|  |
| --- |
|  |

|  |
| --- |
| CHANGE REQUEST |
| Meeting ID:\* |  SDS #52 |
| Source:\* | Andreas Kraft, DT, A.Kraft@telekom.de Andreas Neubacher, DT, Andreas.Neubacher@magenta.at  |
| Date:\* | 2021-12-03 |
| Reason for Change/s:\* | Fix attribute names and short names in TS-0022 (R3) |
| CR against: Release\* | Release 3 |
| CR against: WI\* | [ ]  Active WI-xxxx[x]  MNT maintenance / < Work Item number(optional)>Is this a mirror CR? Yes [ ]  No [ ] mirror CR number: (Note to Rapporteur - use latest agreed revision)[ ]  STE Small Technical Enhancements / < Work Item number (optional)>Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TS-0022, V3.0.3 |
| Clauses \* | 7.1.2, 7.1.4, 7.2.2, 7.2.4, 9.2 |
| Type of change: \* | [ ]  Editorial change[ ]  Bug Fix or Correction[x]  Change to existing feature or functionality[ ]  New feature or functionalityOnly ONE of the above shall be ticked |
| Impacted other TS/TR(s) |  |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES [x]  NO [ ] This CR may break backwards compatibility with the last approved version of the TS? YES [ ]  NO [x]  |
| Template Version: January 2017 (Do not modify) |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

GUIDELINES for Change Requests:

Provide an informative introduction containing the problem(s) being solved, and a summary list of proposals.

Each CR should contain changes related to only one particular issue/problem.

In case of a correction, and the change apply to previous releases, a separate “mirror CR” should be posted at the same time of this CR

Mirror CR: applies only when the text, including clause numbering are exactly the same.

Companion CR: applies when the change means the same but the baselines differ in some way (e.g. clause number).

Follow the principle of completeness, where all changes related to the issue or problem within a deliverable are simultaneously proposed to be made E.g. A change impacting 5 tables should not only include a proposal to change only 3 tables. Includes any changes to references, definitions, and acronyms in the same deliverable.

Follow the drafting rules.

All pictures must be editable.

Check spelling and grammar to the extent practicable.

Use Change bars for modifications.

The change should include the current and surrounding clauses to clearly show where a change is located and to provide technical context of the proposed change. Additions of complete clauses need not show surrounding clauses as long as the proposed clause number clearly shows where the new clause is proposed to be located.

Multiple changes in a single CR shall be clearly separated by horizontal lines with embedded text such as, start of change 1, end of change 1, start of new clause, end of new clause.

When subsequent changes are made to content of a CR, then the accepted version should not show changes over changes. The accepted version of the CR should only show changes relative to the baseline approved text.

Introduction

As discussed in SDS for the last months some attributes and short names are overlapping or have other conflicts with other definitions in either TS-0004 and/or TS-0032. Since technically there is not a real clash it was found desirable to remove these discrepancies to avoid confusion in implementations.

The following table reflects the agreements of the discussion.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **shortname**  | **TS-0022** - R2, R3, R4  | **TS-0004**  | **TS-0032** - R2, R3  | **Suggested new SN**  | **Remark**  |
| cpt  | coapPort  | completeTime  |    | copt  | Change TS-0022  |
| tri  | triggerRecipientID  | Trigger-Recipient-ID  |    |    | Change TS-0022  long name to Trigger-Recipient-ID  |
| aski  | symmKeyID  |    | assignedSymmKeyID  |    | Different long names in TS-0022 & TS-0032. Change long name in TS-0022  |
| cst  |  | cseType  | certSubjectType  | cest  | Change TS-0032  |
| csi  |  | CSE-ID  | certSubjectID  | cesi  | Change TS-0032  |

The changes in this document are:

Change the attribute name *triggerRecipientID* to *Trigger-Recipient-ID*
This fixes the different spelling of the attribute in different specification documents.

Change the short name for *coapPort* from *cpt* to *copt*.
This fixes the overlap with the short name of the same name for the *completeTime* attribute.

