|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | SEC-28.3 |
| Source:\* | Colin Blanchard [colin.blanchard@bt.com](mailto:colin.blanchard@bt.com) |
| Date:\* | 2017-05-25 |
|  |  |
| Reason for Change/s:\* | Addition of details for the Certificate Provisioning Procedure |
| CR against: Release\* | Release 2.x |
| CR against: WI\* | Active WI-0057  MNT maintenance / < Work Item number(optional)>  Is this a companion CR? Yes  No  Companion CR number: (Note to Rapporteur - use latest agreed revision)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-003 v2.8.0 |
| Clauses \* |  |
| 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) | <TS/TR number>, <Version Number>, and <Description on which aspect should be reflected in this TS/TR> |
| 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 contribution provides the text describing Certificate Provisioning Procedure, and the details for the Certificate Provisioning Procedure using SCEP. Five functions are defined:

1. Initial configuration of the SCEP client with Provisioning Profiles
2. Device specific intelligence,
3. Client side message agent (SCEP Client in this instance),
4. Server side message responder (SCEP Responder) and
5. Locally significant Certificate Authority that establishes PKI hierarchy and issues certificates

### -----------------------Start of new clause-------------------------------------------

### 8.3.6 Certificate Provisioning Procedure Details

#### 8.3.6.1 Introduction

The Certificate Provisioning procedure includes the following actors:

* MEF Client: a Security Principal requesting provisioning of an MEF-Provisioned Certificate. The MEF Client uses the MEF-Provisioned Certificate for subsequent authentication of itself to the MEF. The Security Principal can use the MEF-Provisioned Certificate for subsequent authentication of itself in other oneM2M Security Protocols.
* MEF CA: issuing MEF-Provisioned Certificates.
* MEF: serving requests from the MEF Client, and acting as a Registration Authority (RA) to forward Certificate Signing Requests (CSRs) towards the MEF CA. The MEF can request the MEF CA to add attributes to those attributes already present in the CSR, and can request deletion or modification of attributes present in the CSR.

The Certificate Provisioning Procedure only specifies the interaction between the MEF Client and the MEF.

NOTE 1: The present specification does not describe the interaction between the MEF and MEF CA.

The Certificate Provisioning Procedure achieve the following outcomes:

* The MEF Client obtains MEF-Provisioned Certificate.
* The MEF Client obtains the MEF CA’s Certificate(s). This certificate(s) shall be used by the MEF Client for subsequent validation of certificates authenticating the MEF. This certificate(s) may be used by the Security Principal for subsequent validation of certificates authenticating other Security Principals and MAFs.

NOTE 2: Additional trust anchor CA certificates for validation of other Security Principals and MAFs can also be provisioned by configuration of MOs based on the [*trustAnchorCred*] resource.

The Certificate Provisioning Procedure comprises two procedures:

* Initial Certificate Provisioning Procedure: used when the MEF Client does not possess a valid MEF-Provisioned Certificate that was previously provisioned by the MEF.
* Certificate Re- Provisioning Procedure: used by a MEF Client to renew/rekey its existing valid MEF-Provisioned Certificate that was previously provisioned by the MEF.

This specification describes use of the following protocol for the Certificate Provisioning Procedure:

* Enrolment over Secure Transport (EST), specified in IETF RFC 7030 [59]. The use of this protocol is described in clause 8.3.6.2.
* Certificate Provisioning functions using Simple Certificate Enrolment Protocol (SCEP) [x+2]. The use of this protocol is described in clause 8.3.6.3.

### -----------------------Start of new clause-------------------------------------------

#### 8.3.6.3 Certificate Provisioning procedures using SCEP

##### 8.3.6.3.1 Introduction

The Simple Certificate Enrolment Protocol (SCEP) is specified in <https://tools.ietf.org/html/draft-nourse-scep-23> [x+2] and <https://datatracker.ietf.org/doc/draft-gutmann-scep/> [y+1]. While there are a number of existing implementations, there are no new ones in development. To document existing implementations, reference to the both the current [y+1] and version [x=2] marked as historic are given.

. When SCEP is used for Certificate Provisioning procedures, the following mapping of concepts shall be applied.

