- The entity's Certificate (and if applicable, Certificate Chain) as described in clause 10.1.1 “Certificate Profiles”.
- In the case of a CSE-ID certificate the entity shall be configured with the entity’s CSE-ID.
- In the case of an AE-ID certificate the entity shall be configured with the entity’s AE-ID.

8.1.1.2.4 Information Needed for Certificate Authentication of another Entity

An entity must trust the following information in order to authenticate another entity using certificates:

- An indication of the public key certificate flavour of other entity’s Certificate (that is, raw public key certificate, device certificate, CSE-ID certificate, AE-ID certificate, or an MEF certificate).
- In the case where other entity’s certificate is a raw public key certificate:
    - A public key identifier for the raw public key in the certificate (see clause 10.1.2 “Public Key Identifiers”). The public key identifier can be available
- In the case where other entity’s certificate is an device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate:
    - **A Globally unique identifier:** The globally unique identifier for the entity which is also present in the subjectAltName extension of the other entity’s certificate
        - Device Certificate: A globally unique hardware instance identifier (such as the object identifier M2M Device ID in Annex H “Object Identifier Based M2M Device Identifier” TS-0001 [1]) that is present in the device certificate.
        - CSE-ID Certificate: The full URI representation of the CSE-ID
        - AE-ID Certificate: The full URI representation of the AE-ID
        - FQDN Certificate: The FQDN of the MEF or MAF
    - **Trust Anchor Certificates:** One or more trust anchor certificates for the other entity’s certificate chain (see clause 8.1.1.2.2 “Path Validation and Certificate Status Verification”)

8.1.1.2.5 Certificate Verification

This clause describes how an entity authenticates the other entity in the Security Handshake of a Certificate-Based Security Framework.

The other entity's Certificate is received during the Security Handshake.

The other entity's Certificate is verified as follows:

- If the certificate information configured during the Association Configuration or Bootstrap Instruction Configuration indicates that the other entity's Certificate is a raw public key certificate, then the entity verifies that the public key identifier (received during Association Configuration or Bootstrap Instruction Configuration) corresponds matches the raw public key certificate (received during the Security Handshake) using the process described in clause 10.1.2 “Public Key Identifiers”.
- If the certificate information configured during the Association Configuration or Bootstrap Instruction Configuration indicates that the other entity's Certificate is a device certificate, CSE-ID certificate, AE-ID certificate or FQDN certificate, then the entity shall perform the following verifications:
    - The entity shall look for a match between the globally unique identifier described in clause 8.1.1.2.4 “Information Needed for Certificate Authentication of another Entity” (received during Association Configuration or Bootstrap Instruction Configuration) and the values in the subjectAltName extension of the other entity's Certificate (received during the Security Handshake). If there is not an exact match, then the entity shall abort the (D)TLS handshake.
        - In the case of device certificate, the globally unique identifier is a globally unique hardware instance identifier (such as the object identifier M2M Device ID in Annex H “Object Identifier Based M2M

© OneM2MPartners

Device Identifier" TS-0001 [1]). In this case, the notion of a "match" depends on how the globally unique hardware instance identifier can be represented in the subjectAltName extension.

  - In the case of a CSE-ID certificate, the globally unique identifier is the CSE-ID, and a match is a URI that is an exact match for the CSE-ID.
  - In the case of an AE-ID certificate, the globally unique identifier is the AE-ID, and a match is a URI that is an exact match for the AE-ID.
  - In the case of an FQDN certificate, the globally unique identifier is the FDQN of the M2M Authentication Function or M2M Enrolment Function, and a match is a URI, FQDN or dNSName that is an exact match for the FDQN of the M2M Authentication Function or M2M Enrolment Function.

- The entity shall perform path validation and certificate status verification using the trust anchor certificate as described in clause 8.1.1.2.2 "Path Validation and Certificate Status Verification"). If this verification fails, then the entity shall abort the (D)TLS handshake.

NOTE: After a successful Security Handshake in which the other entity provides a Certificate Chain, the other entity's identity (received during Association Configuration or Bootstrap Instruction Configuration) can be associated with additional information extracted from the other entity's Certificate Chain (e.g. the other entity Manufacturer, other entity owner, or conformance criteria). These details are not described in the present document.

8.1.2 General Introduction to the Centralized Security Frameworks

A Centralized Security Framework relies on a Central Key Distribution Server in charge of establishing a symmetric key that will be shared between two entities. This framework could be used either in the scope of Security Association Establishment or in the scope of Remote security provisioning. The type of the server playing the role of the Central Key Distribution Server depends on the scope. In case of Remote security provisioning, the Centralized Key Distribution Server is the MEF. In case of Security Association Establishment, the Central Key Distribution Server can be the M2M Authentication Function (MAF) or the Bootstrapping Server Function (BSF). The BSF is an element of GBA framework.

Generic Bootstrapping Architecture (GBA), described below, is a framework that could be used as Centralized Security Frameworks either for Security Association Establishment or Remote security provisioning.

8.1.2.1 General Introduction to the GBA (Generic Bootstrapping Architecture) Framework

In case of scenario where the M2M Service Provider and the operator of the underlying network have an agreement to use the underlying network credentials as the basis for security between a M2M Application Service/Middle Node and Infrastructure Node (including the case that the M2M Service Provider and the operator of an underlying network are actually the same entity), GBA procedure could be used.

It is important that this feature is used only within the scope of an appropriate agreement between the M2M Service Provider and the operator of the underlying network. The normative text for the GBA-Based Security Association Establishment Framework (clause 8.2.2.2) and the GBA-Based Security Bootstrap Framework (clause 8.3.2.2) implicitly assumes that such an agreement is already in place. Since the present document is a technical specification, it does not address the details of such an agreement.

A general introduction to GBA is included in TR-0008 [i.6].

After a successful GBA bootstrapping, the M2M Application Service/Middle Node and the BSF share a security association which consists of a bootstrapping transaction identifier (B-TID) and key material (GBA bootstrap Ks).

This security association may be used by the M2M Application Service/Middle Node to derive NAF keys (Ks_(ext/int)_NAF) shared between a M2M Application Service/Middle Node and a M2M Infrastructure Node or an M2M Authentication Function.

There are two modes of GBA: ME-based GBA (GBA_ME) and UICC-based GBA (GBA_U). In case of GBA_ME, one NAF-specific key is derived: the key Ks_NAF. In case of GBA_U, two NAF-specific keys are derived: Ks_ext_NAF (available in the ME) and Ks_int_NAF (which remains inside the UICC).

© OneM2MPartners

GBA_U requires that the UICC is GBA aware.

The BSF determines which mode to run based on the UICC capability indicated in the GBA User Security Settings (GUSS).

The usage of GBA_U is recommended since it provides a higher level of security than GBA_ME. The implication of this recommendation is that the entity, AE or CSE, using the GBA_U-based NAF keys should be resident in the UICC.

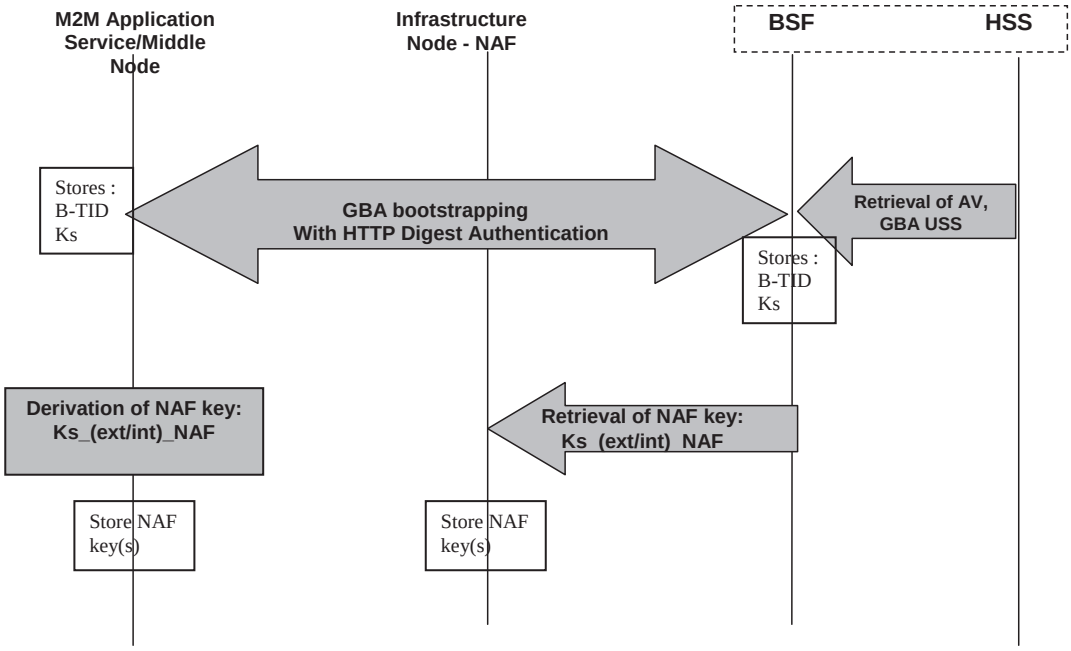


Figure 8.1.2.2-1: GBA framework. Note that the Network application Function (NAF) may be an Infrastructure Node or an M2M Authentication Function

8.2 Security Association Establishment Frameworks

8.2.1 Overview on Security Association Establishment Frameworks

In the present document, security associations are restricted to single hop on Mcc, Mcc' or Mca reference point.

The oneM2M system supports the following Security Association Establishment Frameworks:

- **Direct Security Association Establishment Frameworks:**
  - **Provisioned M2M Secure Connection Key** Security Association Establishment. A symmetric key is pre-provisioned to the entities: this is called the Provisioned M2M Secure Connection Key, and denoted Kpsa. The entities authenticate each other by verifying Message Integrity Codes (MIC) in the Security Handshake which were generated using the symmetric key. For more details see clause 8.2.2.1.
  - **Certificate-Based** Security Association Establishment: The entities are each issued with
    - a Private Signing Key that is known only to that entity,
    - a Certificate containing the corresponding Public Verification Key, and

© OneM2MPartners

    - (Optionally) a Certificate Chain from the entity's Certificate to a Root Certificate.

      The entities must validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, entity A creates a digital signature of the session parameters using its private signing key and entity B verifies the digital signature using entity A's public verification key. Then the roles are reversed: entity B creates a digital signature and entity A verifies it. For more details see clause 8.2.2.2.

- **Centralized Security Association Establishment Frameworks:** In such schemes, entity A and a Central Key Distribution Server authenticate each other and derive a M2M Secure Connection key (Kc) that the Central Key Distribution Server delivers to entity B. The entities then authenticate each other using the M2M Secure Connection key (Kc). The oneM2M authentication Frameworks using centralized key distribution are:

  - **GBA based Security Association Establishment**. This Security Association Establishment Framework uses 3GPP or 3GPP2 symmetric keys to authenticate entity A and the Central Key Distribution Server. The details are specified by 3GPP [13] and 3GPP2 [14]. For more details see clause 8.2.3.2.

  - **M2M Authentication Function (MAF)-based Security Association Establishment**. This Security Association Establishment Framework uses symmetric keys to authenticate the entity A and the Central Key Distribution Server. For more details see clause 8.2.3.1.

For a more detailed description of the above Security Association Establishment Frameworks, it is useful to compare the following aspects of the Security Association Establishment Frameworks:

- **Credential Configuration:**

  - For Central Key Distribution Security Association Establishment Frameworks:

    - Entity A is configured with (or otherwise establishes) the Master Credential (Km) that the entity A will use to authenticate the entity A to the Central Key Distribution Server.

    - The Central Key Distribution Server is configured with the Master Credential (Km) that will be used to authenticate the Central Key Distribution Server to entity A.

    The details for the GBA-Based Security Association Establishment Framework are out of scope.

  - For the Provisioned M2M Secure Connection Key Security Association Establishment Framework, each entity is provisioned with the Pre-Provisioned M2M Secure Connection Key that entities will use to authenticate each other using pre-provisioning or remote provisioning.

  - For the Certificate-Based Security Association Establishment Frameworks, each entity is pre-provisioned with the Credential that the entity will use to authenticate itself to the other entity.

- **Association Configuration:** Configuration of entity identifiers (that is, CSE-ID or AE-ID) for the entities to be authenticated.

  Additionally, in the case of Certificate-Based Authentication Framework: each entity is configured with the Certificate Name and Root of Trust that the entity will use to verify the other entity.

- **Association Security Handshake:** Identification, authentication and security context establishment between the entities.

  - **Central Key Distribution Server Handshake**: When a Centralized Security Association Establishment Framework is used, entity A and the Central Key Distribution Server (MAF or GBA-BSF) perform mutual authentication and generate a M2M Secure Connection Key (Kc) which is then used in the Security Handshake for mutual authentication between entity A and entity B. This is not applicable to Direct Security Association Establishment Frameworks.

Figure 8.2.1-1 provides a summary of the above defined four Security Association Establishment Frameworks.

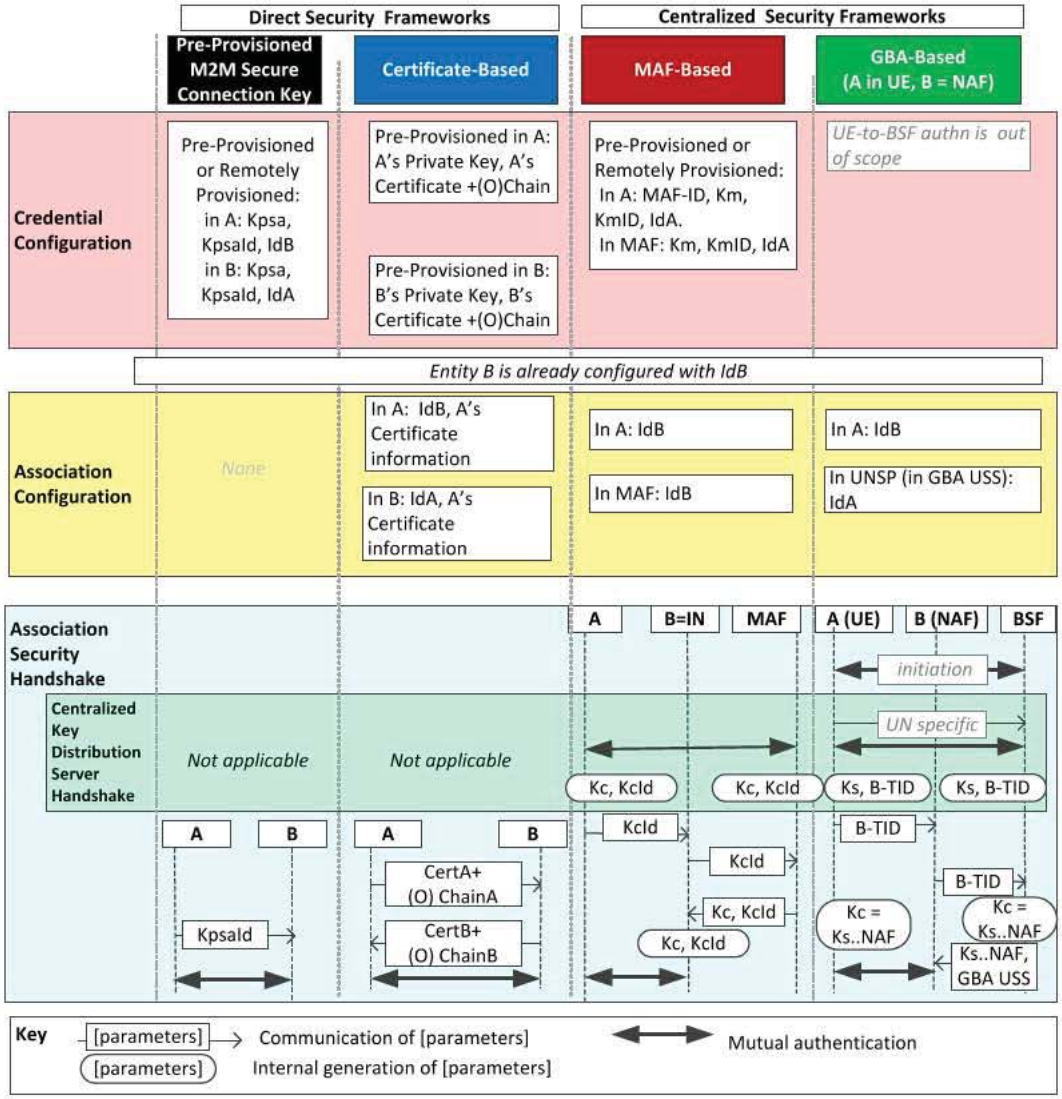


Figure 8.2.1-1: Overview of the Security Association Establishment Frameworks supported by oneM2M.

8.2.2 Direct Security Association Establishment Frameworks

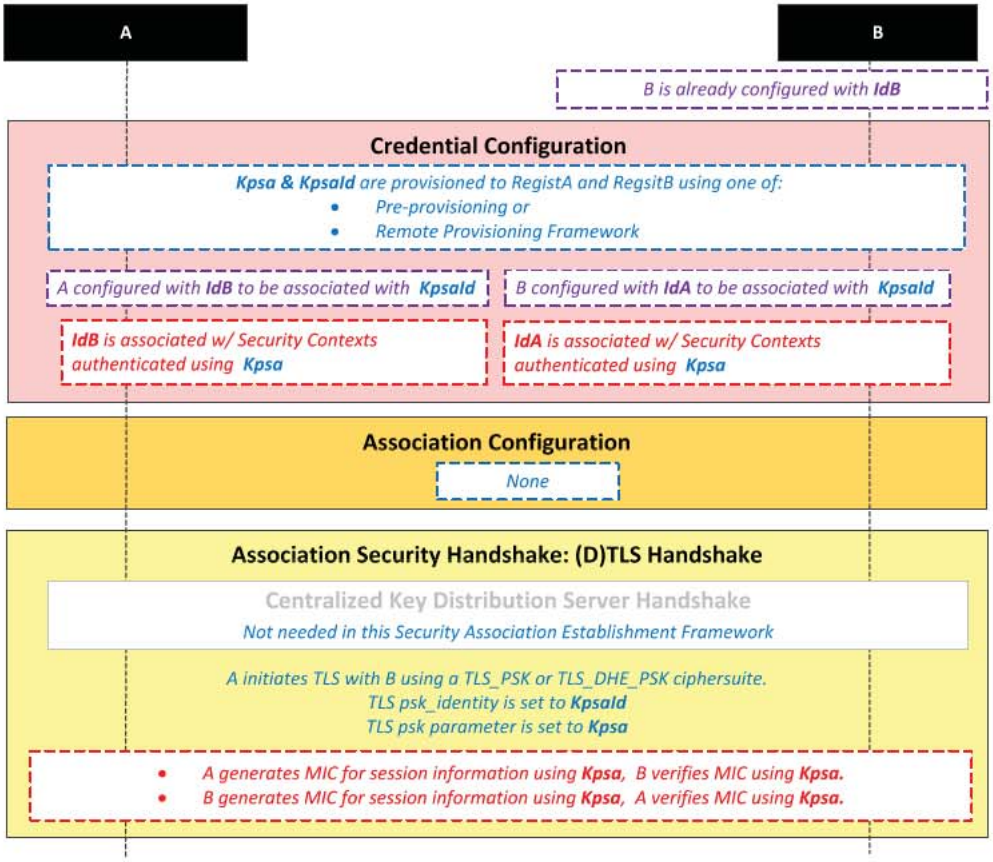
8.2.2.1 Provisioned Symmetric Key Security Association Establishment Frameworks

This clause describes the Provisioned Secure Connection Key Security Association Establishment Framework. This framework enables mutual authentication of two entities corresponding to either two CSEs or a CSE and an AE. The Credential for this framework is a long-term symmetric key that has been provisioned into the entities to be authenticated. This key is called a Provisioned Secure Connection Key and is denoted Kpsa. The provisioning of Kpsa could be a pre-provisioning or a remote provisioning thanks to Remote Security Provisioning Frameworks, as described in clause 8.3. The entities authenticate each other by verifying message authentication codes in the Security Handshake which were generated using the Provisioned Secure Connection Key.