Change the long name for symmKeyID to assignedSymmKeyID (as defined in TS-0032).
This addresses the different attribute names for the same aspect.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.1.2 Resource [registration]

This specialization of <*mgmtObj*> is used to convey the service layer configuration information needed to register an AE or CSE with a Registrar CSE.



Figure 7.1.2-1: Structure of [*registration*] resource

The[*registration*] resource shall contain the child resource specified in table 7.1.2-1.

Table 7.1.2-1: Child resources of *[registration]* resource

| **Child Resources of *[registration]*** | **Child Resource Type** | **Multiplicity** | **Description** |
| --- | --- | --- | --- |
| *[variable]* | *<subscription>* | 0..n | See clause 9.6.8 of oneM2M TS-0001 [2] |

The [*registration*] resource shall contain the attributes specified in table 7.1.2-2.

Table 7.1.2-2: Attributes of *[registration]* resource

| **Attributes of *[reboot]*** | **Multiplicity** | **RW/****RO/****WO** | **Description** |
| --- | --- | --- | --- |
| *resourceType* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *resourceID* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *resourceName* | 1 | WO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *parentID* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *expirationTime* | 1 | RW | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *accessControlPolicyIDs* | 0..1 (L) | RW | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *creationTime* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *lastModifiedTime* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *labels* | 0..1(L) | RW | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *mgmtDefinition* | 1 | WO | See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1020 ("registration"). |
| *objectIDs* | 0..1 (L) | WO | See clause 9.6.15 of oneM2M TS-0001 [2]. |
| *objectPaths* | 0..1 (L) | WO | See clause 9.6.15 of oneM2M TS-0001 [2]. |
| *description* | 0..1 | RW | See clause 9.6.15 of oneM2M TS-0001 [2]. |
| *originatorID* | 0..1 | RW | CSE-ID of the CSE hosted on the ASN/MN or the AE-ID of an AE hosted on an ASN/MN or ADN node.If the setting is for a CSE, then this attribute shall be present. |
| *poA* | 1 | RW | The point of access URI of the Registrar CSE. See note. |
| *appID* | 0..1 | RW | The App-ID of an AE. This attribute shall only be present when this resource is used for the registration of an AE. |
| *externalID* | 0..1 | RW | The M2M-Ext-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger Recipient Identifier of oneM2M TS-0001 [2]. |
| *Trigger-Recipient-ID* | 0..1 | RW | The Trigger-Recipient-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger Recipient Identifier of oneM2M TS-0001 [2]. |
| *mgmtLink* | 0..1 | RW | A link to a <*mgmtObj*> resource instance containing the information for establishing a security association with the Registrar CSE. |
| NOTE: Protocol binding is determined from the protocol schema in this URI. |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.1.4 Resource [authenticationProfile]

The [*authenticationProfile*] specialization of the <*mgmtObj*> is used to convey the configuration information regarding establishing mutually-authenticated secure communications. The security principal using this configuration information can be a CSE or AE or the Managed ADN/ASN/MN acting as security principal on behalf of AEs on the Node.

An [*authenticationProfile*] instance identifies a security framework, TLS cipher suites, and credentials to be used. The applicable security framework is identified by the SUID attribute. The interpretation of SUID is specified in Table 7.1.4‑3.

NOTE 1: The present document does not support using [authenticationProfile] for identifying ESData credentials.

The [*authenticationProfile*] resource does not include any credentials, but either identifies credentials which are stored locally on the Managed Entity or identifies an M2M Authentication Function (MAF) which is to be used to facilitate establishing symmetric keys. The intended security principal on the Managed Entity is the security principal which can use either all the credentials identified by the [*authenticationProfile*] resource, or (in the case that a MAF is identified) all of the credentials required for mutual authentication with the MAF.

NOTE 2: The other security principal can be any of the following: CSE; AE; a Node terminating the security protocol on behalf of AE on Node; and an M2M Authentication Function (MAF).



Figure 7.1.4-1: Structure of [*authenticationProfile*]

The[*authenticationProfile*] resource shall contain the child resource specified in table 7.1.4-1.