* The M2M Enrolment Function (MEF) Client acts as the SCEP Client.
* The MEF acts as the SCEP Server (also known as a SCEP Responder).
* The MEF CA acts as the SCEP CA.
* The MEF-Provisioned Certificate is equivalent to the SCEP Client Certificate.

If a MEF or MEF Client claim support of the Certificate Provisioning Procedure using SCEP, then:

NOTE 1: ].

* The MEF or MEF Client may support linking identity and Proof-of-Possession information (section 3.5 [xx]).

NOTE 2: Until widely-used cryptographic libraries are available which support this functionality, it is unlikely that this functionality would be supported by the MEF or MEF Client.

* The MEF or MEF Client shall use the HTTP-based client authentication feature of SCEP (section 3.2.3 [xx]).

NOTE 3: HTTP-based client authentication in SCEP can be used in scenarios where the MEF Client is authorized using user authentication as discussed in 2.2.3 [xx]. These scenarios have not yet been considered by the present specification. These scenarios can be supported in the future by adding support for HTTP-based client authentication.

The MEF Client shall support generation of private/public key pairs

The figures below show a high level outline of the procedures for use with Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) for determining certificate status.

The figures identify 5 distinct building blocks of any certificate automation service.

1. Profile Provisioning is the primary and authoritative actor in any automation system. Provisioning informs the *device’s automation client*, and the PKI service – the credential issuer, though the establishment of pre-authorised device credentials, that a number of unique devices will be calling home to request dedicated unique client certificate(s)
2. The provisioning capability informs both the remote device and the PKI service over an authenticated and confidential channel of their unique Provisioning Profiles. The Provisioning Profiles may be revised at any time, allowing existing credentials to be forced changed if necessary. Typical provisioning protocols include TR-069, OMA, MDM etc.
3. The *device automation client*, or certificate application intelligence provides a state machine that uses the provisioning data, a.k.a Provisioning Profiles, to generate keys and request and replace certificates at pre-determined periods in time by making requests of a native SCEP client. Typically the intelligence is time driven, ensuring timely renewal of existing keys and certificates; however it can also be event driven by the receipt of revised Provisioning Profiles from the provisioning system. The SCEP client is a native application installed on systems, servers or devices, it communicates with a SCEP responders using a protocol defined in IETF Historic draft [draft-nourse-scep-23](https://tools.ietf.org/html/draft-nourse-scep-23) [x+2]. The particular SCEP responder(s) are identified within the various Provisioning Profiles.
4. The figures identify a number of example SCEP message request response messages – these are documented within the IETF Historic draft. The SCEP responder on receipt of a chain certificate request, responds by supplying the requested certificate, on receipt of a client certificate request the SCEP responder first validates the requestor’s identity and proof of possession of a unique credential, before requesting the Issuing CA issue a new certificate, forwarding the new certificate back to the SCEP client.
5. The SCEP Responder may also reject the certificate request, or indicate issuance is pending based on an Issuing CA action. On receipt of a replacement certificate chain the *device automation client* will validate the certificate chain received including testing against either CRL or OCSP responses. Only if the new certificate chain is known to be good will the certificate chain be written to the application certificate store, over writing the previous certificate. On renewal a peer’s trust anchor(s) may also be renewed.



Figure 8.3.6.3.1-1 SCEP Provisioning Procedure Overview using Online Certificate Status Protocol (OCSP)



Figure 8.3.6.3.1-2 SCEP Provisioning Procedure Overview using Certificate Revocation List (CRL)

The SCEP certificate automation solution consists of five functions:

1. Initial configuration of the SCEP client with Provisioning Profiles
2. Device Intelligence & State Machine
3. SCEP Client
4. SCEP Responder
5. Locally Significant PKI & Certificates

##### 

##### 8.3.6.3.2 Initial configuration of the SCEP client with Provisioning Profiles

**Purpose:** Initial configuration of the SCEP client addresses the need to establish sets of context specific Provisioning Profiles within an end point device. The two obvious options for providing Provisioning Profiles are:

1 Manually configure each device, and

2 Automate provisioning from a device manager or element manager service. For example by the procedures in oneM2M TS-0022.

NOTE 4: The number of sets Provisioning Profiles must match the number of Application Security Stacks required.

