* resource type, the common attribute *accessControlPolicyIDs* for such resources (defined in table 9.6.1.3.2-1) contains a list of identifiers which link that resource to *<accessControlPolicy>* resources. The CSE Access Decision for such a resource shall follow the evaluation of the set of access control rules expressed by the *privileges* attributes defined in the *<accessControlPolicy>* resources.

The *selfPrivileges* attribute shall represent the set of access control rules for the *<accessControlPolicy>* resource itself.

The CSE Access Decision for *<accessControlPolicy>* resource shall follow the evaluation of the set of access control rules expressed by the *selfPrivileges* attributes defined in the *<accessControlPolicy>* resource itself.



**Figure 9.6.2-1: Structure of <accessControlPolicy> resource**

The *<accessControlPolicy>* resource shall contain the child resource specified in table 9.6.2-1.

**Table 9.6.2-1: Child resources of <accessControlPolicy> resource**

| Child Resources of *<accessControlPolicy>* | Child Resource Type | Multiplicity | Description | *<accessControlPolicyAnnc>* Child Resource Types |
| --- | --- | --- | --- | --- |
| *[variable]* | *<subscription>* | 0..n | See clause 9.6.8 | *<subscription>* |

The *<accessControlPolicy>* resource shall contain the attributes specified in table 9.6.2-2.

**Table 9.6.2-2: Attributes of <accessControlPolicy> resource**

| Attributes of *<accessControlPolicy>* | Multiplicity | RW/  RO/  WO | Description | *<accessControlPolicyAnnc>* Attributes |
| --- | --- | --- | --- | --- |
| *resourceType* | 1 | RO | See clause 9.6.1.3. | NA |
| *resourceID* | 1 | RO | See clause 9.6.1.3. | NA |
| *resourceName* | 1 | WO | See clause 9.6.1.3. | NA |
| *parentID* | 1 | RO | See clause 9.6.1.3. | NA |
| *expirationTime* | 1 | RW | See clause 9.6.1.3. | MA |
| *labels* | 0..1(L) | RW | See clause 9.6.1.3. | MA |
| *creationTime* | 1 | RO | See clause 9.6.1.3. | NA |
| *lastModifiedTime* | 1 | RO | See clause 9.6.1.3. | NA |
| *announceTo* | 0..1 (L) | RW | See clause 9.6.1.3. | NA |
| *announcedAttribute* | 0..1 (L) | RW | See clause 9.6.1.3. | NA |
| *privileges* | 1 | RW | A set of access control rules that applies to resources referencing this *<accessControlPolicy>* resource using the *accessControlPolicyID* attribute. | MA |
| *selfPrivileges* | 1 | RW | A set of access control rules that apply to the *<accessControlPolicy>* resource itself and *accessControlPolicyIDs* attribute of any other resource which is linked to this <accessControlPolicy> resource. | MA |

The set of access control rules represented in *privileges* and *selfPrivileges* attributes are comprised of 3-tuples (*accessControlOriginators*, *accessControlContexts*, *accessControlOperations*) with parameters shown in table 9.6.2-3 which are further described in the following clauses.

If *privileges* attribute contains no 3-tuples then this represent an empty set of the access control rules.

The *selPrivileges* attribute shall contain at least one 3-tuples.

The CSE access granting mechanism shall follow the procedure described in oneM2M TS-0003 [3] in clause 7.1 (Access Control Mechanism).

**Table 9.6.2-3: Parameters in access-control-rule-tuples**

| Name | Description |
| --- | --- |
| *accessControlOriginators* | See clause 9.6.2.1 |
| *accessControlContexts* | See clause 9.6.2.2 |
| *accessControlOperations* | See clause 9.6.2.3 |

#### 9.6.2.1 accessControlOriginators

The *accessControlOriginators* is a mandatory parameter in an access-control-rule-tuple. It represents the set of Originators that shall be allowed to use this access control rule. The set of Originators is described as a list of parameters, where the types of the parameter can vary within the list. Table 9.6.2.1-1 describes the supported types of parameters in *accessControlOriginators*. The following Originator privilege types shall be considered for access control policy check by the CSE.

**Table 9.6.2.1-1: Types of Parameters in accessControlOriginators**

| Name | Description |
| --- | --- |
| *domain* | A SP domain or SP sub-domain |
| *originatorID* | CSE-ID or AE-ID which represent an Originator identity |
| *all* | Any Originators are allowed to access the resource within the *accessControlOriginators* constraints |

#### 9.6.2.2 accessControlContexts

The *accessControlContexts* is an optional parameter in an access-control-rule-tuple that contains a list, where each element of the list, when present, represents a context that is permitted to use this access control rule. Each request context is described by a set of parameters, where the types of the parameters can vary within the set. Table 9.6.2.2-1 describes the supported types of parameters in *accessControlContexts*.

The following Originator *accessControlContexts* shall be considered for access control policy check by the CSE.

**Table 9.6.2.2-1: Types of Parameters in accessControlContexts**

| Name | Description |
| --- | --- |
| *accessControlTimeWindow* | Represents a time window constraint which is compared against the time that the request is received at the Hosting CSE. |
| *accessControlLocationRegion* | Represents a location region constraint which is compared against the location of the Originator of the request. |
| *accessControlIpIPAddress* | Represents an IP address constraint or IP address block constraint which is compared against the IP address of the Originator of the request. |

#### 9.6.2.3 accessControlOperations

The *accessControlOperations* is a mandatory parameter in an access-control-rule-tuple that represents the set of operations that are authorized using this access control rule. Table 9.6.2.3-1 describes the supported set of operations that are authorized by *accessControlOperations*.

The following *accessControlOperations* shall be considered for access control policy check by the CSE.

**Table 9.6.2.3-1: Types of parameters in accessControlOperations**

| Name | Description |
| --- | --- |
| RETRIEVE | Privilege to retrieve the content of an addressed resource |
| CREATE | Privilege to create a child resource |
| UPDATE | Privilege to update the content of an addressed resource |
| DELETE | Privilege to delete an addressed resource |
| DISCOVER | Privilege to discover the resource |
| NOTIFY | Privilege to receive a notification |

### -----------------------End of change 1----------------------------------------------

CHECK LIST

* Does this change request include an informative introduction containing the problem(s) being solved, and a summary list of proposals.?
* Does this CR contain changes related to only one particular issue/problem?
* Have any mirror crs been posted?
* Does this change request make **all** the changes necessary to address the issue or problem? E.g. A change impacting 5 tables should not only include a proposal to change only 3 tables. Includes any changes to references, definitions, and acronyms in the same deliverable?
* Does this change request follow the drafting rules?
* Are all pictures editable?
* Have you checked the spelling and grammar?
* Have you used change bars for all modifications?
* Does the change include the current and surrounding clauses to clearly show where a change is located and to provide technical context of the proposed change? (Additions of complete sections need not show surrounding clauses as long as the proposed section number clearly shows where the new section is proposed to be located.)
* Are multiple changes in this CR clearly separated by horizontal lines with embedded text such as, start of change 1, end of change 1, start of new clause, end of new clause.?