Table 7.1.4-1: Child resources of *[authenticationProfile]* resource

| **Child Resources of *[authenticationProfile]*** | **Child Resource Type** | **Multiplicity** | **Description** |
| --- | --- | --- | --- |
| *[variable]* | *<subscription>* | 0..n | See clause 9.6.8 of oneM2M TS-0001 [2] |

The [*authenticationProfile*] resource shall contain the attributes specified in table 7.1.4-2.

Table 7.1.4-2: Attributes of *[authenticationProfile]* resource

| **Attributes of *[authenticationProfile]*** | **Multiplicity** | **RW/****RO/****WO** | **Description** |
| --- | --- | --- | --- |
| *resourceType* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *resourceID* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *resourceName* | 1 | WO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *parentID* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *expirationTime* | 1 | RW | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *accessControlPolicyIDs* | 0..1 (L) | RW | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *creationTime* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *lastModifiedTime* | 1 | RO | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *labels* | 0..1(L) | RW | See clause 9.6.1.3 of oneM2M TS-0001 [2]. |
| *mgmtDefinition* | 1 | WO | See clause 9.6.15 of oneM2M TS-0001 [2]. This attribute shall have the fixed value 1022 ("authenticationProfile"). |
| *objectIDs* | 0..1 (L) | WO | See clause 9.6.15 of oneM2M TS-0001 [2]. |
| *objectPaths* | 0..1 (L) | WO | See clause 9.6.15 of oneM2M TS-0001 [2]. |
| *description* | 0..1 | RW | See clause 9.6.15 of oneM2M TS-0001 [2]. |
| *SUID* | 1 | WO | Describes how the authentication profile is to be used. Further details about interpretation of each SUID are specified in Table 7.1.4-3 of the present document. |
| *TLSCiphersuites* | 0..1(L) | RW | If the security framework identified by *SUID* uses TLS, then this attributes provides a list of allowed TLS cipher suites. |
| assignedSymmKeyID | 0..1 | WO | Present when a symmetric key is to be used for mutual authentication. Identifier for a symmetric key already stored locally on the Managed Entity, or to be provisioned to the Managed Entity |
| *symmKeyValue* | 0..1 | WO | Optionally present when a symmetric key is to be used for mutual authentication. Contains the value of the symmetric key to be used for mutual authentication. |
| *MAFKeyRegLabels* | 0..1(L) | WO | Optionally present when a MAF is to be used to facilitate establishing a symmetric key for mutual authentication. Provides the content of the *labels* parameter in the MAF Key Registration request; see Table 8.8.2.7-1, oneM2M TS‑0003 [3]. |
| *MAFKeyRegDuration*  | 0..1 | WO | Present when a MAF is to be used to facilitate establishing one or more symmetric keys for mutual authentication. Provides the maximum duration for which an established symmetric key may be used. |
| *mycertFingerprint* | 0..1 | WO | Present when certificate-based authentication is to be used. Provides a hash value for identifying the certificate to be used by the intended security principal on the Managed Entity to authenticate itself to other security principals. |
| *rawPubKeyID* | 0..1 | WO | Present when certificate-based authentication is to be used and the other security principal will authenticate itself with a Raw Public Key Certificate. |
| *mgmtLink* | 0..1(L) | RW | Present when MAF is to be used to facilitate establishing one or more symmetric keys for mutual authentication or certificate-based authentication is to be used. In the former case, the list contains one reference to a [*MAFClientRegCfg*] resource. In the latter case, the list contains one or more references pointing to *[trustAnchorCred]* resources. |

Table 7.1.4-3: SUID which are currently supported in the [*authenticationProfile*] resource, along with reference to the authentication procedure in oneM2M TS-0003 [3] and mapping to symmetric key

