|  |
| --- |
|  |

|  |
| --- |
| CHANGE REQUEST |
| Meeting ID:\* | SEC#31 |
| Source:\* | Saïd GHAROUT, Orange, said.gharout@orange.com |
| Date:\* | 2017-09-17 |
| Reason for Change/s:\* | Editorial changes |
| CR against: 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)[x]  STE Small Technical EnhancementsOnly ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0003 v3.5.0  |
| Clauses \* | 6.1.2, 6.2, 6.3, D |
| 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 |
| Impacted other TS/TR(s) |  |
| 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.

## Introduction

Editorial changes.

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

### 6.1.2 High level sequence of events

#### 6.1.2.1 Enrolment phase

M2M equipment typically requires provisioning and configuration phases before being put in actual operation. This can be performed by a pre-provisioning that can be integrated in the manufacturing or product deployment phase, or by means of a security bootstrapping procedure (i.e. remote security provisioning) that takes place before the equipment starts actual operation.

At the service layer level, such provisioning and configuration requires selection of the stakeholder that will provide services through the equipment, especially the M2M Service Provider. This Enrolment phase requires contractual agreements between the stakeholders.

Enrolment phase may occur several times during the lifecycle of an M2M equipment, but is only repeated when a change in the Service Provider affects the provisioning or configuration of the equipment.

The security provisioning phase for the different layers can be combined using a common method of security pre-provisioning.

Remote Security Provisioning Frameworks (RSPF) provides post-provisioning of the essential information to establish a security association between a Field Domain entity and the M2M Authentication Function of a chosen M2M Service Provider. The essential security information includes the security credentials and identifiers. Remote Security Provisioning procedures rely on an M2M Enrolment Function which can be external to the M2M Service Provider to establish appropriate credentials.

* **Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning** **Framework:** A symmetric key is pre-provisioned to the Enrolee and M2M Enrolment Function for the mutual authentication of those entities. For more details, see clause 8.3.2.1.
* **Certificate-Based Remote Security Provisioning Framework:** The Enrolee and M2M Enrolment Function are each issued and authenticate themselves with private signing keys and Certificates containing the corresponding Public Verification Key. For more details see clause 8.3.2.2.
* **GBA-based Remote Security Provisioning Framework**. In this case, the M2M Enrolment Function includes the functionality of a GBA Bootstrap Server Function. This framework uses 3GPP or 3GPP2 symmetric keys to authenticate the Enrolee and the M2M Enrolment Function (which is also a GBA BSF). The details are specified by 3GPP TS 33.220 [13] and 3GPP2 S.S0109-A [14]. For more details see clause 8.3.2.3.

Figure 6.1.2.1-1 illustrates the different Remote Security Provisioning Frameworks. Note there is no communication between M2M Entities A and B in the Remote Security Provisioning procedure. After successful completion of the Remote Security Provisioning procedure, a Security Association Establishment procedure is applied.

**M2M**

**Entity**

**A**

**M2M**

**Entity**

**B**

**UN-SP Domain**

**Field Domain**

**3rd Party Domain**

**or M2M-SP**

**Infrastructure**

**Domain**

**M2M-SP**

**Infrastructure**

**Domain**

**GBA**

**BSF**

**(=MEF)**

**MAF**

**MEF**

**SAEF after RSPF**

Figure 6.1.2.1-1: Entities involved in Remote Security Provisioning

#### 6.1.2.2 Operational phase

##### 6.1.2.2.1 M2M Service Access

M2M services are offered by CSEs to AEs and/or other CSEs. To be able to use M2M services offered by one CSE, the AEs and/or CSEs need to be mutually identified and authenticated with that CSE, in order to provide protection from unauthorized access and Denial of Service attacks. This mutual authentication enables to additionally provide encryption and integrity protection for the exchange of messages across a single Mca, Mcc or Mcc' reference point. In addition, communicating AEs that require similar protection for their own information exchanges can be provisioned to apply the same security method to their communications.

