|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | TST#23, SEC#23 |
| Title:\* | Test Suite Structure and Test Purposes from TS-0003-V1.4.2 |
| Source:\* | Franck Le Gall & Scott Cadzow, Easy Global Market, franck.le-gall@eglobalmark.com |
| Uploaded Date:\* | 2015-05-12 |
| Document(s)  Impacted\* | N/A |
| Intended purpose of  document:\* | Decision  Discussion  Information  Other <specify> |
| Decision requested or recommendation:\* | Review of the TSS&TP derived from TS-0003-V1.4.2 |
| Template Version:23 February 2015 (Dot 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.

# Test Suite Structure for oneM2M\_003 - Security of oneM2M

The structure of the oneM2M-003 security test suite is shown graphically as a tree in figure 1 and is based on the functionality and follows as far as is practical the Table of Contents of the source document, TS-0003-V1.4.2 [1].

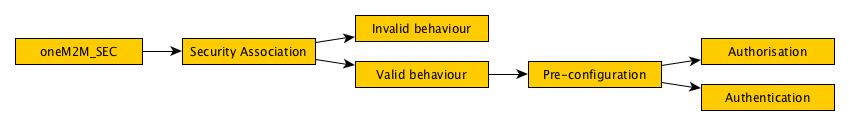


Figure 1: Graphical representation of the Test Suite Structure for oneM2M TS-0003-V1.4.2

The remainder of the present document addresses the TSS&TP more formally using the TPLan (Test Specification Language) guidelines.

Test purposes are generally to be written in the form <*pre-condition*><*stimulus*><*response*>. The specific formulation in TPLan is for the Test Purpose to be written from the viewpoint of the Implementation Under Test (IUT). A short outline of TPs and the use of TPLan is given at the end of this document.

**TSS** : oneM2M\_SEC

**Title** : 'oneM2M Security TSS and TP'

**Version** : 0.0.1

**Date** : 05.05.2016

**Author** : 'Scott Cadzow','Frank le Gall'

A large number of the Test Purposes for TS-0003 have a pre-requisite to have the parties (mutually) authenticated thus this is stated as:

**with** { **A-Party** 'authenticated by B-party' **and** **B-Party** 'authenticated by A-party' }

In addition the TSS&TP allows for direct reference to the requirements source and this is identified as follows for this particular TSS&TP against oneM2M-TS-0003:

-- Cross references

**xref** RQ\_001 {oneM2M-TS-00030V1.4.2}

In order to define the entities involved in the TSS&TP reference is made back to TS-0003 in order to identify the end-points, or users or actors, in the tests that are described.



Figure 1: High level overview of the Security architecture (from TS-0003 Figure 5.1-1)

In testing, in general, it is essential to identify the point of observation and control (PoOaC) - in other words the point at which a stimulus can be given and the response read. From the high level architecture diagram of Figure 1 the PoOaC may be considered as the API (Mca, Mcc) but as noted these are not specified. The alternative identification of the PoOaC from the security functional architecture similarly identifies Mca, Mcc and Mcn as APIs between AE, CSE and NSE but again the APIs are not specified.



Figure 2: oneM2M Functional Architecture (from TS-0003 Figure 5.3-1)

However given the above observations the message structures for requests and responses are outlined in the TS-0003 and may be formalised in TPLan as proposed below alongside the testable entities.

-- Entities

**def** **entity** FD\_AE {Field domain AE}

**def** **entity** FD\_CSE {Field domain CSE}

**def** **entity** FD\_NSE {Field domain NSE}

**def** **entity** ID\_AE {Infrastructure domain AE}

**def** **entity** ID\_CSE {Infrastructure domain CSE}

**def** **entity** ID\_NSE {Infrastructure domain NSE}

**def entity** REG\_CSE {Registrar CSE}

-- Messages

**def** **event** request\_message {} --

**def event** access-control-rule-tuple {}

-- Values

**def** **value** PERMIT -- Access control decision

**def value** DENY -- Access control decision

-- Keywords - Pre-conditions

**def** **word** **configured**

-- Keywords - Stimuli

**def** **word** **indicates**

**def** **word** **requested**

**def** **word** **requiring**

**def** **word** **send**

**def** **context** {**is** ~**requested** **to**}

-- Keywords - Responses

**def** **word** **decrements**

**def** **word** **discards**

**def** **word** **receipt**

**def** **word** **response**

**def** **word** **unchanged**

**def** **context** {**sends** **no** ~**response**}

**def** **context** {**sends** **a valid** ~**response**}

-- Keywords - Glue

**def** **word** **between**

**def** **word** **exactly**

**def** **word** **greater**

**def** **word** **less**

**def** **word** **same**

**def** **word** **than**

**def** **word** **valid**

Formalising the test purpose for "AE Impersonation Prevention" as defined in clause 7.2 of TS-0003 is as below:

**TP** **id** : TP\_SEC\_7\_2

**Summary** : 'AE Impersonation Prevention'

**RQ** **ref** : RQ\_001

**with** { REG\_CSE **configured** 'with a valid security association to AE '

**and** REG\_CSE **configured** 'to associate the SA with a unique requester id'

}

**ensure** **that** {

**when** { REG\_CSE **receives** **a** request 'containing the fr parameter'

**not containing** AE **as** **the** from\_parameter }

**then** { REG\_CSE **sends** **a** **invalid** **response** **to** AE }

}

This tests the behaviour described in figure 3 below.



Figure 3: AE impersonation checking procedure (from TS-0003 figure 7.2-1)

# Requirements catalogue from TS-0003-V.1.4.2

Prior to determining what to test it is essential to identify the requirements to be tested. In this respect TS-0003 does not have an explicit requirements catalogue and table 1 below is an initial attempt to build one. This has been constructed by extracting text from TS-0003 by making a simple search for mandates (i.e. sentences containing "shall" or ''shall not" as defined in clause 4 of the TS and the referred to oneM2M Drafting Rules).

