|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | SDS-44.3 |
| Source:\* | Poornima Shandilya, C-DoT, [poornima@cdot.in](mailto:poornima@cdot.in)  Anupama Chopra, [anupama@cdot.in](mailto:anupama@cdot.in)  Prateek Varshney, [prateekv@cdot.in](mailto:prateekv@cdot.in)  Suman, [ssheoran@cdot.in](mailto:ssheoran@cdot.in)  Preeti, [preetir@cdot.in](mailto:preetir@cdot.in) |
| Date:\* | 2020-04-02 |
| Reason for Change/s:\* | Refer to Introduction section. |
| CR against: Release\* | Release 4 |
| CR against: WI\* | Active <Work Item number>  MNT maintenance / WI-0083  Is this a mirror CR? Yes  No  mirror CR number: (Note to Rapporteur - use latest agreed revision)  STE Small Technical Enhancements  Only ONE of the above shall be ticked |
| CR against: TS/TR\* | TR-0054 Version 0.7.0 |
| Clauses \* | 7.6, New section 7.8 |
| Type of change: \* | Editorial change  Bug Fix or Correction  Change to existing feature or functionality  New feature or functionality  Only ONE of the above shall be ticked |
| Impacted other TS/TR(s) | N.A. |
| Post Freeze checking:\* | This CR contains only essential changes and corrections? YES  NO  This CR may break backwards compatibility with the last approved version of the TS? YES  NO |
| 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

The M2M Service Subscription defines the technical part of the contract between an M2M Subscriber (typically an M2M Application Service Provider) and an M2M Service Provider as highlighted below. However, the current specification lacks the capability to identify what happens when the contract between an M2M Subscriber and M2M Service Provider expires.

**TS-0001**

|  |
| --- |
| The M2M Service Subscription defines the technical part of the contract between an M2M Subscriber (typically an M2M Application Service Provider) and an M2M Service Provider. |

|  |
| --- |
| 11.1 Enrolling M2M Nodes and M2M Applications for oneM2M Services Though M2M Nodes in the field domain are assumed to communicate without human involvement, individuals or organizations remain responsible for setting the access control policies used to authorize their M2M Nodes to access M2M services. In the following text, M2M Nodes refers to M2M field nodes.  In particular, individuals or organizations acquiring M2M Nodes can subscribe to a contract with an M2M Service provider (M2M Service Subscription) under which they enrol their M2M Nodes (e.g. using identifiers pre-provisioned on the nodes, such as Node-ID). This in turn may require an M2M Service provisioning step (including Security provisioning) that takes place on the target M2M Nodes themselves, for which interoperable procedures are specified by oneM2M (see clause 11.2.1). Following M2M service provisioning, the nodes can be identified and authenticated for association with an M2M Service Subscription, whose properties reflect the contractual agreement established between their owner and the M2M Service Provider.  Similarly, it may be possible for an M2M Service Provider to mandate that an M2M Application accessing M2M services be associated with a security credentials used to authorize specific operations to instance of that M2M Application, i.e. AEs (see clause 11.2.2). This step facilitates the deployment and management of M2M Applications that are instantiated in great numbers, as it enables all instances of an M2M Application to be managed through common security policies that are set once for all. It also enables keeping control over M2M Applications issued by untrusted sources.  The above steps may be delegated to an M2M trust enabler, when this role is not assumed by the M2M Service Provider. 11.2 M2M Initial Provisioning Procedures11.2.1 M2M Node Enrolment and Service Provisioning M2M service provisioning is the process by which M2M Nodes are loaded with the specific information needed to seamlessly access the M2M Services offered by an M2M Service Provider. This is an initial step performed only when an M2M Node is enrolled for using the M2M services of an M2M Service Provider. Though this process can be performed during device manufacturing, there is a need to enable this process to take place during field deployment in an interoperable way. M2M service provisioning assumes the existence of an M2M service subscription contracted with the target M2M Service Provider for the target M2M Node. Remote provisioning scenarios require the M2M Node to be mutually authenticated using pre-existing credentials (e.g. Node-ID and associated credential) with an M2M enrolment function, to securely exchange the provisioning information with the contracted M2M Service Provider. The M2M Service Provisioning takes place between an M2M Node (without provisioned CSE) and an M2M Service Provider via an M2M enrolment function. As a result of provisioning, M2M Nodes are provided with necessary credentials and possibly other M2M service related parameters (e.g. CSE-ID, M2M-Sub-ID).  The first step of M2M service provisioning is the security provisioning procedure, by which M2M service provider specific credentials are either shared between two M2M Nodes, or shared between the M2M Node in the field domain and an M2M authentication function in the infrastructure. Authenticated M2M Nodes can then be associated with an M2M Service Subscription used to determine their specific authorizations.  The following security provisioning scenarios are supported by the oneM2M architecture:   * Pre-provisioning: * Pre-provisioning includes all forms of out-of-band provisioning, e.g. provisioning M2M Nodes with M2M subscription information during the manufacturing stage. * Remote provisioning: * Remote provisioning relies on pre-existing credentials in M2M Nodes (e.g. digital certificates or network access credentials) to provision subscription related parameters through a secure session with an M2M Enrolment Function. This form of provisioning enables M2M Nodes already in the field (e.g. operational M2M Nodes) to be provisioned with M2M Service subscription. * When supported, remote provisioning procedure shall be implemented as described in the oneM2M TS‑0003 [Error: Reference source not found]. * Following M2M service provisioning, the provisioned entity securely stores credentials used for authentication , with an associated lifetime (e.g. corresponding to the duration of the contractual agreement embodied by the M2M service subscription). |