This is the purpose of the Security Association Establishment procedure, which needs to be executed before the service related procedures specified in oneM2M TS-0001 [1] for the corresponding reference point.

On the Mca and Mcc reference points, security association establishment between a field domain AE or CSE, respectively, and an IN-CSE is mandatory.

On the Mcc' reference point, security association establishment between IN-CSE and IN-CSE is mandatory.

On the Mca reference point, security association establishment between AE and the CSE in the field domain is strongly recommended.

NOTE: Security Association Establishment on the Mca interface in a local domain is optional depending on risk assessment, for instance in scenarios where unauthorized access can be prevented by other security measures out of scope of this specification. This includes the following use cases:

* AE and CSE (i.e. Mca end-points) are securely integrated on the same physical device (i.e. an ASN).
* Secure communication is guaranteed by the Underlying Network (e.g. WLAN or VPN).
* Mca communication takes place on a wire (e.g. Ethernet) in a safe physical environment.

The security association establishment phase of the M2M Service Layer and M2M Application Layer are generally independent from similar procedures possibly required by the Network Layer, though they can rely on the security services provided by the Network Layer.

The oneM2M system supports the following authentication mechanisms for Security Association Establishment, described in more detail in clause 8.2.1 "Overview on Security Association Establishment Frameworks":

* **Provisioned Symmetric Key** **Security Association Establishment Framework:** A symmetric key is pre-provisioned to the Security Association end-points. For more details see clause 8.2.2.1.
* **Certificate-Based Security Association Establishment Framework:** Security Association end-points authenticate themselves using private signing keys and Certificates containing the corresponding Public Verification Key. For more details see clause 8.2.2.2.
* **M2M Authentication Function (MAF) Security Association Establishment Framework:** For MAF‑based SAEF, the centralized key distribution server is a MAF hosted either by a 3rd party service provider which has a service relationship with the M2M Service Provider (M2M-SP), or hosted by the M2M-SP itself. The MAF authenticates a Field Domain entity on behalf of an IN-CSE using a symmetric key. For more details see clause 8.2.2.3.

Figure 6.1.2.2.1-1 illustrates the different use cases and entities involved in the various Security Association Establishment Frameworks (SAEF) considered in the present document.

**M2M**

**Entity**

**A**

**M2M**

**Entity**

**B**

**UN-SP Domain**

**Field Domain**

**3rd Party Domain**

**or M2M-SP**

**Infrastructure**

**Domain**

**M2M-SP**

**Infrastructure**

**Domain**

**MAF**

**Provisioned Symmetric Key and Certificate-Based SAEF**

**MAF**

**MAF Based SAEF**

**MAF**

Figure 6.1.2.2.1-1: Entities involved in Security Association Establishment

##### 6.1.2.2.2 Authorization to access M2M resources

Once an AE or CSE has been granted access to M2M services, the Access Control decision procedure specified in clause 7.1.5 of the present document is executed before accessing an M2M resource, as specified in oneM2M TS‑0001 [1].

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

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

## 6.2 Security Service Layer

### 6.2.1 Access Management

#### 6.2.1.1 Authentication

This component provides authentication services to the Application Layer. Annex B provides a general description of Authentication mechanisms.

### 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.

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.

For asymmetric security schemes relying on public / private key pairs, the interoperable framework to interface an M2M device with a secure environment hardware supporting generation of asymmetric key pairs, described in annex L, may be supported, so that private keys are never exposed outside of the secure environment.

#### 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 symmetric key derivation supported in annex D, or generation of asymmetric key pairs in a secure environment as specified in Annex L).

#### 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 clause 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.

## 6.3 Secure Environment Abstraction Layer Components

### 6.3.1 Secure Environment

The Secure Environment component is an entity that provides Sensitive Functions operating on Sensitive Data, Secure Storage and other resources/functions.