NOTE: Long term Provisioned Secure Connection Keys can pose a security risk if not adequately secured, and for this reason long term Provisioned Secure Connection Keys are recommended to be stored in Secure Environments.

© OneM2MPartners

Figure 8.2.2.1-1 illustrates the sequence of events when using the Provisioned Secure Connection Key Security Association Establishment Framework. In this description, "Entity A" and "Entity B" correspond to either two CSEs or a CSE and an AE or an AE and a CSE (respectively).



NOTE: The following font colours differentiate the general topic that the text relates to:
Blue italic text highlights details specific to this particular Security Association Establishment Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.
Red italic text highlights security-related properties.

Figure 8.2.2.1-1: The sequence of events when using the Pre-Provisioned Secure Connection Key Security Association Establishment Framework

Credential Configuration: The Provisioned Secure Connection Key (Kpsa) and the corresponding Provisioned Secure Connection Key Identifier, denoted KpsaId, are provisioned to both entities either with pre-provisioning or remote provisioning.

NOTE 1: The provisioning (by definition) uses mechanisms not specified by oneM2M. The remote provisioning is performed thanks to Security Bootstrap Frameworks described in clause 8.3.

Additionally:

Entity A is configured with Entity B identity (IdB). Entity A is to use this identity for Entity B authenticating using the above arguments. This identity is also used to route the (D)TLS exchange.

NOTE 2: Entity A will associate Entity B's identity with messages secured within Security Contexts established using the Provisioned Secure Connection Key Kpsa associated with the Provisioned Secure Connection Key Identifier KpsaId.

- Entity B is configured Entity A identity (IdA). Entity B is to use this identity for Entity A authenticating using the above arguments.

© OneM2MPartners

NOTE 3: Entity B will associate the configured Entity A identity with messages secured within Security Contexts established using the Provisioned Secure Connection Key Kpsa associated with the Provisioned Secure Connection Key Identifier KpsaId.

Association Configuration: Each entity is configured with the information needed for mutual authentication and identification:

Association Security Handshake: The entities perform a (D)TLS-PSK handshake [15] to establish a secure session.

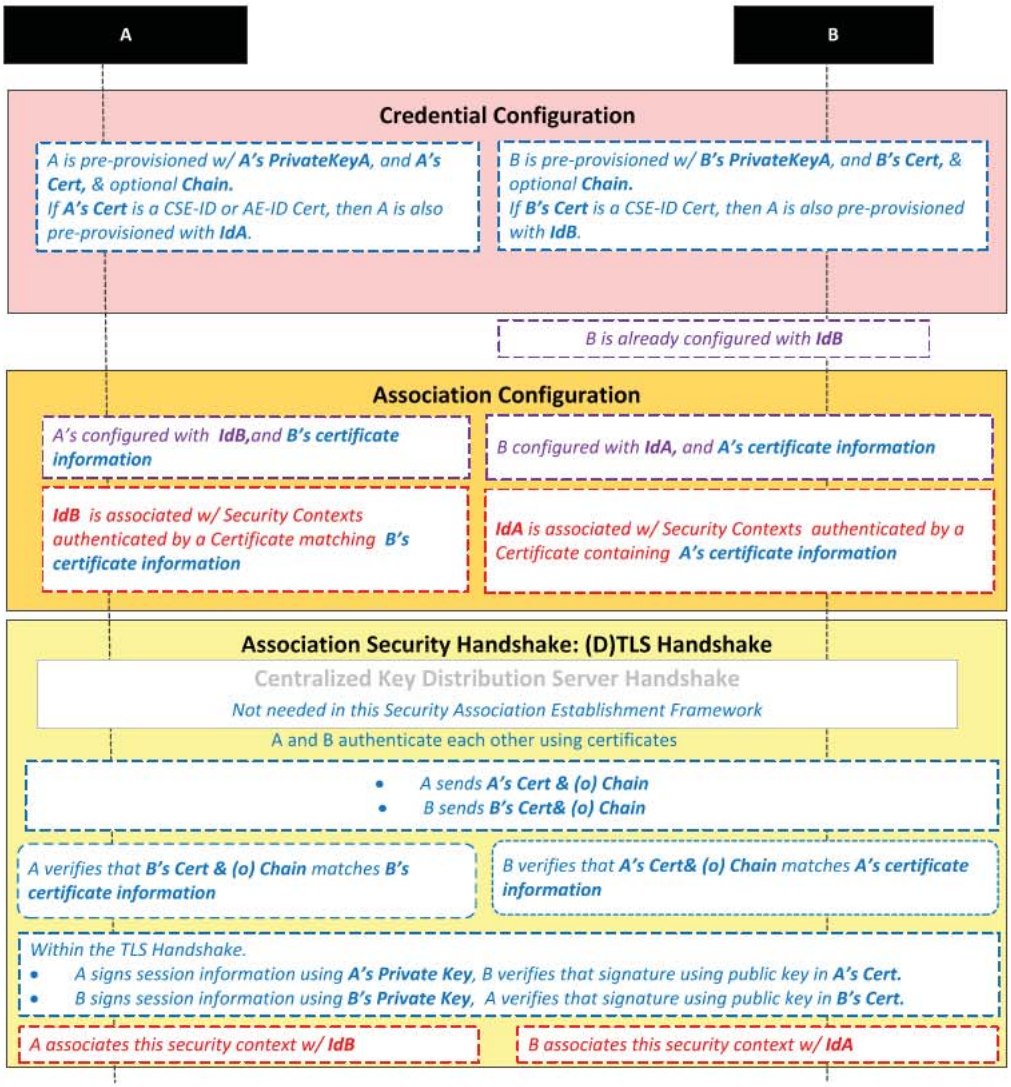
- Centralized Key Distribution Server Handshake: There is no Centralized Key Distribution Server Handshake applied in the Provisioned Secure Connection Key Security Association Establishment Framework.
- The "psk_identity" parameter [15] is set to the value of the Provisioned Secure Connection Key Identifier KpsaId.
- The "psk" parameter [15] is set to the value of the Provisioned Secure Connection Key Kpsa.
- The (D)TLS cipher suite profile for the Provisioned Secure Connection Key Security Association Establishment Framework is specified in clause 10.2.2.

8.2.2.2 Certificate-Based Security Association Establishment Frameworks

This clause describes the Certificate-Based Security Association Establishment Framework.

Figure 8.2.2.2-1 illustrates the sequence of events when using the Certificate-Based Security Association Establishment Framework. In this description, "Entity A" and "Entity B" correspond to either two CSEs or a CSE and an AE.

© OneM2MPartners



NOTE: The following font colours differentiate the general topic that the text relates to:
Blue italic text highlights details specific to this particular Security Association Establishment Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.
Red italic text highlights security-related properties.

Figure 8.2.2.2-1: The sequence of events when using the Certificate-Based Security Association Establishment Framework

Credential Configuration: The private keys and certificates for each entity are pre-provisioned as described in clause 8.1.1.2.1 "Credential Configuration for Certificate-Based Security Frameworks".

Association Configuration: Entity A and Entity B are configured with the information needed for the authentication and identification (during Security Handshake) of Entity B and Entity A respectively:

- Entity A is commanded to initiate a Security Handshake, and the command includes the following arguments:
  - Entity B's certificate information: as described in clause 8.1.1.2.4 "Information Needed for Certificate Authentication of another Entity"
  - Entity B's identity (IdB). Entity A is to use this identity for Entity B authenticating using the above arguments. This is used to route the (D)TLS exchange.

© OneM2MPartners

NOTE 1: The Entity A will associate Entity B's identity with messages secured within Security Contexts established in accordance with the configured Entity B‘s certificate information.

- The Entity B is configured with the following arguments describing Entity A authorized to perform Security Handshake with Entity B:
    - o Entity A’s certificate information: as described in clause 8.1.1.2.4 “Information Needed for Certificate Authentication of another Entity”.
    - Entity A’s identity (IdA). Entity B is to use this entity identity for Entity A authenticating using the above arguments.

NOTE 2: Entity B will associate Entity A's identity with messages secured within Security Contexts established in accordance with the configured Entity A‘s certificate information.

Association Security Handshake:

- **Centralized Key Distribution Server Handshake:** There is no Centralized Key Distribution Server Handshake applied in the Certificate-Based Security Association Establishment Framework.
- Each entity verifies the other entity's certificate as described in clause 8.1.1.2.2 "Certificate Verification".
- The entities authenticate each other using the validated certificates as specified in TLS 1.2 RFC 5246 [16] and DTLS 1.2 RFC 6347 [17] specifications.
- The (D)TLS cipher suite profile for the Certificate-Based Security Association Establishment Framework is specified in clause 10.2.3.

8.2.3 Centralized Security Association Establishment Frameworks

8.2.3.1 MAF-Based Symmetric Key Security Association Establishment Frameworks

This clause describes the MAF-based Security Association Establishment Framework.

This release addresses the scenario where the Entity B is an Infrastructure Node.

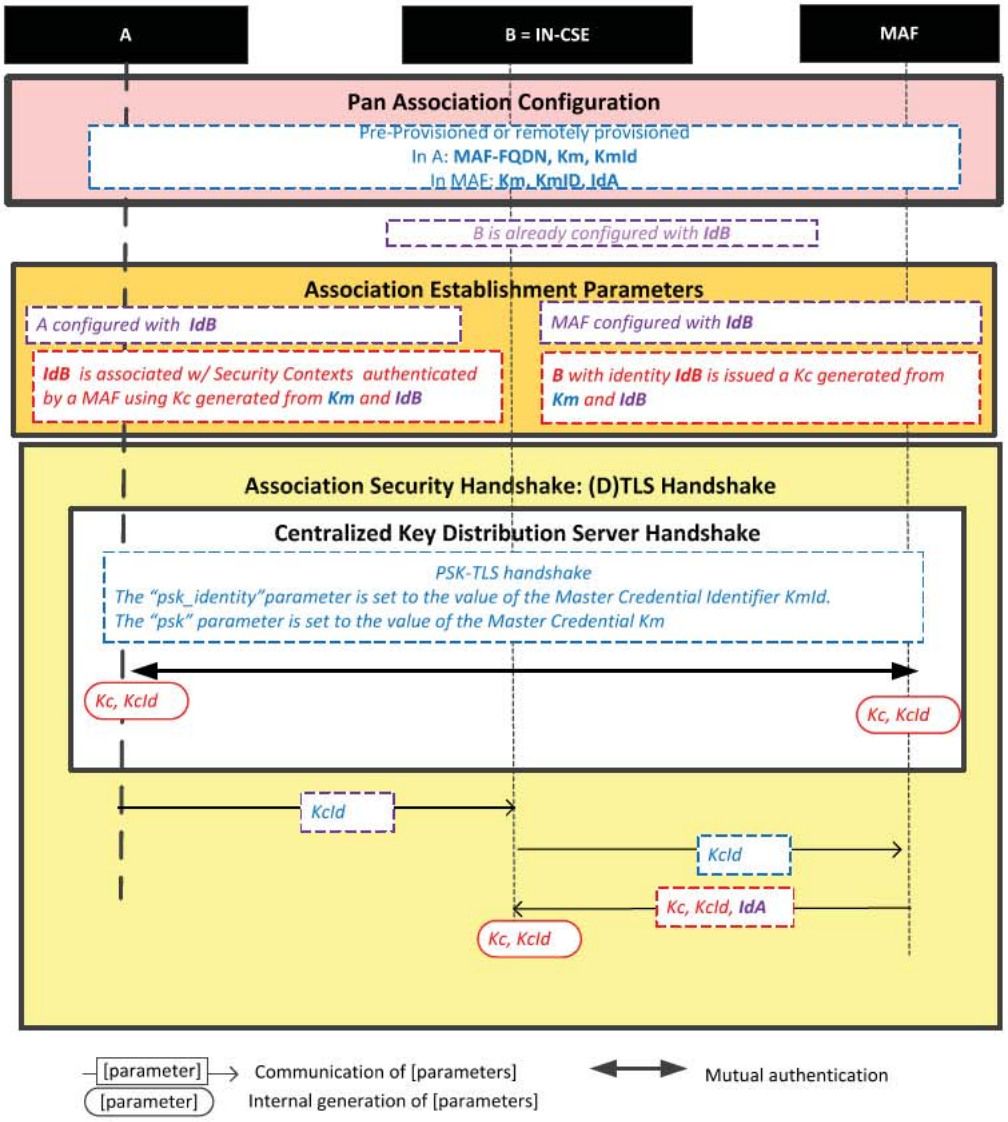


Figure 8.2.3.1-1: The sequence of events when using the MAF-Based Security Association Establishment Framework.

NOTE: The following font colours differentiate the general topic that the text relates to:
Blue italic text highlights details specific to this particular Security Association Establishment Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.
Red italic text highlights security-related properties.

Credential Configuration: The Master Credential (Km) and corresponding Master Credential Identifier (KmId) are either pre-provisioned for Entity A and the MAF or remotely provisioned thanks to Security Bootstrap Frameworks described in Clause 8.3.

Association Configuration: Entity A, Entity B, and the BSF shall be configured with the information needed for the authentication and identification during Centralized Key Distribution Server Handshake and Association Security Handshake:

- Entity A has to know Entity B Identity (IdB)

© OneM2MPartners

- Entity B has to know Entity A Identity (IdA)
- The MAF has to know Entity B Identity (IdB). In this case, IdB corresponds to IN Identity.

Association Security Handshake with Centralized Key Distribution Server Handshake:

- **Centralized Key Distribution Server Handshake**
    - The Centralized Key Distribution Server Handshake in MAF-based Security Association Establishment framework enables the establishment of a M2M Secure Connection Key (Kc) and associated M2M Secure Connection Key Identifier (KcId) shared between the Entity A and the MAF thanks to (D)TLS-PSK handshake [15]
        - The “psk_identity” parameter [15] is set to the value of the Master Credential Identifier KmId.
        - The “psk” parameter [15] is set to the value of the Master Credential Km.
- Entity A sends KcId to Entity B (Infrastructure Node).
- Entity B (Infrastructure Node) can retrieve the M2M Secure Connection Key (Kc) from the MAF.
- The (D)TLS cipher suite profile for the MAF-Based Security Association Establishment Framework is specified in clause 10.2.2.

8.2.3.2 GBA-Based Security Association Establishment Frameworks

This clause describes the GBA-based Security Association Establishment Framework.

To obtain a short term key (Kc) used for M2M Service Connection between a M2M Application Service/Middle Node and a M2M Infrastructure Node, the M2M Application Service/Middle Node shall perform a successful GBA bootstrapping and derive NAF keys (Ks_(ext/int)_NAF). This NAF key is the M2M Secure Connection Key (Kc) used for M2M Service Connection.

In case of GBA, ME, Kc = Ks_NAF.

In case of GBA_U, Kc = Ks_int_NAF, if the application resides in the UICC. Otherwise, Kc = Ks_ext_NAF.

© OneM2MPartners

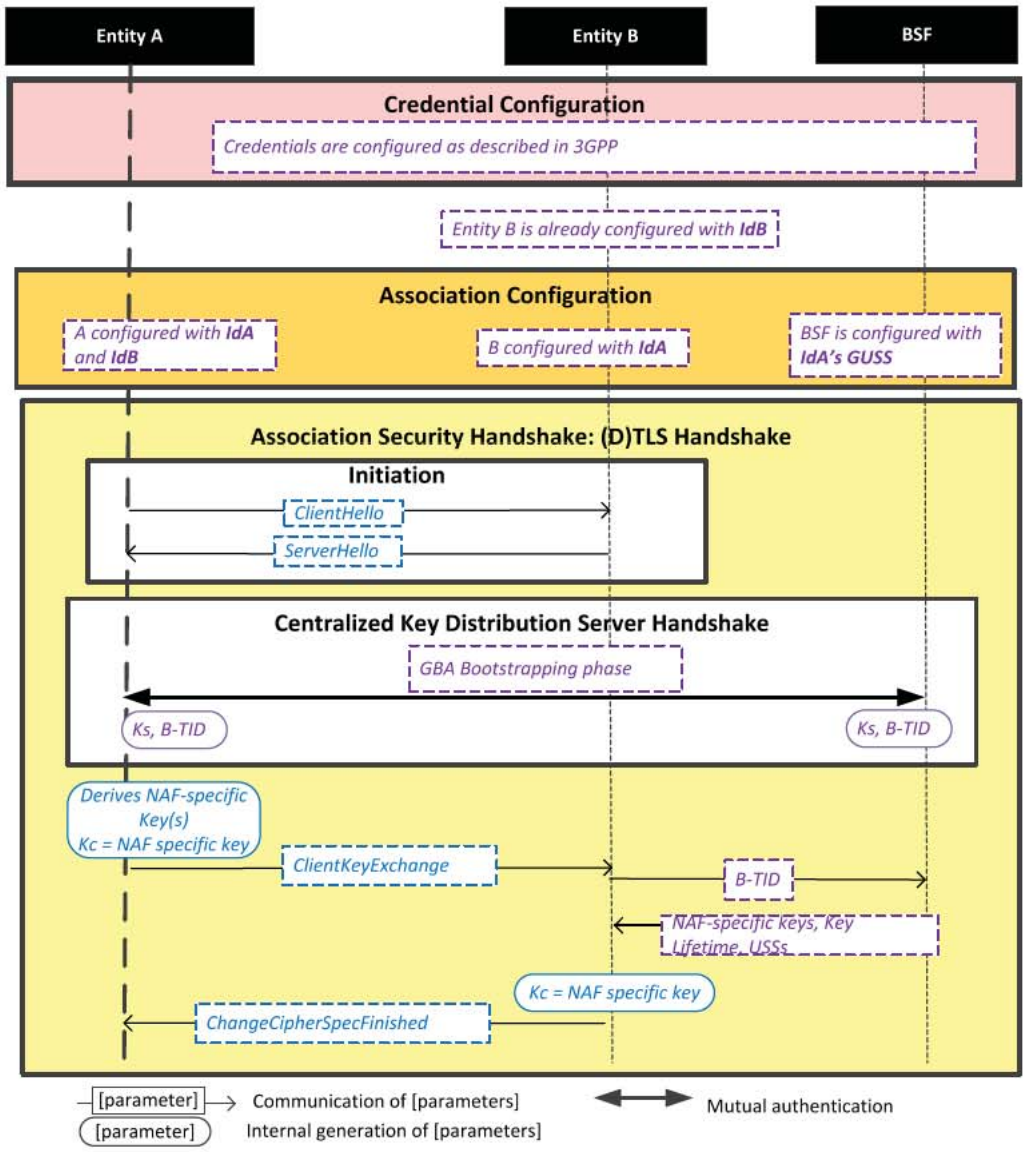


Figure 8.2.3.2-1: The sequence of events when using the GBA-Based Security Association Establishment Framework.

NOTE: The following font colours differentiate the general topic that the text relates to:
Blue italic text highlights details specific to this particular Security Association Establishment Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.