**In TS-0004,**

|  |
| --- |
| If the ***From*** parameter in a request from a Registree AE has any format other than AE-ID-Stem, the Receiver CSE shall reject the request with "BAD\_REQUEST" ***Response Status Code*** parameter value.  If the received request is communicated within an established Security Association (oneM2M TS-0003 [Error: Reference source not found]), and   * the Receiver knows that the Registree using the established Security Association is an AE; and * the Receiver knows the AE-ID(s) of the Registree using the established Security Association; and * the ***From*** parameter does not match the allowed AE-ID(s) of the Registree using the established Security Association;   then the request shall be rejected with an "ORIGINATOR\_HAS\_NOT\_REGISTERED" ***Response Status Code*** parameter value. |

The CR proposes procedure to maintain the value of *status* attribute of <m2mServiceSubscriptionProfile> resource and a new clause to describe the impact of this attribute on incoming request.

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

## Service Subscription Activation/Deactivation Status

### Solution Applicability

It should be possible to identify an ACTIVE and INACTIVE service subscription profile and each oneM2M request should be verified for its service subscription and it should be ensured that it is linked to an Active Service Subscription.

### Solution Description

When a service subscription profile is not yet activated or it reaches deactivation date then it should be marked as INACTIVE.

When a service profile is active then it should be marked as ACTIVE.

The *<m2mServiceSubscriptionProfile>* resource represents an M2M Service Subscription.

Table 7.6.2-1: New *<m2mServiceSubscriptionProfile>* resource attributes

| Attributes of *<m2mServiceSubscriptionProfile>* | Multiplicity | RW/  RO/  WO | Description |
| --- | --- | --- | --- |
| *STATUS* | 1 | RO | Identifies the status of an M2M Service Subscription Profile e.g. “ACTIVE”, “INACTIVE”. |

Below procedure shall be used to maintain the *status* of <*m2mServiceSubscriptionProfile*> resource.

When the *activationTime* in the <*m2mServiceSubscriptionProfile*> indicates a time in the future then the *status* in <*m2mServiceSubscriptionProfile*> shall be INACTIVE.

