|  |
| --- |
| Input Contribution |
| Meeting ID\* | SEC#27  |
| Title:\* | Input on “Authentication” procedure for the Security Developer’s Guide TR-0038 |
| Source:\* | Wolfgang Granzow, Qualcomm, wgranzow@qti.qualcomm.comPhil Hawkes, Qualcomm, phawkes@qti.qualcomm.com |
| Uploaded Date:\* | 2017-02-05 |
| Document(s) Impacted\* | TR-0038v0\_0\_1 |
| Intended purpose ofdocument:\* | [x]  Decision[x]  Discussion[ ]  Information[ ]  Other <specify> |
| Decision requested or recommendation:\* | Include the text proposed in this contribution into TR-0035 .  |
| Template Version:23 February 2015 (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.

**Introduction**

This contribution proposes text for Clause 7.1 “Authentication” of TR-0038.

In order to cover all specified Security Association Establishment Frameworks it is proposed to describe one example each for:

* Provisioned Symmetric Key SAE (between door locks and Home Gateway)
* Pre-provisioned Certificate Based SAE (between Home Gateway and IN-CSE)
* MAF Based Symmetric Key SAEF (between the smartphone and IN-CSE)

Use cases for the Remote Security Provisioning Frameworks can be added at a later stage to clause 7.

*======== Text proposed for TR-0038 starts here =============================*

# 7 Procedures and call flows

## 7.1 Security Association Establishment

### 7.1.1 General

M2M services are offered by CSEs to AEs and/or other CSEs. To be able to use M2M services offered by one CSE, the AEs and/or CSEs need to be mutually identified and authenticated by that CSE, in order to provide protection from unauthorized access and Denial of Service attacks.

This mutual authentication enables to additionally provide encryption and integrity protection for the exchange of messages across a single Mca, Mcc or Mcc' reference point. In addition, communicating AEs that require similar protection for their own information exchanges can be provisioned to apply the same security method to their communications. This is the purpose of the Security Association Establishment (SAE) procedure.

When CoAP binding of oneM2M primitives is used, i.e. the Underlying Network communication uses UDP/IP transport, Authentication is performed by means of a DTLS Handshake.

When HTTP, MQTT or WebSocket binding of oneM2M primitives is used, i.e. the Underlying Network communication uses TCP/IP transport, Authentication is performed by means of a TLS Handshake.

For the use cases in this guideline document it is assumed that HTTP binding is employed between all applicable pairs of entities (see also TR-0025 [xx])

In order to exemplify the use of all three Security Association Establishment Frameworks (SAEF) defined in TS-0003 the following use cases are described:

* Provisioned Symmetric Key SAE between Door Locks and Home Gateway,
* Pre-provisioned Certificate Based SAE between Home Gateway and IN-CSE,
* MAF Based Symmetric Key SAEF between the smartphone and IN-CSE.

Communication between the MN-AE and MN-CSE internally to the Home Gateway is assumed to not require Security Association Establishment.

### 7.1.2 Provisioned Symmetric Key SAE between the Locks and the Home Gateway

In this example it is assumed that authentication between the Locks (ADN-AE1 and ADN-AE2) and the Home Gateway (MN-CSE) is performed using provisioned keys (Kpsa) and key identifiers (KpsaID).

**Configuration of ADN-AE1 and ADN-AE2:**

The AEs are configured with the set of allowed TLS ciphersuites when using TLS-PSK as defined in clause 10.2.2 of TS-0003 [x]. The set of ciphersuites includes TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA256.

The AE is assumed to be configured with the CSE-ID of the Home Gateway which is a unique identifier within the M2M-SPs domain. The CSE-ID value is assumed as mn-cse-123456.

The AE is assumed to be configured with a pair of credentials (psk, psk\_identity) associated with the CSE-ID. An example of credential configuration is given in Table 7.1.2-1. The length of the keys Kpsa is not mandated by TS-0003 [x] and left to implementation. In this example the key length of 8 bytes (64 bits) is chosen. The key identifiers comply with the format specified in clause 10.5 of TS-0003 [x].