Credential Configuration: The credentials configuration for Entity A, Entity B and the BSF is described in 3GPP specification TS 33.220 [13]. The credentials used to perform mutual authentication between Entity A and BSF are UNSP specific.

Association Configuration: Entity A, Entity B, and the BSF shall be configured with the information needed for the authentication and identification during Centralized Key Distribution Server Handshake and Association Security Handshake:

- Entity A's GBA User Security Settings (GUSS) enables to indicate if Entity A is allowed to establish a NAF-specific key with Entity B (NAF) or/and if the BSF can distribute a NAF specific key to Entity B.

© OneM2MPartners

Association Security Handshake with Centralized Key Distribution Server Handshake:

- **Initiation**
    - Entity A and Entity B shall initiate TLS handshake thanks to procedure described in 3GPP TS 33.222 [28]. Informative Annex F of 3GPP TS 24.109 [29] gives signalling flows for TLS-PSK with GBA bootstrapped security association
    - Entity A shall indicate to Entity B that it supports PSK-based TLS by adding one or more PSK ciphersuites to the ClientHello message. This message shall also contain the hostname of Entity B in the server_name extension.
    - Entity B selects one of the PSK-based ciphersuites offered by Entity A and sends it back in the ServerHello message. If UICC is used as M2M Secure Environment supporting Security Association Establishment, GBA-U with Kc = Ks_int_NAF shall be used for authentication and key exchange, In this case the ServerKeyExchange message shall contain a constant string "3GPP-bootstrapping-uicc" as the PSK-identity hint, indicating use of Kc=Ks_int_NAF. Otherwise the ServerKeyExchange message shall contain a constant string "3GPP-bootstrapping" as the PSK-identity hint to indicate that Kc=Ks_NAF in the case of GBA_ME or Kc=Ks_ext_NAF in the case of GBA_U is used for authentication and key exchange. Entity B shall finish the reply to Entity A by sending a ServerHelloDone message.
- **Centralized Key Distribution Server Handshake**
    - The Centralized Key Distribution Server Handshake in Security Association Establishment framework enables the establishment of a GBA bootstrapped key (Ks) shared between the Entity A and the BSF with associated Bootstrapping Transaction Identifier (B-TID) and key lifetime, by performing to the GBA Bootstrapping phase described in 3GPP TS 33.220 [13].
    - If a bootstrapped key Ks is already shared between the Entity A and the BSF and still valid, then the Centralized Key Distribution Server Handshake phase is not needed. The Association Security Handshake can take place with the existing GBA Bootstrapped key Ks.
    - Entity A shall derive the NAF-specific keys by performing the procedure described in 3GPP TS 33.220 [13] using the GBA bootstrapped key Ks and B-TID obtained during Centralized Key Distribution Server Handshake. In case of GBA_ME, the M2M Secure Connection Key (Kc) shall be Ks_NAF. In case of GBA_U, the M2M Secure Connection Key (Kc) shall be Ks_int_NAF if HTTP Client application resides in the UICC. Otherwise, Kc = Ks_ext_NAF.

- Entity A then sends a ClientKeyExchange message with PSK-identity containing a prefix "3GPP-bootstrapping-uicc" if Entity A resides in the UICC is used as the M2M Secure Environment supporting Security Association Establishment procedure or "3GPP-bootstrapping" otherwise, a separator character ";" and the B-TID. Entity A shall conclude the TLS handshake by sending the ChangeCipherSpec and Finished messages to the Network M2M Node.
- Entity B shall extract B-TID from the ClientKeyExchange message and use it to retrieve Kc=Ks_NAF or Kc=Ks_ext_NAF or Kc=Ks_int_NAF, and associated key lifetime from the BSF. The retrieval shall be done over the Zn interface as specified in 3GPP TS 29 109 [30]. As a result, Entity A and Entity B share the NAF-specific key which is to be used as the M2M Secure Connection Key (Kc).
- Entity A shall conclude the TLS handshake by sending the ChangeCipherSpec and Finished message to Entity A.
- The (D)TLS cipher suite profile for the GBA-Based Security Association Establishment Framework is specified in clause 10.2.2.

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

Security Bootstrap Frameworks enable the provisioning of a symmetric key shared between two entities. Those two entities can be either a CSE/AE and a M2M Authentication Function (MAF) or two CSEs/AEs.

The provisioned symmetric key can be used for Provisioned Symmetric Key Security Association Establishment Framework or MAF-based Symmetric Key Security Association Establishment Frameworks.

- **Provisioned Symmetric Key Security Association Establishment**

Provisioned Symmetric Key Association Establishment uses a symmetric key Kpsa and corresponding KpsaId, shared between two entities (Entity A and Entity B), to establish security associations between those two entities (CSE/AEs), as described in clause 8.2.2.1. This symmetric key Kpsa and corresponding KpsaId shall be either pre-provisioned or remotely provisioned to the two CSE/AEs thanks to Security Bootstrap Frameworks.

- **MAF-based Symmetric Key Security Association Establishment**

The MAF-based Security Association Establishment Framework uses a Master Credential (Km) and corresponding Master Credential Identifier (KmId), shared by a CSE/AE and an M2M Authentication Function, to establish security associations between the CSE/AE and other CSEs and/or AEs as described in clause 8.2.3.

The Master Credential (Km) and corresponding Master Credential Identifier (KmId) shall either be pre-provisioned or remotely provisioned to the CSE/AE and M2M Authentication Function.

- **General**

The method for pre-provisioning can be deployment dependent. An interoperable pre-provisioning framework based on UICC is described in Annex D.

Clause 8.3 describes the set of remotely provisioning mechanisms; called *Remote Security Provisioning Frameworks*. An M2M Enrolment Function facilitates the remote provisioning.

8.3.1.2 Overview on Remote Security Provisioning Frameworks

An AE or CSE that requires remote provisioning of a Master Credential and Master Credential Identifier or a Provisioned Secure Connection Key (Kpsa) and Provisioned Secure Connection Key Identifier (KpsaId) is called an *Enrolee.* The AE or CSE with whom the enrolee is to establish a security association is called *Enrolee B.* The AE or CSE or M2M Authentication Function with whom the enrolee is to establish a shared key is called an *Enrolment Target*.

The oneM2M system supports the following Security Bootstrap Frameworks:

- **Centralized Remote Security Provisioning Frameworks**
  - **Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework:** A symmetric key is pre-provisioned to the Enrolee and M2M Enrolment Function for the mutually authentication of those entities. For more details, see clause 8.3.2.1.
  - **Certificate-Based Remote Security Provisioning Framework:** The Enrolee and M2M Enrolment Function are each issued with
    - a Private Signing Key that is known only to that entity,
    - a Certificate containing the corresponding Public Verification Key, and
    - (In the case of a device certificate, CSE-ID certificate or AE-ID certificate) a Certificate Chain from the entity's Certificate to a Trust Anchor Certificate.

    The Enrolee and M2M Enrolment Function shall validate each other's Certificate before trusting the Public Verification Keys in the Certificate. Within the Security Handshake, the M2M Enrolment Function creates a digital signature of the session parameters using its private signing key and the Enrolee verifies the digital signature using the M2M Enrolment Function's public verification key. Then the roles are reversed: the Enrolee creates a digital signature and the M2M Enrolment Function verifies it. For more details see clause 8.3.2.2.
  - **GBA-based Remote Security Provisioning Framework**. In this case, the role of the M2M Enrolment Function is performed by a GBA Bootstrap Server Function. This framework uses 3GPP or 3GPP2 symmetric keys to authenticate the Enrolee and the M2M Enrolment Function (which is also a GBA BSF). The details are specified by 3GPP [13] and 3GPP2 [14]. For more details see clause 8.3.2.3.

© OneM2MPartners

For a more detailed description of the above Remote Security Provisioning Frameworks, it is useful to compare the following aspects of the Remote Security Provisioning Frameworks.

- **Bootstrap Credential Configuration:** The Enrolee and M2M Enrolment Function are pre-provisioned with the Bootstrap Credential that the entity will use to authenticate itself to the other entity. The mechanisms for this pre-provisioning are not described in this specification.

- **Bootstrap Instruction Configuration:** The Enrolee and M2M Enrolment Function are provided with

  - Either the M2M Authentication Function Identifier (MAF-ID) identifying the M2M Authentication Function for which the Enrolee is to be remotely provisioned when used in conjunction with a MAF-based security association establishment framework; or the identifier of Enrolee B (Enrolee B-ID), when used in conjunction with a Provisioned Symmetric Key Security Association Establishment.

NOTE 1: The identity of the M2M Authentication Function or the Enrolee B is assumed to have been configured prior to the Bootstrap Instruction Configuration phase.

  - The M2M Enrolment Function is provided with the CSE-ID or AE-ID that the M2M Authentication Function or Enrolee B is to associate with the Enrolee.

  Additionally, in the case of Certificate-Based Remote Security Provisioning Framework:

  - The Enrolee is configured with the M2M Enrolment Function URI (for the purpose of routing the (D)TLS messages to the M2M Enrolment Function), M2M Enrolment Function Certificate Name and M2M Enrolment Function Trust Anchor Certificatesthat the Enrolee will use to verify the M2M Enrolment Function.

  - The M2M Enrolment Function is configured with the Enrolee Certificate Name and Enrolee Root of Trust that the M2M Enrolment Function will use to verify the Enrolee.

- **Bootstrap Enrolment Handshake:** Identification, authentication and security context establishment between the Enrolee and M2M Enrolment Function.

- **Enrolment Key Generation:** generating a symmetric Enrolment Key,(Ke) and corresponding Enrolment Key Identifier (KeId) shared by the Enrolee and M2M Enrolment Function, which is used for subsequent generation of the Master Credential (Km) or Provisioned M2M Secure Connection Key (Kpsa).

- **Integration to the Association Security Handshake:**

  For MAF-based symmetric Key Security Association, the following steps occur during the Centralized Key Distribution Server Handshake of the MAF-Based Security Association Establishment:

  - The Enrolee derives the Master Credential (Km) from the Enrolment Key (Ke) and M2M Authentication Function Identifier (MAF-ID). Details of the derivation are provided in clause 9.4.

  - The Enrolee generates the Master Credential Identifier (KmId) from Master Credential (Km) as described in clause 9.1, and stores Km and KmId.

  - The Enrolee passes the Enrolment Key Identifier (KeId) to the M2M Authentication Function (see "Centralized Key Distribution Server Handshake" in clause 8.2.3.1)

NOTE 2: When the Enrolee first communicates with the M2M Authentication Function, then the M2M Authentication Function has not yet retrieved the Km from the M2M Enrolment Function. Consequently, the Enrolee provides the KeId to the M2M Authentication function, which is then passed to the M2M Enrolment Function to identify the Enrolment Key. The M2M Enrolment Function then returns the Km from which the M2M Authentication Function can derive the KmId. In subsequent Security Establishments, the Enrolee may provide the KmId or the KeId, and the M2M Authentication Function will know that both identifiers indicate the retrieved Km. For more details, see "Centralized Key Distribution Server Handshake" in clause 8.2.3.1.

  - Upon receipt of the KeId, the M2M Authentication Function determines if it already has the corresponding Km and CSE-ID or AE-ID of the Enrolee

© OneM2MPartners

- If the M2M Authentication Function already has the corresponding Km and CSE-ID or AE-ID of the Enrolee, then the Km is used for mutual authentication (see "Centralized Key Distribution Server Handshake" in clause 8.2.3.1)
- If the M2M Authentication Function does not have the corresponding Master Credential (Km) and CSE-ID or AE-ID of the Enrolee, then the following steps are followed.
  - The M2M Authentication Function (securely) passes the KeId to the M2M Enrolment Function, along with the M2M Authentication Function's URI.
  - The M2M Authentication Function initiates establishing a mutually-authenticated TLS Session with the M2M Enrolment Function.
    - The M2M Authentication Function authenticates itself to the M2M Enrolment Function using an FQDN certificate containing the FQDN of the M2M Authentication Function.
    - The M2M Enrolment Function authenticates itself to the M2M Authentication Function using an FQDN certificate containing the FQDN of the M2M Enrolment Function.
  - The M2M Enrolment Function derives the Km from the Ke and MAF-ID. Details of the derivation are provided in clause clause 10.3.2“Derivation of Master Credential from Enrolment Key”.
  - The M2M Enrolment Function returns the Km to the M2M Authentication Function. The M2M Enrolment Function also passes the CSE-ID or AE-ID of the Enrolee.
  - The M2M Authentication Function generates the Master Credential Identifier (KmId) from Master Credential (Km) as described in clause 9.1, and stores Km and KmId.
  - The Master Credential (Km) is used for mutual authentication and generation of Kc and KcId as described in MAF-Based Security Association Establishment Framework (see "Centralized Key Distribution Server Handshake" in clause 8.2.3.1).
  - The Enrolee and M2M Authentication Function set Master Credential Identifier (KmId) to the value of the Enrolment Key Identifier (KeId).
  - The Enrolee and M2M Authentication Function store Km and KmId.

For Provisioned Symmetric Key Security Association Establishment, similar procedure applies where Enrolee B plays the role of M2M Authentication Function, Kpsa plays the role of Km, KpsaId is generated instead of KmId. Generation of Kpsa is described in 10.3.3 “Derivation of Provisioned Secure Connection Key from Enrolment Key”.

Figure 8.3.1.2-1 provides a summary of the above defined Remote Security Provisioning Frameworks.

© OneM2MPartners

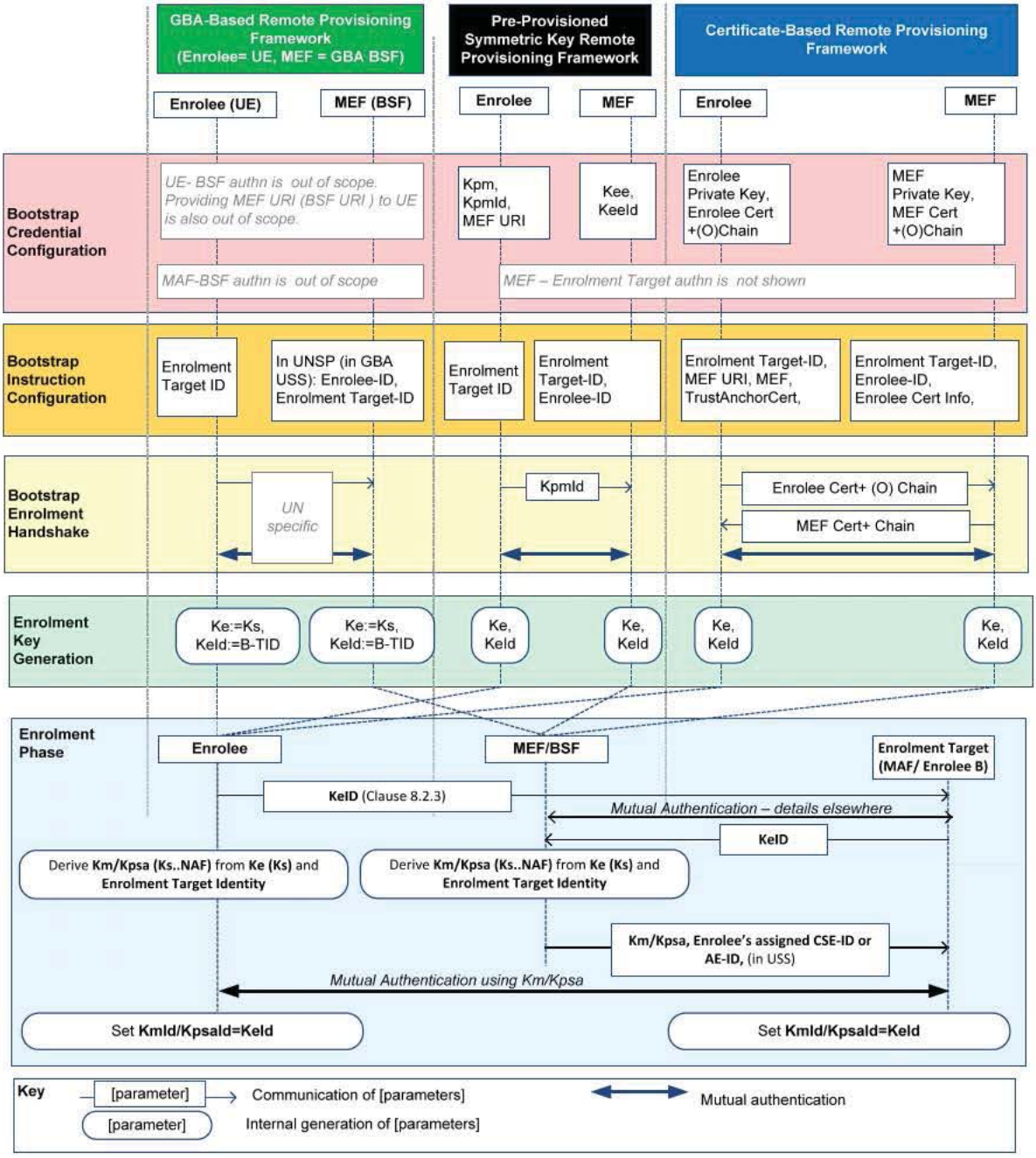


Figure 8.3.1.2-1: Overview of the Remote Security Provisioning Frameworks supported by oneM2M

8.3.2 Centralized Remote Security Provisioning Framework

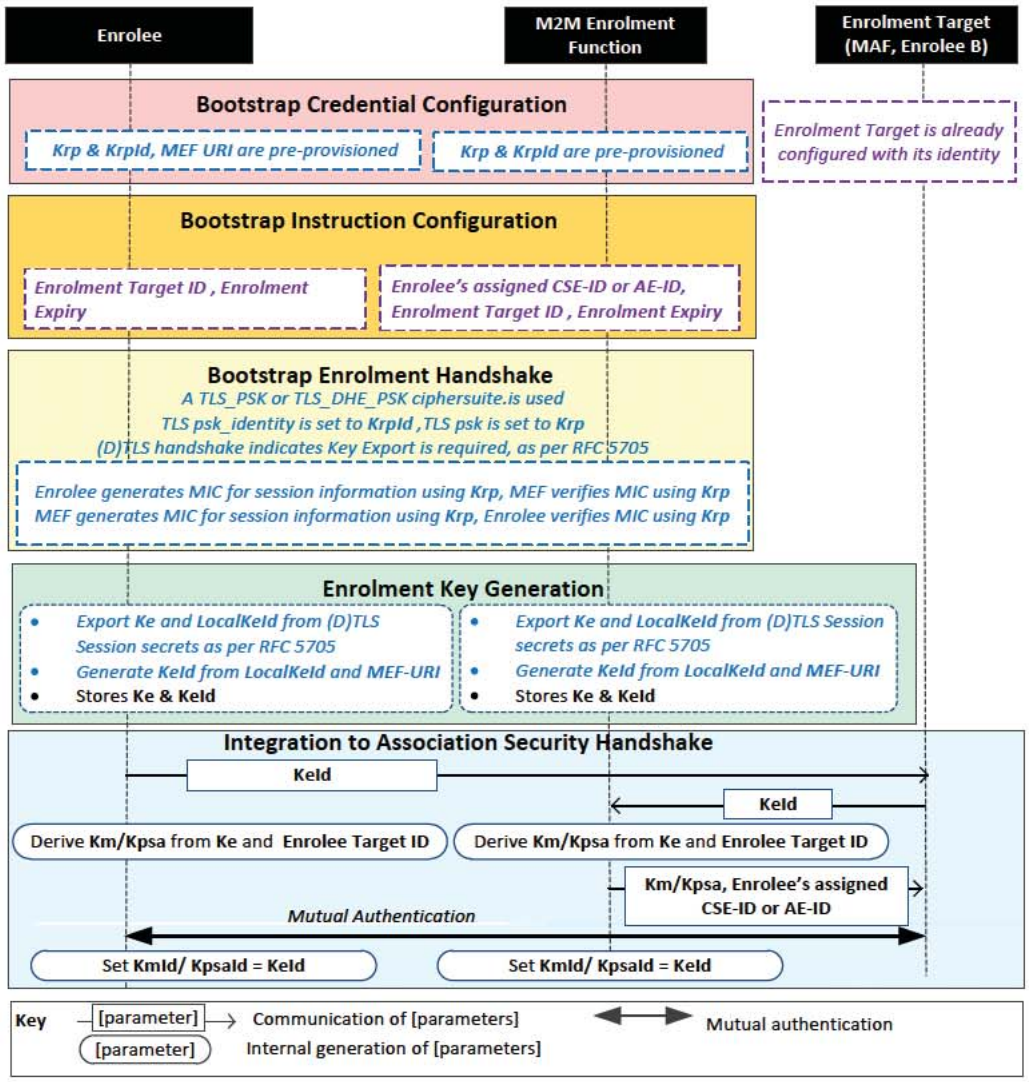
8.3.2.1 Pre-Provisioned Symmetric Key Remote Security Provisioning Framework

This clause describes the Pre-Provisioned Symmetric Key Remote Security Provisioning Framework. The Bootstrap Credential for this framework is a long-term symmetric key that has been pre-provisioned into the Enrolee and M2M Enrolment Function; this key is called a Pre-Provisioned Symmetric Enrolee Key and is denoted Kpm.

