|  |  |
| --- | --- |
| CHANGE REQUEST

|  |
| --- |
|  |

 |

|  |  |
| --- | --- |
| Meeting ID:\* |  SDS #65.2 |
| Source:\* | Mohd Uvaish Siddiqui, C-DOT, uvaish@cdot.inPrateek Varshney, C-DOT, prateekv@cdot.inPoornima Shandilya, C-DOT, poornima@cdot.inAnupama Chopra, C-DOT, anupama@cdot.in |
| Date:\* | 2024-07-22  |
| Reason for Change/s:\* | TS-0001 – accessControlObjectDetails handling in <accessControlPolicy> resource for operations other than Create |
| CR against: Release\* | Release 5 |
| CR against: WI\* | [ ]  Active WI-xxxx[ ]  MNT maintenance / < Work Item number(optional)>Is this a mirror CR? Yes [ ]  No [ ] mirror CR number: (Note to Rapporteur - use latest agreed revision)[x]  STE Small Technical Enhancements / < Work Item number (optional)>Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0001 v.5.6.0 |
| Clauses \* | 9.6.2.0 and 9.6.2.4 |
| Type of change: \* | [ ]  Editorial change[ ]  Bug Fix or Correction[x]  Change to existing feature or functionality[ ]  New feature or functionalityOnly ONE of the above shall be ticked |
| Impacted other TS/TR(s) | TS-0003 and TS-0004 |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES [x]  NO [ ] This CR may break backwards compatibility with the last approved version of the TS? YES [ ]  NO [x]  |
| Template Version: January 2017 (Do 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 separate “mirror CR” should be posted at the same time of this CR

Mirror CR: applies only when the text, including clause numbering are exactly the same.

Companion CR: applies when the change means the same but the baselines differ in some way (e.g. clause number).

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 clauses need not show surrounding clauses as long as the proposed clause number clearly shows where the new clause 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

This CR proposes changes to *accessControlObjectDetails* attribute in access control rule of <accessControlPolicy> resource for handling of Create, Retrieve, Update, Delete and Discovery operations on a target resource. This is in continuation to discussion of SDS-2024-0078R02-oneM2MResourceTypeACR presented in SDS session of TP-65 on 24th June 2024. Two proposals were discussed for handling of resourceType. Proposal no. 2 was agreed and the changes for the same are introduced in this CR.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 9.6.2.0 Introduction

The Access Control Policies (ACPs) shall be used by the CSE to control access to the resources and their attributes as specified in the present document and in oneM2M TS-0003 [Error: Reference source not found].

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 of *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 *accessControlOperations*) within specified contexts (defined as *accessControlContexts*) and are used by the CSEs in making Access Decision to all or specific parts (i.e. child resources or attributes) of the targeted resource or the targeted resource itself (defined as *accessControlObjectDetails* and *accessControlAttributes*).

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.

Logically an authorization system may comprise four sub-functions: enforcing access control decision, making access control decision, providing access control policies and providing access control information (e.g. roles). As specified in oneM2M TS-0003 [Error: Reference source not found], these sub-functions are modelled as policy enforcement point (PEP), Policy Decision Point (PDP), Policy Retrieval Point (PRP) and Policy Information Point (PIP) respectively. In a oneM2M System these authorization sub-functions may coexist in one CSE or may be distributed in different CSEs in different combinations.

In the *<accessControlPolicy>* resource three operational attributes are defined for holding the information about where to find the distributed authorization sub-functions. These attributes are: *authorizationDecisionResourceIDs*, *authorizationPolicyResourceIDs* and *authorizationInformationResourceIDs*.

The *authorizationDecisionResourceIDs* attribute contains a list of addresses of <*authorizationDecision*> resources. Each <*authorizationDecision*> resource represents a PDP to which an access control decision request shall be sent in order to obtain an access control decision. See clause 9.6.41 for further details of <*authorizationDecision*> resource type.

The *authorizationPolicyResourceIDs* attribute contains a list of addresses of <*authorizationPolicy*> resources. Each <*authorizationPolicy*> resource represents a PRP to which an access control policy request shall be sent in order to obtain access control policies. See clause 9.6.42 for further details of <*authorizationPolicy*> resource type.

The *authorizationInformationResourceIDs* attribute contains a list of addresses of <*authorizationInformation*> resources. Each <*authorizationInformation*> resource represents a PIP to which an access control information request shall be sent in order to obtain requested access control information (e.g. role and/or token) for making an access control decision. See clause 9.6.43 for further details of <*authorizationInformation*> resource type.

When processing a request to a targeted resource, the Hosting CSE shall progress through the different types of authorization (if supported) as described in clause 10.2.3.1.