The security sensitive data and security functions contained in M2M field domain nodes are intended to be protected from unauthorized access or alteration, as determined by risk analysis. Sensitive data and functions include security credentials and algorithms that manipulate them. The purpose of a Secure Environment is to provide the required protection level (see table 6.3.1-1) to sensitive data during storage and usage, including primarily any long term symmetric or asymmetric cryptographic secret used during operation. Additionally, isolation of security sensitive data and functions controlled by different stakeholders within an M2M node can be ensured by distinct secure environments. This is especially critical for M2M Nodes that can be remotely or physically accessed by potential attackers.

The choice of a Secure Environment is guided by a risk analysis considering all layers of an M2M application, though it should leverage where possible on capabilities provided by the M2M Service Layer or the Underlying Network, e.g. UICC in 3GPP and 3GPP2 networks, or Trusted Execution Environment requirements.

There is no assumption made on the particular implementation of the Secure Environment. A SE may be implemented as an independent HW Secure Element or as an integrated SW function. Each Secure Environment can be associated with one certain Security Level depending on the particular implementation of the SE. Different Secure Environments provide different Security Levels and protection levels as indicated in table 6.3.1-1.

Table 6.3.1-1: Classification of Protection levels

|  |  |
| --- | --- |
| Protection Level | Description |
| 0 | No protection. The data are exposed even without active attacks. |
| 1 | Low protection, data are protected from passive observers but could be exposed by active attacks, be they local or remote.E.g. software solutions exist that rely on general purpose processing hardware of the supporting equipment. |
| 2 | Medium protection, protection of the data from remote attacks is addressed, but local attacks, especially physical attacks, remain possible, i.e. Medium protection provides countermeasures against software attacks onlyE.g. Software solutions to protect data and sensitive functions rely on specific processing providing enforced isolation and enables sensitive code and data to be kept away from an unprotected operating environment, software and memory. The code running in the protected environment is cryptographically verified for integrity assurance. |
| 3 | High protection, addressing both remote and local attacks to access the data, including attacks involving physical access. This includes strong counter measures against software and hardware attacks, such as detection of abnormal operating conditions and scrambling plus hardware masking of the memory and side channel analysis of operations involving sensitive data. |

There is intended to be at least one Secure Environment in each M2M node providing secure storage to the local CSEs and AEs, however there could be multiple.

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

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

Annex D (normative):
UICC security framework to support symmetric key based oneM2M Services

# D.0 Introduction

This annex is applicable when UICC (a type of Independent Secure Element compliant with ETSI TS 102 221 [24] and ETSI TS 102 671 [23]) is involved in M2M service layer security using Pre-Shared symmetric Keys, whether it only serves as a mean to pre-provision M2M Service layer material in M2M Devices/Gateways, or it is further used as Secured Environment in an M2M Device/Gateway.

In case of M2M deployments using asymmetric credentials (e.g. Public Key cryptography), or in case support of advanced UICC features such as File System support is not desired, Annex X of the present document provides an interoperable framework that can be implemented on tamper resistant hardware secure elements without relying on UICC specific features.

Specifically, the involvement of UICC in oneM2M security may include any of the following steps:

* Pre-provisioning of initial PSK credentials in M2M nodes by any of the following methods:
* Simple pre-provisioning and administration of M2M Service material (initial credentials and other pre-provisioned parameters), i.e. UICC-based M2M service provisioning;
* Support for infrastructure assisted bootstrapping of the M2M symmetric credentials by derivation from symmetric Access Network credentials stored in the UICC, using GBA.
* Derivation of a security association key directly derived from symmetric Access Network Credentials, using GBA. Note that this process can be supported by a Network Access Application on the UICC independently of the presence of the information structure specified in the present annex.

The support of UICC provisioning of M2M service subscription information shall be indicated in the M2M Service Table for the corresponding M2M Service Subscription as specified in the present annex.

The support of key derivation using GBA that may be used for bootstrapping or security association shall always be indicated in the Service Table of the UICC application of the Access Network Operator supporting the GBA infrastructure.