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Value** | **Interpretation (see note)** | Authentication Procedure in oneM2M TS-0003 [3] | **Derived Symmetric Key**  | **DTLS/TLS Notes** |
| 10 | A pre-provisioned symmetric key intended to be shared with a MEF | 8.3.2.1 | Kpm | See TLS-PSK Profile in clause 10.2.2 of oneM2M TS-0003 [3] |
| 11 | A pre-provisioned symmetric key intended to be shared with a MAF  | 8.8.2.2 | Km |
| 12 | A pre-provisioned symmetric key intended for use in a Security Associated Establishment Framework (SAEF) | 8.2.2.1 | Kpsa |
| 13 | A pre-provisioned symmetric key intended for use in End-to-End Security of Primitives (ESPrim) | 8.4.2 | pairwiseESPrimKey | DTLS/TLS is not used |
| 21 | A symmetric key, provisioned via a Remote Security Provisioning Framework (RSPF), and intended to be shared with a MAF  | RSPF: 8.3.1.2MAF: 8.8.2.2, 8.8.3.1 | Km | See TLS-PSK Profile in clause 10.2.2 of oneM2M TS-0003 [3] |
| 22 | A symmetric key, provisioned via a RSPF, and intended for use in a SAEF | RSPF: 8.3.1.2SAEF: 8.2.2.1, 9.1.1.1 | Kpsa |
| 23 | A symmetric key, provisioned via a RSPF, and intended for use in ESPrim | RSPF: 8.3.1.2ESPrim: 8.4.2 | pairwiseESPrimKey | DTLS/TLS is not used |
| 32 | A MAF-distributed symmetric key intended for use in a SAEF | MAF: 8.8.2.7, 8.8.3.3SAEF: 8.2.2.3, 9.1.1.1 | Kpsa | See TLS-PSK Profile in clause 10.2.2 of oneM2M TS-0003 [3] |
| 33 | A MAF-distributed symmetric key intended for use in ESPrim | MAF: 8.8.2.7, 8.8.3.3ESPrim: 8.4.2 | pairwiseESPrimKey |
| 40 | A certificate intended to be shared with a MEF | 8.3.2.2 | NP | See certificate-based TLS profile in clause 10.2.3 of oneM2M TS‑0003 [3] |
| 41 | A certificate intended to be shared with a MAF  | 8.8.2.2 | NP |
| 42 | A certificate intended for use in a Security Associated Establishment Framework (SAEF) | 8.2.2.2 | NP |
| 43 | A certificate intended for use in End-to-End Security Certificate-based Key Establishment (ESCertKE) to establish a pairwiseESPrimKey for End-to-End Security of Primitives (ESPrim) | ESCertKE: 8.7ESPrim: 8.4.2 | NP | For ESCertKE, see certificate-based TLS profile in clause 10.2.3 of oneM2M TS-0003 [3]. For ESPrim, DTLS/TLS is not used |
| NOTE: The interpretation is copied from definition of m2m:suid in oneM2M TS-0004 [4]. The oneM2M TS-0004 [4] description takes precedence. |

The Managed Entity shall allow only TLS cipher suites identified in *TLSCiphersuites* in the TLS Handshakes for a [*authenticationProfile*] instance. The final column of table 7.1.4-3 provides references to clauses in oneM2M TS‑0003 [3] specifying the TLS Profiles to be used with the SUID values. The *TLSCiphersuite* attribute shall be present only when the value of *SUID* identifies a security framework that uses TLS or DTLS.

If the value of *SUID* is 10, 11, 12, 21, 22 or 23, then the *assignedSymmKeyID* attribute shall be present. The *assignedSymmKeyID* provides the symmetric key identifier for a symmetric key which shall be retrieved from local storage on the Managed Entity for use in the TLS Handshake. The symmetric key value may be configured in the *symmKeyValue*. Otherwise, the symmetric key, and associated symmetric key identifier, may be provisioned to the Managed Entity before or after the [*authenticationProfile*] is configured. Pre-provisioning or Remote Security Provisioning Frameworks (RSPFs), specified in oneM2M TS-0003 [3], should be used whenever possible to establish symmetric keys. Special care is recommended to ensure the confidentiality and integrity of the credentials when using the *symmKeyValue* to configure symmetric keys.