It is suggested that not all of the resultant requirements catalogued can be tested and an indication of the "testability" of each requirement is given in the table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Req\_no | Text | Source in document TS-0003V1.4.2 | Comment | TP to be defined |
| TS-0003-1 | The security administration component shall enable administration of all sensitive resources (data and functions) and shall also allow configuration and extension of Security services itself | 5.1 | Not testable without explicit specification of the protocol and method of administration. Similarly conditions of extension not explicitly defined here. | No |
| TS-0003-2 | The Secure Environment within the CSE is accessed via the Secure Environment Abstraction layer and shall hold all sensitive resources | 5.1 | Not testable without explicit specification of "all sensitive resources" and not clear if any "sensitive resource" can be held outside the SE. | No |
| TS-0003-3 | Prior to authorization mutual authentication between the originator CSE or AE and hosting CSE shall be performed | 5.1.2 | Needs to specify the mutual authentication procedure. Not testable in this formulation. However a test purpose for verification of pre-conditions is proposed. | Yes as a precondition |
| TS-0003-4 | A Plug-in associated to the type of Secure Environment shall provide physical/logical connectivity to the secure environment | 5.2.2 |  | No |
| TS-0003-5 | The Secure Environment Abstraction Layer shall also be accessible on the Service Layer. | 5.2.2 |  | No |
| TS-0003-6 | This is the purpose of the Security Association Establishment procedure, which shall take place before execution of the service related procedures specified in oneM2M TS-0001 [] for the corresponding reference point | 6.1.2.2.1 | TS-0001 specifies the service related procedures. | Yes but only as a precondition |
| TS-0003-7 | On the Mca and Mcc reference points, security association establishment between a field domain AE or CSE, respectively, and an IN-CSE is mandatory | 6.1.2.2.1 | Need to be more explicit in the capabilities established by the security association. Not testable in this formulation. | Yes but only as a precondition |
| NOTE: The phrasing here ("is mandatory") implies a requirement but the actual requirement is not specified in a testable way. | | | |  |
| TS-0003-8 | On the Mcc' reference point, security association establishment between IN-CSE and IN-CSE is mandatory | 6.1.2.2.1 | Need to be more explicit in the capabilities established by the security association. Not testable in this formulation. | Yes but only as a precondition |
| NOTE: The phrasing here ("is mandatory") implies a requirement but the actual requirement is not specified in a testable way. | | | |  |
| TS-0003-9 | Once an AE or CSE has been granted access to M2M services, the Access Control procedure specified in clause 7 of the present document shall be executed before accessing an M2M resource, as specified in oneM2M TS-0001 [] | 6.1.2.2.2 | TS-0001 specifies the resources. Clause 7 only specifies (in part) the access control policy using a model based on XACML Policy Enforcement. The policies are not defined. The core requirements for RBAC are stated in clause 9.4 of TR-0008. |  |
| TS-0003-10 | The Security Administration service shall provide functions to manage the Security functions, resources and attributes. | 6.2.3 |  |  |
| TS-0003-11 | This {*Security Administration service*} shall include management of resources provided via the secure environment | 6.2.3 |  |  |
| TS-0003-12 | *Remote security administration differs from standard device management by the requirement that* the secure channel established with the administration server shall have its endpoint in the Secure Environment of the M2M Node | 6.2.3.2 |  |  |
| TS-0003-13 | Sensitive Functions shall include "Secure Storage" | 6.2.5 |  | No |
| TS-0003-14 | This service shall provide AEs and CSEs with access to Sensitive Functions of the SE. |  | This is an architectural constraint. | No |
| TS-0003-15 | This service shall provide AEs and CSEs with access to the secure storage capability of the SE. Data securely stored by the AE or CSE shall only be accessible through the Security API and by authorized entities. Secure Storage should be managed by the Secure Environment. Stored data shall be associated with the entity owning the data, i.e. the entity that requested the data to be stored within the secure storage. |  | Multiple requirements are stated here. |  |
| TS-0003-16 | M2M Master Credentials, used to mutually authenticate CSEs/AEs before granting them access to M2M services, shall be securely stored in a specific infrastructure functionality named M2M Authentication Function (MAF). |  |  |  |
| TS-0003-17 | The security sensitive data and security functions contained in M2M field domain nodes shall 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 the Secure Environment is to provide the required protection level (see Table 6.3.1-1) and isolation of security sensitive data and functions within an M2M node. This is especially critical for M2M Nodes that can be remotely or physically accessed by potential attackers. |  |  |  |
| TS-0003-18 | There is no assumption made on the particular implementation of the Secure Environment. A SE may be implemented as an independent HW Security Element or as an integrated SW function. Each Secure Environment shall be associated with one certain Security Level depending on the particular implementation of the SE. Different Secure Environments may provide different Security Levels and protection levels as indicated in table 6.3.1-1. |  |  |  |
| TS-0003-19 | There shall be at least one Secure Environment, however there may be multiple. |  |  |  |
| TS-0003-20 | For case where an AE initiates a new registration request to a CSE and has no preference for an assigned AE-ID value, the fr parameter shall not be sent in the request.  All other requests shall have the fr parameter present in the request. |  |  |  |
| TS-0003-21 | The accessControlTimeWindow parameter represents a list of elements that comply to the extended crontab syntax as defined in clause 7.3.8 of oneM2M TS-0004 [4]. It allows definition of periodically recurring time intervals at which access shall be granted, when the rq\_time parameter associated with the access request message falls into such interval. |  |  |  |
| TS-0003-22 | When the Registrar CSE receives a request,the Registrar CSE shall perform the following procedure. |  |  |  |
| TS-0003-23 | Use: A FQDN certificate shall be used to authenticate an M2M Enrolment Function to an Enrolee during a Bootstrap Enrolment Handshake phase in a Certificate-Based Remote Security Provisioning Framework. |  |  |  |
| TS-0003-24 | If an entity is to authenticate another entity using a device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate, then the entity shall perform basic path validation (section 6.1of IETF RFC 5280 [34]) as part of verifying the other entity's certificate (see clause 8.1.2.4 "Certificate Verification"). |  |  |  |
| TS-0003-25 | CA certificates shall include the name constraint extensions (clause 4.2.1.10 "Name Constraints" of IETF RFC 5280 [34]) and shall constrain the names (object identifier M2M Device IDs from Annex H "Object Identifier Based M2M Device Identifier" oneM2M TS-0001 [1], public domain name representation of the CSE-ID, Absolute AE-ID or FQDNs) which may be in the subsequent certificate used to authenticate the entity (device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate respectively). |  |  |  |
| TS-0003-26 | Certificate status verification: In the case of an Infrastructure Domain entity receiving an MEF certificate, the entity shall verify the status of the certificate using a Certificate Revocation List as described in IETF RFC 5280 [34]. oneM2M support for certificate status checking in Field Domain entities requires further study. A mapping of the Online Certificate Status Protocol (OCSP) onto HTTP may be used, as described in Appendix A of IETF RFC 6960 [35], however a mapping of OCSP onto CoAP is not currently defined. Furthermore, OCSP may also not be easily applicable in all environments. An alternative approach may be using the TLS Certificate Status Request extension (section 8 of IETF RFC 6066 [44]; also known as "OCSP stapling") or preferably the Multiple Certificate Status Extension (IETF RFC 6961 [36]), if available. |  |  |  |
| TS-0003-27 | If an entity is to authenticate itself using a Certificate-Based Security Framework, then the entity shall be pre-provisioned with the following information: |  |  |  |
| TS-0003-28 | In the case of a CSE-ID certificate the entity shall be configured with the entity's CSE-ID. |  |  |  |
| TS-0003-29 | In the case of an AE-ID certificate the entity shall be configured with the entity's AE-ID. |  |  |  |
| TS-0003-30 | Entity A shall be configured to trust the following information in order to authenticate Entity B using the certificate-Based SAEF: |  |  |  |
| TS-0003-31 | Entity B shall be configured to trust the following information in order to authenticate Entity A using the Certificate-Based SAEF: |  |  |  |
| TS-0003-32 | In order to authenticate the M2M Enrolment Function using the certificate-based RSPF, an Enrolee shall be configured to trust the trust anchor information of the M2M Enrolment Function’s certificate chain. |  |  |  |
| TS-0003-33 | An M2M Enrolment Function shall be configured to trust the following information in order to authenticate an Enrolee using the certificate-based RSPF: |  |  |  |
| TS-0003-34 | If the certificate information configured during the Association Configuration or Bootstrap Instruction Configuration indicates that the other entity's Certificate is a device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate, then the entity shall perform the following verifications: |  |  |  |
| TS-0003-35 | The entity shall look for a match between the globally unique identifier described in clause 8.1.2.4 "Information Needed for Certificate Authentication of another Entity" (received during Association Configuration or Bootstrap Instruction Configuration) and the values in the subjectAltName extension of the other entity's Certificate (received during the Security Handshake). If there is not an exact match, then the entity shall abort the (D)TLS handshake. |  |  |  |
| TS-0003-36 | The entity shall perform path validation and certificate status verification using the trust anchor certificate as described in clause 8.1.2.2 "Path Validation and Certificate Status Verification"). If this verification fails, then the entity shall abort the (D)TLS handshake. |  |  |  |
| TS-0003-37 | The entities shall validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, entity A creates a digital signature of the session parameters using its private signing key and entity B verifies the digital signature using entity A's public verification key. Then the roles are reversed: entity B creates a digital signature and entity A verifies it. For more details see clause 8.2.2.2. |  |  |  |
| TS-0003-38 | Entity A shall be configured with IdB, the CSE-ID for Entity B. |  |  |  |
| TS-0003-39 | Otherwise, the CSE-ID or AE-ID(s) shall be made available to Entity B via one of the following approaches. |  |  |  |
| TS-0003-40 | Credential Configuration: The Provisioned Secure Connection Key (Kpsa) and the corresponding Provisioned Secure Connection Key Identifier, denoted KpsaId, are provisioned to both entities either with pre-provisioning or remote provisioning. The format of KpsaId is defined in clause 10.5 “KpsaId Format”. If Entity A is a CSE, then Entity A shall also be configured with its CSE-ID (not shown in the figure). |  |  |  |
| TS-0003-41 | Credential Configuration: The private keys and certificates for each entity are pre-provisioned as described in clause 8.1.2.3 "Credential Configuration for Certificate-Based Security Frameworks". If Entity A is a CSE, then Entity A shall also be configured with its CSE-ID (not shown in the figure). |  |  |  |
| TS-0003-42 | Credential Configuration: The Master Credential (Km) and corresponding Master Credential Identifier (KmId) are either pre-provisioned for Entity A and the MAF or remotely provisioned thanks to Remote Security Provisioning Frameworks described in clause 8.3. The format of KmId is defined in clause 10.6 “KmId Format”. Entity A is also provisioned with the MAF URI to contact during the MAF Handshake. If Entity A is a CSE, then Entity A shall also be configured with its CSE-ID (not shown in the figure). |  |  |  |
| TS-0003-43 | Association Configuration: Entity A and the MAF shall be configured with the information needed for the authentication and identification during MAF Handshake and Association Security Handshake: |  |  |  |
| TS-0003-44 | The MAF returns Kc, Kc Lifetime, and KmId to Entity B. If MAF is configured with CSE-ID or AE-ID for Entity A (see clause 8.2.1 “Overview of Security Association Establishment Frameworks”), then the MAF shall pass this information to Entity B also. |  |  |  |
