|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | ARC 31 |
| Source:\* | Wei Zhou, Datang, zhouwei@catt.cn |
| Date:\* | 2017-09-18 |
| Reason for Change/s:\* | TS-0001 clause6 security description update R3 |
| CR against: Release\* | Release 3 |
| 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-0001 Version 3.7.0 |
| Clauses \* | 6.2.10 |
| 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

Reorganize security-related descriptions based on the relevant content contained in the current TS-0001 and TS-0003.

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

### 6.2.10 Security

#### 6.2.10.1 General Concepts

The Security (SEC) CSF comprises the following functionalities:

* Sensitive data handling;
* Security administration;
* Security association establishment;
* Remote security provisioning;
* Identification and authentication;
* Authorization;
* Identity management.

Sensitive data handling functionality in the SEC CSF protects the local credentials on which security relies during storage and manipulation. Sensitive data handling functionality performs other sensitive functions such as security algorithms. This functionality is able to support several cryptographically separated security environments. Those secure environments are accessible via the Mcs reference point. This reference point abstracts different types of secure environments and is defined in oneM2M TS-0016 Secure Environment Abstraction [9].

Security management capabilities are provided by the Security Administration functionality as specified in oneM2M TS-0003 [2].

NOTE: ASM and DMG CSFs do not include security management capabilities of the SEC CSF.

Security administration functionality enables services such as the following:

* Creation and administration of dedicated security environment supported by Sensitive Data Handling functionality.
* Post-provisioning of a root credential protected by the security environment.
* Provisioning and administration of subscriptions related to M2M Common Services and M2M Application Services.

Security association establishment functionality establishes security association between corresponding M2M Nodes, in order to provide services such as confidentiality and integrity.

Identification checks if the identity provided for authentication is valid and authentication validates if identity supplied in the identification step is associated with a trustworthy credential.

Authorization functionality authorizes services and specific operations (e.g. create, retrieve, update, delete, etc.) on resources identified and authenticated entities, according to provisioned access control policies.

Identity management provides secure storage for oneM2M identifiers. This functionality also provides pseudonyms which serve as temporary identifiers which cannot be linked to the true identity of either the associated entity or its user.

#### 6.2.10.2 Detailed Descriptions

The functionalities supported by the SEC CSF are as follows:

* Sensitive data handling:
* Provides the capability to protect the local credentials on which security relies during storage and manipulation.
* Extends sensitive data handling functionality to other sensitive data used in the M2M Systems such as subscription related information, access control policies and personal data pertaining to individuals.
* Performs other sensitive functions as well, such as security algorithms running in cryptographically separated secure environments.
* Security administration:
* Creates and administers dedicated secure environment supported by sensitive data handling functionality.
* Post-provisions master credentials protected by the secure environment.

NOTE: The secure environment can also be pre-provisioned with a master credentials prior to deployment; therefore this capability is not always required. Post-provisioning is required when secure remote provisioning needs to be performed or re-initiated after deployment.

* Provisioning and administration of subscriptions related to M2M Services and M2M application services. Besides the associated master credentials, a subscription includes other information classified as sensitive data such as authorization roles and identifiers for access control management.
* Security association establishment:
* Establishes security associations between corresponding M2M Nodes in order to provide specific security services (e.g. confidentiality, integrity, or support for application level signature generation and verification) involving specified security algorithms and sensitive data. This involves key derivation based on provisioned master credentials. This functionality of the SEC CSF is mandatory when security is supported.
* MAF-based security association establishment
* These security frameworks use a M2M Authentication Function (MAF) to provide authentication and distribution of symmetric key for use by a Source End-Point initiating establishment of the symmetric key, and one or more target end-points. The symmetric key can be used in one of Security Association Establishment Framework, End-to-end security of Data (ESData) and End-to-end security of Primitives (ESPrim).
* End-to-end security of Data (ESData) and Primitives (ESPrim)
* End-to-End Security of Primitives (ESPrim) allows 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. End-to-End Security of Data (ESData) provides an interoperable framework for protecting data such that it can be transported via transit CSEs which do not need to be trusted.
* Remote Security Provisioning
* Remote Security Provisioning Frameworks (RSPFs) enable an M2M Enrolment Function (MEF) to provision credentials to an Enrolee, which is a CSE or AE, as part of the Enrolment of the Enrolee to an M2M SP or third party M2M Trust Enabler (MTE). The credentials are either a symmetric key shared by the Enrolee and an Enrolment Target or Certificate(s) for which the Enrolee knows the corresponding private key, and a set of trust anchors for authenticating the M2M SP or MTE's MAF or other entities enrolled with the M2M SP or MTE.
* Identification and authentication
* Identification is the process of checking if the identity provided for authentication is valid. How to perform an identification process will depend on the purpose of authentication.
* Authentication is the process of validating if the identity supplied in the identification step is associated with a trustworthy credential. How to perform an authentication process will depend on using which mutual authentication mechanism.
* Authorization:
* In general authorization function authorizes services and operations (e.g. create, retrieve, update, delete, etc.) on resources to the identified and authenticated entities, according to the provisioned access control policies.
* Role Based Access Control (RBAC) allows the Hosting CSE to authorize accesses on resources according to the roles assigned to the Originators.
* Token Based Access Control allows the Hosting CSE to authorize accesses on resources according to the authorization information in tokens provided by the Originators.
* Dynamic Authorization provides an interoperable framework for an Originator to be dynamically issued with temporary permissions providing the Originator with access to one or more resources on one or more CSEs at runtime.
* The entire authorization function can be split into four sub-functions: Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Retrieval Point (PRP) and Policy Information Point (PIP). Distributed Authorization provides an interoperable framework which allows PEP, PDP, PRP and PIP to be distributed in different CSEs.
* Identity management:
* Provides oneM2M identifiers to the requesting entity in case those identifiers are stored within the secure environment.
* Provides pseudonyms to be used instead of the unique identifiers of an entity to serve as temporary identifiers not linkable to the true identity of either the associated entity or its user.

Detailed functionalities are described in the oneM2M TS-0003 [2].

Sensitive security functions and information within a node are protected by local Secure Environments (SE). A Secure Environment is an abstraction of a secure area, within a computing system on a node (ADN, ASN, MN or IN), that provides a defined level of protection for code and data at rest, i.e. in storage, and in use, i.e. during process execution or data manipulation, as specified in TS-0016[9]. An SE provides resources for the purposes described above that can be manipulated via the Mcs reference point. Details on the SE resources can be found in TS-0016 [9].

### -----------------------End of change 2---------------------------------------------

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.?