At the most basic level, UICC-based M2M pre-provisioning requires an interoperable framework to store and administrate related information in the UICC. Further involvement requires a framework for discovery of available services offered by the UICC for the hosting M2M field node. The purpose of the present annex is to specify this framework, which enables both initial service provisioning and remote security administration of the subscription information during the subscription lifetime.

A common scenario is where an M2M field node holds a UICC application protecting Access Network security credentials, and these credentials are used to derive M2M Service Layer security credentials used for M2M service bootstrapping or security association establishment in the service layer. As these scenarios require a trust agreement between the involved Access Network operator and M2M Service Provider, UICC support for M2M services in such situation shall be handled within the context of the associated Network Access application on the UICC. In particular, the UICC support for M2M credentials derivation using GBA shall be indicated within the UICC application of the Access Network operator. This is specified in clause D.1.

Even when the M2M Service Layer credentials are not derived from Access Network Credentials, the UICC may be used as a secure environment that securely protects the symmetric credential used to root security in an M2M field node. In such cases, the M2M subscription information and related methods constitute an independent application that resides on a UICC, in the sense of ETSI TS 102 221 [24]. In particular, ETSI TS 102 221 [24] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

NOTE: A terminal in the sense of TS ETSI 102 221 [24] is the part of the M2M field node that holds the UICC, e.g. a communication modem or an M2M Node processing environment.

The specific properties of the M2M Service Provider Identity Module application holding symmetric credentials is specified in clause D.2.

The storage of M2M information elements in the UICC and the procedures used for communication between the hosting M2M field node and the UICC shall be as specified in the present annex. The present annex uses abbreviations and coding conventions defined in ETSI TS 102 221 [24].

# D.1 Access Network UICC-based oneM2M Service Framework

## D.1.1 Access Network UICC-based oneM2M Service Framework characteristics

An Access Network UICC-based oneM2M Service Framework is always associated with a single M2M Service Subscription and consists of a single DF, DF1M2M, complying with the specifications in clause D.1.3, implemented in the ADF of a Network Access Application on the UICC. This situation addresses the case where a trust relationship has been established between the M2M SP and the AN operator owning the hosting ADF.

NOTE 1: This does not necessarily imply that the Access Network credentials of the corresponding ADF are used to derive the M2M Service Layer Credentials: e.g. an Access Network operator may refuse derivation from Access Network credentials to an M2M Service Provider, but may still accept to provide space on its UICC to pre-provision independent credentials or support service infrastructure-assisted bootstrapping.

There may be several oneM2M service frameworks (DF1M2M) within the ADF of a single Access Network subscription, in case this Access Network subscription is used by several independent M2M Service subscriptions. The file IDs of the DF1M2M in any ADF shall be listed under the corresponding entry in EFDIR as specified in clause D.1.2.

NOTE 2: A single M2M service layer subscription can also use multiple access networks: such subscriptions are best provisioned in a dedicated ADF as specified in clause D.2.

The content of any DF1M2M in an Access Network application ADF shall be as specified in clause D.1.3.

## D.1.2 M2M Service Framework discovery for Access Network UICC

When a UICC Network Access application supports one or more M2M Service subscriptions, with a DF1M2M, the EFDIR entry corresponding to this UICC Network Access Application shall contain the following M2M related Data Objects:

* oneM2M Service Framework DO: defining the association between the identifier of one M2M Service Subscription provisioned in the ADF and the related DF corresponding to this M2M subscription. Likewise, each M2M Service Subscription is associated to one DF. Each of these DFs is hereafter referred as DF1M2M.

There shall be as many oneM2M Service Framework Data Objects as there are M2M Service Subscriptions provisioned in the ADF.

