|  |
| --- |
|  |

|  |  |
| --- | --- |
| CHANGE REQUEST | |
| Meeting ID:\* | SEC #35 |
| Source:\* | Chengfang Fang, Huawei, [fang.chengfang@huawei.com](mailto:fang.chengfang@huawei.com)  Jie Shi, Huawei, [shi.jie1@huawei.com](mailto:shi.jie1@huawei.com) |
| Date:\* | 2018-05-16 |
| Reason for Change/s:\* | Add RSPF for IBC-Based Credential to support IBC-Based SAEF |
| CR against: Release\* | Release 4 |
| CR against: WI\* | Active <WI-0066>  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\_0003 and v3.8.0 |
| Clauses \* | Clauses 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) |  |
| 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 IBC-Based Security Association Establishment Frameworks in TR-0041 is proposed to be added into TS-0003

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

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] oneM2M Drafting Rules.

NOTE: Available at <http://www.onem2m.org/images/files/oneM2M-Drafting-Rules.pdf>.

[i.2] Void.

[i.3] Void.

[i.4] oneM2M TR-0008: "Analysis of Security Solutions".

[i.5] eXtensible Access Control Markup Language (XACML) Version 3.0. 22 January 2013. OASIS Standard.

[i.6] Handbook of Applied Cryptography, A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, CRC Press, 1996.

[i.7] Recommendation ITU-T X.509 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.8] Void.

[i.9] OMA-TS-REST-NetAPI-TerminalLocation-V1-0-20130924-A: "RESTful Network API for Terminal Location", Version 1.0.

[i.10] ISO 3166-1:2013: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[i.11] ISO/IEC 7816-5: "Identification cards - Integrated circuit cards - Part 5: Registration of Application Providers".

[i.12] Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162.

NOTE: Available at <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf>.

[i.13] National Institute of Standards and Technology: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[i.14] Void.

[i.15] oneM2M TR-0019: "Dynamic Authorization for IoT".

[i.16] oneM2M TR-0012: "oneM2M End-to-End security and Group Authentication".

[i.17] oneM2M TR-0001: "Use Cases collection".

[i.18] IANA JSON Web Token (JWT) registry.

NOTE: Available at <http://www.iana.org/assignments/jwt/jwt.xhtml>.

[i.19] IETF RFC 6455: "The Web Socket Protocol", December 2011.

[i.20] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[i.21] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[i.22] GlobalPlatform Device Technology, Generic API to access Secure Elements, Open Mobila API Spêcifications, Version 3.2.

[i.23] ETSI TS 102 600: "Smart Cards; UICC – Terrminal Interface; Characteristics of the USB Interface".

[i.24] ETSI TS 102 622: "Smart Cards; UICC – Contactless Front-End (CLF) Interface; Host Controller Interface".

[i.25] IEEE P1363 “Standard Specifications for Public Key Cryptography”.

[i.26] <https://github.com/certnanny/sscep>

[i.27] <https://github.com/jscep/jscep>

[i.28] <https://github.com/certnanny/sscep/issues/42>

[i.29] oneM2M TS-0005: "[Management Enablement (OMA)](http://member.onem2m.org/Application/documentApp/documentinfo/?documentId=25523&fromList=Y)".

[i.30] oneM2M TS-0006: "[Management Enablement (BBF)](http://member.onem2m.org/Application/documentApp/documentinfo/?documentId=25523&fromList=Y)".

[i.31] IETF RFC 6507: “Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)”, February, 2012.