| TS-0003-45 | Entity A and Entity B may establish a fresh (D)TLS-PSK handshake using Kc at any time within the Kc Lifetime. Once Kc Lifetime expires, then Entity B shall fail the (D)TLS-PSK handshake, which indicates to Entity B that a fresh MAF Handshake is required. |  |  |  |
| TS-0003-46 | Provisioned Symmetric Key Association Establishment uses a symmetric key Kpsa and corresponding KpsaId, shared between two entities (Entity A and Entity B), to establish security associations between those two entities (CSE/AEs), as described in clause 8.2.2.1. This symmetric key Kpsa and corresponding KpsaId shall be either pre-provisioned or remotely provisioned to the two CSE/AEs thanks to Security Bootstrap Frameworks. |  |  |  |
| TS-0003-47 | The Master Credential (Km) and corresponding Master Credential Identifier (KmId) shall either be pre-provisioned or remotely provisioned to the CSE/AE and M2M Authentication Function. |  |  |  |
| TS-0003-48 | The Enrolee and M2M Enrolment Function shall validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, the M2M Enrolment Function creates a digital signature of the session parameters using its private signing key and the Enrolee verifies the digital signature using the M2M Enrolment Function's public verification key. Then the roles are reversed: the Enrolee creates a digital signature and the M2M Enrolment Function verifies it. For more details see clause 8.3.2.2. |  |  |  |
| TS-0003-49 | - The M2M Enrolment Function authorizes M2M Authentication Function, i.e. the M2M Enrolment Function shall verify whether the requested Enrolee(i.e. KeId associated with an Enrolee) information and credentials can be provisioned to M2M Authentication Function. |  |  |  |
| TS-0003-50 | To share a long term Master Credential (Km) or Provisioned Secure Connection Key (Kpsa) between an Application Service/Middle Node and an Enrolment Target, the M2M Application Service/Middle Node shall perform a successful GBA bootstrapping and derive a NAF key (Ks\_(ext/int)\_NAF). This NAF key is the Master Credential (Km) or Provisioned Secure Connection Key (Kpsa). |  |  |  |
| TS-0003-51 | Bootstrap Instruction Configuration: The Enrolee, the MEF and the Enrolment Target shall be configured with the information needed for authorizing the remote provisioning. |  |  |  |
| TS-0003-52 | The Enrolee shall be configured with the Enrolment Target Identity: identifying the Enrolment Target for which the Enrolee is to be provisioned. |  |  |  |
| TS-0003-53 | The MEF shall be configured with the Enrolee-ID and the Enrolment Target Identity: |  |  |  |
| TS-0003-54 | The Enrolment Key (Ke) shall be the GBA Bootstrapped key (Ks) established during the Bootstrap Enrolment Handshake. |  |  |  |
| TS-0003-55 | The Enrolment Key Identifier (Ke-ID) shall be the Bootstrapping Transaction Identifier ( B-TID) generated during the Bootstrap Enrolment Handshake. |  |  |  |
| TS-0003-56 | The Enrolee and the Enrolment Target shall establish the Master Credential (Km) or the Provisioned Secure Connection Key (Kpsa) thanks to procedures described in 3GPP TS 33.220 [13] using the Enrolment Key (Ke) as GBA bootstrapped key Ks and the Enrolment Key Identifier (Ke-ID) as B-TID. The Enrolment Target plays the role of a NAF. |  |  |  |
| TS-0003-57 | The Enrolee and the Enrolment Target shall establish NAF-specific key(s) as described in 3GPP TS 33.220 [13]. A key lifetime is associated to the NAF-specific keys. The Enrolment Target also receives the Enrolee's User Security Settings (USS) from the MEF/BSF: |  |  |  |
| TS-0003-58 | The FQDN of the NAF, used as input to generate the Ks\_(int/ext)\_NAF, shall be set as follows: |  |  |  |
| TS-0003-59 | The Master Credential (Km) ) or the Provisioned Secure Connection Key (Kpsa) shall be the NAF-specific key: |  |  |  |
| TS-0003-60 | The Enrolee and the Enrolment Target shall set the Master Credential Identifier (Km-Id) or the Provisioned Secure Connection Key Identifier (Kpsa-Id) to the value of KeId. |  |  |  |
| TS-0003-61 | Enrolee and Enrolment Target shall perform (D)TLS-PSK handshake (IETF RFC 4279 [15]) with the Master Credential (Km) or Provisioned Secure Connection Key (Kpsa) as Pre-Shared Key in compliance with clause 10.2.2 "TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks". If UICC is used as Secure Environment supporting Remote Security Provisioning, GBA-U with Km/Kpsa = Ks\_int\_NAF shall be used for authentication and key exchange. |  |  |  |
| TS-0003-62 | Entity B and MAF shall be able to establish mutually-authenticated secure communication. The details are not specified in the present document |  |  |  |
| TS-0003-63 | Entity B and MAF shall be able to establish mutually-authenticated secure communication. The details are not specified in the present document |  |  |  |
| TS-0003-64 | The Credential Configuration of M2M Authentication Framework shall be achieved through either: |  |  |  |
| TS-0003-65 | Mechanisms for Association Configuration of Entity A shall authenticate the configuration source and provide integrity protection for the configured information communicated from the configuration source to the entity. |  |  |  |
| TS-0003-66 | Mechanisms for Association Configuration of Entity B shall authenticate the configuration source and provide integrity protection for the configured information communicated from the configuration source to the entity. |  |  |  |
| TS-0003-67 | The Bootstrap Credential Configuration of an Enrolee for the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework shall authenticate the configuration source and shall provide confidentiality and integrity protection of the configured information communicated from the configuration source to the secured environment of the Enrolee. The present document does not specify any such mechanisms. |  |  |  |
| TS-0003-68 | Mechanisms for Bootstrap Instruction Configuration of Enrolees shall authenticate the configuration source and shall provide at least integrity protection of the configured information communicated from the configuration source to the Enrolee. |  |  |  |
| TS-0003-69 | All certificates shall conform to the following profile: |  |  |  |
| TS-0003-70 | Certificates shall conform to IETF RFC 5280 [34]. |  |  |  |
| TS-0003-71 | The certificate shall include a SubjectPublicKeyInfo that indicates an algorithm of id-ecPublicKey with namedCurves secp256r1 [34]; this curve is equivalent to the NIST P-256 curve [39]. |  |  |  |
| TS-0003-72 | The public key format shall be uncompressed [46]. |  |  |  |
| TS-0003-73 | The hash algorithm shall be SHA-256. |  |  |  |
| TS-0003-74 | The key usage extension shall be included and shall indicate at least digitalSignature. |  |  |  |
| TS-0003-75 | Raw public key certificates shall conform to clause 10.1.1.1 "Common Certificate Details" and IETF RFC 7250 [37]. |  |  |  |
| TS-0003-76 | Certificates with Certificate Chains shall conform to the following description: |  |  |  |
| TS-0003-77 | These certificates shall conform to clause 10.1.1.1 "Common Certificate Details". |  |  |  |
| TS-0003-78 | Certificates shall be signed with ECDSA using secp256r1, and the signature shall use SHA-256. |  |  |  |
| TS-0003-79 | Device certificates shall conform to the following description: |  |  |  |
| TS-0003-80 | Device certificates shall conform to clause 10.1.1.3 "Details Common to the Certificates with Certificate Chains". |  |  |  |
| TS-0003-81 | The subjectAltName extension of device certificates shall include one or more globally unique hardware instance identifiers. |  |  |  |
| TS-0003-82 | Certificate Authority Certificates in the certificate chain for a device certificate shall conform to the following description: |  |  |  |
| TS-0003-83 | These certificates shall conform to clause 10.1.1.3 "Details Common to the Certificates with Certificate Chains". |  |  |  |
| TS-0003-84 | AE-ID certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 "Details Common to Certificates with Certificate Chains". |  |  |  |
| TS-0003-85 | The full URI representation of the AE-ID shall be included in the subjectAltName extension. |  |  |  |
| TS-0003-86 | The certificate used to sign the AE-ID certificate shall include nameConstraints satisfied by the hostname part of the full URI representation of the AE-ID. |  |  |  |
| TS-0003-87 | AE-ID certificates shall not include wildcards. |  |  |  |
| TS-0003-88 | FQDN Certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 "Details Common to Certificates with Certificate Chains". |  |  |  |
| TS-0003-89 | An FQDN Certificate shall include the FQDN of the subject M2M Enrolment Function in the subjectAltName extension. |  |  |  |
| TS-0003-90 | FQDN Certificates shall not include wildcards. |  |  |  |
| TS-0003-91 | CSE-ID certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 “Details Common to Certificates with Certificate Chains”. |  |  |  |
| TS-0003-92 | The subjectAltName extension shall include the public domain name representation of the CSE-ID as defined in TS-0001 [1]. |  |  |  |
| TS-0003-93 | CSE-ID certificates shall not include wildcards. |  |  |  |
| TS-0003-94 | The public key identifier for a raw public key certificate shall calculated as described in section 2 of IETF RFC 6920 [40] using the SHA-256 hash algorithm. The public key identifier shall be generated using one of the sha-256-120, sha-256-128 or sha-256 hash algorithms specified in IETF RFC 6920 [40]. |  |  |  |
| TS-0003-95 | Where TCP payloads are to be secured, TLS v1.2 [5] shall be used. |  |  |  |
| TS-0003-96 | Where UDP payloads are to be secured, DTLS v1.2 [6] shall be used, noting that the DTLS v1.2 ciphersuites are identical to the TLS v1.2 ciphersuites. |  |  |  |
| TS-0003-97 | All implementations shall support the Server Name Indication (SNI) to indicate their authority in the SNI HostName field as defined in section 3 of IETF RFC 6066 [44]. This is needed so that when a host that acts as a virtual server for multiple Authorities receives a new TLS or DTLS connection, it knows which keys to use for the TLS or DTLS session. |  |  |  |
| TS-0003-98 | (D)TLS Clients on any Node and (D)TLS Servers on MNs shall support at least one of the TLS ciphersuites indicated in clause 10.2.2. “TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks” or 10.2.3 “TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks”. |  |  |  |
| TS-0003-99 | (D)TLS Servers on INs shall support all of the TLS ciphersuites indicated in clause 10.2.2. “TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks” and 10.2.3 “TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks”. |  |  |  |
| TS-0003-100 | shall use one of the key exchange algorithms defined in IETF RFC 4279 [15]. |  |  |  |
| TS-0003-101 | TLS implementations in entities supporting these security frameworks shall implement at least the following TLS ciphersuite: |  |  |  |
| TS-0003-102 | DTLS implementations supporting these security frameworks shall implement at least the following ciphersuites |  |  |  |
| TS-0003-103 | shall use the standard TLS handshake (IETF RFC 5246 [5]) with the ECDHE\_ECDSA Key Exchange (IETF RFC 4492 [43]). |  |  |  |
| TS-0003-104 | TLS implementations supporting these security frameworks shall implement at least the following ciphersuite: |  |  |  |
| TS-0003-105 | DTLS implementations supporting these security frameworks shall implement at least the following TLS ciphersuite: |  |  |  |
| TS-0003-106 | Implementations supporting these security frameworks shall support authenticating other entities using all available public key certificate flavours (see clause 8.1.2.1 "Public Key Certificate Flavours"): |  |  |  |
| TS-0003-107 | Raw public key certificate: using the mechanism specified in IETF RFC 7250 [37], Implementation shall support receiving and processing raw public keys compliant with section 9.1.3.2 "Raw Public Key Certificates" in IETF RFC 7252 [38]. |  |  |  |
| TS-0003-108 | All other certificates: X.509 certificates including device hardware identifier. Implementation shall support receiving and processing raw public keys compliant with section 9.1.3.3 "X.509 Certificates" in IETF RFC 7252 [38]. |  |  |  |
| TS-0003-109 | The following information shall be used when generating Km from Ke: |  |  |  |
| TS-0003-110 | the M2M Authentication Function Identifier (MAF-ID) shall be encoded to an octet string according to UTF‑8 encoding rules as specified in IETF RFC 3629 [19] and apply Normalization Form KC (NFKC) as specified in [20]. |  |  |  |
| TS-0003-111 | The value of Km shall be generated as: |  |  |  |
| TS-0003-112 | The following information shall be used when generating Kpsa from Ke: |  |  |  |
| TS-0003-113 | Enrolee B's CSE-ID or AE-ID (Enrolee-B-ID), which shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19] and apply Normalization Form KC (NFKC) as specified in [20]. |  |  |  |
| TS-0003-114 | The value of Kpsa shall be generated as: |  |  |  |
| TS-0003-115 | The KeId value shall be formed as: |  |  |  |
| TS-0003-116 | The KcId value shall be formed as |  |  |  |
| TS-0003-117 | The KpsaId shall be of the form |  |  |  |
| TS-0003-118 | Issuer\_Relative\_KpsaId is composed of the Roman alphabet, numerals, ‘.’, ‘\_’ and ‘-‘ characters. The issuer of KpsaId shall ensure that no two Kpsa have identical Issuer\_Relative\_KpsaId. |  |  |  |
| TS-0003-119 | The KmId shall be of the form |  |  |  |