When the *deactivationTime* in the <*m2mServiceSubscriptionProfile*> indicates a time in the past then the *status* in <*m2mServiceSubscriptionProfile*> shall be INACTIVE.

When current timestamp lies within the given *activationTime* and *deactivationTime,* then *status* in <*m2mServiceSubscriptionProfile*> shall be ACTIVE.

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

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

## M2M Service Subscription Status Validation

### Solution Applicability

The M2M Service Subscription defines the technical part of the contract between an M2M Subscriber (typically an M2M Application Service Provider) and an M2M Service Provider. However, the current specification lacks the capability to identify what happens when the contract between an M2M Subscriber and M2M Service Provider expires.

If the technical contract between two parties is not yet ACTIVE or has expired then the CSE should have capability to handle the same.

Currently, applicable Service subscription profile is validated at the time of AE registration. But if the technical contract between two parties is not yet active or has been deactivated then it should be possible to reject such registration request.

Also, if there is an active registration, but the technical contract has expired i.e SSP status has become INACTIVE , then it should be possible to check the same and reject the requests.

### Solution Description

*Status* attribute in <m2mServiceSubscriptionProfile> maintains the status of a service subscription i.e. contractual agreement between M2M Service Provider and its subscribers. When agreement between two parties is INACTIVE (i.e. not yet ACTIVE or reached deactivation) then the CSE should not process such request and corresponding error should be given.

**Procedure on activation of an SSP:**

When the IN-CSE receives a request to activate a service subscription profile, it shall update SSP *status* as “ACTIVE”. It shall also send a request to all the registrar CSE(s) associated with this service subscription to update the SSP ID, status locally.

**Procedure on deactivation of an SSP:**

When the IN-CSE receives a request to deactivate a service subscription profile, it shall update SSP *status* as “INACTIVE”. It shall also send a request to all the registrar CSE(s) associated with this service subscription to update the SSP ID, status locally.

**Processing at each request:**

**When security association is established:**

The credentials for an entity are associated with their service subscription profile at the time of configuration. *M2M-Sub-ID* attribute is added in [authenticationProfile] for management of credentials corresponding to a service subscription. This mapping can be used in identifying whether the credentials are associated with an ACTIVE or INACTIVE SSP.

AE/CSE establishes a security association with the Registrar CSE. Upon receiving the request, the Registrar CSE verifies whether the credentials are associated with an ACTIVE service subscription, if not then the request shall be rejected with “INACTIVE\_SERVICE\_SUBSCRIPTION” response status code else the request shall be processed normally.

**When security association is not established:**

For a field node AE, where security association is not mandatory, the Registrar CSE shall find the associated SSP at the time of registration request and shall check the SSP status.

If the SSP status is not ACTIVE then registration request shall be rejected with “INACTIVE\_SERVICE\_SUBSCRIPTION” response status code. If SSP status is ACTIVE then the registrar CSE shall maintain the mapping of AE, SSP ID and its status locally. For any other request, the Registrar CSE shall check the status of SSP using this mapping before processing the request.

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

No mixed AND/OR filter operation will be supported.CHECK LIST

* Does this Change Request include an informative introduction containing the problem(s) being solved, and a summary list of proposals.?
* Does this CR contain changes related to only one particular issue/problem?
* Have any mirror CRs been posted?
* Does this Change Request make **all** the changes necessary to address the issue or problem? E.g. A change impacting 5 tables should not include a proposal to change only 3 tables?Does this Change Request follow the drafting rules?
* Are all pictures editable?
* Have you checked the spelling and grammar?
* Have you used change bars for all modifications?
* Does the change include the current and surrounding clauses to clearly show where a change is located and to provide technical context of the proposed change? (Additions of complete clauses need not show surrounding clauses as long as the proposed clause number clearly shows where the new clause is proposed to be located.)
* Are multiple changes in this CR clearly separated by horizontal lines with embedded text such as, start of change 1, end of change 1, start of new clause, end of new clause.?