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

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

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in oneM2M TR-0004 [i.2] and the following abbreviations apply:

(D)TLS-PSK (D)TLS Pre-Shared Key (ciphersuites)

3GPP2 3rd Generation Partnership Project 2

AAA Authentication, Authorization and Accounting

ABAC Attribute Based Access Control

ACP AccessControlPolicy Instance

AEAD Authenticated Encryption with Associated Data

AE-ID Application Entity Identifier

App-ID Application Identifier

ASE Asymmetric Secure Element

ASN-CSE CSE which resides in the Application Service Node

AuthorSignReqInfo Authorization Signature Request Information

AuthorSign Authorization Signature

AuthorRelMapRecord Authorization Relationship Mapping Record

AuthorRelIndicator Authorization Relationship Indicator

AuthorSignIndicator Authorization Signature Indicator

BSF Bootstrapping Server Function

B-TID Bootstrapping Transaction Identifier

CA Certification Authority or Certificate Authority

CIDR Classless Inter-Domain Routing

CoAP Constrained Application Protocol

CSE-ID Common Service Entity Identifier

CSR Certificate Signing Request

DTLS Datagram Transport Layer Security (Protocol)

(D)TLS-PSK (D)TLS Pre-Shared Key (ciphersuites)

ECC Elliptic Curve Cryptography

EKU Extended Key Usage

ESCertKE End-to-End Certificate-based Key Establishment

Enrolee-ID Enrolee Identity

ESData End-to-End Security of Data

ESF End-to-End Security Function

ESPrim End-to-end Security of Primitives

EST Enrolment over Secure Transport

ETSI European Telecommunications Standards Institute

FQDN Fully Qualified Domain Name

GBA\_ME ME-based GBA

GBA\_U GBA with UICC-based enhancements

GUSS GBA User Security Settings

HLR Home Location Register

HSS Home Subscriber System

HTTP HyperText Transfer Protocol

HW Hardware

ID Identifier

IdA Identifier for entity A

IdB Identifier for entity B

IN-CSE CSE which resides in the Infrastructure Node

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

IV Initialization Vector

Kc M2M Secure Connection Key

KcID M2M Secure Connection Key Identifier

Ke Enrolment Key

KeID Enrolment Key Identifier

Ker Enrolment Re-Authentication Key

Km Master Credential

KmID Master Credential Identifier

Kpm pre-provisioned credential for Master Credential provisioning

KpmID pre-provisioned credential for Master Credential provisioning Identifier

Kpsa provisioned credential for M2M Security Association Establishment

KpsaID provisioned credential for M2M Security Association Establishment Identifier

Ks temporary Key material referred to in GBA

Ks..NAF Abbreviation of Ks\_(int/ext)\_NAF

Ks\_(ext/int)\_NAF Derived key in GBA\_ME or Derived key in GBA\_U which remains on UICC

Ks\_ext\_NAF Derived key in GBA\_U sent to the ME

Ks\_int\_NAF Derived key in GBA\_U which remains on UICC

Ks\_NAF Derived key in the ME

M2M-SP M2M Service Provider

MAF M2M Authentication Function

MAF-ID M2M Authentication Function Identifier

Mca Reference Point for M2M Communication with AE

Mcc Reference Point for M2M Communication with CSE

Mcc' Reference Point for M2M Communication with CSE of different M2M Service Provider

Mcn Reference Point for M2M Communication with NSE

MEF M2M Enrolment Function

MIC Message Integrity Code

MN-CSE CSE which resides in the Middle Node

MTE M2M Trust Enabler

NAF Network Application Function

OAEP Optimal Asymmetric Encryption Padding

OCSP Online Certificate Status Protocol

PDP Policy Decision Point

PEP Policy Enforcement Point

PII Personally Identifiable Information

PIN Personal Identification Number

PIP Policy Information Point

PKI Public Key Infrastructure

PRP Policy Retrieval Point

RA Registration Authority

RSA Rivest, Shamir and Adleman

RSAES RSA Encryption Scheme

RSASSA RSA Signature Scheme Algorithm

RSPF Remote Security Provisioning Framework

SAEF Security Association Establishment Framework

SCEP Simple Certificate Enrolment Protocol

SE Secure Environment

SUID Security Usage Identifier

SW Software

T&C Terms and Conditions

TEE Trusted Execution Environment

TEF Trust Enabling Function

TLS Transport Layer Security (Protocol)