| TS-0003-120 | MAF\_RELATIVE\_ KmId is composed of the Roman alphabet, numerals, ‘.’, ‘\_’ and ‘-‘ characters. The MAF\_RELATIVE\_KmId is not case sensitive. The MAF shall ensure that no two Km have identical MAF\_RELATIVE\_ KmID. |  |  |  |
| TS-0003-121 | In case of UICC (SE compliant with ETSI TS 102 671 [23]), OTA mechanisms as specified in [7] and [8], and its extensions [9], [10] for 3GPP underlying networks or [11] and [12] for 3GPP2 underlying networks shall be used to securely administrate the sensitive data of the M2M Service Layer. UICC provides the highest protection level 3 against attacks according the Classification of Protection levels table 6.2.1-1 in clause 6.2.1. |  |  |  |
| TS-0003-122 | In case the secure environment is implemented as a Trusted Execution Environment (TEE) according to GlobalPlatform [22], remote administration shall be performed according to GlobalPlatform Remote Administration [21]. TEE provides the medium protection level 2 against attacks according the Classification of Protection levels table 6.2.1-1 in clause 6.2.1. |  |  |  |
| TS-0003-123 | 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. |  |  |  |
| TS-0003-124 | 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. |  |  |  |
| TS-0003-125 | 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. |  |  |  |
| TS-0003-126 | 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]. |  |  |  |
| TS-0003-127 | 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. |  |  |  |
| TS-0003-128 | The content of any DF1M2M in an Access Network application ADF shall be as specified in clause D.1.3. |  |  |  |
| TS-0003-129 | When a UICC Network Access application supports one or more M2M Service subscription, with a DF1M2M, the EFDIR entry corresponding to this UICC Network Access Application shall contain the following M2M related Data Objects: |  |  |  |
| TS-0003-130 | There shall be as many oneM2M Service Framework Data Objects as there are M2M Service Subscriptions provisioned in the ADF. |  |  |  |
| TS-0003-131 | 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. |  |  |  |
| TS-0003-132 | 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: |  |  |  |
| TS-0003-133 | 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. |  |  |  |
| TS-0003-134 | This EF contains the oneM2M Subscription Identifier, M2M-Sub-ID. There shall be only one TLV object within this EF. |  |  |  |
| TS-0003-135 | 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'. |  |  |  |
| TS-0003-136 | 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. |  |  |  |
| TS-0003-137 | The M2M-SP-ID Value field shall contain the M2M-SP-ID encoded as specified in TS-0004 [TS0004]. The tag value of the M2M-SP-ID TLV data object shall be '80'. |  |  |  |
| TS-0003-138 | 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. |  |  |  |
| TS-0003-139 | The M2M-Node-ID Value field shall contain the M2M-Node-ID encoded as specified in oneM2M TS-0004 [4]. |  |  |  |
| TS-0003-140 | 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. |  |  |  |
| TS-0003-141 | The CSE-ID Value field shall contain the local CSE-ID formatted as a URI. |  |  |  |
| TS-0003-142 | 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'. |  |  |  |
| TS-0003-143 | 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. |  |  |  |
| TS-0003-144 | The Value field shall contain the M2M AE-ID formatted as a URI. |  |  |  |
| TS-0003-145 | The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19]. |  |  |  |
| TS-0003-146 | 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. |  |  |  |
| TS-0003-147 | The Value field shall contain the IN-CSE-ID formatted as a URI. |  |  |  |
| TS-0003-148 | The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19]. |  |  |  |
| TS-0003-149 | 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. |  |  |  |
| TS-0003-150 | 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'. |  |  |  |
| TS-0003-151 | 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. |  |  |  |
| TS-0003-152 | This field shall be set to the type of the MEF address according to the following: |  |  |  |
| TS-0003-153 | 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]. |  |  |  |
| TS-0003-154 | Unused bytes shall be set to 'FF'. |  |  |  |
| TS-0003-155 | Files at the UICC MF level are application independent as specified in ETSI TS 102 221 [24]. Only the EFDIR and EFICCID files are mandatory on UICC for the purpose of 1M2MSM applications. In any case all files shall be as specified in ETSI TS 102 221 [24]. |  |  |  |
| TS-0003-156 | The EFs in the 1M2MSM ADF contain oneM2M subscription related information that is required for M2M field nodes operating in an oneM2M environment. This ADF shall be selected using its AID and information in EFDIR. The AID for 1M2MSM applications shall be constructed as specified in ETSI TS 101 220 [27]. |  |  |  |
| TS-0003-157 | The DF1M2M substructure used to isolate the provisioning of network access dependent M2M service related information in a Network Access Application ADF is not needed for access network independent provisioning of an M2M service subscription in a 1M2MSM ADF. Therefore, all the EFs specified in clause D.1.3 shall be present at the 1M2MSM ADF level. The file structure of the ADF1M2MSM is illustrated in figure D.2. |  |  |  |
| TS-0003-158 | This clause specifies the procedures that shall be executed by M2M field nodes to interact with a oneM2M Service Subscription on UICC. They are applicable independently of the file structure supporting the oneM2M Service Subscription (1M2MSM ADF or DF1M2M under a Network Access Application ADF), unless otherwise indicated. |  |  |  |
| TS-0003-159 | If the M2M field node wants to engage in M2M operation, then after UICC activation (see ETSI TS 102 221 [24]), the M2M field node shall select a 1M2MSM application, if a 1M2MSM application is listed in the EFDIR file, using the SELECT by DF name as defined in ETSI TS 102 221 [24]. |  |  |  |
| TS-0003-160 | After a successful oneM2M application selection, the selected oneM2M AID is stored on the UICC. This application is referred to as the last selected 1M2MSM application. The last selected 1M2MSM application shall be available on the UICC after a deactivation followed by an activation of the UICC. |  |  |  |
| TS-0003-161 | If a oneM2M application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a 1M2MSM application. Furthermore if a 1M2M application is selected using a partial DF name as specified in ETSI TS 102 221 [24] indicating in the SELECT command the last occurrence, the UICC shall select the oneM2M application stored as the last oneM2M application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code. |  |  |  |
| TS-0003-162 | The M2M field node shall indicate to the oneM2M UICC application that the termination procedure is starting, by sending a particular STATUS command. |  |  |  |
| TS-0003-163 | To actually terminate the session, the M2M field node shall then use one of the mechanisms described in ETSI TS 102 221 [24]. |  |  |  |
| TS-0003-164 | The M2M field node shall perform the reading procedure with EF1M2MST. If no oneM2M related service is indicated as available, the M2M field node shall assume that only the provisioning of mandatory parameters is available in this ADF. |  |  |  |
| TS-0003-165 | The M2M field node shall perform the reading procedure with EF1M2MSID and EF1M2MSPID, and EFCSEID, EFM2MNID, EFINCSEID, EFMAFFQDN according to available services indicated in EF1M2MST. |  |  |  |
| TS-0003-166 | Condition: Service number 4 shall be available in the oneM2M Service Table. |  |  |  |
| TS-0003-167 | Under this condition, the M2M field node shall perform the reading procedure with EFM2MAEID. |  |  |  |
| TS-0003-168 | Condition: Service number 5 shall be available in the oneM2M Service Table. |  |  |  |
| TS-0003-169 | Under this condition, the M2M field node shall perform the reading procedure with EFMEFID, if the related service is available. |  |  |  |
| TS-0003-170 | After identifying the supported authentication framework, the M2M field node shall check availability of Service number 7 in EF1M2MST: If the service is available, the D/G M2M Node shall perform GBA-related procedures with AUTHENTICATE - GBA security context (Bootstrapping Mode and Derivation Mode) with the parameters for GBA secure provisioning. |  |  |  |
| TS-0003-171 | After identifying the supported authentication framework, the M2M field node shall check availability of Service number 12 in EF1M2MST: If the service is available, the M2M field node shall perform a GBA-related procedures with AUTHENTICATE - GBA security context (Bootstrapping Mode and Derivation Mode) with the parameters for GBA Security Association. |  |  |  |
| TS-0003-172 | When a request (resource access) is evaluated by a Hosting CSE and an accessControlLocationRegions parameter is defined in the privileges attribute of the <accessControlPolicy> resources, the Hosting CSE checks whether the location of the Originator of a request is in the specific regions or not. Therefore, the Hosting CSE retains the location of the Originator otherwise the Hosting CSE shall acquire the location or deny the access. This annex describes how to describe the location regions and obtain the location of the Originator. |  |  |  |
| TS-0003-173 | The practical way of describing the region or area is the circular presentation and generally the circle is characterized by the co-ordinates of a center point of the circle and a radius. Geographically, the center point and radius is described as longitude and latitude, and meter respectively. For this description, the accessControlLocationRegions parameter shall be represented as a circle. |  |  |  |
| TS-0003-174 | As mentioned above, when accessControlLocationRegions parameter is defined, the Hosting CSE shall check the location of the Originator for access control. This clause describes how the Hosting CSE checks or obtains the location. The procedures shall be varies based on the region description, circle and country. |  |  |  |
| TS-0003-175 | If the circular description is used as the location context constraints, the Hosting CSE shall check whether it has the current location of Originator or not. If not, it shall obtain the location of Originator. TS-0001 [1] defines a resource type for acquisition of location of a Target Node, <locationPolicy>. In order to , therefore, obtain the location of Originator, the Hosting CSE shall create <locationPolicy> and set the relevant attributes as follows: |  |  |  |
| TS-0003-176 | locationSource: Reliability of the location information is crucial so the location shall be obtained from trusted network. If the location is obtained by the other sources, the location information can be easily masqueraded. (i.e. GPS spoofing). Therefore, the locationSource attribute shall be set to ‘network-based'. |  |  |  |
| TS-0003-177 | locationTargetID: The Target Node shall be the Originator that needs to authorize the sent requests. The locationTargetID attribute shall be set to identifier of the Originator. |  |  |  |
| TS-0003-178 | Note that the other attributes are determined by local policies of Hosting CSE as described in clause 9.6.9 of oneM2M TS-0001 [1] and in order to obtain the location from the network, the Hosting CSE shall transform the oneM2M specified location request into network specified request. |  |  |  |
| TS-0003-179 | 2. The Hosing CSE shall evaluate the received request against the linked <accessControlPolicy> resource. If one of rule tuples that is about the request originator contains the accessControlLocationRegions parameter (circular description) and the Hosting CSE does not store the location of the Originator, the Hosting CSE shall do either continue the next step or deny the access. If the Hosting CSE has the location of the Originator, it is used for applying access control policy. |  |  |  |
| TS-0003-180 | NOTE 2: The Hosting CSE shall deny the access due to the fact that the Originator is not subscriber of the network or any other reasons (e.g. connection lost, server malfunction). |  |  |  |
| TS-0003-181 | 4. The Hosting CSE subscribes to a new area location notification service toward Location Server in the Network. The area information shall be based on the area defined by the accessControlLocationRegions parameters. If the multiple regions are defined, the multiple subscriptions shall be set. |  |  |  |
| TS-0003-182 | 8. When the Originator crossed in(enter) or out(leave) the area, the Location Server shall notify of the Hosting CSE the location change. Thus, the Hosting CSE can keep track of the location's Originator and easily evaluate the access against location context constraint. |  |  |  |
| TS-0003-183 | Generally, the Originator's country-scale location can be determined by the Originator's IP address. If the Hosting CSE can distinguish the country using the Originator's IP address and it is also matched with the defined acccessControlLocationRegions parameter, the Hosting CSE shall grant the request subject to the acceptance of the other access control policies. Note that how to transform the IP address into country is out of scope. |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Summary of TPLan (ETSI ES 202 553 [])