If the value of *SUID* is 32 or 33, then the *MAFKeyRegDuration* attribute shall be present, the *MAFKeyRegLabels* attribute may be present, and a [*MAFClientRegCfg*] specialization shall be configured as a child of the [*authenticationProfile*] resource. These attributes provide the configuration controlling how the Managed Entity shall interact with a MAF to establish the symmetric key subsequently used for mutual authentication. The fqdn attribute of the [*MAFClientRegCfg*] specialization identifies the MAF.

* If the Managed Entity has not already performed MAF Client Registration procedure with the identified MAF, then the MAF shall perform MAF Client Registration procedure in clause 8.8.2.3 of oneM2M TS‑0003 [3] using the information in the [*MAFClientRegCfg*] specialization of the <*mgmtObj*> specified in clause 7.1.7.
* The Managed Entity shall perform the MAF Key Registration Procedure in clause 8.8.2.7 of oneM2M TS‑0003 [3] with the identified MAF, with the parameters of table 8.8.2.7-1 of oneM2M TS-0003 [3] set as follows:
* The *MAF-FQDN* parameter shall be set to the value of the *fqdn* attribute in the [*MAFClientRegCfg*] specialization which is the child of the [*authenticationProfile*] resource.
* The *expirationTime* Parameter shall be set to the time obtained by adding the *MAFKeyRegDuration* attribute to the present time.
* If *MAFKeyRegLabels* attribute is present in the [*authenticationProfile*] resource, then the *labels* parameter shall be set to the value of the *MAFKeyRegLabels* attribute. Otherwise, the *labels* parameter shall not be present.
* The *SUID* parameter shall be set to the *SUID* attribute.
* The *targetIDs* parameter shall be set to the CSE-ID in the [*registration*] or [*dataCollection*] resource.

If the value of SUID is 40, 41, 42, or 43, then the *mycertFingerprint* attribute shall be present, and either the *rawPubKeyID* attribute shall be present or one or more [*trustAnchorCred*] specializations shall be configured as children of the [*authenticationProfile*] resource. The Managed Entity shall use the certificate matching *mycertFingerprint* to authenticate itself. The hash value portion of *mycertFingerprint* shall be computed over the X.509 ASN.1 DER encoded certificate:

* If the *rawPubKeyID* attribute is present, then the Managed Entity shall compare this value against the public key identifier (similar to a certificate fingerprint) generated from the raw public key certificate presented by the other entity, as specified in clause 10.1.2 of oneM2M TS-0003 [3]. If the *rawPubKeyID* attribute is present, the Managed Entity shall ignore [*trustAnchorCred*] resource(s) configured as children of the [*authenticationProfile*].
* If the *rawPubKeyID* attribute is not present, then the Managed Entity shall use the one or more [*trustAnchorCred*] resource instance(s) configured as children of the [*authenticationProfile*] resource instance to retrieve Certificate Authority certificates to be used by the Managed Entity as a trust anchor certificate (also known as a "root CA certificate" or "trust root certificate") when validating the certificate chains provided by other entities. The Managed Entity shall allow the TLS handshake only if the other entity provides a certificate chaining to one of these trust anchors, using the process specified in clause 8.1.2.2 in oneM2M TS-0003 [3].

[*authenticationProfile*] resources are expected to be protected by a secure environment on the Managed Entity, in order to preserve integrity of the attributes. Optimal protection is provided when the integrity protection of the management protocol message is verified in the secure environment.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.2.2 Resource [registration]

#### 7.2.2.1 Introduction

This specialization of <*mgmtObj*> is used to convey the service layer configuration information needed to register an AE or CSE with a Registrar CSE.

Table 7.2.2.1-1: Data Type Definition of [*registration*]

|  |  |  |
| --- | --- | --- |
| **Data Type ID** | **File Name** | **Note** |
| registration | DCFG-registration-v3\_0\_0.xsd |  |

Table 7.2.2.1-2: Resource specific attributes of [*registration*]