Table D.1: Coding of oneM2M related DOs

|  |  |  |  |
| --- | --- | --- | --- |
| Bytes | Length | Description | Status |
| 1 | 1 | Discretionary template tag = '73' | M |
| 2 | 1 | Length of the discretionary template = X | M |
| 3 to (2+X) | X | Discretionary Template | X |

Table D.2: Coding of oneM2M Discretionary Template related DOs

|  |  |  |  |
| --- | --- | --- | --- |
| Bytes | Length | Description | Status |
| 1 | 1 | oneM2M service specific data content tag = 'A2' | M |
| 2 | 1 | M2M service specific data content length = Y | M |
| 3 to (2+Y) | Y | M2M service specific data content | M |

Table D.3: Coding of oneM2M Service Specific Data Content related DOs

|  |  |  |  |
| --- | --- | --- | --- |
| Bytes | Length | Description | Status |
| 1 | 1 | oneM2M supported service provisioning tag = '80' | M |
| 2 | 1 | Length of the M2M supported service provisioning tag = A | M |
| 3 to 4 | 2 | M2M Dedicated File Identifier for following M2M service subscription | M |
| 5 to (A+2) | (A-2) | M2M Subscription Identifier  | M |

Coding:

* M2M Dedicated File identifier:
* Contain the file identifier of the DF1M2M associated to the provisioning of the M2M Service subscription identified in the DO.
* M2M Subscription Identifier:
* The identifier of the M2M service subscription provisioned in the DF1M2M indicated in the Data Object, encoded in binary format.

## D.1.3 Content of files at the DF1M2M level

### D.1.3.0 Introduction

This clause specifies the EFs for the M2M service provisioning specific to a single M2M service provider, defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

The file structure for DF1M2M is illustrated in figure D.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ADFhosting AN |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | DF1M2M(FID in EFDIR) |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | EF1M2MST |  | EF1M2MSID | EF1M2MSPID |  | EFM2MNID  |  |
|  |  |  |  | '6F0A' |  | '6F02' |  | '6F03' |  | '6F04' |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | EFCSEID |  | EFM2MAEID | EFINCSEIDS |  | EFMAFFQDN |  |
|  |  |  |  | '6F05' |  | '6F06' |  | '6F08' |  | '6F09' |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | EFMEFID |  |  |  |  |  |  |  |
|  |  |  |  | '6F07' |  |  |  |  |  |  |  |

Figure D.1: File identifiers and directory structures of DF1M2M in an hosting
Access Network application ADF

### D.1.3.1 EF1M2MST (oneM2M Service Table)

This EF indicates which optional oneM2M services are available for the corresponding subscription. If a service is not indicated as available in the oneM2M DF, the hosting M2M field node shall not select this service. The presence of this file is mandatory if optional services are provided by the subscription.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F0A' | Structure: transparent | Mandatory |
| SFI: '0A' |  |
| File size: X bytes, X ≥ 1 | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 | Services n°1 to n°8 | M | 1 byte |
| 2 | Services n°9 to n°16 | O | 1 byte |
| 3 | Services n°17 to n°24 | O | 1 byte |
| 4 | Services n°25 to n°32 | O | 1 byte |
| etc. |  |  |  |
| X | Services n°(8X‑7) to n°(8X) | O | 1 byte |
|  |  |  |  |
| ‑Services |  |  |
|  Contents: | Service n°1: | Local CSE-ID provisioning |
|  | Service n°2 | IN-CSE-ID list provisioning |
|  | Service n°3 | MAF FQDN provisioning |
|  | Service n°4 | Local M2M AE-ID list provisioning |
|  | Service n°5 | Bootstrapping: MEF address provisioning |
|  | Service n°6Service n°7Service n°8 | M2M-Node-ID informationGBA Secure Provisioning (see note)GBA Secure Connection (see note) |
| NOTE: Services n°7 and 8 can only be available in a oneM2M Service Table located in a DF1M2M hosted in the ADF of the Network Access Application from which the M2M Service Layer credentials are expected to be derived. |

The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. Coding:

 1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

* Service available means that the M2M Service Subscription provisioned in the current DF or ADF has the capability to support the service and that the service is available for the user of the M2M Service Subscription.
Service not available means that the service shall not be used by the M2M Service Subscription user, even if the M2M Service Subscription has the capability to support the service.