The applicability of the *authorizationDecisionResourceIDs*, *authorizationPolicyResourceIDs* and *authorizationInformationResourceIDs* attributes for the distributed authorization depends on the deployment form of authorization sub-functions:

* In the case the privileges attribute is not NULL, the access control rules in the privileges attribute shall be used for access control, and the authorizationDecisionResourceIDs, authorizationPolicyResourceIDs and authorizationInformationResourceIDs attributes shall not be present.
* In the case the privileges attribute is NULL, how to process further depends on which authorization method is adopted. In the case distributed authorization method is supported, authorizationDecisionResourceIDs or authorizationPolicyResourceIDs attribute shall be considered for obtaining access control decision or access control policies from another CSE. However, authorizationDecisionResourceIDs and authorizationPolicyResourceIDs attributes shall not be present at the same time.
* In case the authorizationInformationResourceIDs attribute is present, the access control information request (e.g. for role information) related to the access control policy specified in the privileges attribute shall be sent to one of the addresses listed in this attribute.

The details of distributed authorization procedures are described in oneM2M TS-0003 [Error: Reference source not found].

The *<accessControlPolicy>* resource shall contain the child resource specified in table 9.6.2.0-1.

Table 9.6.2.0-1: 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>* |
| *[variable]* | *<transaction>* | 0..n | See clause 9.6.48 | *<transaction>* |

The *<accessControlPolicy>* resource shall contain the attributes specified in table 9.6.2.0-2.

Table 9.6.2.0-2: 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 |
| *resource Name* | 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 |
| *announceSyncType* | 0..1 | RW | See clause 9.6.1.3. | MA |
| *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 |
| *authorizationDecisionResourceIDs* | 0..1 (L) | RW | A list of addresses of <*authorizationDecision*> resources. See clause 9.6.41 for further details. | MA |
| *authorizationPolicyResourceIDs* | 0..1 (L) | RW | A list of addresses of <*authorizationPolicy*> resources. See clause 9.6.42 for further details. | MA |
| *authorizationInformationResourceIDs* | 0..1 (L) | RW | A list of addresses of <*authorizationInformation*> resources. See clause 9.6.43 for further details. | MA |

The set of access control rules represented in *privileges* and *selfPrivileges* attributes are comprised of access-control-rule-tuples (*accessControlOriginators*, *accessControlContexts*, *accessControlOperations, accessControlObjectDetails, accessControlAuthenticationFlag* and *accessControlAttributes*) with parameters shown in table 9.6.2.0-3 which are further described in the following clauses.

If the *privileges* attribute contains no access-control-rule-tuples, then this represents an empty set of the access control rules.

The *selfPrivileges* attribute shall contain at least one access-control-rule-tuple.

The CSE access granting mechanism shall follow the procedure described in oneM2M TS-0003 [Error: Reference source not found] clause 7.1 (Access Control Mechanism).

Table 9.6.2.0-3: 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 |
| *accessControlObjectDetails* | See clause 9.6.2.4 |
| *accessControlAuthenticationFlag* | See clause 9.6.2.5 |
| *accessControlAttributes* | See clause 9.6.2.6 |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 9.6.2.4 accessControlObjectDetails

The *accessControlObjectDetails* is an optional parameter of an access control rule. It specifies the resource type of targeted resource and a subset of child resource types of the targeted resource to which the access control rule applies. The *accessControlObjectDetails* parameter shall consist of the elements listed in table 9.6.2.4-1.

For Retrieve, Update, Delete and Discovery operations, one of the *resourceType* or *specialization* element, whichever applicable shall be present in *accessControlObjectDetails* and the CSE shall match the type of resource or specialization of the targeted resource with the value specified in the *resourceType* or *specialization* element respectively. However, *childResourceType* element shall not be present in this case.

For Create operation, *childResourceType* element shall be present in the accessControlObjectDetails. If either the *resourceType* or *specialization* element is also present in *accessControlObjectDetails*, the CSE shall match the type of resource or specialization of the targeted resource with the value specified in the *resourceType* or *specialization* element. Further, checking of *childResourceType* shall be done only if the *resourceType* or *specialization* match occurs. However, if the *resourceType* and *specialization* elements are not provided, only *childResourceType* match shall be performed.

Table 9.6.2.4-1: Types of Parameters in *accessControlObjectDetails*

| **Name** | **Description** |
| --- | --- |
| *resourceType* | Identifier of the resource type to which this access control rule applies. |
| *specializationType* | When the *resourceType* is *mgmtObj* or *flexContainer*, the identifier of the specialization as defined by *mgmtDefinition* or *containerDefinition* attribute, respectively, shall be specified. |
| *childResourceType* | List of child resource types and/or the identifier of the specialization. The identifier of the specialization shall be specified when the *resourceType* is *mgmtObj* or *flexContainer*. |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*