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute Name** | **Request Optionality**  | **Data Type** | **Default Value and Constraints** |
| **Create** | **Update** |
| mgmtDefinition | M | NP | See clause 7.4.15of oneM2M TS-0004 [4]. | "registration"  |
| objectIDs | O | NP | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |
| objectPaths | O | NP | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |
| description | O | O | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |
| originatorID | O | O | m2m:ID | CSE-ID of the CSE hosted on the ASN/MN or the AE-ID of an AE hosted on an ASN/MN or ADN node.If the setting is for a CSE, then this attribute shall be present. |
| poA | M | O | xs:anyURI | The point of access URI of the Registrar CSE.Note; protocol binding is determined from the protocol schema in this URI. |
| appID | O | O | m2m:ID | The APP\_ID of an AE. This attribute shall only be present when this resource is used for the registration of an AE. |
| externalID | O | O | m2m:externalID | The M2M-Ext-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger Recipient Identifier of oneM2M TS-0001 [2]. |
| Trigger-Recipient-ID | O | O | m2m:triggerRecipientID | The Trigger-Recipient-ID of the ASN/MN CSE. This attribute can be present when the originatorID is a CSE-ID and the CSE uses the dynamic registration defined in clause 7.1.10 Trigger Recipient Identifier of oneM2M TS-0001 [2]. |
| mgmtLink | O | O | m2m:mgmtLinkRef | 1 link to a [*authenticationProfile*] resource instance. See note.  |
| NOTE: The SUID in the linked [*authenticationProfile*] instance constrains the security framework to be used with the Authentication Profile. The security frameworks used with the [registration] resource are Security Association Establishment Frameworks (SAEF). The entity composing a [*registration*] instance is expected to confirm that the linked Authentication Profile contains a SUID corresponding to an SAEF. The SAEF SUIDs are the values 12, 22, 32 or 42 as defined in oneM2M TS-0004 [4]. |

#### 7.2.2.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004, '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 4 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 7.2.4 Resource [authenticationProfile]

#### 7.2.4.1 Introduction

Table 7.2.4.1-1: Data Type Definition of [*authenticationProfile*]

|  |  |  |
| --- | --- | --- |
| **Data Type ID** | **File Name** | **Note** |
| authenticationProfile | DCFG-authenticationProfile-v3\_0\_0.xsd |  |

Table 7.2.4.1-2: Resource specific attributes of [*authenticationProfile*]

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute Name** | **Request Optionality**  | **Data Type** | **Default Value and Constraints** |
| **Create** | **Update** |
| mgmtDefinition | M | NP | See clause 7.4.15 of oneM2M TS-0004 [4]. | "authenticationProfile"  |
| objectID | O | NP | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |
| objectPaths | O | NP | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |
| description | O | O | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |
| SUID | M | NP | m2m:suid | Allowed values are listed in table 7.1.4‑3. |
| TLSCiphersuites | O | O | dcfg:listOfTLSCiphersuite |  |
| assignedSymmKeyID | O | NP | sec:credentialID |  |
| symmKeyValue | O | NP | xs:hexBinary | The minimum key length is 256 bits. |
| MAFKeyRegLabels | O | NP | m2m:labels |  |
| MAFKeyRegDuration  | O | NP | xs:duration |  |
| mycertFingerprint | O | NP | dcfg:niURI or dcfg:nihURI  |  |
| rawPubKeyID | O | NP | dcfg:niURI or dcfg:nihURI  |  |
| mgmtLink | O | O | See clause 7.4.15 of oneM2M TS-0004 [4]. |  |

Table 7.2.4.1‑3: Child resources of [*authenticationProfile*] resource

|  |  |  |  |
| --- | --- | --- | --- |
| **Child Resource Type**  | **Child Resource Name** | **Multiplicity** | **Ref. to in Resource Type Definition** |
| <subscription> | [variable] | 0..n | Clause 7.4.8 of oneM2M TS-0004 [4] |

#### 7.2.4.2 Resource specific procedure on CRUD operations

When management is performed using technology specific protocols, the procedures defined in clause 7.4.15.2 of oneM2M TS-0004 [4], '<*mgmtObj*> specific procedures' shall be used. There is no change from the generic procedures in clause 7.2.2 of oneM2M TS-0004 [4] for operations on this resource. oneM2M TS-0005 [5] and oneM2M TS‑0006 [6] provide the mapping of these resources into the technology specific protocol data model.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 4 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change 5 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 9.2 Common and Field Device Configuration specific oneM2M Resource attributes

In protocol bindings, resource attribute names shall be translated into short names of table 9.2-1 and in table 8.2.3-1 of oneM2M TS-0004 [4].