**Pre-Conditions:** None

**Description of Function:**

This function downloads a set of Provisioning Profiles from the device manager or element manager service to enable the following actions:-

* A unique x509v3 cryptographic credential chaining to a trusted Root CA shall be established. allowing the end point device to subsequently bootstrap its setup
* A locally significant unique key pair shall be established
* An associated certificate signing request shall be generated
* A trust anchor shall be validated out of band by verification of a finger print within the Provisioning Profile
* Each subordinate CAs retrieved shall be validated in turn against its superior
* The request of a client certificate from a pre-authorised issuer (the SCEP responder) shall be authenticated and secured using a username and password.
* The trust anchor of a trusted peer may also be downloaded and validated. These peer trust anchors may be updated based on a revised Provisioning Profile.

##### 8.3.6.3.3 Device Intelligence & State Machine

**Purpose:** The device intelligence and state machine is the heart of any SCEP, CMPv2 or EST solution. Logically a good state machine can drive any message responder where SCEP is considered here.

**Pre-Conditions:**

The state machine is triggered by a complete and valid set of Provisioning Profiles

**Description of Function:**

This function, while intended to operate autonomously in the context of unattended IoT devices without a web browser user interface, has been written to reflect a browser based user journey. The intention is to maintain compatibility with any manual test and diagnostic processes required for IoT devices and with elements of the service that do have a traditional user interface, for example, use of a smart phone in the oneM2M Home Domain

The key steps are:

1. The device shall request its own Trust Anchor (Root CA)
2. The device’s own Trust Anchor (Root CA) shall be validated against a fingerprint provided by a Provisioning Profile.
3. The device shall request its own intermediate certificates one by one.
4. The device intermediate certificates shall be validated against the superior issuer to protect against MITMA.
5. The device shall request a first client certificate. This assumes a device has no client certificate, but is in possession of a valid set of Provisioning Profiles. (This step shall always request the issuing CA to provide confidentiality for certificate requests. The SCEP client recovers the public key for the ICA. The certificate request is encrypted with the public key so that only the CA or RA private key can decrypt the request).
6. If directed by provisioning authority, the device shall request a new certificate, or request the renewal of an existing certificate immediately ( NOTE 5: this might be against a different PKI),
7. Automated renewal of an existing certificate, based for example on a configured percentage of the current certificates lifetime has elapsed, shall also be supported.
8. All certificates shall be parsed to request associated CRLs or OCSP response.
9. The client shall request the peers Trust Anchor, if it is different from its own. Trust Anchor
10. The intermediate and issuing CA of a peer shall be requested to allow mutual authentication if required.
11. Once a new, or replacement, certificate chain has been established, the certificate chain shall be validated, as it will likely be used to replace the existing good certificate chain.
12. The key material shall be moved to the appropriate application stores.
13. The provisioning authority of current certificate shall be notified with information as required.
14. Expired certificate artefacts shall be deleted.

NOTE 6: The above list is not meant to imply a state machine order, or indicate a solution. However, it is assumed sophisticated solutions will exceed the states identified, and simpler solutions may choose to omit states not required by the device solution.

##### 8.3.6.3.4 SCEP Client

**Purpose:**

A SCEP client is typically an open source piece of software developed to perform certificate request actions against the SCEP responder. The SCEP Client is directed by the state machine described in 8.3.6.2.3 using the data provisioned as described in 8.3.6.2.2

**Pre-Conditions:**

The SCEP client should be standards compliant and can be sourced from the open source communities, if a native client doesn’t exist today. For example see <https://github.com/certnanny/sscep>. [y+2] - based on original work by Martin Bartosch.

This SCEP Client was selected because the authors have modified their SCEP client behaviour to support long chain PKI. See <https://github.com/certnanny/sscep/issues/42> [y+4]

An alternative is the JSCEP client at <https://github.com/jscep/jscep> [y+3] by Dave Grant and team, NOTE 5: This has also be modified to support long chained PKI and recently forked to specifically address Android requirements by Wes Bunton

##### 8.3.6.3.5 SCEP Responder

**Purpose:** A SCEP responder is an additional component of both Enterprise and Managed PKI services. Essentially a SCEP responder should be considered as an additional RA (Registration Authority) service.

