|  |
| --- |
| CHANGE REQUEST |
| Meeting ID:\* |  SDS 54 |
| Source:\* | Rana Kamill, BT, rana.kamill@bt.com |
| Date:\* | 2022-05-12 |
| Reason for Change/s:\* | CR TS-0003 Diagram Update R2 – R3 mirror  |
| CR against: Release\* | Release 3 |
| CR against: WI\* | [ ]  Active <Work Item number> [x]  MNT maintenance / < Work Item number(optional)>Is this a mirror CR? Yes [x]  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 v3.15 |
| Clauses \* | 5.1.0, 5.2.1, 6.2.1.1, 6.3.2, 6.3.3 |
| Type of change: \* | [x]  Editorial change[ ]  Bug Fix or Correction[ ]  Change to existing feature or functionality[ ]  New feature or functionalityOnly ONE of the above shall be ticked |
| Other TS/TR(s) impacted | <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 [x]  |
| Template Version: January 2020 (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.

If this is a correction, and the change applies to previous releases, a separate “mirror CR” should be posted at the same time as 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. Include any changes to references, definitions, and abbreviations in the same deliverable.

Follow the drafting rules.

All pictures must be editable.

Check spelling and grammar.

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 proposed new clause is 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 the 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 some updates, as a mirror CR of the R2 version, to the TS-0003 Release 3 according to the conclusions of ITU-T SG20 and oneM2M joint meeting held on 19 June 2020.

More information about these comments can be found in TP-2018-0195-LS\_on\_the\_progress\_of\_oneM2M\_related\_work\_items and TP-2018-0198-ITU-T\_comments\_and\_resolutions.

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

# 5 Security Architecture

## 5.1 Overview

### 5.1.0 Introduction

Figure 5.1.0-1 provides a high level overview of the Security architecture.

The architecture consists of following layers:

* Security Functions layer:
* This layer contains a set of security functions that are exposed at reference point Mca and Mcc. These security functions can be classified into six categories; they are Identification, Authentication, Authorization, Security Association, Sensitive Data Handling and Security Administration.
* Security Environment Abstraction Layer:
* This layer implements various security capabilities such as key derivation, data encryption/decryption, signature generation/verification, security credential read/write from/to the Secure Environments, and so on. The security functions in the Security Functions Layer invoke these functions in order to protect the operations in the Secure Environments. In addition this layer also provides physical access to the Secure Environments. Implementation of this is out of scope of the present document. This layer is not specified in the present release but is expected to be considered in future releases.
* Secure Environment layer:
* This layer contains one or multiple secure environments that provide various security services providing adequate protection to sensitive data storage and sensitive function execution. The sensitive data includes SE capability, security keys such as long term symmetric keys and asymmetric private keys, local credentials, security policies, identity information, subscription information, and so on. The sensitive functions include data encryption, data decryption, and so on. Though implementation of secure environments is out of scope of the present document, a reference framework to interface M2M entities with UICCs is provided in Annex D.



Figure 5.1.0-1: High level overview of the Security architecture

**Design principles:**

* Security Services are modular and configurable according to the needs of the hosting CSE, its supported reference points and its purpose.
* The architecture is split into several components and sub-components providing a modular design. With this design, mapping of the architecture to different nodes and entities is enabled.
* Depending on the requirements of each entity, Security consists of components relevant to fulfil the requirements of the respective node or entity and the intended use case.
* The architecture needs to be adapted to be suitable for implementation in different entities. For example, the architecture can be mapped to different device classes.
* The security administration component is supposed to enable administration of all sensitive resources (data and functions) and also allow configuration and extension of Security services itself.
* The Secure Environment within the CSE is accessed via the Secure Environment Abstraction layer and is expected to provide adequate level of protection to the sensitive information listed in clause 6.2.3.2.

### 5.1.1 Identification and Authentication

The Identification and Authentication function is in charge of identification and mutual authentication of CSEs and AEs.

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. For example, in the case of resource access, the authentication function can require the identification to check if the AE or CSE has registered with the local CSE; in the case of AE or CSE registration, the authentication function can require the identification to check if the identity provided by an AE or CSE fits a certificate. Once passing this checking process, the AE or CSE is identified, and the identified identity will be supplied to authentication process.

