|  |
| --- |
|  |

|  |
| --- |
| CHANGE REQUEST |
| Meeting ID:\* |  SDS #52 |
| Source:\* | Andreas Kraft, DT, A.Kraft@telekom.de Andreas Neubacher, DT, Andreas.Neubacher@magenta.at  |
| Date:\* | 2021-07-26 |
| Reason for Change/s:\* | Adding [credentials] specialization to TS-0022 |
| CR against: Release\* | Release 5 |
| 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, V4.2.0 |
| Clauses \* | TS-0022: 7.1.11, 7.2.11, 8.1.3.3, 9.2, 9.3 |
| Type of change: \* | [ ]  Editorial change[ ]  Bug Fix or Correction[ ]  Change to existing feature or functionality[x]  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

This CR proposes a new <mgmtObj> specialization to store general credentials for a device.

In addition to, for example, network identification and authentication, a device might also need credentials to authenticate with third party components such as message broker or an additional non-oneM2M backend components which are out-of-scope of the common oneM2M Mca communication specification. Beside the already available specializations, for example for OAuth2, storing simple username/password combinations or tokens are currently not supported. Though it is recommended to utilize more modern authentication schemes, basic or token-based authentication is still widely used in legacy installations, and in installations that cannot afford or utilize an operated trust infrastructure.

The following diagram shows the general flow. An AE on an ADN requires credentials to access services on a non-oneM2M service. A CSE stores the credentials for that ADN together with other management information and makes them available via Mca. The usual oneM2M security and access methods do apply here, though an implementation may choose to store credentials in a more secure way.



A similar <flexContainer> specialization is specified in TS-0023, 5.3.1.27 “credentials”. That specialization may be added or referenced to <flexContainer> - based device management in TS-0023 to provide the same functionality as well. This would be for another CR.

Changes 1, 2, 3, 4 and 5 present the necessary changes for TS-0022, Field Device Configuration. Change 3 is provided under the assumption that the shortname tables are not integrated in TS-0004, yet.

R01: Split the CR into different CRs for TS-0022, TS-0004, and TS-0001.

R02: Removed the first sentence in Change 2, 7.2.11.2 .
Note: Further discussions how this functionality will be mapped to TS-0005 and TS-0006 can be solved in future discussions.

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

### 7.1.11 Resource [*credentials]*

This specialization of <mgmtObj> is used to store credentials on the client device.



Figure 7.1.11-1: Structure of *[credentials]* resource

The *[credentials]* resource shall contain the child resources specified in table 7.1.11-1.

Table 7.1.11-1: Child resources of *[credentials]* resource

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

The *[credentials]* resource shall contain the attributes specified in table 7.1.11.-2

Table 7.1.11-2: Attributes of *[credentials]* resource

| Attributes of *[wifiClient]* | 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 1029(credentials).  |
| *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]. |
| *purpose* | 0..1 | RW | Indicates the intended use of this credentials set. |
| *credentialID* | 0..1 | RW | Indicates a username or credential ID for authentication. |
| *credentialSecret* | 0..1 | RW | Indicates a password or credential secret for authentication. |
| *credentialToken* | 0..1 | RW | Indicates a token for authentication. |

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

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

### 7.2.11 Resource [credentials]

#### 7.2.11.1 Introduction

This specialization of <mgmtObj> is used to store credentials on the client device for authentications.

Table 7.2.11.1‑1: Data Type Definition of [credentials]

|  |  |  |
| --- | --- | --- |
| Data Type ID | File Name | Note |
| credentials | DCFG-credentials-v4\_0\_0.xsd |  |

Table 7.2.11.1‑2: Resource specific attributes of [credentials]

|  |  |  |  |
| --- | --- | --- | --- |
| 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].  | 1029 (credentials) |
| 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].  |  |
| purpose | O | O | xs:string |  |
| credentialID | O | O | xs:string |  |
| credentialSecret | O | O | xs:string |  |
| credentialToken | O | O | Xs:string |  |

#### 7.2.11.2 Resource specific procedure on CRUD operations

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 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