Table 9.2-1: Common and Field Device Configuration specific oneM2M Attribute Short Names

| **Attribute Name** | **Occurs in** | **Short Name** | **Notes** |
| --- | --- | --- | --- |
| *resourceType* | All | ***ty*** | Defined in oneM2M TS-0004 [4]. |
| *resourceID* | All | ***ri*** | Defined in oneM2M TS-0004 [4]. |
| *resourceName* | All | ***rn*** | Defined in oneM2M TS-0004 [4]. |
| *parentID* | All | ***pi*** | Defined in oneM2M TS-0004 [4]. |
| *expirationTime* | All | ***et*** | Defined in oneM2M TS-0004 [4]. |
| *creationTime* | All | ***ct*** | Defined in oneM2M TS-0004 [4]. |
| *labels* | All | ***lbl*** | Defined in oneM2M TS-0004 [4]. |
| *lastModifiedTime* | All | ***lt*** | Defined in oneM2M TS-0004 [4]. |
| *description* | All | ***dc*** | Defined in oneM2M TS-0004 [4]. |
| *mgmtDefinition* | All | ***mgd*** | Defined in oneM2M TS-0004 [4]. |
| *objectIDs* | All | ***obis*** | Defined in oneM2M TS-0004 [4]. |
| *objectPaths* | All | ***obps*** | Defined in oneM2M TS-0004 [4]. |
| *mgmtLink* | All | ***cmlk*** | Defined in oneM2M TS-0004 [4]. |
| *originatorID* | registration | ***oid*** |  |
| *poA* | registration | ***poa*** |  |
| *appID* | registration | ***apid*** |  |
| *externalID* | registration | ***eid*** |  |
| *Trigger-Recipient-ID* | registration | ***tri*** | Defined in oneM2M TS-0004 [4]. |
| *containerPath* | dataCollection | ***cntp*** |  |
| *reportingSchedule* | dataCollection | ***rpsc*** |  |
| *measurementSchedule* | dataCollection | ***mesc*** |  |
| *SUID* | authenticationProfile | ***suid*** |  |
| *TLSCiphersuites* | authenticationProfile | ***tlcs*** |  |
| *assignedSymmKeyI* | authenticationProfile | ***aski*** |  |
| *symmKeyValue* | authenticationProfile | ***skv*** |  |
| *MAFKeyRegLabels* | authenticationProfile | ***mkrl*** |  |
| *MAFKeyRegDuration* | authenticationProfile | ***mkrd*** |  |
| *mycertFingerprint* | authenticationProfile | ***mcfp*** |  |
| *rawPubKeyID* | authenticationProfile | ***rpki*** |  |
| *SUIDs* | myCertFileCred | ***suids*** |  |
| *myCertFileFormat* | myCertFileCred | ***mcff*** |  |
| *myCertFileContent* | myCertFileCred | ***mcfc*** |  |
| *certFingerprint* | trustAnchorCred | ***cfp*** |  |
| *URI* | trustAnchorCred | ***uri*** | Defined in oneM2M TS-0004 [4]. |
| *fqdn* | MEFClientRegCfg,MAFClientRegCfg | ***fq*** | Defined in oneM2M TS-0032 [9]. |
| *adminFQDN* | MEFClientRegCfg, MAFClientRegCfg | ***adfq*** | Defined in oneM2M TS-0032 [9]. |
| *httpPort* | MEFClientRegCfg, MAFClientRegCfg | ***hpt*** | Defined in oneM2M TS-0032 [9]. |
| *coapPort* | MEFClientRegCfg, MAFClientRegCfg | ***copt*** | Defined in oneM2M TS-0032 [9]. |
| *websocketPort* | MEFClientRegCfg, MAFClientRegCfg | ***wpt*** | Defined in oneM2M TS-0032 [9]. |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change 5 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*