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. For example, in the case of using certificate based authentication mechanism, the authentication function can require the authentication to verify a digital signature; in the case of using symmetric key based authentication mechanism, the authentication function can require the authentication to verify a Message Integrity Code (MIC). When this validating process has been completed, the AE or CSE is authenticated.

### 5.1.2 Authorization

The Authorization function is responsible for authorizing services and data access to authenticated entities according to provisioned Access Control Policies (ACPs) and assigned roles.

Access control policy is defined as sets of conditions that define whether entities are permitted access to a protected resource. The authorization function can support different authorization mechanisms, such as Access Control List (ACL), Role Based Access Control (RBAC), etc. The Authorization function could need to evaluate multiple access control policies in an authorization process in order to get a final access control decision. This process is further described in clause 7 "Authorization".

Authorization evaluation process is based on the Service Subscription resource which specifies what M2M Services and M2M Service roles the authenticated entity has subscribed to and the access control policies associated with the protected resource. The authorization evaluation process can also consider contextual attributes such as time or geographic location.

Prior to authorization mutual authentication between the originator CSE or AE and hosting CSE can be performed as specified in clause 8. Clause 6.1.2.2.1 describes the conditions under which mutual authentication is mandatory. An access control rule can also include an indicator that the access control rule applies only when mutual authentication has been performed successfully and the result of mutual authentication is still current; see clause 7.1.3 for details.

### 5.1.3 Identity Management

The Identity Management function provides oneM2M identities/identifiers to the requesting entity in case those identities are stored within the secure environment. oneM2M identifiers as defined in the oneM2M Architecture (oneM2M TS-0001 [1]) can also be treated as sensitive data that are accessible to AEs or CSEs and used independently of Authentication or Authorization functions.

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

### ---------------------Start of change 2---------------------------------------------

5.2 Security Layers

5.2.1 Security Service Layer

The security service layer provides the following services:

* Access Management:
* Identification and Authorization.
* Authentication.
* Access Control.
* Sensitive Data Handling:
* Sensitive Functions protection.
* Secure Storage.
* Data error detection.
* Trust Enabling Security Functions:
* MEF (M2M Enrolment Function).
* MAF (M2M Authentication Function)
* DAS (Dynamic Authorisation System)
* PPM (Privacy Policy Manager)
* Security Association Establishment:
* Secure Connection via secure session establishment.
* Secure Connection via object security.
* Security Administration (including remote security provisioning).
* Identity Protection.

Each of these services provides functions and resources on the Security Service and Administration API.

5.2.2 Secure Environment Abstraction Layer

The Secure Environment Abstraction Layer (not specified in the present document) provides access to the Secure Environment via a general Security Transport API. A Plug-in associated to the type of Secure Environment provides physical/logical connectivity to the secure environment. The Secure Environment Abstraction Layer also has to be accessible on the Service Layer.

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

---------------------Start of change 3--------------------------------------------

## 6.2 Security Service Layer

### 6.2.1 Access Management

6.2.1.1 Identification and Authentication

This component provides authentication services to the Application Layer. Annex B provides a general description of Authentication mechanisms. oneM2M mutual authentication schemes allow oneM2M entities to prove that they know related credentials such as Master Credentials, without having to exchange value of those credentials, and sensitive data such as security identities and security identifiers. To prevent reading and copying of credentials, a secure environment within the Security CSF provides protection against tampering of those credentials and related processed information. For more information see Annex B.

### 6.2.2 Authorization Architecture

Figure 6.2.2-1 provides a high level overview of a generic authorization architecture. This architecture comprises four subcomponents that are described as follows:

* Policy Enforcement Point (PEP):
* PEP intercepts resource access requests, makes access control decision requests, and enforces access control decisions. The PEP coexists with the entity that needs authorization services.
* Policy Retrieval Point (PRP):
* PRP obtains applicable authorization policies according to an access control decision request. These applicable policies should be combined in order to get a finial access control decision. The PRP is located in the Authorization service.
* Policy Information Point (PIP):
* PIP provides attributes that are needed for evaluating authorization policies, for example the IP address of the requester, creation time of the resource, current time or location information of the requester. The PIP is located in the Authorization service.
* Policy Decision Point (PDP):
* PDP interacts with the PRP and PIP to get applicable authorization polices and attributes needed for evaluating authorization policies respectively, and then evaluates access request using authorization policies for rendering an access control decision. The PDP is located in the Authorization service.