© OneM2MPartners

NOTE: Long term Pre-Provisioned Symmetric Enrolee Keys can pose a security risk if not adequately secured, and for this reason it is recommended that Long term Pre-Provisioned Symmetric Enrolee Keys are stored in Secure Environments.

Figure 8.3.2.1-1 illustrates the sequence of events when using the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework.



NOTE: The following font colours differentiate the general topic that the text relates to:
Black text contains Remote Security Provisioning-Framework-independent details
Blue italic text highlights details specific to this particular Remote Security Provisioning Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.

Figure 8.3.2.1-1: The sequence of events when using the Pre-Provisioned Symmetric Key Remote Security Provisioning Framework

Bootstrap Credential Configuration: The Pre-Provisioned Symmetric Enrolee Key (Kpm) and the corresponding Pre-Provisioned Symmetric Enrolee Key Identifier, denoted KpmId, are pre-provisioned to both entities. The Enrolee is also provisioned with the M2M Enrolment Function's URI (MEF URI), for the purpose of routing the (D)TLS exchange.

NOTE 1: This pre-provisioning (by definition) uses mechanisms not specified by oneM2M.

© OneM2MPartners

Bootstrap Instruction Configuration: The Enrolee and M2M Enrolment Function are configured with the information needed for authorizing the remote provisioning:

- The Enrolee is configured with (or otherwise obtains) the following arguments to initiate remote provisioning :
  - The Enrolment Target identity: Identifying the Enrolment Target for which the Enrolee is to be provisioned.
  - The Enrolee associates these arguments with the M2M Enrolment Function. The M2M Enrolment Function can be identified to the Enrolee using the Pre-Provisioned Symmetric Enrolee Key Identifier (KpmId) or the M2M Enrolment Function URI.
- M2M Enrolment Function is configured with the following arguments to authorize the M2M Enrolment Function to remotely provision the Enrolee for an Enrolment Target:
  - The Enrolment Target Identity: Identifying the Enrolment Target for which the Enrolee is to be provisioned.
  - Enrolee's assigned CSE-ID or AE-ID (Enrolee-ID). The M2M Enrolment Function is to provide this entity identity for the Enrolee with the Km or Kpsa to the Enrolment Target, when requested by the Enrolment Target.
  - The M2M Enrolment Function associates these arguments with an Enrolee. The Enrolee can be identified to the M2M Enrolment Function using the Pre-Provisioned Symmetric Enrolee Key Identifier (KpmId).

Bootstrap Security Handshake: The Enrolee and M2M Enrolment Function perform a (D)TLS-PSK handshake [15] to establish a secure session.

- The "psk_identity" parameter [15] is set to the value of the Pre-Provisioned Symmetric Enrolee Key Identifier (KpmId).
- The "psk" parameter [15] is set to the value of the Pre-Provisioned Symmetric Enrolee Key (Kpm).
- The (D)TLS cipher suite profile for this 's assigned CSE-ID or AE-ID is specified in clause 10.2.2 "TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks".

Enrolment Key Generation:

a) The Enrolment Key (Ke) and RelativeKeId is generated from the (D)TLS session secrets by the Enrolee and M2M Enrolment Function using TLS Key Export (RFC 5705) [18], as described in clause 10.3.1 "TLS Key Export Details".

b) The Enrolment Key Identifier (KeId) is generated from the RelativeKeId and the M2M Enrolment Function's FQDN by the Enrolee and M2M Enrolment Function, as described in clause 10.3.4 "Generating KeId".

c) The Enrolee and M2M Enrolment Function store the Enrolment Key (Ke) and Enrolment Key Identifier (KeId).

NOTE 2: The Enrolment Key Generation for the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework is identical to the Enrolment Key Generation for the Certificate-Based Remote Security Provisioning Framework.

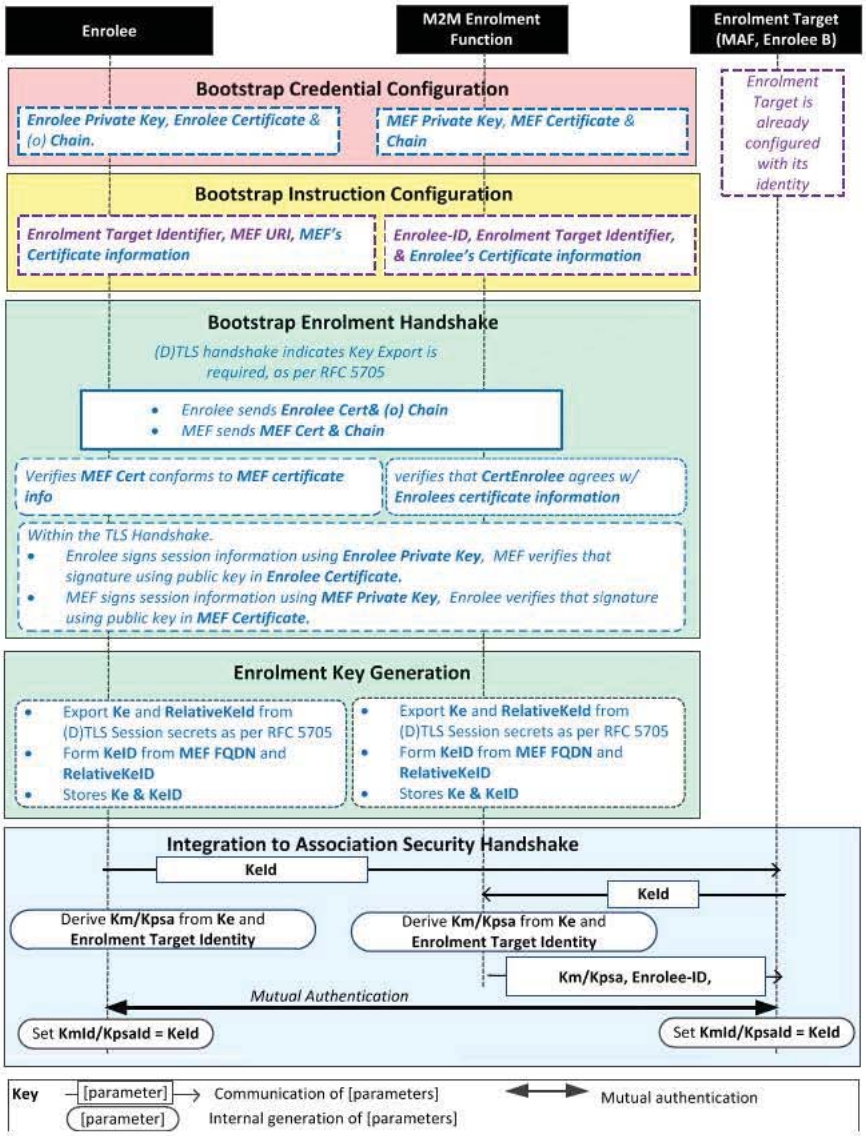
Integration to the Association Security Handshake: See "Overview of Remote Security Provisioning Frameworks" in clause 8.3.1.

8.3.2.2 Certificate-Based Remote Security Provisioning Framework

This clause describes the Certificate-Based Remote Security Provisioning Framework. The Bootstrap Credentials for this framework are Certificates.

Figure 8.3.2.2-1 illustrates the sequence of events when using the Certificate-Based Remote Security Provisioning Framework.

© OneM2MPartners



NOTE: The following font colours differentiate the general topic that the text relates to:
Black text contains Remote Security Provisioning -Framework-independent details.
Blue italic text highlights details specific to this particular Remote Security Provisioning Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.
Red italic text highlights security-related properties.

Figure 8.3.2.2-1: The sequence of events when using the Certificate-Based Remote Security Provisioning Framework.

Bootstrap Credential Configuration: For this Remote Security Provisioning Framework, Enrolee and M2M Enrolment Function authenticate each other using a Public Key Certificate. The Bootstrap Credentials for the Enrolee and M2M Enrolment Function are pre-provisioned as described in clause 8.1.1.2.1 "Credential Configuration for Certificate-Based Security Frameworks".

NOTE 1: The identities of the M2M Enrolment Function and Enrolment Target are assumed to have been configured prior to this phase.

Bootstrap Instruction Configuration: The Enrolee and M2M Enrolment Function are configured with the information needed for authorizing the remote provisioning:

- The Enrolee is configured with (or otherwise obtains) the following arguments to initiate remote provisioning:

© OneM2MPartners

- The URI of the M2M Enrolment Function which will facilitate the remote provisioning, for the purpose of routing the (D)TLS exchange.
- Information needed for certificate authentication of the M2M Enrolment Function using an MEF certificate as described in clause 8.1.1.2.4 “Information Needed for Certificate Authentication of another Entity”;
- The Enrolment Target Identity : Identifying the Enrolment Target for which the Enrolee is to be provisioned.

- The M2M Enrolment Function is configured with the following arguments describing Enrolee authorized to perform Security Handshake with M2M Enrolment Function:
  - Information needed for certificate authentication of the Enrolee, as described in clause 8.1.1.2.4 “Information Needed for Certificate Authentication of another Entity”
  - The Enrolment Target Identity : Identifying the Enrolment Target for which the Enrolee (authenticated using the above Enrolee Certificate information) is to be provisioned.
  - The Enrolee’s assigned CSE-ID or AE-ID (Enrolee-ID). The M2M Enrolment Function is to provide this entity identity for the Enrolee with the Km or Kpsa to the Enrolemnt Target, when requested by the Enrolment Target.

Bootstrap Security Handshake: The Enrolee and M2M Enrolment Function perform a (D)TLS handshake as specified in TLS 1,2 RFC 5246 [16] and DTLS 1.2 RFC 6347 [17] specifications.to establish a secure session.

- Each entity (Enrolee and M2M Enrolment Function) verifies the other entity's certificate as described in clause 8.1.1.2.5 "Certificate Verification".
- The Enrolee and M2M Enrolment Function authenticate each other using the validated certificates as specified in TLS 1.2 RFC 5246 [16] and DTLS 1.2 RFC 6347 [17] specifications.
- The (D)TLS cipher suite profile for this ’s assigned CSE-ID or AE-ID is specified in clause 10.2.3 “TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks”.

Enrolment Key Generation:

The steps are identical to those shown for “Enrolment Key Generation” in clause 8.3.2.1 “Pre-Provisioned Symmetric Key Remote Security Provisioning Framework”

Integration to the Association Security Handshake: See "Overview of Remote Security Provisioning Frameworks" in clause 8.3.1.

8.3.2.3 GBA-Based Remote Security Provisioning Framework

To share a long term Master Credential (Km) or Provisioned Secure Connection Key (Kpsa) between an Application Service/Middle Node and an Enrolment Target, the M2M Application Service/Middle Node shall perform a successful GBA bootstrapping and derive a NAF key (Ks_(ext/int)_NAF). This NAF key is the Master Credential (Km) or Provisioned Secure Connection Key (Kpsa).

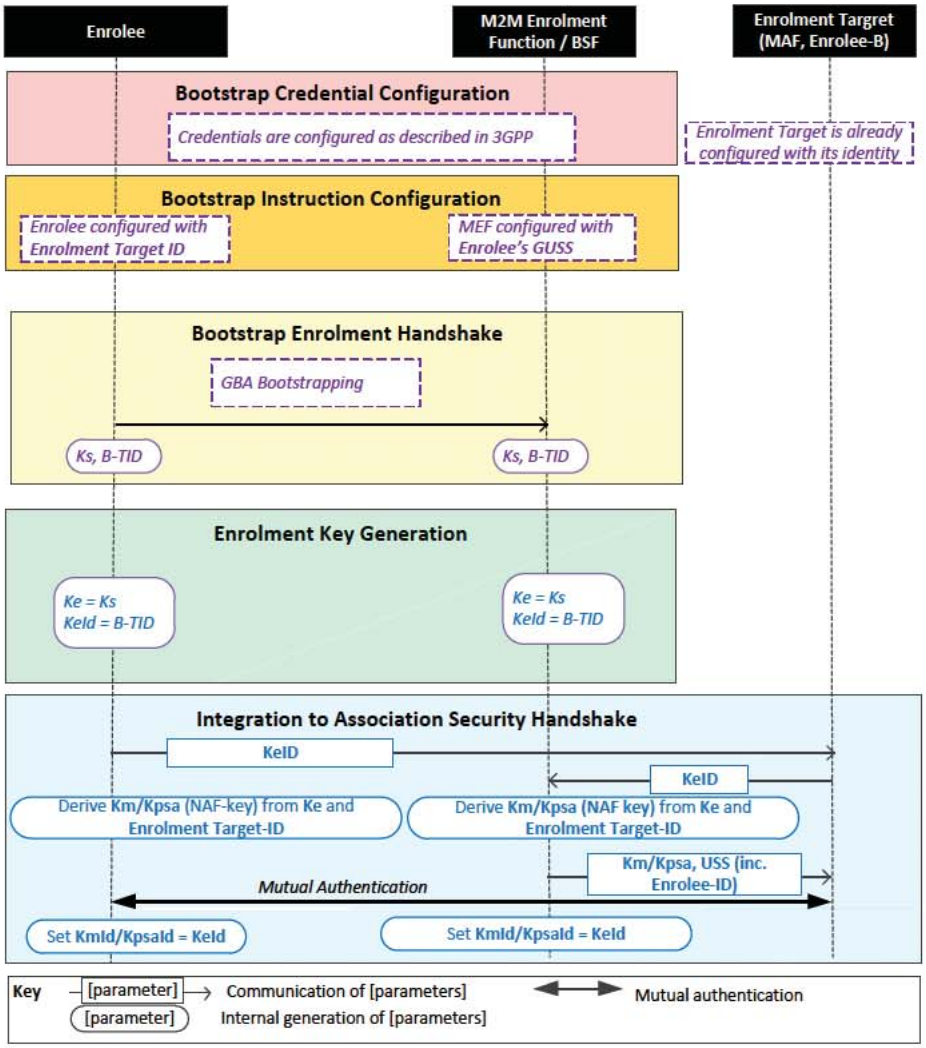


Figure 8.3.2.3-1: The sequence of events when using the GBA-Based Remote Security Provisioning Framework.

NOTE: The following font colours differentiate the general topic that the text relates to:
Black text contains Remote Security Provisioning -Framework-independent details.
Blue italic text highlights details specific to this particular Remote Security Provisioning Framework.
Purple italic text highlights technical actions that may include steps not specified by oneM2M.

Bootstrap Credential Configuration: The credentials configuration for Enrolee and M2M Enrolment Function (MEF) is described in 3GPP specification TS 33.220 [13]. The MEF plays the role of the BSF. The credentials used to perform mutual authentication between Enrolee and MEF are UNSP specific.

Bootstrap Instruction Configuration: the Enrolee, the MEF and the MAF shall be configured with the information needed for authorizing the remote provisioning.

- The Enrolee shall be configured with the Enrolment Target Identity: identifying the Enrolment Target for which the Enrolee is to be provisioned.
- The MEF shall be configured with the Enrolee-ID and the Enrolment Target Identity
  - The Enrolment Target Identity: Identifying the Enrolment Target for which the Enrolee (authenticated using the GBA) is to be provisioned

© OneM2MPartners

- The Enrolee's assigned CSE-ID or AE-ID (Enrolee-ID), The M2M Enrolment Function is to provide this entity identity for the Enrolee with the Km or Kpsa to the Enrolment Target, when requested by the Enrolment Target.
- Enrolee's GBA User Security Settings (GUSS) enables to indicate if Enrolee is allowed to establish a NAF-specific key with the MAF or/and if the BSF can distribute a NAF specific key to the MAF.

Bootstrap Enrolment Handshake:

The Bootstrap Enrolment Handshake enables the establishment of a GBA bootstrapped key (Ks) shared between the Enrolee and the MEF with associated Bootstrapping Transaction Identifier (B-TID) and key lifetime, by performing to the GBA Bootstrapping phase described in 3GPP TS 33.220 [13].

If a bootstrapped key Ks is already shared between Enrolee and the MEF and still valid, then the Bootstrap Enrolment Handshake phase is not needed. The Enrolment Key Generation phase can take place with the existing GBA Bootstrapped key Ks.

Enrolment Key Generation phase

The Enrolment Key (Ke) shall be the GBA Bootstrapped key (Ks) established during the Bootstrap Enrolment Handshake.

The Enrolment Key Identifier (Ke-ID) shall be the Bootstrapping Transaction Identifier (B-TID) generated during the Bootstrap Enrolment Handshake.

Integration to the Association Security Handshake:

- The Enrolee and the Enrolment Target shall establish the Master Credential (Km) or the Provisioned Secure Connection Key (Kpsa) thanks to procedures described in 3GPP TS 33.220 [13] using the Enrolment Key (Ke) as GBA bootstrapped key Ks and the Enrolment Key Identifier (Ke-ID) as B-TID. The Enrolment Target plays the role of a NAF.
    - The Enrolee and the Enrolment Target shall establish NAF-specific key(s) as described in 3GPP TS 33.220 [13]. A key lifetime is associated to the NAF-specific keys. The Enrolment Target also receives the Enrolee's User Security Settings (USS) from the MEF/BSF.
        - In case of GBA_ME, NAF-specific key is Ks_NAF
        - In case of GBA_U, NAF-specific keys are Ks_int_NAF and Ks_ext_NAF.
    - The Master Credential (Km)) or the Provisioned Secure Connection Key (Kpsa) shall be the NAF-specific key:
        - In case of GBA_ME, Km/Kpsa = Ks_NAF
        - In case of GBA_U, Km/Kpsa = Ks_int_NAF if HTTP Client application resides in the UICC. Otherwise, Km/Kpsa = Ks_ext_NAF.
    - The Enrolee and the Enrolment Target shall set the Master Credential Identifier (Km-Id) or the Provisioned Secure Connection Key Identifier (Kpsa-Id) to the value of KeId.