TPLan is a semi-formal notation for expressing Test Purposes with the intent to be used as the basis of development of specific Test Cases.

The general structure of a TP is:

*Pre-conditions* *-- optional initial conditions*

*TP behaviour description* *-- comprising sequences of:*

*Stimuli and Responses*

Each TP behaviour description shall begin with the keywords **ensure** **that** followed by the remainder of the description enclosed in curly braces ('{' and '}').

For example:

**ensure that** {

*-- TP behaviour description goes here*

}

The **when** and **then** statements describe stimuli and responses (interactions) as seen from the point of view of the IUT. Generally these are of the form:

**ensure** **that** {

**when** { *...* } *-- stimuli described from the viewpoint of the IUT*.

**then** { *...* } *-- IUT responses and other behaviour*

}

This pair of statements may be repeated any number of times to define a sequence of stimulus/response pairs, for example:

**ensure** **that** {

**when** { ... }

**then** { ... }

**when** { ... }

**then** { ... }

}

For the cases where preconditions need to be fulfilled prior to testing the <stimulus><response> behaviour TPLan specifies the use of the **with** statement used to express the initial state or condition of the **IUT** from which the TP description begins. If used, the **with** statement shall precede the **ensure that** statement. The **with** statement does not define the steps or actions needed to reach the starting condition, only the condition itself. The conditions shall be expressed as free text. Multiple conditions shall be logically concatenated using the Boolean operators **and**, **or**, **not**. The general format of the **with** statement is:

**with** { **IUT** 'condition 1' **and** 'condition 2' **and** **not** ...etc...}

# Unformatted simple requirements capture from TS-003

| Requirement number | Requirement text | Source line number |
| --- | --- | --- |
| 1 | NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. NO oneM2M PARTNER TYPE 1 SHALL BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY THAT PARTNER FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL oneM2M BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. oneM2M EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER. | Page 2Line 18 |
| 2 | The keywords "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1]. | Page 14Line 27 |
| 3 | The security administration component shall enable administration of all sensitive resources (data and functions) and shall also allow configuration and extension of Security services itself. | Page 15Line 14 |
| 4 | The Secure Environment within the CSE is accessed via the Secure Environment Abstraction layer and shall hold all sensitive resources. | Page 16Line 16 |
| 5 | Prior to authorization mutual authentication between the originator CSE or AE and hosting CSE shall be performed. | Page 16Line 28 |
| 6 | 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 shall provide physical/logical connectivity to the secure environment. The Secure Environment Abstraction Layer shall also be accessible on the Service Layer. | Page 17Line 9 |
| 7 | This is the purpose of the Security Association Establishment procedure, which shall take place before execution of the service related procedures specified in oneM2M TS-0001 [1] for the corresponding reference point. | Page 19Line 18 |
| 8 | Once an AE or CSE has been granted access to M2M services, the Access Control procedure specified in clause 7 of the present document shall be executed before accessing an M2M resource, as specified in oneM2M TS-0001 [1]. | Page 20Line 18 |
| 9 | The Security Administration service shall provide functions to manage the Security functions, resources and attributes. This shall include management of resources provided via the secure environment. In addition it should 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 may be used for remote administration of those SEs. | Page 23Line 2 |
| 10 | Security sensitive data and functions that are protected and isolated within the SE may remain remotely accessible to legitimate security admistrators after deployment. Remote security administration differs from standard device management by the requirement that the secure channel established with the administration server shall have its endpoint in the Secure Environment of the M2M Node. 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. | Page 23Line 16 |
| 11 | Sensitive Functions shall include following functions: | Page 23Line 35 |
| 12 | This service shall provide AEs and CSEs with access to Sensitive Functions of the SE. | Page 24Line 5 |
| 13 | This service shall provide AEs and CSEs with access to the secure storage capability of the SE. Data securely stored by the AE or CSE shall only be accessible through the Security API and by authorized entities. Secure Storage should be managed by the Secure Environment. Stored data shall be associated with the entity owning the data, i.e. the entity that requested the data to be stored within the secure storage. | Page 24Line 7 |
| 14 | M2M Master Credentials, used to mutually authenticate CSEs/AEs before granting them access to M2M services, shall be securely stored in a specific infrastructure functionality named M2M Authentication Function (MAF). | Page 24Line 22 |
| 15 | The security sensitive data and security functions contained in M2M field domain nodes shall 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 the Secure Environment is to provide the required protection level (see Table 6.3.1-1) and isolation of security sensitive data and functions within an M2M node. This is especially critical for M2M Nodes that can be remotely or physically accessed by potential attackers. | Page 25Line 36 |
| 16 | There is no assumption made on the particular implementation of the Secure Environment. A SE may be implemented as an independent HW Security Element or as an integrated SW function. Each Secure Environment shall be associated with one certain Security Level depending on the particular implementation of the SE. Different Secure Environments may provide different Security Levels and protection levels as indicated in table 6.3.1-1. | Page 25Line 4 |
| 17 | There shall be at least one Secure Environment, however there may be multiple. | Page 25Line 29 |
| 18 | For case where an AE initiates a new registration request to a CSE and has no preference for an assigned AE-ID value, the fr parameter shall not be sent in the request.  All other requests shall have the fr parameter present in the request. | Page 27Line 2 |
| 19 | The accessControlTimeWindow parameter represents a list of elements that comply to the extended crontab syntax as defined in clause 7.3.8 of oneM2M TS-0004 [4]. It allows definition of periodically recurring time intervals at which access shall be granted, when the rq\_time parameter associated with the access request message falls into such interval. | Page 28Line 43 |
| 20 | When the Registrar CSE receives a request,the Registrar CSE shall perform the following procedure. | Page 31Line 22 |
| 21 | Use: A FQDN certificate shall be used to authenticate an M2M Enrolment Function to an Enrolee during a Bootstrap Enrolment Handshake phase in a Certificate-Based Remote Security Provisioning Framework. | Page 33Line 21 |
| 22 | If an entity is to authenticate another entity using a device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate, then the entity shall perform basic path validation (section 6.1of IETF RFC 5280 [34]) as part of verifying the other entity's certificate (see clause 8.1.2.4 "Certificate Verification"). | Page 33Line 29 |
| 23 | CA certificates shall include the name constraint extensions (clause 4.2.1.10 "Name Constraints" of IETF RFC 5280 [34]) and shall constrain the names (object identifier M2M Device IDs from Annex H "Object Identifier Based M2M Device Identifier" oneM2M TS-0001 [1], public domain name representation of the CSE-ID, Absolute AE-ID or FQDNs) which may be in the subsequent certificate used to authenticate the entity (device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate respectively). | Page 33Line 32 |
| 24 | Certificate status verification: In the case of an Infrastructure Domain entity receiving an MEF certificate, the entity shall verify the status of the certificate using a Certificate Revocation List as described in IETF RFC 5280 [34]. oneM2M support for certificate status checking in Field Domain entities requires further study. A mapping of the Online Certificate Status Protocol (OCSP) onto HTTP may be used, as described in Appendix A of IETF RFC 6960 [35], however a mapping of OCSP onto CoAP is not currently defined. Furthermore, OCSP may also not be easily applicable in all environments. An alternative approach may be using the TLS Certificate Status Request extension (section 8 of IETF RFC 6066 [44]; also known as "OCSP stapling") or preferably the Multiple Certificate Status Extension (IETF RFC 6961 [36]), if available. | Page 34Line 1 |
| 25 | If an entity is to authenticate itself using a Certificate-Based Security Framework, then the entity shall be pre-provisioned with the following information: | Page 34Line 12 |
| 26 | In the case of a CSE-ID certificate the entity shall be configured with the entity's CSE-ID. | Page 34Line 19 |
| 27 | In the case of an AE-ID certificate the entity shall be configured with the entity's AE-ID. | Page 34Line 20 |
| 28 | Entity A shall be configured to trust the following information in order to authenticate Entity B using the certificate-Based SAEF: | Page 34Line 22 |
| 29 | Entity B shall be configured to trust the following information in order to authenticate Entity A using the Certificate-Based SAEF: | Page 34Line 39 |
| 30 | In order to authenticate the M2M Enrolment Function using the certificate-based RSPF, an Enrolee shall be configured to trust the trust anchor information of the M2M Enrolment Function’s certificate chain. | Page 35Line 6 |
| 31 | An M2M Enrolment Function shall be configured to trust the following information in order to authenticate an Enrolee using the certificate-based RSPF: | Page 35Line 8 |
| 32 | If the certificate information configured during the Association Configuration or Bootstrap Instruction Configuration indicates that the other entity's Certificate is a device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate, then the entity shall perform the following verifications: | Page 35Line 37 |
| 33 | The entity shall look for a match between the globally unique identifier described in clause 8.1.2.4 "Information Needed for Certificate Authentication of another Entity" (received during Association Configuration or Bootstrap Instruction Configuration) and the values in the subjectAltName extension of the other entity's Certificate (received during the Security Handshake). If there is not an exact match, then the entity shall abort the (D)TLS handshake. | Page 36Line 40 |
| 34 | The entity shall perform path validation and certificate status verification using the trust anchor certificate as described in clause 8.1.2.2 "Path Validation and Certificate Status Verification"). If this verification fails, then the entity shall abort the (D)TLS handshake. | Page 36Line 17 |
| 35 | The entities shall validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, entity A creates a digital signature of the session parameters using its private signing key and entity B verifies the digital signature using entity A's public verification key. Then the roles are reversed: entity B creates a digital signature and entity A verifies it. For more details see clause 8.2.2.2. | Page 37Line 19 |
| 36 | Entity A shall be configured with IdB, the CSE-ID for Entity B. | Page 38Line 19 |
| 37 | Otherwise, the CSE-ID or AE-ID(s) shall be made available to Entity B via one of the following approaches. | Page 39Line 11 |
| 38 | Credential Configuration: The Provisioned Secure Connection Key (Kpsa) and the corresponding Provisioned Secure Connection Key Identifier, denoted KpsaId, are provisioned to both entities either with pre-provisioning or remote provisioning. The format of KpsaId is defined in clause 10.5 “KpsaId Format”. If Entity A is a CSE, then Entity A shall also be configured with its CSE-ID (not shown in the figure). | Page 41Line 12 |
| 39 | Credential Configuration: The private keys and certificates for each entity are pre-provisioned as described in clause 8.1.2.3 "Credential Configuration for Certificate-Based Security Frameworks". If Entity A is a CSE, then Entity A shall also be configured with its CSE-ID (not shown in the figure). | Page 43Line 9 |
| 40 | Credential Configuration: The Master Credential (Km) and corresponding Master Credential Identifier (KmId) are either pre-provisioned for Entity A and the MAF or remotely provisioned thanks to Remote Security Provisioning Frameworks described in clause 8.3. The format of KmId is defined in clause 10.6 “KmId Format”. Entity A is also provisioned with the MAF URI to contact during the MAF Handshake. If Entity A is a CSE, then Entity A shall also be configured with its CSE-ID (not shown in the figure). | Page 46Line 10 |
| 41 | Association Configuration: Entity A and the MAF shall be configured with the information needed for the authentication and identification during MAF Handshake and Association Security Handshake: | Page 46Line 1 |
| 42 | The MAF returns Kc, Kc Lifetime, and KmId to Entity B. If MAF is configured with CSE-ID or AE-ID for Entity A (see clause 8.2.1 “Overview of Security Association Establishment Frameworks”), then the MAF shall pass this information to Entity B also. | Page 46Line 29 |
| 43 | Entity A and Entity B may establish a fresh (D)TLS-PSK handshake using Kc at any time within the Kc Lifetime. Once Kc Lifetime expires, then Entity B shall fail the (D)TLS-PSK handshake, which indicates to Entity B that a fresh MAF Handshake is required. | Page 47Line 5 |
| 44 | Provisioned Symmetric Key Association Establishment uses a symmetric key Kpsa and corresponding KpsaId, shared between two entities (Entity A and Entity B), to establish security associations between those two entities (CSE/AEs), as described in clause 8.2.2.1. This symmetric key Kpsa and corresponding KpsaId shall be either pre-provisioned or remotely provisioned to the two CSE/AEs thanks to Security Bootstrap Frameworks. | Page 47Line 16 |
| 45 | The Master Credential (Km) and corresponding Master Credential Identifier (KmId) shall either be pre-provisioned or remotely provisioned to the CSE/AE and M2M Authentication Function. | Page 47Line 24 |