UE (3GPP) User Equipment

UNSP Underlying Network Service Provider

URI Uniform Resource Identifier

USS User Security Settings

XACML eXtensible Access Control Markup Language

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

### -----------------------Start of change 3-------------------------------------------

## 8.3 Remote Security Provisioning Frameworks

### 8.3.1 Overview on Remote Security Provisioning Frameworks

#### 8.3.1.1 Purpose of Remote Security Provisioning Frameworks

Remote Security Provisioning Frameworks (RSPFs) provision credentials to an Enrolee, which is a Security Principal in a Node or CSE or AE, as part of the Enrolment of the Enrolee to an M2M SP or M2M Trust Enabler. The MEF provides its services on behalf of *administrating stakeholders* such as M2M SPs or third party M2M Trust Enablers (MTE). An administrating stakeholder authorizes the MEF Service Provider to provide services to MEF clients, and oversees authorizing the management of credentials.

The credentials are either:

* A symmetric key shared by the Enrolee and an Enrolment Target, which may be a MAF or Node or CSE or AE:
* If the Enrolment target is an MAF, then the credential can be used for MAF-based SAEF, MAF-based ESPrim and MAF-based ESData Protection Options, with the provisioned symmetric key used for mutual authentication of the Enrolee and the MAF.
* If the Enrolment target is a Node or CSE or AE, then the credential can be used for only one of PSK-based SAEF or PSK- based ESPrim or PSK-based ESData Protection Options. The provisioned symmetric key used for mutual authentication of the Enrolee and the other Node or CSE or AE.

NOTE: This case should be employed only in cases where the Enrolee is expected to require a symmetric key with relatively few CSE or AE.

* Certificate(s) for which the Enrolee knows the corresponding private key, and a set of trust anchors for authenticating the M2M SP or MTE's MAF or other entities enrolled with the M2M SP or MTE. These credentials can be used for:
* Securing communication directly with other Nodes or CSEs or AEs using Certificate-Based SAEF, Direct End-to-End Key Establishment using Certificates (ESCertKE), and certificate-based ESData protection options. The other Nodes or CSEs or AEs would authenticate themselves using their own certificate(s), chaining to a provisioned trust anchor CA certificate, in these security frameworks.
* MAF-based SAEF, MAF-based ESPrim, and MAF-based ESData protection options, with the certificate used for authentication of the Enrolee to the MAF. The MAF would authenticate using its own certificate chaining to a provisioned trust anchor CA certificate.
* The oneM2M specifications also support provisioning of credentials using the device configuration mechanisms specified in oneM2M TS-0022 [57], and pre-provisioning; that is, provisioning using means other than a Remote Security Provisioning Framework. The method for pre-provisioning can be deployment dependent. Interoperable frameworks enabling pre-provisioning are described in annex D for UICC and in Annex L for independent hardware based secure environments supporting asymmetric cryptography.
* IBC credentials (ID, SSK, PVT, KPAK) including: an ID which is the identity of the Enrolee, a Secret Signing Key (SSK), a corresponding Public Validation Token (PVT) and a Key Management Service (KMS) Public Authentication Key (KPAK). These credentials can be used for:
* Securing communication directly with other Nodes or CSEs or AEs using IBC-Based SAEF. The other Nodes or CSEs or AEs would derive a shared secret from their respective SSK, their respective peers’ ID and peers’ PVT together with the KPAK.

NOTE: The RSPFs are specified to provide an interoperable interface for Field Domain entities to interact with an MEF. Use of the specified RSPFs are recommended for use by Field Domain entities because they have been reviewed by the security experts of oneM2M. The RSPFs can also be used by Infrastructure Domain entities (Nodes, AEs, CSEs and MAFs) for interacting with an MEF. It is expected that the MEF may include additional “backend” interfaces, not specified by oneM2M, for coordination of information with administrating stakeholders and MAF Service Providers.

### -----------------------End of change 3---------------------------------------------

### -----------------------Start of change 4--------------------------------------------

8.3.4 Enrolment Exchange

8.3.4.1 Enrolment Exchange Procedures

The following procedures may occur within an Enrolment Exchange:

* MEF Client Registration procedures;
* Symmetric Key Provisioning procedures;
* Certificate Provisioning procedure;
* IBC-based Credential Provisioning procedures;
* Device Configuration procedures, per oneM2M TS-0022 [57] can be applied, with the MEF interacting with a DM Server and MEF Client interacting with the DM Client on the Managed Entity;
* MEF Client Command Procedures (i.e. CRUD procedures targeting at a <*mefClientCmd*> resource), which enable the MEF to control the sequence of Enrolment Exchange procedures.