First byte:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | b8 | b7 | b6 | B5 | b4 | b3 | b2 | b1 |
|  |  |  |  |  |  |  |  |  |  | Service n°1 |
|  |  |  |  |  |  |  |  |  |  | Service n°2 |
|  |  |  |  |  |  |  |  |  |  | Service n°3 |
|  |  |  |  |  |  |  |  |  |  | Service n°4 |
|  |  |  |  |  |  |  |  |  |  | Service n°5 |
|  |  |  |  |  |  |  |  |  |  | Service n°6 |
|  |  |  |  |  |  |  |  |  |  | Service n°7 |
|  |  |  |  |  |  |  |  |  |  | Service n°8 |

Second byte:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | b8 | b7 | b6 | B5 | b4 | b3 | b2 | b1 |
|  |  |  |  |  |  |  |  |  |  | Service n°9 |
|  |  |  |  |  |  |  |  |  |  | Service n°10 |
|  |  |  |  |  |  |  |  |  |  | Service n°11 |
|  |  |  |  |  |  |  |  |  |  | Service n°12 |
|  |  |  |  |  |  |  |  |  |  | Service n°13 |
|  |  |  |  |  |  |  |  |  |  | Service n°14 |
|  |  |  |  |  |  |  |  |  |  | Service n°15 |
|  |  |  |  |  |  |  |  |  |  | Service n°16 |

etc.

### D.1.3.2 EF1M2MSID (oneM2M Subscription Identifier)

This EF contains the oneM2M Subscription Identifier, M2M-Sub-ID. There shall be only one TLV object within this EF.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F02' | Structure: transparent | Mandatory |
| SFI: '02' |  |
| File size: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 | M2M Subscription Identifier TLV data object | M | X bytes |

The M2M Subscription Identifier value field shall contain the M2M-Sub-ID encoded as specified in oneM2M TS‑0004 [4]. The tag value of the oneM2M Subscription Identifier TLV data object shall be '80'.

### D.1.3.3 EF1M2MSPID (oneM2M Service Provider Identifier)

This EF contains the oneM2M Service Provider Identifier, M2M-SP-ID, of the M2M Service Provider related to the subscription in EF1M2MSID. There shall be only one TLV object within this EF.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F03' | Structure: transparent | Mandatory |
| SFI: '03' |  |
| File size: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 | M2M-SP-ID TLV data object | M | X bytes |

The M2M-SP-ID Value field shall contain the M2M-SP-ID encoded as specified in oneM2M TS‑0004 [4]. The tag value of the M2M-SP-ID TLV data object shall be '80'.

### D.1.3.4 EFM2MNID (M2M Node Identifier)

This EF contains the M2M-Node-ID supporting the local CSE. It may be used to logically bind a UICC to a specific M2M Node. If service n°6 is "available", this file shall be present. There shall be only one TLV object within this EF.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F04' | Structure: transparent | Optional |
| SFI: '04' |  |
| File size: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 to X | M2M-Node-ID TLV object | M | X bytes |

The M2M-Node-ID Value field shall contain the M2M-Node-ID encoded as specified in oneM2M TS-0004 [4].

### D.1.3.5 EFCSEID (local CSE Identifier)

This EF contains the local CSE Identifier, CSE-ID, for the M2M field node associated to the subscription in EF1M2MSID. If present, this file is used by the M2M field node to pre-provision the CSE-ID. If service n°1 is "available", this file shall be present. There shall be only one TLV object within this EF.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F05' | Structure: transparent | Optional |
| SFI: '05' |  |
| File size: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 | CSE-ID TLV data object | M | X bytes |

**CSE-ID TLV**

Contents:

* The CSE-ID Value field shall contain the local CSE-ID formatted as a URI.

Coding:

* The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19]. The tag value of the URI TLV data object shall be '80'.