The Authorization service can comprise any of the subcomponents: PDP, PRP and/or PIP. This means that the subcomponents PEP, PRP, PDP and PIP could be distributed across different nodes. For example the PEP is located in an ASN/MN and the PDP is located in the IN.

The present release supports separation of PRP and PIP on different CSE from PDP as detailed in clause 7.5. The generic procedure described below is provided for information and to support further extensions, while clause 7 provides the details of authorization mechanisms in the current release.



Figure 6.2.2-1: Overview of the authorization architecture

The generic authorization procedure is shown in figure 6.2.2-2.



Figure 6.2.2-2: Authorization Procedure

Step 001: Mutual authentication (Pre-requisite).

Step 002: Access Requester sends an Access Request to the PEP.

Step 003: PEP makes an Access Control Decision Request according to the requester's Access Request, and sends the Access Control Decision Request to the PDP.

Step 004: PDP sends an Access Control Policy Request that is generated based on the Access Control Decision Request to the PRP.

Step 005: PRP finds all applicable access control policies to the access request and sends them back to the PDP. When multiple access control policies are involved, the PRP also provides a policy combination algorithm for combining multiple evaluation results into one finial result.

Step 006 PDP sends Attribute Request to the PIP if any attributes are required for evaluating these access control policies.

Step 007: PIP gets required attributes and sends them back to the PDP.

Step 008: PDP evaluates Access Request using access control policies. When there are multiple applicable access control policies, the PEP needs to calculate a final Access Control Decision using the policy combination algorithm.

Step 009: PDP returns the Access Control Decision back to the PEP.

Step 010: PEP enforces the access control decision, i.e. either forwards the Access Request to the resource or denies this access.

Step 011: PEP returns access result back to the Access Requester.

### 6.2.3 Security Administration

#### 6.2.3.0 Introduction

The Security Administration service provides the capability to manage the Security functions, resources and attributes. This includes management of resources provided via the secure environment. In addition it can provide functions to manage sensitive data with their associated identifiers and subscriptions on behalf of other entities. Security administration is therefore dependent upon the type of secure environment being used (independent hardware module, integrated trusted execution environment or software protection). Depending on the type of Secure Environment, distinct existing standards can be used for remote administration of those Secure Environments

#### 6.2.3.1 Security Pre-Provisioning of SE

Several sensitive data and associated objects are often configured by pre-provisioning of a secure environment (see clause 6.3.1 "Secure Environment") prior to deploying the M2M device it is associated with.

UICCs specified in ETSI TS 102 671 [23] and ETSI TS 102 221 [24] are commonly used for such purpose because their use is required to access some underlying networks, they provide a high security level, and they offer an interoperable transport interface specified in ETSI TS 102 221 [24]. UICC-based oneM2M pre-provisioning shall follow the framework specified in annex D to ensure interoperability.

#### 6.2.3.2 Remote security administration of SE

Security sensitive data and functions that are protected and isolated within the SE may remain remotely accessible to legitimate security administrators after deployment. Remote security administration differs from standard device management by the expectation that a secure channel is intended to be established between the administration server and the Secure Environment of the M2M Node (i.e. the secret used to secure the connection is not available in the M2M node outside of the Secure Environment). Applicable remote security administration protocols are dependent on the risk level of each M2M application and not just on the underlying network technologies. Widespread technologies that enable remote security administration for the different security levels distinguished in oneM2M TR‑0008 [i.4] are considered in annex C.