Enrolee and Enrolment Target shall perform (D)TLS-PSK handshake (RFC 4279 [15]) with the Master Credential (Km) or Provisioned Secure Connection Key (Kpsa) as Pre-Shared Key in compliance with clause 10.2.2 "TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks". If UICC is used as Secure Environment supporting Remote Security Provisioning, GBA-U with Kc = Ks_int_NAF shall be used for authentication and key exchange.

9 Security Framework Procedures and Parameters

This clause specifies procedures and parameters of the phases of Security Association Establishment Frameworks (clause 8.2) and Remote Security Provisioning Frameworks (clause 8.3).

9.1 Security Association Establishment Framework Procedures and Parameters

9.1.1 Credential Configuration Parameters

The following Credential Configuration procedures are described in the present clause:

- Credential Configuration of Entity A and Entity B , see Clause 9.1.1.1,
- Credential Configuration of M2M Authentication Functions, see Clause 9.1.1.2,

The following Credential Configuration procedures are specified by other organizations:

- Credential Configuration of Underlying Network Service Provider authentication server (e.g. HLR, HSS or AAA) for the GBA-Based Security Association Establishment Framework. These details are specified by 3GPP TS 33.220 [13], 3GPP2 S.S0109-A [14].
- Credential Configuration of Entity A in the Field-Domain for the GBA-Based Security Association Establishment Framework. These details are specified by 3GPP TS 33.220 [13], 3GPP2 S.S0109-A [14].

9.1.1.1 Credential Configuration of Entity A and Entity B

Table 9.1.1.1-1 lists the parameters configured to a Field-Domain Security Association End-Points in the Credential Configuration phase.

Table 9.1.1.1-1 Parameters configured to a Field Domain Security Association end-point during the Credential Configuration phase.

Security Association Establishment Framework		Parameter
Provisioned M2M Secure Connection Key		Kpsa
		KpsaId
Certificate Based	Entity authenticates itself using a Raw Public Key Certificate	Entity's Private Key
		Entity's Raw Public Key Certificate
	Entity authenticates itself using a Device Certificate	Entity's Private Key
		Entity's Certificate and Chain
	Entity authenticates itself using a CSE-ID Certificate	Entity's CSE-ID
		Entity's Private Key
		Entity's Certificate and Chain
	Entity authenticates itself using an AE-ID Certificate	Entity's AE-ID
		Entity's Private Key
		Entity's Certificate and Chain
MAF-Based	Entity A	MAF Identifier (MAF-ID)
		Master Credential (Km Id)
		Master Credential Identifier (KmId)
	Entity B	Entity B and MAF shall be able to establish mutually-authenticated secure communication. The details are not specified in the present document
GBA-Based	Entity B plays role of NAF. Details specified in 3GPP 33.220 [13]. Where this description differs from [13], [13] takes precedence	NAF Private Key
		NAF Certificate and Chain
		BSF trust anchor certificate

The Credential Configuration of Entity A, Entity B and the MAF for the Provisioned M2M Secure Connection Key Security Association Establishment Framework, or the MAF-Based Security Association Establishment Framework is achieved through either:

- Pre-provisioning via mechanisms which are not specified in the present document.
- Remote provisioning via one of the Remote Security Provisioning Frameworks in Clause 8.3.

© OneM2MPartners

The Credential Configuration of Entity A and Entity B for the Certificate Security Association Establishment Frameworks is performed by pre-provisioning via mechanisms which are not specified in the present document .

9.1.1.2 Credential Configuration of M2M Authentication Functions

Table 9.1.1.2-1 lists the parameters configured to M2M Authentication Functions in the Credential Configuration phase. The M2M Authentication Function's identifier (MAF-ID) is presumed to have been configured prior to the Credential Configuration phase.

Table 9.1.1.2-1 Parameters configured to a M2M Authentication Functions during the Credential Configuration phase.

Security Association Establishment Framework		Parameter
MAF-Based	A-to-MAF Authentication	Entity A's CSE-ID or AE-ID (IdA)
		masterCredential (Km)
		masterCredentialIdentifier (KmId)
	B-to-MAF Authentication	Entity B and MAF shall be able to establish mutually-authenticated secure communication. The details are not specified in the present document

The Credential Configuration of M2M Authentication Framework shall be achieved through either:

- Business logic of the Stakeholder operating the M2M Authentication Function, and the details are not described in this specification.
- Remote provisioning via one of the Remote Security Provisioning Frameworks in Clause 8.3.

9.1.2 Association Configuration Procedures and Parameters

The following Association Configuration procedures are described in this clause:

- Association Configuration of Entity A and Entity B, see Clause 9.1.2.1,
- Association Configuration of M2M Authentication Functions, see Clause 9.1.2.2, and
- Association Configuration of Underlying Network Service Provider authentication servers (e.g. HLR, HSS or AAA), see Clause 9.1.2.3.

9.1.2.1 Association Configuration of Entity A and Entity B

Table 9.1.2.1-1 lists the parameters configured to Entity A and Entity B in the Credential Configuration phase.

Table 9.1.2.1-1 Parameters configured to Entity A and Entity B during the Credential Configuration phase.

Security Association Establishment Framework		Parameters specific to the Security Association Establishment Frameworks
Pre-Provisioned M2M Secure Connection Key		None
Certificate Based	Other entity is authenticated using Raw Public Key Certificate	Other entity's identity (IdA or IdB)
		Other entity's Public key identifier
	Other entity is authenticated using Device Certificate	Other entity's identity (IdA or IdB)
		Other entity's globally unique hardware instance identifier
		Other entity's trust anchor certificates
	Other entity is authenticated using CSE-ID Certificate	Other entity's CSE-ID (IdA or IdB)
		Other entity's trust anchor certificates
	Other entity is authenticated using AE-ID Certificate	Other entity's AE-ID (IdA or IdB)
		Other entity's trust anchor certificates
MAF-Based	Configured to Entity A	Entity B's CSE-ID or AE-ID (IdB)
GBA-Based	Configured to Entity A	Entity B's CSE-ID or AE-ID (IdB)

© OneM2MPartners

Mechanisms for Association Configuration of an entity shall authenticate the configuration source and provide integrity protection for the configured information communicated from the configuration source to the entity.

9.1.2.2 Association Configuration of M2M Authentication Functions

Table 9.1.2.2-1 lists the parameters configured to M2M Authentication Functions in the Association Configuration phase.

Table 9.1.2.2-1 Parameters configured to a M2M Authentication Functions during the Association Configuration phase.

Security Association Establishment Framework		Parameter
MAF-Based	A-to-MAF Authentication	Entity B's CSE-ID or AE-ID (IdB)

This specification assumes that Association Configuration of the M2M Authentication Functions will utilize business logic of the Stakeholder that operates the M2M Authentication Function, and the details are not described in this specification.

9.1.2.3 Association Configuration of UNSP Authentication Servers

Table 9.1.2.3-1 lists the parameters configured to an Underlying Network Service Provider authentication server (e.g. HLR, HSS or AAA) in the Association Configuration phase.

Table 9.1.2.3-1 Parameters configured to an Underlying Network Service Provider authentication server (e.g. HLR, HSS or AAA) during the Association Configuration phase.

Security Association Establishment Framework	Parameter
GBA-Based. Parameters are configured to UE's GBA User Security Settings (GUSS). GUSS details are specified in 3GPP 33.220 [13]. Where this description differs from [13], [13] takes precedence	Entity A's CSE-ID or AE-ID (IdA)
	Entity B's CSE-ID or AE-ID (IdB)

The Association Configuration of the Underlying Network Service Provider authentication server is achieved by updating the GBA User Security Settings (GUSS) (3GPP 33.220 [13]) of the User Equipment (UE) upon which the Enrolee is executed. This specification assumes that this Association Configuration will utilize business logic of the Underlying Network Service Provider, and the details are not described in this specification.

9. 2 Remote Security Provisioning Framework Procedures and Parameters

9.2.1 Bootstrap Credential Configuration Procedures and Parameters

The following Bootstrap Credential Configuration procedures are described in this clause:

- Bootstrap Credential Configuration of Enrolees and Enrolment Targets (except for the GBA-Based case as discussed below), see Clause 9.2.1.1,
- Bootstrap Credential Configuration of M2M Enrolment Functions (except for the GBA-Based case as discussed above), see Clause 9.2.1.2.

The following Bootstrap Credential Configuration procedures are specified by other organizations:

- Bootstrap Credential Configuration of Underlying Network Service Provider authentication servers (e.g. HLR, HSS or AAA) for the GBA-Based Security Association Establishment Framework. These details are specified by 3GPP TS 33.220 [13], 3GPP2 S.S0109-A [14].

© OneM2MPartners

- Bootstrap Credential Configuration of Enrolees for the GBA-Based Security Association Establishment Framework. These details are specified by 3GPP TS 33.220 [13], 3GPP2 S.S0109-A [14].

9.2.1.1 Bootstrap Credential Configuration of Enrolee and Enrolment Targets

Table 9.2.1.1-1 lists the parameters configured to Enrolees and Enrolment Targets in the Bootstrap Credential Configuration phase for authentication with the M2M Enrolment Function in the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Table 9.2.1.1-1 Parameters configured to Enrolees and Enrolment Targets during the Bootstrap Credential Configuration phase.

Remote Security Provisioning Framework		Parameter
Pre-Provisioned M2M Secure Connection Key authentication. Not applicable to MAF.		Kpm
		KpmId
		MEF URI
Certificate-Based authentication	Entity authenticates itself using a raw public key	Entity's Private Key
		Entity's Raw Public Key Certificate
	Entity authenticates itself using a device certificate	Entity's Private Key
		Entity's Certificate and Chain
	Entity authenticates itself using a CSE-ID or AE-ID certificate	Entity's Private Key
		Entity's Certificate and Chain

The Bootstrap Credential Configuration of an Enrolee or Field Domain Enrolment Target for the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework shall authenticate the configuration source and shall provide confidentiality and integrity protection of the configured information communicated from the configuration source to the secured environment of the Enrolee or Field Domain Enrolment Target. The present document does not specify any such mechanisms.

The Bootstrap Credential Configuration of an Infrastructure Domain Enrolment Target (including an M2M Authentication Functions) expected to use business logic of the Stakeholder operating the Infrastructure Domain Enrolment, and the details are not described in this specification.

9.2.1.2 Bootstrap Credential Configuration of M2M Enrolment Functions

It is assumed that an M2M Enrolment Function already knows its FQDN.

Table 9.2.1.2-1 lists the parameters configured to M2M Enrolment Functions in the Bootstrap Credential Configuration phase for mutual authentication with Enrolees and Enrolment Targets using the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Table 9.2.1.2-1 Parameters configured to the M2M Enrolment Function during the Bootstrap Credential Configuration phase for mutual authentication with Enrolees and Enrolment Targets using the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Remote Security Provisioning Framework	Parameters specific to the Remote Security Provisioning Frameworks
Pre-Provisioned Symmetric Enrolment Key authentication of Enrolee or Enrolment Target	Kpm
	KpmId
Certificate Based authentication of Enrolee or Enrolment Target	MEF PrivateKey
	MEF Certificate and Chain

The Bootstrap Credential Configuration of M2M Enrolment Functions is expected to use business logic of the stakeholder operating the M2M Enrolment Function, and the details are not described in this specification.

© OneM2MPartners

9.2.2 Bootstrap Instruction Configuration Procedures and Parameters

The following Bootstrap Instruction Configuration procedures are described in this clause:

- Bootstrap Instruction Configuration of Enrolees, see Clause 9.2.2.1,
- Bootstrap Instruction Configuration of Enrolment Targets, see Clause 9.2.2.2,
- Bootstrap Instruction Configuration of M2M Enrolment Functions, see Clause 9.2.2.3
- Bootstrap Instruction Configuration of Underlying Network Service Provider authentication servers (e.g. HLR, HSS or AAA), see Clause 9.2.2.4.

9.2.2.1 Bootstrap Instruction Configuration of Enrolees

Table 9.2.2.1-1 lists the parameters configured to an Enrolee during the Bootstrap Instruction Configuration phase which are common to all Remote Security Provisioning Frameworks.

Table 9.2.2.1-1 Parameters configured to an Enrolee during the Bootstrap Instruction Configuration phase of which are common to all Remote Security Provisioning Frameworks.

Parameter common to all Remote Security Provisioning Frameworks
Enrolment Target Identifier (Enrolee B's AE-ID or CSE-ID, or MAF-ID)

Table 9.2.2.1-2 lists the Remote Security Provisioning Framework–specific parameters configured an Enrolee in the Bootstrap Instruction Configuration phase of the Remote Security Provisioning Framework.

Table 9.2.2.1-2 Remote Security Provisioning Framework –specific parameters configured to an Enrolee during the Instruction Configuration phase of the Remote Security Provisioning Framework.

Remote Security Provisioning Framework	Remote Security Provisioning Framework-specific Parameters
Pre-Provisioned Symmetric Enrolment Key	*None*
Certificate Based	MEF URI
	MEF TrustAnchor Certificates
GBA-Based	*None*

Mechanisms for Bootstrap Instruction Configuration of Enrolees shall authenticate the configuration source and shall provide at least integrity protection of the configured information communicated from the configuration source to the Enrolee.

9.2.2.2 Bootstrap Instruction Configuration of Enrolment Targets

Table 9.2.2.2-1 lists the parameters configured to Enrolment Targets during the Bootstrap Instruction Configuration phase.

Table 9.2.2.2-1 Parameters configured to Enrolment Targets during the Bootstrap Instruction Configuration phase.

Mechanism for authenticating the Enrolment Target	Remote Security Provisioning Framework-specific Parameters
Pre-Provisioned Symmetric Enrolment Key. *Not applicable to MAF.*	*None*
Certificate Based	MEF/BSF Trust Anchor Certificates

Mechanisms for Bootstrap Instruction Configuration of Enrolment Targets shall authenticate the configuration source and shall provide at least integrity protection of the configured information communicated from the configuration source to the Enrolment Targets.

© OneM2MPartners

This specification assumes that Bootstrap Instruction Configuration of Infrastructure Domain Enrolment Targets (including M2M Authentication Functions) utilizes business logic of the Stakeholder that operates the M2M Authentication Function, and the details are not described in this specification.

9.2.2.3 Bootstrap Instruction Configuration of M2M Enrolment Functions

Table 9.2.2.3-1 lists the parameters configured to an M2M Enrolment Function during the Bootstrap Instruction Configuration phase which are common to the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Table 9.2.2.3-1 Parameters configured to M2M Enrolment Functions during the Bootstrap Instruction Configuration phase of which are common to the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Parameter common to all Remote Security Provisioning Frameworks
Enrolee's assigned CSE-ID or AE -ID
Enrolment Target Identity (Enrolee B's CSE-ID or AE-ID, or MAF-ID)

Table 9.2.2.3-2 lists the Remote Security Provisioning Framework–specific parameters configured to an M2M Enrolment Functions in the Bootstrap Instruction Configuration phase of the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Table 9.2.2.3-2 Remote Security Provisioning Framework–specific parameters configured to an M2M Enrolment Function during the Instruction Instruction Configuration phase of the Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework and Certificate-Based Remote Security Provisioning Framework.

Remote Security Provisioning Framework		Remote Security Provisioning Framework-specific Parameters
Pre-Provisioned Symmetric Enrolment Key		*None*
Certificate Based	Enrolee is authenticated using a raw public key certificate	Enrolee's Public key identifier
	Enrolee is authenticated using a device certificate	Enrolee's M2M Device ID
		Enrolee's Trust Anchor Certificates
	Enrolee is authenticated using a CSE-ID or AE-ID certificate	Enrolee's Trust Anchor Certificates

Table 9.2.2.3-3 lists the parameters configured to an M2M Enrolment Functions for authentication of the Enrolment Target when the Enrolment Target is Enrolee B (a CSE or AE).

Table 9.2.2.3-3 Remote Security Provisioning Framework–specific parameters configured to an M2M Enrolment Function during the Bootstrap Instruction Configuration phase for authentication of the Enrolment Target when the Enrolment Target is Enrolee B (a CSE or AE)..

Mechanism for Authenticating Enrolee B		Parameters specific to the mechanism for authenticating Enrolee B
Pre-Provisioned Symmetric Enrolment Key		*None*
Certificate Based	Enrolee B is authenticated using a raw public key certificate	Enrolee B's Public key identifier
	Enrolee B is authenticated using a device certificate	Enrolee B's M2M Device ID
		Enrolee B's Trust Anchor Certificates
	Enrolee B is authenticated using a CSE-ID or AE-ID certificate	Enrolee B's Trust Anchor Certificates

Table 9.2.2.2-4 lists the parameters configured to an M2M Enrolment Function for authenticating the Enrolment Target when the Enrolment Target is an M2M Authentication Function.

© OneM2MPartners

Table 9.2.2.2-4 The parameters configured to an M2M Enrolment Function for identifying and authenticating the Enrolment Target when the Enrolment Target is an M2M Authentication Function.

Parameter common to all Remote Provisioning Frameworks
MAF Trust Anchor Certificates

This specification assumes that Bootstrap Instruction Configuration of the M2M Enrolment Functions utilizes business logic of the Stakeholder that operates the M2M Enrolment Function, and the details are not described in this specification.

9.2.2.4 Bootstrap Instruction Configuration of UNSP Authentication Server

Table 9.2.2.4-1 lists the parameters configured to an Underlying Network Service Provider authentication server (e.g. HLR, HSS or AAA) during the Bootstrap Instruction Configuration phase of the GBA-Based Remote Security Provisioning Framework.

Table 9.2.2.4-1 Parameters configured to M2M Enrolment Functions during the Bootstrap Instruction Configuration phase of the GBA-Based Remote Security Provisioning Framework.

Parameter	Mandatory /Optional for all Remote Security Provisioning Frameworks
Enrolee's assigned CSE-ID or AE-ID	Mandatory
Enrolment Target Identifier (Enrolee B's CSE-ID or AE-ID, or MAF-ID)	Mandatory

The Bootstrap Instruction Configuration of the Underlying Network Service Provider authentication server is achieved by updating the GBA User Security Settings (GUSS) (3GPP TS 33.220 [13]) of the User Equipment (UE) upon which the Enrolee is executed. This specification assumes that this Bootstrap Instruction Configuration utilizes business logic of the Underlying Network Service Provider, and the details are not described in this specification.

10 Protocol and Algorithm Details

10.1 Certificate-Based Security Framework Details

10.1.1 Certificate Profiles

NOTE: These certificate profiles are compliant with the CoAP specification RFC 7252 [38].

10.1.1.1 Common Certificate Details

All certificates shall conform to the following profile:

- Certificates shall conform to RFC 5280 [34].
- The certificate shall include a SubjectPublicKeyInfo that indicates an algorithm of id-ecPublicKey with namedCurves secp256r1 [34]; this curve is equivalent to the NIST P-256 curve [39].
- The public key format shall be uncompressed [46].
- The hash algorithm shall be SHA-256.
- The key usage extension shall be included and shall indicate at least digitalSignature.

10.1.1.2 Raw Public Key Certificate Profile

Raw public key certificates shall conform to clause 10.1.1.1 "Common Certificate Details" and RFC 7250 [37].

© OneM2MPartners

10.1.1.3 Details Common to Certificates with Certificate Chains

Certificates with Certificate Chains shall conform to the following description:

- These certificates shall conform to clause 10.1.1.1 “Common Certificate Details”.
- Certificates shall be signed with ECDSA using secp256r1, and the signature shall use SHA-256.
- Certificate chains should limit the number of intermediate CA certificates to avoid having a negative impact in constrained environments.