| 46 | The Enrolee and M2M Enrolment Function shall validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, the M2M Enrolment Function creates a digital signature of the session parameters using its private signing key and the Enrolee verifies the digital signature using the M2M Enrolment Function's public verification key. Then the roles are reversed: the Enrolee creates a digital signature and the M2M Enrolment Function verifies it. For more details see clause 8.3.2.2. | Page 48Line 5 |
| 47 | - The M2M Enrolment Function authorizes M2M Authentication Function, i.e. the M2M Enrolment Function shall verify whether the requested Enrolee(i.e. KeId associated with an Enrolee) information and credentials can be provisioned to M2M Authentication Function. | Page 49Line 37 |
| 48 | To share a long term Master Credential (Km) or Provisioned Secure Connection Key (Kpsa) between an Application Service/Middle Node and an Enrolment Target, the M2M Application Service/Middle Node shall perform a successful GBA bootstrapping and derive a NAF key (Ks\_(ext/int)\_NAF). This NAF key is the Master Credential (Km) or Provisioned Secure Connection Key (Kpsa). | Page 56Line 38 |
| 49 | Bootstrap Instruction Configuration: The Enrolee, the MEF and the Enrolment Target shall be configured with the information needed for authorizing the remote provisioning. | Page 56Line 12 |
| 50 | The Enrolee shall be configured with the Enrolment Target Identity: identifying the Enrolment Target for which the Enrolee is to be provisioned. | Page 56Line 14 |
| 51 | The MEF shall be configured with the Enrolee-ID and the Enrolment Target Identity: | Page 56Line 16 |
| 52 | The Enrolment Key (Ke) shall be the GBA Bootstrapped key (Ks) established during the Bootstrap Enrolment Handshake. | Page 57Line 15 |
| 53 | The Enrolment Key Identifier (Ke-ID) shall be the Bootstrapping Transaction Identifier ( B-TID) generated during the Bootstrap Enrolment Handshake. | Page 57Line 17 |
| 54 | The Enrolee and the Enrolment Target shall establish the Master Credential (Km) or the Provisioned Secure Connection Key (Kpsa) thanks to procedures described in 3GPP TS 33.220 [13] using the Enrolment Key (Ke) as GBA bootstrapped key Ks and the Enrolment Key Identifier (Ke-ID) as B-TID. The Enrolment Target plays the role of a NAF. | Page 57Line 20 |
| 55 | The Enrolee and the Enrolment Target shall establish NAF-specific key(s) as described in 3GPP TS 33.220 [13]. A key lifetime is associated to the NAF-specific keys. The Enrolment Target also receives the Enrolee's User Security Settings (USS) from the MEF/BSF: | Page 57Line 24 |
| 56 | The FQDN of the NAF, used as input to generate the Ks\_(int/ext)\_NAF, shall be set as follows: | Page 57Line 27 |
| 57 | The Master Credential (Km) ) or the Provisioned Secure Connection Key (Kpsa) shall be the NAF-specific key: | Page 57Line 35 |
| 58 | The Enrolee and the Enrolment Target shall set the Master Credential Identifier (Km-Id) or the Provisioned Secure Connection Key Identifier (Kpsa-Id) to the value of KeId. | Page 57Line 40 |
| 59 | Enrolee and Enrolment Target shall perform (D)TLS-PSK handshake (IETF RFC 4279 [15]) with the Master Credential (Km) or Provisioned Secure Connection Key (Kpsa) as Pre-Shared Key in compliance with clause 10.2.2 "TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks". If UICC is used as Secure Environment supporting Remote Security Provisioning, GBA-U with Km/Kpsa = Ks\_int\_NAF shall be used for authentication and key exchange. | Page 58Line 42 |
| 60 | Entity B and MAF shall be able to establish mutually-authenticated secure communication. The details are not specified in the present document | Page 58Line 44 |
| 61 | Entity B and MAF shall be able to establish mutually-authenticated secure communication. The details are not specified in the present document | Page 59Line 17 |
| 62 | The Credential Configuration of M2M Authentication Framework shall be achieved through either: | Page 59Line 21 |
| 63 | Mechanisms for Association Configuration of Entity A shall authenticate the configuration source and provide integrity protection for the configured information communicated from the configuration source to the entity. | Page 60Line 20 |
| 64 | Mechanisms for Association Configuration of Entity B shall authenticate the configuration source and provide integrity protection for the configured information communicated from the configuration source to the entity. | Page 60Line 36 |
| 65 | The Bootstrap Credential Configuration of an Enrolee for the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework shall authenticate the configuration source and shall provide confidentiality and integrity protection of the configured information communicated from the configuration source to the secured environment of the Enrolee. The present document does not specify any such mechanisms. | Page 61Line 39 |
| 66 | Mechanisms for Bootstrap Instruction Configuration of Enrolees shall authenticate the configuration source and shall provide at least integrity protection of the configured information communicated from the configuration source to the Enrolee. | Page 63Line 47 |
| 67 | All certificates shall conform to the following profile: | Page 64Line 6 |
| 68 | Certificates shall conform to IETF RFC 5280 [34]. | Page 64Line 7 |
| 69 | The certificate shall include a SubjectPublicKeyInfo that indicates an algorithm of id-ecPublicKey with namedCurves secp256r1 [34]; this curve is equivalent to the NIST P-256 curve [39]. | Page 64Line 8 |
| 70 | The public key format shall be uncompressed [46]. | Page 64Line 10 |
| 71 | The hash algorithm shall be SHA-256. | Page 64Line 11 |
| 72 | The key usage extension shall be included and shall indicate at least digitalSignature. | Page 64Line 12 |
| 73 | Raw public key certificates shall conform to clause 10.1.1.1 "Common Certificate Details" and IETF RFC 7250 [37]. | Page 64Line 14 |
| 74 | Certificates with Certificate Chains shall conform to the following description: | Page 64Line 16 |
| 75 | These certificates shall conform to clause 10.1.1.1 "Common Certificate Details". | Page 64Line 17 |
| 76 | Certificates shall be signed with ECDSA using secp256r1, and the signature shall use SHA-256. | Page 64Line 18 |
| 77 | Device certificates shall conform to the following description: | Page 64Line 23 |
| 78 | Device certificates shall conform to clause 10.1.1.3 "Details Common to the Certificates with Certificate Chains". | Page 64Line 24 |
| 79 | The subjectAltName extension of device certificates shall include one or more globally unique hardware instance identifiers. | Page 64Line 26 |
| 80 | Certificate Authority Certificates in the certificate chain for a device certificate shall conform to the following description: | Page 65Line 6 |
| 81 | These certificates shall conform to clause 10.1.1.3 "Details Common to the Certificates with Certificate Chains". | Page 65Line 8 |
| 82 | AE-ID certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 "Details Common to Certificates with Certificate Chains". | Page 65Line 20 |
| 83 | The full URI representation of the AE-ID shall be included in the subjectAltName extension. | Page 65Line 22 |
| 84 | The certificate used to sign the AE-ID certificate shall include nameConstraints satisfied by the hostname part of the full URI representation of the AE-ID. | Page 65Line 23 |
| 85 | AE-ID certificates shall not include wildcards. | Page 65Line 25 |
| 86 | FQDN Certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 "Details Common to Certificates with Certificate Chains". | Page 65Line 27 |
| 87 | An FQDN Certificate shall include the FQDN of the subject M2M Enrolment Function in the subjectAltName extension. | Page 65Line 29 |
| 88 | FQDN Certificates shall not include wildcards. | Page 65Line 31 |
| 89 | CSE-ID certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 “Details Common to Certificates with Certificate Chains”. | Page 65Line 33 |
| 90 | The subjectAltName extension shall include the public domain name representation of the CSE-ID as defined in TS-0001 [1]. | Page 65Line 35 |
| 91 | CSE-ID certificates shall not include wildcards. | Page 65Line 37 |
| 92 | The public key identifier for a raw public key certificate shall calculated as described in section 2 of IETF RFC 6920 [40] using the SHA-256 hash algorithm. The public key identifier shall be generated using one of the sha-256-120, sha-256-128 or sha-256 hash algorithms specified in IETF RFC 6920 [40]. | Page 66Line 2 |
| 93 | Where TCP payloads are to be secured, TLS v1.2 [5] shall be used. | Page 66Line 37 |
| 94 | Where UDP payloads are to be secured, DTLS v1.2 [6] shall be used, noting that the DTLS v1.2 ciphersuites are identical to the TLS v1.2 ciphersuites. | Page 66Line 38 |
| 95 | All implementations shall support the Server Name Indication (SNI) to indicate their authority in the SNI HostName field as defined in section 3 of IETF RFC 6066 [44]. This is needed so that when a host that acts as a virtual server for multiple Authorities receives a new TLS or DTLS connection, it knows which keys to use for the TLS or DTLS session. | Page 66Line 40 |
| 96 | (D)TLS Clients on any Node and (D)TLS Servers on MNs shall support at least one of the TLS ciphersuites indicated in clause 10.2.2. “TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks” or 10.2.3 “TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks”. | Page 67Line 43 |
| 97 | (D)TLS Servers on INs shall support all of the TLS ciphersuites indicated in clause 10.2.2. “TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks” and 10.2.3 “TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks”. | Page 67Line 3 |
| 98 | shall use one of the key exchange algorithms defined in IETF RFC 4279 [15]. | Page 67Line 14 |
| 99 | TLS implementations in entities supporting these security frameworks shall implement at least the following TLS ciphersuite: | Page 67Line 15 |
| 100 | DTLS implementations supporting these security frameworks shall implement at least the following ciphersuites | Page 67Line 18 |
| 101 | shall use the standard TLS handshake (IETF RFC 5246 [5]) with the ECDHE\_ECDSA Key Exchange (IETF RFC 4492 [43]). | Page 67Line 28 |
| 102 | TLS implementations supporting these security frameworks shall implement at least the following ciphersuite: | Page 67Line 30 |
| 103 | DTLS implementations supporting these security frameworks shall implement at least the following TLS ciphersuite: | Page 67Line 32 |
| 104 | Implementations supporting these security frameworks shall support authenticating other entities using all available public key certificate flavours (see clause 8.1.2.1 "Public Key Certificate Flavours"): | Page 67Line 34 |
| 105 | Raw public key certificate: using the mechanism specified in IETF RFC 7250 [37], Implementation shall support receiving and processing raw public keys compliant with section 9.1.3.2 "Raw Public Key Certificates" in IETF RFC 7252 [38]. | Page 68Line 36 |
| 106 | All other certificates: X.509 certificates including device hardware identifier. Implementation shall support receiving and processing raw public keys compliant with section 9.1.3.3 "X.509 Certificates" in IETF RFC 7252 [38]. | Page 68Line 1 |
| 107 | The following information shall be used when generating Km from Ke: | Page 68Line 23 |
| 108 | the M2M Authentication Function Identifier (MAF-ID) shall be encoded to an octet string according to UTF‑8 encoding rules as specified in IETF RFC 3629 [19] and apply Normalization Form KC (NFKC) as specified in [20]. | Page 68Line 25 |
| 109 | The value of Km shall be generated as: | Page 68Line 28 |
| 110 | The following information shall be used when generating Kpsa from Ke: | Page 68Line 35 |
| 111 | Enrolee B's CSE-ID or AE-ID (Enrolee-B-ID), which shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19] and apply Normalization Form KC (NFKC) as specified in [20]. | Page 68Line 37 |
| 112 | The value of Kpsa shall be generated as: | Page 69Line 40 |
| 113 | The KeId value shall be formed as: | Page 69Line 5 |
| 114 | The KcId value shall be formed as | Page 69Line 12 |
| 115 | The KpsaId shall be of the form | Page 70Line 2 |
| 116 | Issuer\_Relative\_KpsaId is composed of the Roman alphabet, numerals, ‘.’, ‘\_’ and ‘-‘ characters. The issuer of KpsaId shall ensure that no two Kpsa have identical Issuer\_Relative\_KpsaId. | Page 70Line 5 |
| 117 | The KmId shall be of the form | Page 70Line 10 |
| 118 | MAF\_RELATIVE\_ KmId is composed of the Roman alphabet, numerals, ‘.’, ‘\_’ and ‘-‘ characters. The MAF\_RELATIVE\_KmId is not case sensitive. The MAF shall ensure that no two Km have identical MAF\_RELATIVE\_ KmID. | Page 70Line 13 |
| 119 | In case of UICC (SE compliant with ETSI TS 102 671 [23]), OTA mechanisms as specified in [7] and [8], and its extensions [9], [10] for 3GPP underlying networks or [11] and [12] for 3GPP2 underlying networks shall be used to securely administrate the sensitive data of the M2M Service Layer. UICC provides the highest protection level 3 against attacks according the Classification of Protection levels table 6.2.1-1 in clause 6.2.1. | Page 74Line 9 |