The clauses below describe triggering mechanisms specific to each set of procedures. Alternatively, other mechanisms, not specified by oneM2M, can be used to trigger any Enrolment Exchange procedure, with the condition that such mechanisms provide a satisfactory level of security. Example mechanisms include pre-configuration and manual configuration.

#### 8.3.4.2 MEF Client Registration

MEF Client Registration procedures are specified in clauses 8.3.5.2.3, 8.3.5.2.4, 8.3.5.2.5, and 8.3.5.2.6.

MEF Client Registration procedures can only be performed within an Enrolment Exchange.

MEF Client Registration procedures can be triggered by the following oneM2M-specified mechanisms:

* **Procedures triggered using Device Configuration.** Device Configuration, specified in oneM2M TS-0022 [57], can trigger MEF Registration Procedures:
  + Adding a [*MEFClientRegCfg*] MO triggers the MEF Client to perform the MEF Client Registration Procedure, specified in clause 8.3.5.2.3.
  + Deleting a [*MEFClientRegCfg*] MO triggers the MEF Client to stop using the associated MEF Client registration, delete any credentials associated with that MEF Client registration and end the associated MEF Client registration on the MEF. The MEF achieves the final step by performing the MEF Client De-Registration Procedure, specified in clause 8.3.5.2.6.

#### 8.3.4.3 Symmetric Key Provisioning

Symmetric Key Provisioning procedures are specified in clauses 8.3.5.2.7, 8.3.5.2.8, 8.3.5.2.9, and 8.3.5.2.10.

These procedures can only be performed within an Enrolment Exchange.

These procedures can be triggered by the following oneM2M-specified mechanisms:

* **Procedures triggered using a “MO\_Node” MEF Client Command:** Device Provisioning (oneM2M TS-0022 [57]) can be used to configure MEF Client with an [*authenticationProfile*] MO which has a child [*MEFClientRegCfg*] MO node to instruct the MEF Client that Symmetric Key Provisioning will be used for credentials used in that [*authenticationProfile*] MO. If a MEF Client receives of an “MO\_NODE” MEF Client Command matching the path of such a [*authenticationProfile*] MO, then this can trigger a Symmetric Key Provisioning procedure according to the information elements in the MEF Client Command and the current values of the parameters in these MO nodes.

NOTE: Using Device Configuration to update or delete the [*authenticationProfile*] MO and/or its child [*MEFClientRegCfg*] MO node does not implicitly trigger a Symmetric Key Provisioning procedure. The update or delete will not take effect until a Symmetric Key Provisioning procedure is trigger by some other mechanisms.

* **Procedures triggered by an expiry of a MEF Key Registration.** If the MEF Client previously (successfully) executed an MEF Key Registration procedure under the control of an [*authenticationProfile*] MO on the MEF Client, and the current time is greater than the *expirationTime* of the [*authenticationProfile*] resource, and if the current time is close to or greater than the *expirationTime* of the most recent MEF Key Registration, then this can trigger the MEF Client to perform MEF Key Registration. The criteria for being “close to the *expirationTime*” is left up to the implementation of the MEF Client.
* **Procedures triggered by receiving,** **within a oneM2M security protocol, a symmetric key identifier whose FQDN matches the MEF's FQDN**. If a Target MEF Client receives, within a oneM2M security protocol, a symmetric key identifier whose FQDN matches the MEF's FQDN, then this can trigger the Target MEF Client to execute the MEF Key Retrieval Procedure specified in clause 8.3.5.2.8. See steps 6 and 7 in clause 8.3.5.1.

#### 8.3.4.4 Certificate Provisioning

Certificate Provisioning procedures are specified in clause 8.3.6.