Table 7.1.2-1: Example Credentials configured on ADN-AE1 and ADN-AE2

|  |  |  |
| --- | --- | --- |
| **Entity** | **Kpsa (hex format)** | **KpsaID** |
| ADN-AE1 | 1a2b3c4d5e6f7a8b | AE123456789012-Lock@in.provider.com |
| ADN-AE2 | 12345678abcdefab | AE123456789015-Lock@in.provider.com |

**Configuration of MN-CSE (Home Gateway):**

The MN-CSE is configured with the set of allowed TLS ciphersuites when using TLS-PSK as defined in clause 10.2.2 of TS-0003 [x]. The set of ciphersuites includes TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA256.

The MN-CSE is assumed to have a psk-lookup-table with columns for (client identity, psk, psk\_identity), such that when a TLS client provides a particular psk\_identity, then the MN-CSE uses the corresponding psk for establishing a TLS session, and the client identity is associated with the established TLS session. This needs to be integrated to the TLS server. Table 7.1.2-2 shows an example of credentials configured on the Home Gateway to serve ADN-AE1 and ADN-AE2, containing AE-ID, KpsaID, Kpsa. A new row would need to be added to this table for each additional AE allowed to register to the MN-CSE by using TLS\_PSK. .

*Editor’s note: We have noted that e.g. OpenSSL does not provide a psk-lookup-table, but does indicate a spot in the source code where a psk-lookup could be implemented. The psk-look-up-table values could be provided in a configuration file.*

Table 7.1.2-1: Credentials configured on MN-CSE

|  |  |  |
| --- | --- | --- |
| **AE-ID** | **Kpsa (hex format)** | **KpsaID** |
| Clock-AE1 | 1a2b3c4d5e6f7a8b | AE123456789012-Lock@in.provider.com |
| Cllock-AE2 | 12345678abcdefab | AE123456789015-Lock@in.provider.com |

**Operation of ADN-AE1 and ADN-AE2**

When the AE is triggered to establish a TLS-PSK session with the MN-CSE using some pair (Kpsa, KpsaID), the following should occur automatically based on the AE’s configuration:

AE’s TLS Client is triggered to perform a TLS-PSK handshake with the TLS values (psk, psk\_identity) set to the values of (Kpsa, KpsaID), and with the configured list of TLS ciphersuites.

On completion of the TLS handshake, the AE associates the established TLS session with the MN-CSE’s CSE-ID.

**Operation of MN-CSE**

The MN-CSE’ TLS Server is listening on the TLS Server port and the following should occur automatically based on the MN-CSE’s configuration:

A TLS handshake is started at the MN-CSE TLS Server on receiving a TLS handshake Client\_Hello message. In the case of the AE, this includes the list of TLS-PSK ciphersuites supported by the AE for use with the MN-CSE. The MN-CSE will select a ciphersuite that is also in its configured list.

A later TLS handshake message will include the psk\_identity element set to KpsaID.

The MN-CSE’s TLS Server looks up the psk-lookup-table using KpsaID as an index, and retrieves the AE’s AE-ID, Kpsa). If AE-ID is not available, then the MN-CSE may query the node’s <serviceSubscribedAppRule> resource

The MN-CSE’s TLS client continues the TLS handshake with the TLS value psk set to the value of Kpsa.

On completion of the TLS handshake, the MN-CSE associates the established TLS session with the AE’s AE-ID.

*Editor’s note: A detailed description of the TLS handshake procedures will be added into an Annex in a future revision of this document.*

### 7.1.3 Certificate-based SAE between Home Gateway and IN-CSE

<Text>

### 7.1.4 MAF-based SAE between Smartphone and IN-CSE

<Text>

### 7.1.5 Registration upon successful SAE

*Editor’s note: this clause will provide an example of the registration procedure following successful Security Association Establishment. This procedure is independent of the SAE procedures described in clauses 7.1.2 to 7.1.4. It will also include an example of AE impersonation checking procedure*.

## 7.2 Authorisation

<Text>

## 7.3 Secure communications

<Text>