| 120 | In case the secure environment is implemented as a Trusted Execution Environment (TEE) according to GlobalPlatform [22], remote administration shall be performed according to GlobalPlatform Remote Administration [21]. TEE provides the medium protection level 2 against attacks according the Classification of Protection levels table 6.2.1-1 in clause 6.2.1. | Page 74Line 20 |
| 121 | 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. | Page 75Line 16 |
| 122 | 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. | Page 75Line 18 |
| 123 | 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. | Page 75Line 26 |
| 124 | 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]. | Page 76Line 43 |
| 125 | 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. | Page 76Line 13 |
| 126 | The content of any DF1M2M in an Access Network application ADF shall be as specified in clause D.1.3. | Page 76Line 18 |
| 127 | When a UICC Network Access application supports one or more M2M Service subscription, with a DF1M2M, the EFDIR entry corresponding to this UICC Network Access Application shall contain the following M2M related Data Objects: | Page 76Line 21 |
| 128 | There shall be as many oneM2M Service Framework Data Objects as there are M2M Service Subscriptions provisioned in the ADF. | Page 76Line 26 |
| 129 | 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. | Page 78Line 42 |
| 130 | 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: | Page 78Line 30 |
| 131 | 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. | Page 78Line 36 |
| 132 | This EF contains the oneM2M Subscription Identifier, M2M-Sub-ID. There shall be only one TLV object within this EF. | Page 79Line 14 |
| 133 | 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'. | Page 79Line 27 |
| 134 | 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. | Page 79Line 30 |
| 135 | The M2M-SP-ID Value field shall contain the M2M-SP-ID encoded as specified in TS-0004 [TS0004]. The tag value of the M2M-SP-ID TLV data object shall be '80'. | Page 80Line 43 |
| 136 | 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. | Page 80Line 2 |
| 137 | The M2M-Node-ID Value field shall contain the M2M-Node-ID encoded as specified in oneM2M TS-0004 [4]. | Page 80Line 15 |
| 138 | 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. | Page 80Line 17 |
| 139 | The CSE-ID Value field shall contain the local CSE-ID formatted as a URI. | Page 80Line 33 |
| 140 | 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'. | Page 80Line 35 |
| 141 | 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. | Page 80Line 38 |
| 142 | The Value field shall contain the M2M AE-ID formatted as a URI. | Page 81Line 3 |
| 143 | The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19]. | Page 81Line 5 |
| 144 | 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. | Page 81Line 8 |
| 145 | The Value field shall contain the IN-CSE-ID formatted as a URI. | Page 81Line 23 |
| 146 | The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19]. | Page 81Line 25 |
| 147 | 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. | Page 81Line 28 |
| 148 | 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'. | Page 82Line 5 |
| 149 | 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. | Page 82Line 8 |
| 150 | This field shall be set to the type of the MEF address according to the following: | Page 82Line 33 |
| 151 | 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]. | Page 82Line 41 |
| 152 | Unused bytes shall be set to 'FF'. | Page 83Line 44 |
| 153 | Files at the UICC MF level are application independent as specified in ETSI TS 102 221 [24]. Only the EFDIR and EFICCID files are mandatory on UICC for the purpose of 1M2MSM applications. In any case all files shall be as specified in ETSI TS 102 221 [24]. | Page 83Line 12 |
| 154 | The EFs in the 1M2MSM ADF contain oneM2M subscription related information that is required for M2M field nodes operating in an oneM2M environment. This ADF shall be selected using its AID and information in EFDIR. The AID for 1M2MSM applications shall be constructed as specified in ETSI TS 101 220 [27]. | Page 83Line 16 |
| 155 | The DF1M2M substructure used to isolate the provisioning of network access dependent M2M service related information in a Network Access Application ADF is not needed for access network independent provisioning of an M2M service subscription in a 1M2MSM ADF. Therefore, all the EFs specified in clause D.1.3 shall be present at the 1M2MSM ADF level. The file structure of the ADF1M2MSM is illustrated in figure D.2. | Page 83Line 23 |
| 156 | This clause specifies the procedures that shall be executed by M2M field nodes to interact with a oneM2M Service Subscription on UICC. They are applicable independently of the file structure supporting the oneM2M Service Subscription (1M2MSM ADF or DF1M2M under a Network Access Application ADF), unless otherwise indicated. | Page 84Line 2 |
| 157 | If the M2M field node wants to engage in M2M operation, then after UICC activation (see ETSI TS 102 221 [24]), the M2M field node shall select a 1M2MSM application, if a 1M2MSM application is listed in the EFDIR file, using the SELECT by DF name as defined in ETSI TS 102 221 [24]. | Page 84Line 7 |
| 158 | After a successful oneM2M application selection, the selected oneM2M AID is stored on the UICC. This application is referred to as the last selected 1M2MSM application. The last selected 1M2MSM application shall be available on the UICC after a deactivation followed by an activation of the UICC. | Page 84Line 10 |
| 159 | If a oneM2M application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a 1M2MSM application. Furthermore if a 1M2M application is selected using a partial DF name as specified in ETSI TS 102 221 [24] indicating in the SELECT command the last occurrence, the UICC shall select the oneM2M application stored as the last oneM2M application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code. | Page 84Line 13 |
| 160 | The M2M field node shall indicate to the oneM2M UICC application that the termination procedure is starting, by sending a particular STATUS command. | Page 84Line 22 |
| 161 | To actually terminate the session, the M2M field node shall then use one of the mechanisms described in ETSI TS 102 221 [24]. | Page 84Line 25 |
| 162 | The M2M field node shall perform the reading procedure with EF1M2MST. If no oneM2M related service is indicated as available, the M2M field node shall assume that only the provisioning of mandatory parameters is available in this ADF. | Page 84Line 29 |
| 163 | The M2M field node shall perform the reading procedure with EF1M2MSID and EF1M2MSPID, and EFCSEID, EFM2MNID, EFINCSEID, EFMAFFQDN according to available services indicated in EF1M2MST. | Page 84Line 35 |
| 164 | Condition: Service number 4 shall be available in the oneM2M Service Table. | Page 85Line 40 |
| 165 | Under this condition, the M2M field node shall perform the reading procedure with EFM2MAEID. | Page 85Line 1 |
| 166 | Condition: Service number 5 shall be available in the oneM2M Service Table. | Page 85Line 7 |
| 167 | Under this condition, the M2M field node shall perform the reading procedure with EFMEFID, if the related service is available. | Page 85Line 8 |
| 168 | After identifying the supported authentication framework, the M2M field node shall check availability of Service number 7 in EF1M2MST: If the service is available, the D/G M2M Node shall perform GBA-related procedures with AUTHENTICATE - GBA security context (Bootstrapping Mode and Derivation Mode) with the parameters for GBA secure provisioning. | Page 85Line 13 |
| 169 | After identifying the supported authentication framework, the M2M field node shall check availability of Service number 12 in EF1M2MST: If the service is available, the M2M field node shall perform a GBA-related procedures with AUTHENTICATE - GBA security context (Bootstrapping Mode and Derivation Mode) with the parameters for GBA Security Association. | Page 85Line 21 |
| 170 | When a request (resource access) is evaluated by a Hosting CSE and an accessControlLocationRegions parameter is defined in the privileges attribute of the <accessControlPolicy> resources, the Hosting CSE checks whether the location of the Originator of a request is in the specific regions or not. Therefore, the Hosting CSE retains the location of the Originator otherwise the Hosting CSE shall acquire the location or deny the access. This annex describes how to describe the location regions and obtain the location of the Originator. | Page 88Line 4 |
| 171 | The practical way of describing the region or area is the circular presentation and generally the circle is characterized by the co-ordinates of a center point of the circle and a radius. Geographically, the center point and radius is described as longitude and latitude, and meter respectively. For this description, the accessControlLocationRegions parameter shall be represented as a circle. | Page 88Line 11 |
| 172 | As mentioned above, when accessControlLocationRegions parameter is defined, the Hosting CSE shall check the location of the Originator for access control. This clause describes how the Hosting CSE checks or obtains the location. The procedures shall be varies based on the region description, circle and country. | Page 88Line 22 |
| 173 | If the circular description is used as the location context constraints, the Hosting CSE shall check whether it has the current location of Originator or not. If not, it shall obtain the location of Originator. TS-0001 [1] defines a resource type for acquisition of location of a Target Node, <locationPolicy>. In order to , therefore, obtain the location of Originator, the Hosting CSE shall create <locationPolicy> and set the relevant attributes as follows: | Page 89Line 26 |
| 174 | locationSource: Reliability of the location information is crucial so the location shall be obtained from trusted network. If the location is obtained by the other sources, the location information can be easily masqueraded. (i.e. GPS spoofing). Therefore, the locationSource attribute shall be set to ‘network-based'. | Page 89Line 1 |
| 175 | locationTargetID: The Target Node shall be the Originator that needs to authorize the sent requests. The locationTargetID attribute shall be set to identifier of the Originator. | Page 89Line 4 |
| 176 | Note that the other attributes are determined by local policies of Hosting CSE as described in clause 9.6.9 of oneM2M TS-0001 [1] and in order to obtain the location from the network, the Hosting CSE shall transform the oneM2M specified location request into network specified request. | Page 89Line 6 |
| 177 | 2. The Hosing CSE shall evaluate the received request against the linked <accessControlPolicy> resource. If one of rule tuples that is about the request originator contains the accessControlLocationRegions parameter (circular description) and the Hosting CSE does not store the location of the Originator, the Hosting CSE shall do either continue the next step or deny the access. If the Hosting CSE has the location of the Originator, it is used for applying access control policy. | Page 89Line 21 |
| 178 | NOTE 2: The Hosting CSE shall deny the access due to the fact that the Originator is not subscriber of the network or any other reasons (e.g. connection lost, server malfunction). | Page 89Line 26 |
| 179 | 4. The Hosting CSE subscribes to a new area location notification service toward Location Server in the Network. The area information shall be based on the area defined by the accessControlLocationRegions parameters. If the multiple regions are defined, the multiple subscriptions shall be set. | Page 90Line 1 |
| 180 | 8. When the Originator crossed in(enter) or out(leave) the area, the Location Server shall notify of the Hosting CSE the location change. Thus, the Hosting CSE can keep track of the location's Originator and easily evaluate the access against location context constraint. | Page 90Line 11 |
| 181 | Generally, the Originator's country-scale location can be determined by the Originator's IP address. If the Hosting CSE can distinguish the country using the Originator's IP address and it is also matched with the defined acccessControlLocationRegions parameter, the Hosting CSE shall grant the request subject to the acceptance of the other access control policies. Note that how to transform the IP address into country is out of scope. | Page 90Line 16 |
| 182 | However, if Hosting CSE cannot distinguish the country using the Originator's IP address, The Hosting CSE shall obtain the location coordinate (i.e., longitude and latitude) of the Originator from network and the Hosting CSE can distinguish the country using the location if available. The way of obtaining the location coordinate is defined in annex F of oneM2M TS-0004 [4]. Note that how to transform the location into country is out of scope. | Page 90Line 20 |