Since remote security administration requires the target sensitive information to be remotely modifiable, protection of such sensitive information from remote software hacking of the device is particularly critical. In case the Secure Environment relies on software protection only, remote security administration of the following data should be allowed only where remote access by potential attackers can be mitigated:

* Private key and associated identifiers.
* Long-term shared symmetric key (compared to expected lifetime of the M2M node) and associated identifiers.
* Any process and parameters thereof that manipulates the above information, i.e. security functions.

### 6.2.4 Identity Protection

Identity Protection provides services to the Application Layer such as pseudonyms and protecting the anonymity of transactions.

### 6.2.5 Sensitive Data Handling

#### 6.2.5.0 Introduction

The Sensitive Data Handling service provides certain Sensitive Functions to the Application Layer.

Sensitive Functions comprise the following functions:

* Secure Storage.
* Cryptographic operations.
* Methods for bootstrapping initial secrets (e.g. GBA).

#### 6.2.5.1 Sensitive Functions

This service provides AEs and CSEs with access to Sensitive Functions of the SE.

#### 6.2.5.2 Secure Storage

This service provides AEs and CSEs with access to the secure storage capability of the SE. Data securely stored by the AE or CSE is intended to be accessible only through the Security API and by authorized entities. Secure Storage should be managed by the Secure Environment. Securely stored data is intended to remain under the control of the stakeholder owning the data, i.e. the entity that requested the data to be stored within the secure storage, independently of other stakeholders.

### 6.2.6 Trust Enabling security functions

oneM2M Trust Enabling Architecture may require the presence of security functionalities within the Infrastructure Domain: an M2M Authentication Function (MAF) and an M2M Enrolment Function (MEF), both classified as Trust Enabling Functions (TEF) and serving authentication and end-to-end security purposes, as well as Dynamic Authorization System (DAS) server or Role Authorities serving authorization purposes. The M2M Authentication Function and the M2M Enrolment Functions shall incorporate the ability to provide for End-to-End credential registration and provisioning. In addition, a Privacy Policy Manager functionality (PPM) may be implemented to protect user's privacy. All of these functions can be either under M2M Service Provider control or delegated to a M2M Trust Enabler (i.e. a party trusted by all involved M2M ecosystem stakeholders).

* M2M Enrolment Function (MEF):
* The MEF is used during the enrolment phase and supports the security bootstrap procedure enabling the provisioning of the Master Credentials to be used to mutually authenticate entities accessing the infrastructure of an M2M Service Provider. The MEF relies on an initial credential pre-provisioned in the M2M node (e.g. during manufacturing).
* The credentials provisioned by an MEF can be used for authentication with an M2M Authentication Function in the MAF-Based Security Association Establishment Framework (SAEF), End-to-End Security of Primitives (ESPrim) or End-to-End Security of Data (ESData). Alternatively, the provisioned credentials may be used directly in the SAEF, ESPrim or ESData.
* M2M Authentication Function (MAF), used during the operational phase of M2M Services:
* Master Credentials, used to mutually authenticate CSEs/AEs during the operation phase, are securely stored in a specific infrastructure functionality named M2M Authentication Function (MAF).
* The MAF securely contains the set of Master Credentials that are used for authenticating CSEs/AEs that have been enrolled through the M2M SP or M2M Trust Enabler. The MAF stores the Master Credentials and possibly the identifiers of the associated CSE/AE.
* A single MAF may support all communication security services (SAEF, ESPrim and ESData) or only a selection of them. An MAF providing MAF-based SAEF is operated by the M2M SP, or by an M2M Trust Enabler on behalf of the M2M SP. Other MAF can be operated by M2M Trust Enabler or M2M SP, and there is no assumption of a trust relationship existing between the M2M Trust Enabler and M2M SP in those cases.
* The MAF is also in charge of all security operations involving the usage of the Master Credentials.
* Dynamic Authorization System (DAS) server and Role Authorities: These functionalities manage authorization privileges to access resources that may be assigned during operation and are described in clauses 7.3 and 7.4, respectively.
* Privacy Policy Manager (PPM): This functionality assists in the management of privacy preferences expressed by data subject with respect to service requirements and applicable regulations, and is described in clause 11.

## ---------------------End of change 3--------------------------------------------

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.?