These procedures can only be performed within an Enrolment Exchange.

These procedures can be triggered by the following oneM2M-specified mechanisms:

* **Procedures triggering using MEF Client Command Procedure:** If the MEF Client receives a MEF Client Command identifying a Certificate Provisioning Procedure, then this triggers the MEF Client to execute the Certificate Provisioning procedure using the information elements included in the command.

#### 8.3.4.5 IBC Credential Provisioning

IBC Credential Provisioning procedures are specified in clause 8.3.X.

These procedures can only be performed within an Enrolment Exchange.

These procedures can be triggered by the following oneM2M-specified mechanisms:

* **Procedures triggering using MEF Client Command Procedure:** If the MEF Client receives an MEF Client Command identifying an IBC Credential Provisioning Procedure, then this triggers the MEF Client to execute a IBC Credential Provisioning procedure using the information elements included in the command.

#### 8.3.4.6 Device Configuration

Device Configuration is specified in oneM2M TS-0022 [57].

Device Configuration can be performed within an Enrolment Exchange with a MEF, or in a DM session with other DM servers (separate from an Enrolment Exchange). Clause 8.3.8 specifies use of Device Configuration within an Enrolment Exchange with a MEF.

Device Configuration can be triggered by the following oneM2M-specified mechanisms:

* **Procedures triggered using MEF Client Command Procedure**: If the MEF Client receives a MEF Client Command identifying the Device Configuration Procedure, then this trigger the MEF Client to execute a Device Configuration session using the information elements included in the command.

#### 8.3.4.7 MEF Client Command

MEF Client Command procedures are specified in clause 8.3.9.

MEF Client Command procedures can only be performed within an Enrolment Exchange.

MEF Client Command procedures can be triggered by the following oneM2M-specified mechanisms:

* **Procedures triggered following MEF Client Registration Procedure**
  + A MEF Client Command Retrieve shall be executed following an MEF Client Registration procedure (other than MEF Client De-registration).
* **Procedures triggered according to *retryDuration***
  + When the MEF issues a NO\_MORE\_COMMANDS MEF Client Command, then the *cmdArgs* includes a *retryDuration* providing the duration after which the MEF Client attempts MEF Client Command Retrieve. A *retryDuration* is cancelled whenever the MEF Client successfully interacts with the MEF prior to this time. For further details see clause.8.3.9.6.
* **Procedures triggered following an attempt to perform an issued MEF Client Command**
  + If the MEF Client has attempted executing a previously issued MEF Client Command, then the MEF Client shall perform the MEF Client Command Update procedure to report on the status of that execution. The MEF can issue a MEF Client Command in the response.

An Example of a MEF Client Command procedure is illustrated in figure 8.3.4.6-1.



**Figure 8.3.4.**6**-1:** Example MEF Client Command procedure

1. The MEF client sends an MEF Client Registration request.
2. The MEF creates a <*mefClientReg*> resource.
3. If the MEF wants to issue a MEF Client Command it creates a <*mefClientCmd*> resource as child of the <mefClientReg> resource
4. The MEF sends the MEF Client Registration response which includes a representation of the <*mefClientReg*> resource, including the *childResource* reference, whose value represents the resource ID of a <*mefClientCmd*> resource.
5. The presence of the *childResource* reference triggers the MEF client to retrieve the <*mefClientCmd*> resource. The MEF Client sends a MEF Client Command Retrieve request to the MEF
6. The MEF forms the response.
7. The MEF returns a MEF Client Command Retrieve response which includes the <*mefClientCmd*> resource.
8. The MEF client parses the received response and executes the command included therein.
9. After execution of the command, the MEF client reports the result to the MEF by a MEF Client Command Update Request
10. The MEF updates the <*mefClientCmd*>. If the MEF has a new command for the MEF Client it indicates a trigger in the representation of the <*mefClientCmd*> resource.
11. The MEF sends the MEF Client Command Update Response. If the received response includes another MEF Client Command, steps 8 to 11 are repeated.