### D.1.3.6 EFM2MAE-ID (M2M Application Identifiers list)

This EF contains the list of M2M Application Identifiers (AE-IDs) for the local M2M applications supported by the subscription in EF1M2MSID. If service n°4 is "available", this file shall be present.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F06' | Structure: Linear fixed | Optional |
| SFI: '06' |  |
| Record length: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 to X | M2M AE-ID LV data object | M | X bytes |

**M2M AE-ID LV**

Contents:

* The Value field shall contain the M2M AE-ID formatted as a URI.

Coding:

* The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19].

### D.1.3.7 EFINCSEIDS (M2M IN-CSE IDs list)

This EF contains a list of pre-provisioned IN-CSE-ID used to determine the next point of contact after provisioning or M2M Service Bootstrapping. If service n°2 is "available", this file shall be present.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F08' | Structure: Linear fixed | Optional |
|  |  |
| Record length: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 to X | IN-CSE-ID LV data object | M | X bytes |

**IN-CSE-ID LV**

Contents:

* The Value field shall contain the IN-CSE-ID formatted as a URI.

Coding:

* The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19].

### D.1.3.8 EFMAFFQDN (MAF-FQDN)

This EF is used to pre-provision the FQDN of the MAF to be used for M2M Service Connection after M2M Service Bootstrapping. If service n°3 is "available", this file shall be present. There shall be only one TLV object within this EF.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F09' | Structure: Transparent | Optional |
|  |  |
| Length: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 | MAF FQDN TLV data object | M | X bytes |

**MAF FQDN**

Contents:

* The FQDN address of the MAF.

Coding:

* The MAF-FQDN shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19]. The tag value of the MAF FQDN TLV data object shall be '80'.

### D.1.3.9 EFMEFID (M2M Enrolment Function Identifier)

This EF contains one or more M2M Enrolment Function addresses. The first record in the EF shall be considered to be of the highest priority. The last record in the EF shall be considered to be the lowest priority. If service n°5 is "available", this file shall be present.

|  |  |  |
| --- | --- | --- |
| Identifier: '6F07' | Structure: linear fixed | Optional |
|  |  |
| Record length: X bytes | Update activity: low |
| Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM |
| Bytes | Description | M/O | Length |
| 1 to X | MEF Address LV data object | M | X bytes |

**MEF Address LV data object**

Contents:

* Address of MEF, in the format of a FQDN, an IPv4 address, or an IPv6 address.

Coding:

* The format of the data object is as follows:

|  |  |
| --- | --- |
| Field | Length (bytes) |
| Length | 1 |
| Address Type | 1 |
| MEF Address | Address Length |

* Address Type: Type of the MEF address.
* This field shall be set to the type of the MEF address according to the following:

|  |  |
| --- | --- |
| Value | Name |
| 0x00 | FQDN |
| 0x01 | IPv4 |
| 0x02 | IPv6 |
| All other values are reserved |  |

* MEF Address: Address of the M2M Service Bootstrap Function.
* This field shall be set to the address of the M2M Enrolment Function. When the MEF type is set to 0x00, the corresponding MEF Address shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19].

Unused bytes shall be set to 'FF'.

# D.2 oneM2M Service Module application for symmetric credentials on UICC (1M2MSM)

## D.2.0 Introduction

This clause defines the oneM2M Service Module (1M2MSM), an application used for oneM2M Service Layer security functionalities and subscription provisioning based on symmetric keys . This application resides on the UICC, an IC card specified in ETSI TS 102 221 [24]. In particular, ETSI TS 102 221 [24] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure. There may be several 1M2MSM ADFs on a single UICC, corresponding to independent oneM2M Service Subscriptions.

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

### -----------------------Start of change 4---------------------------------------------

Annex I (informative):
Bibliography

* Open Mobile API specification V3.2.
* GlobalPlatform Device Technology TEE Client API Specification, Version 1.0.
* 3GPP TS 33.222: "Generic Authentication Architecture (GAA), Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 12)".
* 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details (Release 12)".
* 3GPP TS 29.109: "Protocols details Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on Diameter protocol; Stage 3 (Release 12)".

### -----------------------End of change 4---------------------------------------------