|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | PRO 34.2 |
| Source:\* | Bob Flynn, Convida Wireless; [Flynn.bob@convidawireless.com](mailto:Flynn.bob@convidawireless.com) |
| Date:\* | 2018-04-12 |
| Reason for Change/s:\* | Authorization of updates |
| CR against: Release\* | Release 3 |
| CR against: WI\* | Active <WI-0058>  MNT maintenance / < Work Item number(optional)>  Is this a mirror CR? Yes  No  mirror CR number: (Note to Rapporteur - use latest agreed revision)  STE Small Technical Enhancements / < Work Item number (optional)>  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0004 Version 3.7.0 |
| Clauses \* |  |
| 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 |
| Impacted other TS/TR(s) | <TS/TR number>, <Version Number>, and <Description on which aspect should be reflected in this TS/TR> |
| 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 |
| 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

Protocol contribution to reflect changes in ARC-2016-0544R03-CR-Standardize\_Default\_ACP\_Privileges

*“To promote interoperability and address issues encountered at the 3rd oneM2M Interop Event, this contribution proposes that by default a creator of a resource shall have full access control privileges to resources it creates. A Hosting CSE shall apply this default when 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 a valid, existing <accessControlPolicy> resource, or it refers to an <accessControlPolicy> resource that is not reachable (e.g. because it is located on a remote CSE that is offline or not reachable).”*

R01 – rebaseline to V3.7.0

Address email comments

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

#### Check authorization of the originator

Depending on the target resource type, the Hosting CSE shall use *accessControlPolicyIDs* of the different resources.

* If the resource type does not have the *accessControlPolicyIDs* attribute definition, the Hosting CSE shall evaluate the *accessControlPolicyIDs* associated with the parent of that resource (e.g. for <schedule>, <oldest>, <latest>, <contentInstance>)
* Some resources provide specific handling for the *accessControlPolicyIDs* attribute, for such resources these procedures are to be followed (e.g. handling given in TS-0001 clause 9.6 for <container>, <m2mServiceSubscriptionProfile>, <serviceSubscribedNode>).
* For other resources, the Hosting CSE shall evaluate the *accessControlPolicyIDs* of the resource. In case *accessControlPolicyIDs* attribute value is **not** set, or does not point to a valid resource or is not reachable then the following default policy shall apply. The Hosting CSE shall provide access privileges to only the creator of the resource. The Hosting CSE shall keep track of the creator of the resource even if the resource does not support a creator attribute. The default access privilege shall grant the creator unrestricted access to the resource, i.e. it shall include all possible operations for that resource. All other entities shall be denied access by default.

The evaluation procedure shall be performed as following:

1. The Hosting CSE retrieves the access control rules from *privilege* attribute of the <accessControlPolicy> which is linked as the *accessControlPolicyIDs*. If the target is <accessControlPolicy> resource, it retrieves the rules from *selfPrivilege* attribute instead.
2. The Hosting CSE checks the following conditions for the access control rules. If there is any rule satisfying all conditions then the evaluation is successful, otherwise it is failed. For more details, see the clause 7.1.5 in TS-0003 [7].

* *accessControlOriginators* of the rule includes the Originator information. The accessControlOriginators parameter comprises a list of domain, CSE-IDs, AE-IDs, the resource-ID of a <group> resource that contains <AE> or <remoteCSE> as member or Role-ID. The accessControlOriginators parameter can be set to reserved keyword "all" to grant access to all originators. It is allowed to include the wildcard character, "\*", into the URI string of domain, CSE-ID and AE‑ID at any level. See the clause 9.6.2.1 in TS-0001 [6].

Table 7.3.3.15‑1 Types of Parameters in *accessControlOriginators*

| Name | Description | Wildcard applicability |
| --- | --- | --- |
| *domain* | A M2M-SP-ID representing domain | Allowed |
| *originatorID* | CSE-ID | Allowed |
| AE-ID | Allowed |
| *group* | The resource-ID of a <group> resource which contains <AE> or <remoteCSE> as member | Not allowed |
| *all* | Any Originators are allowed | Not allowed |
| *Role-ID* | A Role Identifier as defined in clause 7.1.14 of TS-0001 [6] | Not allowed |

* *accessControlContexts* of the rule includes the request context, if the rule includes the *accessControlContexts.*
* If the accessControlOriginators includes a groupID, the Hosting CSE checks if the Originator is a member of that group resource.
* *accessControlOperations* of the rule matches the operation type of the request.
* If the *accessControlAuthenticationFlag* is TRUE, then access control rule applies only if the Originator is considered to be authenticated by the Hosting CSE according to clause 7.1.2 in TS-0003 [7].

If the evaluation failed, and the Hosting CSE does not support Dynamic Authorization, authorization failure information shall be returned to the Originator. If the evaluation failed and the Hosting CSE supports Dynamic Authorization, then it shall trigger Dynamic Authorization. For more details, see the clause 7.3 in TS-0003 [7]. If Dynamic Authorization results in a failure, authorization failure information shall be returned to the Originator.

### -----------------------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 include a proposal to change only 3 tables?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 clauses need not show surrounding clauses as long as the proposed clause number clearly shows where the new clause 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.?