## 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]. |
| *CSE-ID* | registration | ***csi*** | Defined in oneM2M TS-0004 [4]. |
| *CSEBase* | registration | ***cb*** | Defined in oneM2M TS-0004 [4]. |
| *originatorID* | registration | ***oid*** |  |
| *pointOfAccess* | registration | ***poa*** |  |
| *appID* | registration | ***apid*** |  |
| *externalID* | registration | ***eid*** |  |
| *triggerRecipientID* | registration | ***tri*** |  |
| *containerPath* | dataCollection | ***cntp*** |  |
| *reportingSchedule* | dataCollection | ***rpsc*** |  |
| *measurementSchedule* | dataCollection | ***mesc*** |  |
| *SUID* | authenticationProfile | ***suid*** |  |
| *TLSCiphersuites* | authenticationProfile | ***tlcs*** |  |
| *symmKeyID* | 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 | ***cpt*** | Defined in oneM2M TS-0032 [9]. |
| *websocketPort* | MEFClientRegCfg, MAFClientRegCfg | ***wpt*** | Defined in oneM2M TS-0032 [9]. |
| *purpose* | credentials | ***pur*** |  |
| *credentialID* | credentials | ***crid*** |  |
| *credentialSecret* | credentials | ***crse*** |  |
| *credentialToken* | credentials | ***crtk*** |  |

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

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

## 9.3 Field Device Configuration specific oneM2M Resource types

In protocol bindings, resource type names of the <mgmtObj> specializations shall be translated into the short names of table 9.3-1.

Table 9.3-1: Field Device Configuration specific Resource Type Short Names

| **Resource Type Name** | **Short Name** |
| --- | --- |
| *registration* | ***reg*** |
| *registrationAnnc* | ***regA*** |
| *dataCollection* | ***datc*** |
| *dataCollectionAnnc* | ***datcA*** |
| *authenticationProfile* | ***autp*** |
| *MAFClientRegCfg* | ***macrc*** |
| *MEFClientRegCfg* | ***mecrc*** |
| *myCertFileCred* | ***nycfc*** |
| *trustAnchorCred* | ***tac*** |
| *credentials* | ***crds*** |

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

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

#### 8.1.3.3 Management using the Mcc reference point

Once M2M Service Layer operation is established between the AE or CSE and the Registrar/Hosting CSE, <*mgmtObj*> resources may be managed using the Mcc reference point by the AE or CSE subscribing to receive changes to the <*mgmtObj*> resource using the subscription procedures defined in clause 10.2.11 of oneM2M TS-0001 [2]. Establishment of the M2M Service Layer operations includes actions such as establishing the appropriate security associations and registration of the CSEs and AEs.

While not mentioned in clause 6.1 of the present document, <*mgmtObj*> specializations may be announced depending on the <*mgmtObj*> specialization type.

The following <*mgmtObj*> specializations specified in the present document are announceable (i.e. announceable variants of this resource type are defined in the XSD of the respective <*mgmtObj*> specialization):

*[registration], [dataCollection]*

The following <*mgmtObj*> specializations specified in the present document are not announceable (i.e. announceable variants of this resource type are not defined in the XSD of the respective <*mgmtObj*> specialization):

 *[authenticationProfile], [myCertFileCred], [trustAnchorCred], [MAFClientRegCfg], [MEFClientRegCfg], [OAuth2Authentication], [wificlient], [credentials]*



Figure 8.1.3.3-1: Management using the Mcc reference point

1. Once M2M Service Layer operation is established, the AE or CSE on the ASN/MN/ADN node subscribes to the <*mgmtObj*> resource which is associated with the specific M2M Application functionality creating <subscription> resource.
2. When the Configurator AE creates, updates or delete the <*mgmtObj*> resource, the Configuration AE issues a request on the <*mgmtObj*> resource.
3. The Hosting CSE for the <*mgmtObj*> resource performs the operation on the resource as Receiver.
4. The Hosting CSE notifies the subscribed AE or CSE as the subscribed event message.
5. The AE or CSE configures the M2M Application on the ASN/MN or ADN node.

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