### -----------------------End of change 4---------------------------------------------

### -----------------------Start of change 5-------------------------------------------

8.3.X IBC Credential Provisioning Procedure Details

8.3.X.1 Introduction

Clause 8.3.X describes the details of the IBC Credential Provisioning Procedures.

The IBC Credential Provisioning procedures include the following actors:

* MEF Client: requesting provisioning of an IBC credential. The MEF Client can use the provisioned IBC credential for subsequent authentication of itself to the MEF.
* KMS: issuing IBC credential. The KMS is configured with master public key and master private key. The KMS accepts an entity’s identity and generates a corresponding IBC private key[i.31].
* MEF: serving requests from the MEF Client, and forwarding IBC credentials generation requests towards the KMS.

8.3.X.2 Initial IBC Credential Provisioning procedure

**Purpose:** Enabling an MEF Client to request its first IBC credential from the MEF.

**Pre-Conditions:**

1. The MEF Client is provided with the IBCBasedURI whose FQDN shall match the FQDN of the MEF, and is triggered to perform an IBC Credential Provisioning procedure.
2. The MEF Client and MEF have successfully performed a MEF Handshake and the MEF has established an authenticated identity for the MEF Client. For the Initial IBC Credential Provisioning procedure, one of the following RSPFs shall be used.
3. PPSK-Based RSPF as described in clause 8.3.2.1.
4. Certificate-Based RSPF as described in clause 8.3.2.2.

**Procedure Description:**

1. The MEF Client shall send a request with its identity *ID* (CSE-ID or AE-ID) to the MEF;
2. The MEF shall generate a new *ID\_2* for the enrolee based on the FQDN, the received identity *ID* and the expiration time *expirationTime* for this IBC credential (i.e. *ID\_2* = FQDN@hexBinary(*ID*)@*expirationTime*);

NOTE 1: hexBinary(*ID*) denotes the hexadecimal representation of the binary value of the received identity *ID*. The generated *ID\_2* shall be unique.

NOTE 2: The MEF forwards the *ID\_2* to the Key Management Service (KMS). The KMS generates a private key SSK and a Public Validation Token (PVT) for the received *ID\_2* with the master public KPAK and the master secret key KSAK[i.31]; and sends the SSK, PVT and KPAK back to the MEF.

1. The MEF shall send {*ID\_2*, SSK, PVT, KPAK} to the MEF Client.

8.3.X.3 IBC Credential Re-Provisioning procedure

**Purpose:** Enabling an MEF Client to renew/rekey a currently valid Enrolled IBC credential.

**Pre-Conditions:**

1. The MEF Client has previously performed the Initial IBC Credential Provisioning procedure or IBC Credential Re-Provisioning Procedure with the MEF, and the MEF Client has installed its IBC credential from the most recent such procedure.
2. The MEF Client is provided with the IBCBasedURI whose FQDN shall match the FQDN of the MEF, and is triggered to perform IBC Credential Provisioning procedure.
3. The MEF Client and MEF have successfully performed a MEF Handshake and the MEF has established an authenticated identity for the MEF Client. As in pre-condition B of clause 8.3.X.2.

**Procedure Description:**

1. The MEF Client shall send a request with its *ID\_1* = FQDN@hexBinary(*originalID*)@*expirationTime* to the MEF;
2. The MEF shall generate a new *ID\_2* for the enrolee based on the FQDN, the MEF Client’s identity *originalID* (CSE-ID or AE-ID) and the new expiration time *newExpirationTime* (i.e. *ID\_2* = FQDN@hexBinary(*originalID*)@*newExpirationTime*);

NOTE 3: hexBinary(*originalID*) denotes the hexadecimal representation of the binary value of *originalID*; The generated *ID\_2* shall be unique.

NOTE 4: The MEF forwards the new *ID\_2* to the KMS. The KMS generates corresponding SSK and PVT, and sends the SSK, PVT and KPAK back to the MEF. As in NOTE 2 of clause 8.3.X.2.

1. The MEF shall send {ID\_2, SSK, PVT, KPAK} to the MEF Client.

### -----------------------End of change 5---------------------------------------------

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.?