10.1.1.4 Profile for Device Certificates and their Certificate Chains

10.1.1.4.1 Profile for Device Certificates

Device certificates shall conform to the following description:

- Device certificates shall conform to clause 10.1.1.3 “Details Common to the Certificates with Certificate Chains”.
- The subjectAltName extension of device certificates shall include one or more globally unique hardware instance identifiers.

Example. Annex H “Object Identifier Based M2M Device Identifier” TS-0001 [1] defines an object identifier -based M2M Device ID that can be used for providing a one or more globally unique hardware instance identifier. An object identifier -based M2M Device ID can be representing in an otherName field in the subjectAltName extension, where:

- otherName “type-ID” component is set to the M2M Device Indication ID (Annex H.2.1 “M2M Device Indication ID” TS-0001 [1]) arc of the object identifier M2M Device ID, and
- The otherName “value” component is set to the remainder of the object identifier M2M Device ID: Manufacturer ID arc, Model ID arc, Serial Number ID arc and optional Expanded ID arc (see Annex H.2 “OID Based M2M Device Identifier” TS-0001 [1])

NOTE: Providing the Model ID as part of the M2M Device ID can have privacy implications in some scenarios.

10.1.1.4.2 Profile for Certificate Authority Certificates for Device Certificates

Certificate Authority Certificates in the certificate chain for a device certificate shall conform to the following description:

- These certificates shall conform to clause 10.1.1.3 “Details Common to the Certificates with Certificate Chains”.
- Certificate Authority Certificates for device certificates are recommended to use the name constraints extension (see clause 4.2.1.10 “Name Constraints” of RFC 5280 [34]) to constrain the globally unique hardware instance identifiers in subsequent device certificates in a certification path.

Example. Name constraints are defined in terms of permitted or excluded name subtrees. Subtrees of an object identifier based M2M Device ID name space are represented by an otherName field with

- “type-ID” set to the M2M Device Indication ID (Annex H.2.1 “M2M Device Indication ID” TS-0001 [1]) arc of the applicable object identifier M2M Device ID name space, and
- “value” set to set to the remainder of the object identifier identifying the subtree.

10.1.1.5 Profile for CSE-ID Certificates, AE-ID Certificates and their Certificate Chains

CSE-ID certificates and AE-ID certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 “Details Common to Certificates with Certificate Chains”.

The full URI representation of the CSE-ID or AE-ID shall be included in the subjectAltName extension.

© OneM2MPartners

The certificate used to sign the CSE-ID certificates and AE-ID certificate shall include nameConstraints satisfied by the hostname part of the full URI representation of the CSE-ID or AE-ID.

CSE-ID certificates and AE-ID certificates shall not include wildcards.

10.1.1.6 Profile for FQDN Certificates and their Certificate Chains

FQDN Certificates and all other certificates in the corresponding certificate chain shall conform to clause 10.1.1.3 “Details Common to Certificates with Certificate Chains”.

An FQDN Certificate shall include the FQDN of the subject M2M Enrolment Function or M2M Authentication Function in the subjectAltName extension.

FQDN Certificates shall not include wildcards.

10.1.2 Public Key Identifiers

The public key identifier for a raw public key certificate shall calculated as described in Section 2 of RFC 6920 [40] using the SHA-256 hash algorithm. The public key identifier shall be generated using one of the sha-256-120, sha-256-128 or sha-256 hash algorithms specified in RFC 6920 [40].

It is recommended that the public key identifier be as long as practical within the deployment constraints.

The trusted public key identifier (received during Association Configuration or Bootstrap Instruction Configuration) is matched against the raw public key certificate (received during the Security Handshake) using the following procedure:

1. A check digest value is computed according to Section 2 of RFC 6920 [40] using the hash algorithm identified in the trusted public key identifier.
2. The check digest value is compared against the digest value encoded in the trusted public key identifier. If the values are identical then the raw public key certificate matches the trusted public key identifier. Otherwise, the raw public key certificate does not match the trusted public key identifier.

10.1.3 Support Requirements for each Public Key Certificate Flavour

Table 10.1.3 lists, for each of the various types of entity (Field Domain CSE, Field Domain AE, IN-CSE, IN-AE, M2M Authentication Function and M2M Enrolment Function), the flavour of certificate that may be issued to the entity and the flavour of other entity’s certificates that the entity is required to be able to process. . In this table “O” indicates optional, “M” indicates Mandatory, “CA” indicates that the option is required if the entity supporting the certificate-based security association establishment framework, “CB” indicates conditional on the entity supporting certificate-based Remote Security Provisioning framework.

Table 10.1.3-1 Applicability of certificate flavours issued to an entity and flavours of other entity’s certificates that the entity is required to be able to process.

Entity	Flavour of certificate may be issued to entity					Flavour of other entity’s certificates that the entity is recommended to be able to process.				
	Raw	Device	CSE-ID	AE-ID	FQDN	Raw	Device	CSE-ID	AE-ID	FQDN
Field Domain CSE	O	O	O	-	-	CA	CA	CA	CA	CB
Field Domain AE	O	O	-	O	-	CA	CA	CA	-	CB
IN-CSE	O	-	O	-	-	CA	CA	CA	CA	-
IN-AE	O	-	-	O	-	CA	-	CA	-	-
MAF	-	-	-	-	M	-	-	-	-	M
MEF	-	-	-	-	M	CB	CB	-	-	M

Mutual authentication between remote management servers and remote management clients is not considered in the present document.

© OneM2MPartners

10.2 TLS and DTLS Details

10.2.1 TLS and DTLS Versions

Where TCP payloads are to be secured, TLS v1.2 [16] shall be used.

Where UDP payloads are to be secured, DTLS v1.2 [17] shall be used, noting that the DTLS v1.2 ciphersuites are identical to the TLS v1.2 ciphersuites.

Implementations shall support the Server Name Indication (SNI) to indicate their authority in the SNI HostName field as defined in Section 3 of RFC 6066 [44]. This is needed so that when a host that acts as a virtual server for multiple Authorities receives a new TLS or DTLS connection, it knows which keys to use for the TLS or DTLS session.

10.2.2 TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks

The following Security Association Establishment Frameworks:

- Pre-Provisioned Symmetric Key Security Association Establishment Framework;
- MAF-Based Security Association Establishment Framework;
- GBA-Based Security Association Establishment Framework;
- Pre-Shared Key Remote Security Provisioning Framework;
- GBA-Based Remote Security Provisioning Framework;

shall use one of the key exchange algorithms defined in RFC 4279 [15]:

TLS implementations supporting these security frameworks shall implement at least the following TLS ciphersuite:

- TLS_PSK_WITH_AES_128_CBC_SHA256 (RFC 5487 [42]).

DTLS implementations supporting these security frameworks shall implement at least the following ciphersuites

- TLS_PSK_WITH_AES_128_CCM_8 (RFC 6655) [31].

The security considerations of Section 7 of RFC4279 [15] apply. In particular, applications should carefully weigh whether or not they need Perfect Forward Secrecy (PFS) and select an appropriate ciphersuite (Section 7.1 of RFC4279 [15]).

10.2.3 TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks

The following Security Frameworks:

- Certificate-Based Security Association Establishment Framework:
- Certificate-Based Security Bootstrap Framework;

shall use the standard TLS handshake (RFC 5246 [16]) with the ECDHE_ECDSA Key Exchange (RFC4492 [43]).

TLS implementations supporting these security frameworks shall implement at least the following ciphersuite:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, (RFC 5289) [32].

DTLS implementations supporting these security frameworks shall implement at least the following TLS ciphersuite:

- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8, RFC 7251 [45]

Implementations supporting these security frameworks shall support authenticating other entities using all available public key certificate flavours (see clause 8.1.1.2.1 “Public Key Certificate Flavours”)

© OneM2MPartners

- Raw public key certificate: using the mechanism specified in RFC 7250 [37], Implementation shall support receiving and processing raw public keys compliant with Section 9.1.3.2 “Raw Public Key Certificates” in RFC 7252 [38].

- All other certificates: X.509 certificates including device hardware identifier. Implementation shall support receiving and processing raw public keys compliant with Section 9.1.3.3 “X.509 Certificates” in RFC 7252 [38].

10.3 Direct Security Bootstrap Framework Algorithm Details

10.3.1 TLS Key Export Details

Following successful TLS authentication between the Enrolee and M2M Enrolment Function, the Enrolment Key (Ke) and RelativeKeId are generated from the (D)TLS session secrets by the Enrolee and M2M Enrolment Function by applying TLS Key Export (RFC 5705) [18] using the label “EXPORTER-oneM2M-Bootstrap” and length 48. The Enrolment Key (Ke) is set to the value of the 32 least significant bytes, while RelativeKeId is set to the value of the 16 most significant bytes.

10.3.2 Derivation of Master Credential from Enrolment Key

This clause describes the details when generating a Master Credential (Km) from an Enrolment Key (Ke) in Security Bootstrap Frameworks.

The following information shall be used when generating Km from Ke:

- The value of the Enrolment Key (Ke);

- The M2M Authentication Function Identifier (MAF-ID) shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19] and apply Normalization Form KC (NFKC) as specified in [20].

The value of Km shall be generated as

Km := HMAC-SHA-256(Ke, “oneM2M Enrolment Key to Master Credential derivation” || MAF-ID),

where HMAC-SHA-256 is defined in RFC 2014 [33].

10.3.3 Derivation of Provisioned Secure Connection Key from Enrolment Key

This clause describes the details when generating a Provisioned Secure Connection Key (Kpsa) from an Enrolment Key (Ke) in Remote Provisioning Frameworks.

The following information shall be used when generating Kpsa from Ke:

- The value of the Enrolment Key (Ke);

- Enrolee B’s CSE-ID or AE-ID (Enrolee-B-ID), which shall be encoded to an octet string according to UTF-8 encoding rules as specified in IETF RFC 3629 [19] and apply Normalization Form KC (NFKC) as specified in [20].

The value of Kpsa shall be generated as

Kpsa := HMAC-SHA-256(Ke, “oneM2M Enrolment Key to Provisioned Secure Connection Key derivation” || Enrolee-B-ID),

where HMAC-SHA-256 is defined in RFC 2014 [33].

© OneM2MPartners

10.3.4 Generating KeId

The KeId value shall be formed as

KeId = base64encode(RelativeKeId)@MEF_FQDN,

where

- base64encode(RelativeKeId) denotes the base64 encoding (RFC 3548 [41]) of the value of RelativeKeId, and
- MEF_FQDN denotes the FQDN of the M2M Enrolment Function.

Annex A (informative): Mapping of 3GPP GBA terminology

Table A.1 provides a mapping of terminology and abbreviations used in GBA according to 3GPP specification [13] to corresponding oneM2M terminology and abbreviations as used within the present document.

Table A.1

GBA entities, keys and processes	oneM2M Security Bootstrap entities, keys & processes
UE	Enrolee
BSF	MEF
NAF	MAF
Bootstrapping Procedure	**Bootstrap Security Handshake + Temporary Enrolment Key Generation**
Ks	Ke
B-TID	KeId
Bootstrapping Usage Procedure	**Usage in Centralized Key Distribution Server Handshake**
NAF FQDN	IdMAF
Ks_(ext/int)_NAF	Km (Master Credential)

© OneM2MPartners

Annex B (informative): General Mutual Authentication Mechanism

oneM2M mutual authentication schemes allow oneM2M entities to prove that they know related credentials such as Master Credentials, without having to exchange value of those credentials, and sensitive data such as security identities and security identifiers. To prevent reading and copying of credentials, a secure environment within the Security CSF provides protection against tampering of those credentials and related processed information.

A general mutual authentication protocol is applied to both symmetric and asymmetric key based schemes. Precise protocol messages and parameters depend on the chosen scheme and the security parameters selected. Typically it consists of following steps as shown in figure B.1.

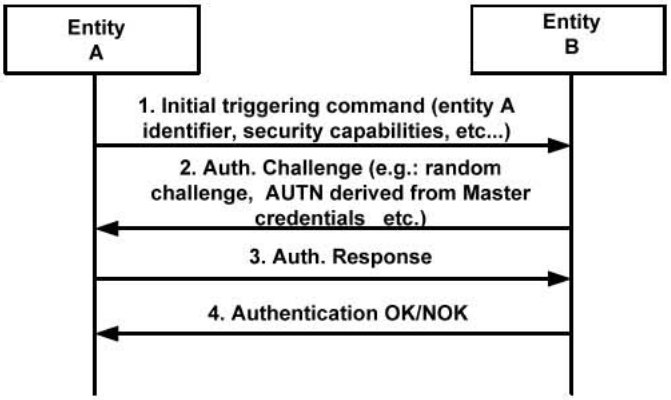


Figure B.1: Mutual Authentication

1. An initial step where an entity A is securely identified to an entity B with whom previous or no previous contact has been made. In this step entity A identifies itself to an entity B protected against eavesdropping, i.e. no exchange of key materials (Master Credentials).

2. In the second step entity B sends a challenge to entity A. The Authentication Challenge consists of a challenge, the authentication token (AUTN) of entity B derived from Master Credentials, etc. The authentication challenge, which may be random or not, depends on the chosen authentication scheme and the security parameters selected for symmetric and asymmetric key based schemes.

3. Entity A replies with an Authentication Response that contains an authentication token (AUTN) derived from its known Master Credentials and the received Authentication Challenge. This Authentication Response is sent if entity B has been successfully authenticated by entity A.

4. Entity B then verifies the relation between entity A's identity and the response received in step 3,. If the verification is positive, entity B is assured that the response has been created by entity A using a secret associated with entity A's identity provided in step 1.

© OneM2MPartners

B.1. Group Authentication

The oneM2M transactions may naturally involve groups of M2M entities rather than individual ones. A number of entities are classified as a group due to their proximate locations, having the same features, belonging to the same owner, or any other reasons [i.10]. To get services, all entities in such a group should be authenticated first. The traditional authentication mechanism has two main solutions, the first authentication mechanism is that the service provider authenticates each entity in the group one by one; the second authentication mechanism is that each entity makes mutual authentication with a group agent, then the group agent makes mutual authentication with the service provider. If the first authentication mechanism is used, the resulting authentication overheads of computation and communication may be too high to afford. If the second authentication mechanism is used, it has the following security weaknesses:

a) It may exist the man-in-the-middle attack by the group agent: The group agent would be placed in unsecure place or owned by different provider rather than the service provider. If the group agent is compromised or lie to service provider, group agent would act as a middle attacker to make fake authentication to entities and report fake identity to service provider since there is no direct authentication from service provider to each M2M entity.

b) Privacy concern: All information from M2M entities is transferred through the group agent, and the group agent knows all information generated by each entity. Based on security consideration, if the group agent is owned by different owner other than the entities' and service providers' owner, the group agent should not get the message.

Hence, the M2M entities (e.g., ASN or ADN) with the same feature can utilize group authentication to service provider (e.g., infrastructure node) in order to provide end-to-end secure tunnel as well as reducing the communication overhead.

Annex C (informative): Security protocols associated to specific SE technologies

The Secure Environment supporting security functions specified by oneM2M provides a level and a type of protection (e .g. integrity protection, confidentiality, tamper resistance) to the information it contains, independently of the method of protection (e.g. UICC, embedded security element, TEE, etc..). Administration of their content is implementation dependent and relies on existing standards within specific Secure Environment technologies. Some of them are listed below for information:

C.1 UICC

In case of UICC (SE compliant with ETSI TS 102 671 [23]), OTA mechanisms as specified in [7] and [8], and its extensions [9], [10] for 3GPP underlying networks or [11] and [12] for 3GPP2 underlying networks are used to securely administrate the sensitive data of the M2M Service Layer. UICC provides the highest protection level 3 against attacks according the Classification of Protection levels Table 6.2.1-1 in clause 6.2.1.

C.2 Other secure element and embedded secure element with ISO 7816 interface

In case the Secure Environment is implemented as a security element or as an embedded security element supporting an ISO/IEC 7816 interface [26], example of remote administration can be according to GlobalPlatform Remote Administration [a]. An embedded secure element provides the highest protection level 3 against attacks according the Classification of Protection levels Table 6.2.1-1 in clause 6.2.1.

C.3 Trusted Execution Environment

In case the secure environment is implemented as a Trusted Execution Environment (TEE) according to GlobalPlatform [b], remote administration is provided according to GlobalPlatform Remote Administration [21]. TEE provides the medium protection level 2 against attacks according the Classification of Protection levels Table 6.2.1-1 in clause 6.2.1.

© OneM2MPartners

C.4 SE to CSE binding

In case the SE is implemented as an independent security element supporting ETSI TS 102 221 [24], the secure channel specified in ETSI TS 102 484 [25] provides logical binding of the SE to a specific CSE or AE. This also protects the information exhanged between the SE and the associated entity on physically exposed interfaces, and is therefore recommended for devices that are physically exposed to attackers.

Annex D (normative): UICC security framework to support oneM2M Services

This annex is applicable when UICC (a type of Independent Security Element compliant with ETSI TS 102 221 [24] and ETSI TS 102 671 [23]) is involved in M2M service layer security, whether it only serves as a mean to pre-provision M2M Service layer material in M2M Devices/Gateways, or it is further used as Secured Environment in an M2M Device/Gateway.

Specifically, the involvement of UICC in oneM2M security may include any of the following steps:

- Pre-provisioning of initial credentials in M2M nodes by any of the following methods:
  - simple pre-provisioning and administration of M2M Service material (initial credentials and other pre-provisioned parameters), i.e. UICC-based M2M service provisioning;
  - support for infrastructure assisted bootstrapping of the M2M symmetric credentials by derivation from symmetric Access Network credentials stored in the UICC, using GBA.
- Derivation of a security association key directly derived from symmetric Access Network Credentials, using GBA. Note that this process can be supported by a Network Access Application on the UICC independently of the presence of the information structure specified in the present annex.

The support of UICC provisioning of M2M service subscription information shall be indicated in the M2M Service Table for the corresponding M2M Service Subscription as specified in the present annex.

The support of key derivation using GBA that may be used for bootstrapping or security association shall always be indicated in the Service Table of the UICC application of the Access Network Operator supporting the GBA infrastructure.

At the most basic level, UICC-based M2M pre-provisioning requires an interoperable framework to store and administrate related information in the UICC. Further involvement requires a framework for discovery of available services offered by the UICC for the hosting M2M field node. The purpose of the present annex is to specify this framework, which enables both initial service provisioning and remote security administration of the subscription information during the subscription lifetime.

A common scenario is where an M2M field node holds a UICC application protecting Access Network security credentials, and these credentials are used to derive M2M Service Layer security credentials used for M2M service bootstrapping or security association establishment in the service layer . As these scenarios require a trust agreement between the involved Access Network operator and M2M Service Provider, UICC support for M2M services in such situation shall be handled within the context of the associated Network Access application on the UICC. In particular, the UICC support for M2M credentials derivation using GBA shall be indicated within the UICC application of the Access Network operator. This is specified in clause D.1.

Even when the M2M Service Layer credentials are not derived from Access Network Credentials, the UICC may be used as a secure environment that securely protects the symmetric or asymmetric credential used to root security in an M2M field node. In such cases, the M2M subscription information and related methods constitute an independent application that resides on a UICC, in the sense of ETSI TS 102 221 [24]. In particular, ETSI TS 102 221 [24] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure.

NOTE: A terminal in the sense of TS ETSI 102 221 [24] is the part of the M2M field node that holds the UICC, e.g. a communication modem or an M2M Node processing environment.

