|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | SDS 40 |
| Source:\* | Wei Zhou, Datang, zhouwei@catt.cn |
| Date:\* | 2019-05-20 |
| Reason for Change/s:\* | Supptoring CSE impersonation prevention |
| CR against: Release\* | Release 4 |
| CR against: WI\* | Active <Work Item number>  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-0003 Version 4.0.0 (TS-0003 Version 3.10.2) |
| Clauses \* | 7.2 |
| 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 |
| Other TS/TR(s) impacted | None |
| 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 2019 (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 contribution addresses the following security related action item:

|  |  |  |
| --- | --- | --- |
| **Number** | **Action** | **Status** |
| A-SEC-33-03 | Check whether AE impersonation prevention could also apply to CSE | Rel-4 |

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

## 7.2 Impersonation Prevention

### 7.2.1 Registrar verification

An AE/CSE can behave maliciously and pretend to be another AE/CSE with its ID changed, the Hosting CSE needs prevention mechanism for AE/CSE impersonation. This mechanism works at Registrar CSE since Registrar CSE is an entry point of M2M system.

When the Registrar CSE receives a request, the Registrar CSE shall perform the following procedure.



Figure 7.2.1-1: Impersonation checking procedure

0. Security association establishment may be performed. Clause 6.1.2.2.1 describes the scenarios when security association establishment between an AE/CSE and CSE is mandatory, and describes the scenarios when security association establishment between an AE/CSE and CSE is recommended. The subsequent procedures shall be performed if a security association has been established.

1. The AE/CSE sends a request to Hosting CSE via its Registrar CSE as specified in oneM2M TS‑0001 [1] (Hosting CSE is not represented on this figure and can either be the Registrar CSE or another CSE).

2. The Registrar CSE checks if the value in the***From*** parameter is the same as the ID associated in security association:

3. If the values are not identical, then the Registrar CSE shall send a response with Response Status Code '4106' ("ORIGINATOR\_HAS\_NOT\_REGISTERED").

4. If the values are identical, then the Registrar CSE shall perform the procedures specified in clause 8.2 of oneM2M TS‑0001 [1]. Depending on the number of Transit CSEs, the Registrar CSE shall either process the request or forward it to the Hosting CSE or to another Transit CSE.

### 7.2.2 Verification Using End-to-End Security of Primitives (ESPrim)

End-to-End Security of Primitives (ESPrim), clause 8.4, allows a Target (a Hosting CSE or AE) to authenticate the Originator of a request primitives that are handled by other CSEs. ESPrim also provides confidentiality and integrity protection of these request and response primitives. The primitives being protected are called the inner primitives. ESPrim encryption is applied to the inner primitives to form ESPrim Objects. Outer primitives are used to transport the ESPrim objects between the Originator and Target CSE or AE. The Originator's Registrar cannot view the encrypted inner primitive, and cannot verify that the ***From*** parameter of the inner primitive is correct. Instead, the Target is expected to verify that the ***From*** parameter of the inner primitive agrees with the authenticated identity of the Originator.

When the Target receives an ESPrim-protected request, the Target shall perform the following procedure.



Figure 7.2.2-1: Impersonation checking procedure

0. The Target and Originator have previously established a symmetric pairwiseESPrimKey. The Target associates an identity with the symmetric pairwiseESPrimKey.

1. The Originator composes the inner request primitive, encrypts it using ESPrim to form an ESPrim Object, and sends it to the Target as described in clause 8.4.

NOTE: Regardless of whether ESPrim is applied, each Mcc "hop" is always protected using an SAEF, and each Mca "hop" is optionally protected using an SAEF; see clause 6.1.2.2.1.

2. The Target applies the procedures in clause 8.4 to decrypt the ESPrim Object and obtain the inner request primitive.

3. The Target checks if the value in the***From*** parameter is the same as the ID associated with the pairwiseESPrimKey:

4. If the values are not identical, then the Target shall send a response with Response Status Code '4116' ("ESPRIM\_IMPERSONATION\_ERROR").

5. If the values are identical, then the Target shall record that the Originator has been authenticated, and performs procedures specified in clause 8.2 of oneM2M TS-0001 [1].

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