**Pre-Conditions:**

On request the SCEP responder(s) will provide Trust Anchors, Intermediate CAs, issuing CAs and Locally Significant certificates.

A private/public key pair has been generated on the device

Requests for certificate issuance would be against a unique username and password held securely within the request SAN and challenge phrase fields of the certificate CSR (See <https://www.ietf.org/id/draft-gutmann-scep-05.txt>). [x+3]

Typically these one-time passwords expire on certificate issuance, needing to be re-set in the future when certificate renewal services are required.

The provisioning solution identified would be authoritative - tracking devices and elements under management, and would pre-provision the SCEP responder with valid username and password pairs, prior to the SCEP client using them.

Unsuccessful authentications would be rejected, and successfully authenticated CSR would be passed to the PKI for fulfilment.

Successful Authentication will return an End Entity Certificate

The provisioning solution may even request revocation of device certificates that can no longer be trusted.

##### 8.3.6.3.6 Locally Significant PKI & Certificates

**Purpose:** A PKI service provides the pre-requisite knowledge, skill and Compliance Framework to support SCEP certificate issuance. The building blocks of a SCEP solution include: PKI&CA, SCEP Responder (RA), Request Authenticator, and Request Authoriser.

**Pre-Conditions:**

It is typical in the CPE or IoT space that a PKI is designed based on a good understanding of the certificate volumes, and an understanding of the required cryptographic operational separation to be enforced.

###### 8.3.6.3.6.1 Certificate authority.

**Description of Function:**

1. A SCEP Certification Authority (CA) shall sign client certificates. The CAs name shall be stored in the issuer field of resulting certificates.
2. Before any PKI operations are invoked, the SCEP responder shall share an issuer 'CA' certificate that is compliant with the profile in [[RFC5280](https://tools.ietf.org/html/rfc5280)] [x+1] with SCEP Client and optionally dedicated RA certificates. This may be a CA certificate that was issued by a higher level CA.
3. The client shall build an entire certificate chain from the trust anchor, validating each certificate in turn.

###### 8.3.6.3.6.2 Registration Authority

**Description of Function:**

1. A SCEP Registration Authority (RA) as a SCEP Responder shall perform validation and authorisation checks of the SCEP requester.
2. A SCEP Registration Authority (RA) as a SCEP Responder shall forward the certification requests to the CA.
3. The SCEP Responder receives a certificate from the CA and forwards this to the SCEP Client.
4. The RAs name shall not appear in the issuer field of resulting certificates.

###### 8.3.6.3.6.3 Requester authentication

**Description of Function:**

1. As with every protocol that uses public-key cryptography, the association between the public keys used in the protocol and the identities with which they are associated shall be authenticated in a cryptographically secure manner. This requirement is needed to prevent a "man-in-the-middle" attack, in which an adversary can manipulate the data as it travels between the protocol participants and subvert the security of the protocol.
2. The communication between the requester and the certification authority shall be secured using SCEP Secure Message Objects which specifies how PKCS#7 is used to encrypt and sign the data of the CSR.

###### 8.3.6.3.6.4 Request Authorisation

The following SCEP authentication methods for certificate authorisation shall be supported.

1. Use of unique usernames and passwords
2. Use of unique end entity certificate and a demonstration of proof of ownership of the private key.

### -----------------------Start of Changes to References Section -------------

## 2.1 Normative references

[x+1] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC5280](https://tools.ietf.org/html/rfc5280)

[x+2] Simple Certificate Enrollment Protocol draft-nourse-scep-23 <https://tools.ietf.org/html/draft-nourse-scep-23>

[x+3] Simple Certificate Enrolment Protocol draft-gutmann-scep-05 <https://www.ietf.org/id/draft-gutmann-scep-05.txt>).

## 2.2 Informative references

[y+1]<https://datatracker.ietf.org/doc/draft-gutmann-scep/>

[y+2] <https://github.com/certnanny/sscep>

[y+3]<https://github.com/jscep/jscep>

[y+4]<https://github.com/certnanny/sscep/issues/42>

### ---End of changes to Definitions, Symbols, Abbreviations, Acronyms ---

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.?