© OneM2MPartners

The specific properties of the M2M Service Provider Identity Module application holding symmetric credentials is specified in clause D.2.

The storage of M2M information elements in the UICC and the procedures used for communication between the hosting M2M field node and the UICC shall be as specified in the present annex. The present annex uses abbreviations and coding conventions defined in ETSI TS 102 221 [24].

D.1 Access Network UICC-based oneM2M Service Framework

D.1.1 Access Network UICC-based oneM2M Service Framework characteristics

An Access Network UICC-based oneM2M Service Framework is always associated with a single M2M Service Subscription and consists of a single DF, DF_{1M2M}, complying with the specifications in D.1.3, implemented in the ADF of a Network Access Application on the UICC. This situation addresses the case where a trust relationship has been established between the M2M SP and the AN operator owning the hosting ADF.

NOTE 1: This does not necessarily imply that the Access Network credentials of the corresponding ADF are used to derive the M2M Service Layer Credentials: e.g. an Access Network operator may refuse derivation from Access Network credentials to an M2M Service Provider, but may still accept to provide space on its UICC to pre-provision independent credentials or support service infrastructure-assisted bootstrapping.

There may be several oneM2M service frameworks (DF_{1M2M}) within the ADF of a single Access Network subscription, in case this Access Network subscription is used by several independent M2M Service subscriptions. The file IDs of the DF_{1M2M} in any ADF shall be listed under the corresponding entry in EF_{DIR} as specified in D.1.2.

NOTE 2: A single M2M service layer subscription can also use multiple access networks: such subscriptions are best provisioned in a dedicated ADF as specified in clause D.2.

The content of any DF_{1M2M} in an Access Network application ADF shall be as specified in clause D.1.3.

D.1.2 M2M Service Framework discovery for Access Network UICC

When a UICC Network Access application supports one or more M2M Service subscription, with a DF_{1M2M}, the EF_{DIR} entry corresponding to this UICC Network Access Application shall contain the following M2M related Data Objects:

- oneM2M Service Framework DO: defining the association between the identifier of one M2M Service Subscription provisioned in the ADF and the related DF corresponding to this M2M subscription. Likewise, each M2M Service Subscription is associated to one DF. Each of these DFs is hereafter referred as DF_{1M2M}.

There shall be as many oneM2M Service Framework Data Objects as there are M2M Service Subscriptions provisioned in the ADF.

Table J.1: Coding of oneM2M related DOs

Bytes	Length	Description	Status
1	1	Discretionary template tag = '73'	M
2	1	Length of the discretionary template = X	M
3 to (2+X)	X	Discretionary Template	X

© OneM2MPartners

Table J.2: Coding of oneM2M Discretionary Template related DOs

Bytes	Length	Description	Status
1	1	oneM2M service specific data content tag = 'A2'	M
2	1	M2M service specific data content length = Y	M
3 to (2+Y)	Y	M2M service specific data content	M

Table J.3: Coding of oneM2M Service Specific Data Content related DOs

Bytes	Length	Description	Status
1	1	oneM2M supported service provisioning tag = '80'	M
2	1	Length of the M2M supported service provisioning tag = A	M
3 to 4	2	M2M Dedicated File Identifier for following M2M service subscription	M
5 to (A+2)	(A-2)	M2M Subscription Identifier	M

Coding:

- M2M Dedicated File identifier:
  - Contain the file identifier of the DF_{1M2M} associated to the provisioning of the M2M Service subscription identified in the DO.
- M2M Subscription Identifier:
  - The identifier of the M2M service subscription provisioned in the DF_{1M2M} indicated in the Data Object, encoded in binary format.

D.1.3 Content of files at the DF_{1M2M} level

This clause specifies the EFs for the M2M service provisioning specific to a single M2M service provider, defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

The file structure for DF_{1M2M} is illustrated in figure D.1:

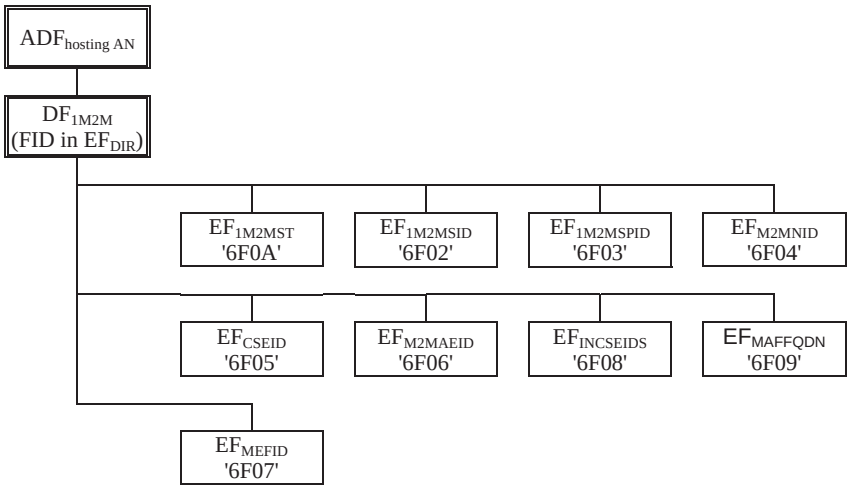


Figure D.1: File identifiers and directory structures of DF_{1M2M} in an hosting Access Network application ADF

© OneM2MPartners

D.1.3.1 EF_{1M2MST} (oneM2M Service Table)

This EF indicates which optional oneM2M services are available for the corresponding subscription. If a service is not indicated as available in the oneM2M DF, the hosting M2M field node shall not select this service. The presence of this file is mandatory if optional services are provided by the subscription.

Identifier: '6F0A'	Structure: transparent	Mandatory
SFI: '0A'		
File size: X bytes, X >= 1	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:		
	Service n°1:	Local CSE-ID provisioning
	Service n°2	IN-CSE-ID list provisioning
	Service n°3	MAF FQDN provisioning
	Service n°4	Local M2M AE-ID list provisioning
	Service n°5	Bootstrapping: MEF address provisioning
	Service n°6	M2M-Node-ID information
	Service n°7	GBA Secure Provisioning (see Note)
	Service n°8	GBA Secure Connection (see Note)

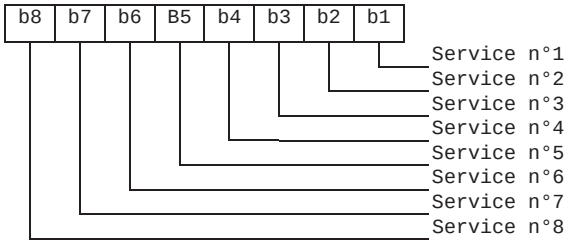
NOTE: Services n°7 and 8 can only be available in a oneM2M Service Table located in a DF_{1M2M} hosted in the ADF of the Network Access Application from which the M2M Service Layer credentials are expected to be derived.

The EF shall contain at least one byte. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. Coding:

1 bit is used to code each service:
bit = 1: service available;
bit = 0: service not available.

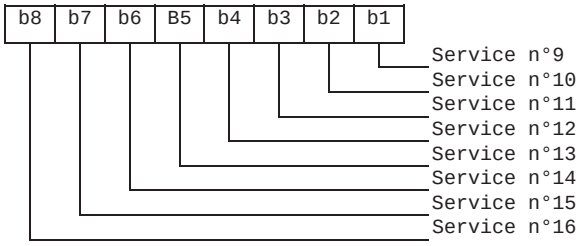
- Service available means that the M2M Service Subscription provisioned in the current DF or ADF has the capability to support the service and that the service is available for the user of the M2M Service Subscription.
  Service not available means that the service shall not be used by the M2M Service Subscription user, even if the M2M Service Subscription has the capability to support the service.

First byte:



© OneM2MPartners

Second byte:



etc.

D.1.3.2 $EF_{1M2MSID}$ (oneM2M Subscription Identifier)

This EF contains the oneM2M Subscription Identifier, M2M-Sub-ID. There shall be only one TLV object within this EF.

Identifier: '6F02'	Structure: transparent	Mandatory
SFI: '02'		
File size: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATEADM ACTIVATEADM		

Bytes	Description	M/O	Length
1	M2M Subscription Identifier TLV data object	M	X bytes

The M2M Subscription Identifier value field shall contain the M2M-Sub-ID encoded as specified in TS-0004 [4]. The tag value of the oneM2M Subscription Identifier TLV data object shall be '80'.

D.1.3.3 $EF_{1M2MSPID}$ (oneM2M Service Provider Identifier)

This EF contains the oneM2M Service Provider Identifier, M2M-SP-ID, of the M2M Service Provider related to the subscription in $EF_{1M2MSID}$. There shall be only one TLV object within this EF.

Identifier: '6F03'	Structure: transparent	Mandatory
SFI: '03'		
File size: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATEADM ACTIVATEADM		

Bytes	Description	M/O	Length
1	M2M-SP-ID TLV data object	M	X bytes

The M2M-SP-ID Value field shall contain the M2M-SP-ID encoded as specified in TS-0004 [TS0004]. The tag value of the M2M-SP-ID TLV data object shall be '80'.

© OneM2MPartners

D.1.3.4 EF_{M2MNID} (M2M Node Identifier)

This EF contains the M2M-Node-ID supporting the local CSE. It may be used to logically bind a UICC to a specific M2M Node. If service n°6 is "available", this file shall be present. There shall be only one TLV object within this EF.

Identifier: '6F04'	Structure: transparent	Optional
SFI: '04'		
File size: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATEADM ACTIVATEADM		

Bytes	Description	M/O	Length
1 to X	M2M-Node-ID TLV object	M	X bytes

The M2M-Node-ID Value field shall contain the M2M-Node-ID encoded as specified in TS-0004 [4].

D.1.3.5 EF_{CSEID} (local CSE Identifier)

This EF contains the local CSE Identifier, CSE-ID, for the M2M field node associated to the subscription in $EF_{1M2MSID}$. If present, this file is used by the M2M field node to pre-provision the CSE-ID. If service n°1 is "available", this file shall be present. There shall be only one TLV object within this EF.

Identifier: '6F05'	Structure: transparent	Optional
SFI: '05'		
File size: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATEADM ACTIVATEADM		

Bytes	Description	M/O	Length
1	CSE-ID TLV data object	M	X bytes

CSE-ID TLV

Contents:

- The CSE-ID Value field shall contain the local CSE-ID formatted as a URI.

Coding:

- The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in RFC 3629 [19]. The tag value of the URI TLV data object shall be '80'.

© OneM2MPartners

D.1.3.6 $EF_{M2MAE-ID}$ (M2M Application Identifiers list)

This EF contains the list of M2M Application Identifiers (AE-IDs) for the local M2M applications supported by the subscription in $EF_{1M2MSID}$. If service n°4 is "available", this file shall be present.

Identifier: '6F06'	Structure: Linear fixed	Optional
SFI: '06'		
Record length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATEADM ACTIVATEADM		

Bytes	Description	M/O	Length
1 to X	M2M AE-ID LV data object	M	X bytes

M2M AE-ID LV

Contents:

- The Value field shall contain the M2M AE-ID formatted as a URI.

Coding:

- TBD

- The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in RFC 3629 [19].

D.1.3.7 $EF_{INCSEIDS}$ (M2M IN-CSE IDs list)

This EF contains a list of pre-provisioned IN-CSE-ID used to determine the next point of contact after provisioning or M2M Service Bootstrapping. If service n°2 is "available", this file shall be present.

Identifier: '6F08'	Structure: Linear fixed	Optional
Record length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATEADM ACTIVATEADM		

Bytes	Description	M/O	Length
1 to X	IN-CSE-ID LV data object	M	X bytes

IN-CSE-ID LV

Contents:

- The Value field shall contain the IN-CSE-ID formatted as a URI

Coding:

- The URI shall be encoded to an octet string according to UTF-8 encoding rules as specified in RFC 3629 [19]

© OneM2MPartners

D.1.3.8 $EF_{MAFFQDN}$ (MAF-FQDN)

This EF is used to pre-provision the FQDN of the MAF to be used for M2M Service Connection after M2M Service Bootstrapping. If service n°3 is "available", this file shall be present. There shall be only one TLV object within this EF.

Identifier: '6F09'	Structure: Transparent	Optional
Length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	MAF FQDN TLV data object	M	X bytes

MAF FQDN

Contents:

- the FQDN address of the MAF

Coding:

- The MAF-FQDN shall be encoded to an octet string according to UTF-8 encoding rules as specified in RFC 3629 [19]. The tag value of the MAF FQDN TLV data object shall be '80'.

D.1.3.9 EF_{MEFID} (M2M Enrolment Function Identifier)

This EF contains one or more M2M Enrolment Function addresses. The first record in the EF shall be considered to be of the highest priority. The last record in the EF shall be considered to be the lowest priority. If service n°5 is "available", this file shall be present.

Identifier: '6F07'	Structure: linear fixed	Optional
Record length: X bytes	Update activity: low	
Access Conditions: READ ALW UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1 to X	MEF Address LV data object	M	X bytes

MEF Address LV data object

Contents:

- Address of MEF, in the format of a FQDN, an IPv4 address, or an IPv6 address.

Coding:

- The format of the data object is as follows:

Field	Length (bytes)
Length	1
Address Type	1
MEF Address	Address Length

© OneM2MPartners

- Address Type: Type of the MEF address.
  - This field shall be set to the type of the MEF address according to the following:

Value	Name
0x00	FQDN
0x01	IPv4
0x02	IPv6
All other values are reserved	

- MEF Address: Address of the M2M Service Bootstrap Function.
  - This field shall be set to the address of the M2M Enrolment Function. When the MEF type is set to 0x00, the corresponding MEF Address shall be encoded to an octet string according to UTF-8 encoding rules as specified in RFC 3629 [19].

Unused bytes shall be set to 'FF'.

D.2 oneM2M Service Module application for symmetric credentials on UICC (1M2MSM)

This clause defines the oneM2M Service Module (1M2MSM), an application used for oneM2M Service Layer security functionalities and subscription provisioning based on symmetric credentials. This application resides on the UICC, an IC card specified in ETSI TS 102 221 [24]. In particular, ETSI TS 102 221 [24] specifies the application independent properties of the UICC/terminal interface such as the physical characteristics and the logical structure. There may be several 1M2MSM ADFs on a single UICC, corresponding to independent oneM2M Service Subscriptions.

D.2.1 oneM2M Service Module application file structure

This clause specifies the EFs for the oneM2M service Layer defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity.

D.2.1.1 Content of UICC files at the Master File (MF) level

Files at the UICC MF level are application independent as specified in ETSI TS 102 221 [24]. Only the EF_{DIR} and EF_{ICCID} files are mandatory on UICC for the purpose of 1M2MSM applications. In any case all files shall be as specified in ETSI TS 102 221 [24].

D.2.1.2 Content of files at the 1M2MSM ADF (Application DF) level

The EFs in the 1M2MSM ADF contain oneM2M subscription related information that is required for M2M field nodes operating in an oneM2M environment. This ADF shall be selected using its AID and information in EF_{DIR}. The AID for 1M2MSM applications shall be constructed as specified in ETSI TS 101 220 [27].

NOTE: The ETSI RID can be used for oneM2M pending assignment of a oneM2M dedicated RID in ISO/IEC 7816-5 [i.13].

The File IDs '6F1X' (for EFs), '5F1X' and '5F2X' (for DFs) with X ranging from '0' to 'F' are reserved under the 1M2MSM ADF for administrative use by the card issuer.

The DF_{1M2M} substructure used to isolate the provisioning of network access dependent M2M service related information in a Network Access Application ADF is not needed for access network independent provisioning of an M2M service subscription in a 1M2MSM ADF. Therefore, all the EFs specified in clause D.1.3 shall be present at the 1M2MSM ADF level. The file structure of the ADF_{1M2MSM} is illustrated in figure D.2.

© OneM2MPartners

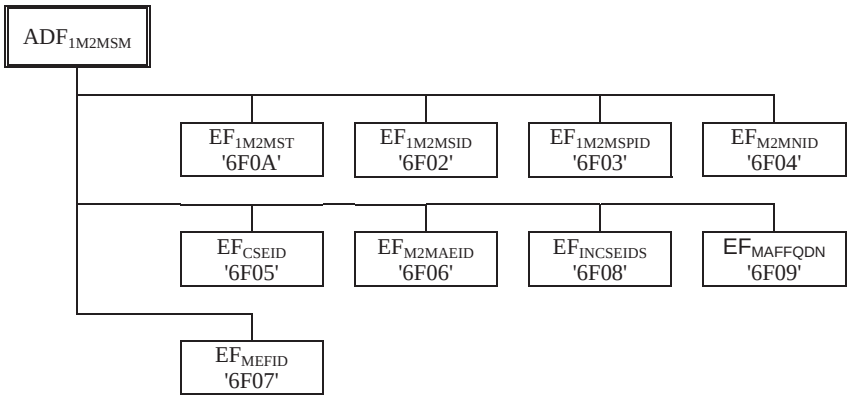


Figure D.2: File identifiers and directory structures of ADF_{1M2MSM}

D.2.2 oneM2M Subscription related procedures for M2M Service

This clause specifies the procedures that shall be executed by M2M field nodes to interact with a oneM2M Service Subscription on UICC. They are applicable independently of the file structure supporting the oneM2M Service Subscription (1M2MSM ADF or DF_{1M2M} under a Network Access Application ADF), unless otherwise indicated.

D.2.2.1 Initialization – 1M2MSM Application selection

This procedure only applies to an M2M subscription supported in a 1M2MSM ADF.

If the M2M field node wants to engage in M2M operation, then after UICC activation (see ETSI TS 102 221 [24]), the M2M field node shall select a 1M2MSM application, if a 1M2MSM application is listed in the EF_{DIR} file, using the SELECT by DF name as defined in ETSI TS 102 221 [24].

After a successful oneM2M application selection, the selected oneM2M AID is stored on the UICC. This application is referred to as the last selected 1M2MSM application. The last selected 1M2MSM application shall be available on the UICC after a deactivation followed by an activation of the UICC.

If a oneM2M application is selected using partial DF name, the partial DF name supplied in the command shall uniquely identify a 1M2MSM application. Furthermore if a 1M2M application is selected using a partial DF name as specified in ETSI TS 102 221 [24] indicating in the SELECT command the last occurrence, the UICC shall select the oneM2M application stored as the last oneM2M application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an application has not been previously selected in the same session and shall return an appropriate error code.

D.2.2.2 1M2MSM session termination

This procedure only applies to a oneM2M subscription supported in a 1M2MSM ADF.
The oneM2M UICC session is terminated by the M2M field node as follows:

- The M2M field node shall indicate to the oneM2M UICC application that the termination procedure is starting, by sending a particular STATUS command.
- Finally, the M2M field node deletes all the M2M subscription related information elements from its memory.
- To actually terminate the session, the M2M field node shall then use one of the mechanisms described in ETSI TS 102 221 [24].

D.2.2.3 oneM2M Service discovery procedure

This procedure is used to discover the oneM2M related services offered by a oneM2M UICC.

© OneM2MPartners

The M2M field node shall perform the reading procedure with EF_{1M2MST}. If no oneM2M related service is indicated as available, the M2M field node shall assume that only the provisioning of mandatory parameters is available in this ADF.

D.2.2.4 oneM2M Service provisioning procedures

These procedures are used by an M2M field node in order to bootstrap an M2M service subscription provisioned on the UICC.

The M2M field node shall perform the reading procedure with $EF_{1M2MSID}$ and $EF_{1M2MSPID,}$ and EF_{CSEID}, EF_{M2MNID}, $EF_{INCSEID}$, $EF_{MAFFQDN}$ according to available services indicated in EF_{1M2MST}.

D.2.2.5 oneM2M Application Identifiers provisioning procedure

This procedure provisions a list of M2M Application Identifiers that may be enabled on the M2M node in relation with the oneM2M Service Subscription.

Condition: Service number 4 shall be available in the oneM2M Service Table.

Under this condition, the M2M field node shall perform the reading procedure with $EF_{M2MAEID}$.

D.2.2.6 oneM2M Secure provisioning related procedures

These procedures are used by the M2M field node to perform M2M Secure Provisioning with the assistance of the UICC, depending on available services in EF_{1M2MST} and the supported AUTHENTICATE commands contexts (e.g. GBA support by a Network Access Application) indicated for the hosting ADF.

Secure Provisioning: MEF address Provisioning:

Condition: Service number 5 shall be available in the oneM2M Service Table.

Under this condition, the M2M field node shall perform the reading procedure with EF_{MEFID}, if the related service is available.

GBA Secure Provisioning:

This procedure is dependent on the Authentication Framework supported by the UICC and indicated in the Service Table of the hosting ADF.

After identifying the supported authentication framework, the M2M field node shall check availability of Service number 7 in EF_{1M2MST}: If the service is available, the D/G M2M Node shall perform GBA-related procedures with AUTHENTICATE - GBA security context (Bootstrapping Mode and Derivation Mode) with the parameters for GBA secure provisioning.

D.2.2.7 oneM2M Security Association related procedures

GBA secure connection:

This procedure is dependent on the Authentication Framework supported by the UICC and indicated in the Service Table of the hosting ADF.

After identifying the supported authentication framework, the M2M field node shall check availability of Service number 12 in EF_{1M2MST}: If the service is available, the M2M field node shall perform a GBA-related procedures with AUTHENTICATE - GBA security context (Bootstrapping Mode and Derivation Mode) with the parameters for GBA Security Association.

© OneM2MPartners

Annex E (informative): Precisions for the UICC framework to support M2M Services

The present annex provides further practical information related to the UICC framework for oneM2M described in annex D.

E.1 Suggested content of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'6F02'	1M2M Service Subscription Identifier	'8000FF…FF'
'6F03'	1M2M Service Provider Identifier	'8000FF…FF'
'6F04'	M2M Node Identifier	'8000FF…FF'
'6F05'	Local CSE Identifier	'8000FF...FF'
'6F06'	M2M Application Identifiers list	'00FF...FF' for each record
'6F07'	MEF Identifier	'00FF…FF' for each record
'6F08'	IN-CSE Identifiers list	'00FF...FF' for each record
'6F09'	MAF FQDN	'8000FF...FF'
'6F0A'	1M2M Service Table	Operator/Service Provider dependant

E.2 EF changes via Data Download or CAT applications

This clause defines if changing the content of an EF by the UICC OTA protocol or by a CAT Application is advisable. Updating of certain EFs "over the air" or "over the Internet" could result in unpredictable behaviour of the UE; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air / over the internet" changes of these EFs be considered.

File identification	Description	Change advised
'6F02'	1M2M Service Subscription Identifier	No
'6F03'	1M2M Service Provider Identifier	No
'6F04'	M2M Node Identifier	Caution
'6F05'	Local CSE Identifier	Caution
'6F06'	M2M Application Identifiers list	Caution
'6F07'	MEF Identifier	Caution
'6F08'	IN-CSE Identifiers list	Caution
'6F09'	MAF FQDN	Caution
'6F0A'	1M2M Service Table	Caution

E.3 List of SFI values at the ADF_{M2MSM} or DF_{M2M} level

File Identification	SFI	Description
'6F02'	'02'	M2M Service Subscription Identifier
'6F03'	'03'	M2M Service Provider Identifier
'6F04'	'04'	M2M Node Identifier
'6F05'	'05'	Local CSE Identifier
'6F06'	'06'	M2M Application Identifiers list
'6F0A'	'0A'	1M2M Service Table

All other SFI values are reserved for future use.

© OneM2MPartners

E.4 UICC related tags defined in annex J

Tag	Name of Data Element	Usage
'80'	MAF FQDN TLV data object	$EF_{MAFFQDN}$
'80'	M2M-Node-ID TLV Data Object	EF_{M2MNID}
'80'	Local CSE-ID TLV data object	EF_{CSEID}
'80'	M2M-SP-ID TLV data object	$EF_{1M2MSPID}$
'80'	M2M Subscription Identifier TLV data object	$EF_{1M2MSID}$
NOTE: The value 'FF' is an invalid tag value.		

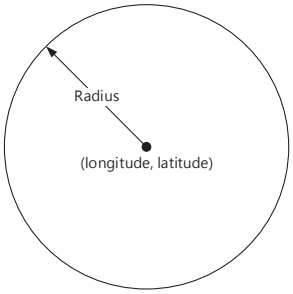
Annex F (normative): Acquisition of Location Information for Location based Access Control

When a request (resource access) is evaluated by a Hosting CSE and an *accessControlLocationRegions* parameter is defined in the *privileges* attribute of the <accessControlPolicy> resources, the Hosting CSE checks whether the location of the Originator of a request is in the specific regions or not. Therefore, the Hosting CSE retains the location of the Originator otherwise the Hosting CSE shall acquire the location or deny the access. This annex describes how to describe the location regions and obtain the location of the Originator.

F.1 Description of Region

F.1.1 Circular Description

The practical way of describing the region or area is the circular presentation and generally the circle is characterised by the co-ordinates of a center point of the circle and a radius. Geographically, the center point and radius is described as longitude and latitude, and meter respectively. For this description, the *accessControlLocationRegions* parameter shall be represented as a circle.



F.1.2 Country Description

Another simple way of describing the region or area is the country presentation. ISO-3166-1 alpha 2 codes [i.12] are two-letter country codes to represent countries and special regions of geographical interest. For example, KR is a code for Korea, Republic of.

F.2 Acquisition of Location Information

As mentioned above, when *accessControlLocationRegions* parameter is defined, the Hosting CSE shall check the location of the Originator for access control. This clause describes how the Hosting CSE checks or obtains the location. The procedures shall be varies based on the region description, circle and country.

© OneM2MPartners

F.2.1 Circular Description

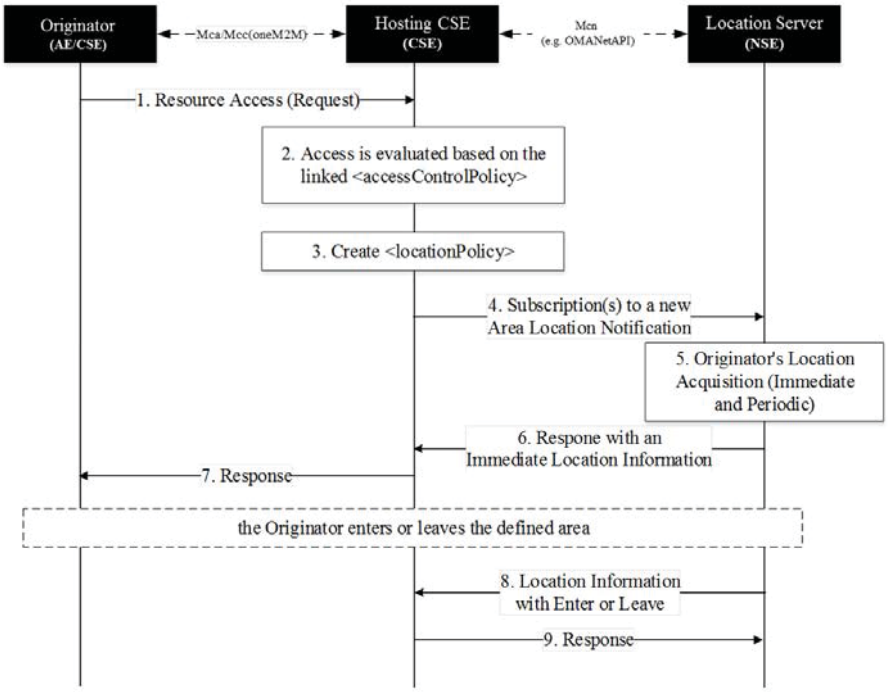
If the circular description is used as the location context constraints, the Hosting CSE shall check whether it has the current location of Originator or not. If not, it shall obtain the location of Originator. TS-0001[1] defines a resource type for acquisition of location of a Target Node, <locationPolicy>. In order to , therefore, obtain the location of Originator, the Hosting CSE shall create <locationPolicy> and set the relevant attributes as follows:

- ***locationSource*** : Reliability of the location information is crucial so the location shall be obtained from trusted network. If the location is obtained by the other sources, the location information can be easily masqueraded. (i.e. GPS spoofing). Therefore, the *locationSource* attribute shall be set to 'network-based'.
- ***locationTargetID* :** The Target Node shall be the Originator that needs to authorize the sent requests. The *locationTargetID* attribute shall be set to identifier of the Originator.

Note that the other attributes are determined by local policies of Hosting CSE as described in clause 9.6.9 of TS-0001 [1] and in order to obtain the location from the network, the Hosting CSE shall transform the oneM2M specified location request into network specified request.

NOTE: Refer to TS-0004 [4] that describes how to convert the oneM2M-specified request to 'OMA RESTful NetAPI for Terminal Location' specified request in clause annex F.

Since the region information (circular description) is defined by the *accessControlLocationRegions* parameter, the Hosting CSE can utilize the circular region information when it requests the location information from the network. OMA RESTful NetAPI for Terminal Location specification [i.11] specifies resource types as an area (region)-based location notification service, 'CircleNotificationSubscription'. If therefore the Hosting CSE subscribes to the notification service with circular region defined as *acccessControlLocationRegions* parameter, the Hosting CSE can always determine whether the Originator is in the regions or not. The figure below demonstrates how to acquire the location of the Originator when the *accessControlLocationRegions* parameter is defined.



1. The Originator sends a request to access a resource.

© OneM2MPartners

2. The Hosing CSE shall evaluate the received request against the linked <accessControlPolicy> resource. If one of rule tuples that is about the request originator contains the *accessControlLocationRegions* parameter (circular description) and the Hosting CSE does not store the location of the Originator, the Hosting CSE shall do either continue the next step or deny the access.
   If the Hosting CSE has the location of the Originator, it is used for applying access control policy.

   NOTE: The Hosting CSE shall deny the access due to the fact that the Originator is not subscriber of the network or any other reasons. (e.g., connection lost, server malfunction)

3. The Hosting CSE creates the <locationPolicy> resource and set relevant attributes as mentioned above.
4. The Hosting CSE subscribes to a new area location notification service toward Location Server in the Network. The area information shall be based on the area defined by the *accessControlLocationRegions* parameters. If the multiple regions are defined, the multiple subscriptions shall be set.
5. The Location Server immediately obtains the location's Originator.
   NOTE: After the immediate location acquisition, the Location Server periodically obtains the location's Originator to check whether the Originator is in the area or not. The frequency and duration can be defined by local policies.

6. The Location Server responses the immediate location information of the Originator toward Hosting CSE.
7. Based on the received location of the Originator and other access control policies the request can be either granted or denied. The Hosting CSE responses regarding the request (step 1).
8. When the Originator crossed in(enter) or out(leave) the area, the Location Server shall notify of the Hosting CSE the location change. Thus, the Hosting CSE can keep track of the location's Originator and easily evaluate the access against location context constraint.
9. The Hosting CSE response the notification.

F.2.2 Country Description

Generally, the Originator's country-scale location can be determined by the Originator's IP address. If the Hosting CSE can distinguish the country using the Originator's IP address and it is also matched with the defined *acccessControlLocationRegions* parameter, the Hosting CSE shall grant the request subject to the acceptance of the other access control policies. Note that how to transform the IP address into country is out of scope.

However, if Hosting CSE cannot distinguish the country using the Originator's IP address, The Hosting CSE shall obtain the location coordinate (i.e., longitude and latitude) of the Originator from network and the Hosting CSE can distinguish the country using the location if available. The way of obtaining the location coordinate is defined in annex F of TS-0004 [4]. Note that how to transform the location into country is out of scope.

Annex G (informative): Access Control Decision Request

An Access Control Decision Request as introduced in the Authorization Architecture in clause 6.2.2 is generated by a PEP according to an Originator's access request and extra information provided by the hosting CSE using the format specified by the PDP. The PEP can send the Access Control Decision Request to a PDP for an access control decision.

The PDP asks the PRP to retrieve all applicable access control policies according to the Access Control Decision Request, and then uses the Access Control Decision Request to evaluate the retrieved access control policies for an access control decision. An Access Control Decision Request from PEP to PDP can contain the following information:

- An Originator: It represents the ID of the Originator that sends an access request to the target resource.
- A Resource: It represents the URI of the target resource which the Originator wants to access.
- An Operation: It represents the operation which the Originator wants to perform on the target resource.

- An AccessTime: It represents the time of access.
- A LocationRegion: It represents the location of the Originator.
- An IPAddress: It represents the IP Address of the Originator.

The URI of the target resource is used to locate the target resource and then find the associated access control policies.

The ID of Originator is used to compare with the rule component subjects in order to check if a rule is applicable to the Access Control Decision Request.

The operation is used to compare with the rule component operations in order to check if the operation is permitted by the rule.

The AccessTime, LocationRegion and/or LocationRegion are used to check the rule component contexts in order to ensure some extra conditions are satisfied to using the rule for making an access control decision.

© OneM2MPartners

History

Draft history (to be removed on publication)		
V.0.0.0	07 Aug 2013	Initial version agreed at SEC#4 in oneM2M-SEC-2013-0026R01-Skeleton_TS_Security_Solutions
V0.1.0	18 Oct 2013	Incorporates following contributions agreed at SEC 7.0: oneM2M-SEC-2013-0041R01-SecurityCSF_Architecture oneM2M-SEC-2013-0044R04-Network-based_bootstrap oneM2M-SEC-2013-0050R03-PKI-Based_Post_Provisioning oneM2M-SEC-2013-0051R01-secure_remote_administration
V0.2.0	21 Jan 2014	Incorporates following contributions agreed at SEC 8.0: oneM2M-SEC-2013-0066R01-Bootstrapping_Definition oneM2M-SEC-2013-0070R03-GBA_framework oneM2M-SEC-2013-0073R04-Security_CSF_Architecture_Figure oneM2M-SEC-2013-0075R01-Clean_up_Security_TS
V0.3.0	25 Mar 2014	Incorporates following contributions agreed at SEC 9.0: SEC-2014-0044R03-SEC_CSF_Architecture_Figure_Update_for_Security_TS SEC-2014-0045R02-SEC_CSF_Authorization_Description_Update_for_Security_TS SEC-2014-0055R04-MAS_and_MTF_description
V0.4.0	15 Apr 2014	Incorporates following contributions agreed at SEC 10.0: SEC-2014-0240R02-SEC_CSF_Authorization_Procedure_for_Security_TS SEC-2014-0241R03-SEC_CSF_Architecture_General_Description_for_Security_TS SEC-2014-0259R01-Credentials_definitions SEC-2014-0260R01-Credentials_abbreviations SEC-2014-0243R03-Overview_of_Security_Frameworks SEC-2014-0242R03-Certificate-Based_Security_Framework_Common_Details

© OneM2MPartners

Draft history (to be removed on publication)		
		SEC-2014-0247R03-Overview_of_Security_Bootstrap_Frameworks SEC-2014-0244R04-Certificate-Based_Security_Bootstrap_Framework SEC-2014-0252R03-Pre-Provisioned_Symmetric_Enrolee_Key_Security_Bootstrap_Framework SEC-2014-0224R07-Overview_of_Security_Association_Establishment_Frameworks SEC-2014-0227R05-Certificate-Based_Security_Association_Establishment_Framework SEC-2014-0226R05-Pre-Provisioned_Symmetric_Association_Key_Framework SEC-2014-0254R02-Precisions_on_M2M_Trust_Functions SEC-2014-0239R01-Clarifications_to_TS-0003 Following actions have been resolved and changes incorporated into this version of the document: A-WG4-TP10_006: extract table from document SEC-2014-0263-Temporary_Enrolment_Key_Terminology and add to TS 0003 as an informative Annex A-WG4-TP10_A02: make the necessary alignments regarding "Master Credential" when integrating the agreed contributions into the TS Several editorial corrections incorporated.
V0.5.0	02 June 2014	Incorporates following documents agreed during conference calls SEC-2014-0288R01-TS0003_V0_4_0_CSFcleanup SEC-2014-0277R03-cleanup_TS0003_clause8 SEC-2014-0249R05-General_Mutual_Authentication_Mechanism SEC-2014-0285R05-AccessControlPolicy_Processing_Summary

© OneM2MPartners

Draft history (to be removed on publication)		
V0.6.0	23 June 2014	Incorporates following contributions agreed at SEC 11.0: SEC-2014-0274R03-SA_Security_Association SEC-2014-0276R05-Remote_Admin_Clarification SEC-2014-0308R01-Clause_9_1_1_Credential_Configuration SEC-2014-0309R02-Clause_9_1_2_Association_Configuration SEC-2014-0310R02-Clause_9_2_1_Bootstrap_Credential_Configuration SEC-2014-0311R02-Clause_9_2_2_Bootstrap_Instruction_Configuration SEC-2014-0313R03-Group_Authentication_Necessity_for_Security_TS SEC-2014-0320-GBA-based_Security_Bootstrap SEC-2014-0329R02-SE_pre-provisioning_framework SEC-2014-0330R01-Completion_of_generic_description_of_GBA SEC-2014-0332R03-Stage3_GBA-based_Security_Association SEC-2014-0338-MAF-based_Security_Association SEC-2014-0340R01-Centralized_Key_Distribution_Server_Handshake_in_Security_Association SEC-2014-0342-Cleaned-up_baseline_for_R1_freeze Note: SEC-2014-0299-Identity_Protection_Description_for_Security_TS was agreed to be incorporated into the next release of the specification. It is therefore not yet implemented in this version of the document.

© OneM2MPartners

Draft history (to be removed on publication)		
V0.7.0	29 July 2014	Incorporates following changes agreed by email correspondence: SEC-2014-0302R02-Clause_10_2_TLS_and_DTLS_Details SEC-2014-0303R02-Clause_10_3_Direct_Security_Bootstrap_Framework_Algorithm_Details In addition following contributions agreed at SEC 12.0 are integrated: SEC-2014-0328R03-Request_for_Changing_the_Text_of_SEC-2014-0249R05 SEC-2014-0356-TS-0003_CR_on_Definitions SEC-2014-0357R03-TS-0003_CR_updating_Annex_D_SE_Provisioning SEC-2014-0358-TS-0003_CR_Informative_Annex_on_SE_provisioning SEC-2014-0362R05-AccessControl_clarifications SEC-2014-0363R01-Configuration_of_Protection_levels SEC-2014-0364R03-Security_Considerations_on_AE SEC-2014-0365R02-oneM2M_Access_Control_Decision_Request_for_Annex SEC-2014-0366R03-Acquisition_of_Location_Information_for_Location_based_Access_Control SEC-2014-0367R01-Proposal_for_Changing_PAP_to_PRP SEC-2014-0368R06-TS-0003_Clause_8_1_etc_Certificate_Text_CR SEC-2014-0371R02-Clause_6_cleanup_CR SEC-2014-0373R02-TS-0003_Clause_10_2_TLS_and_DTLS_Details_Update SEC-2014-0377R01-GBA_missing_references SEC-2014-0378-TS-0003_CR_to_complete_Action_Items_on_8_1 SEC-2014-0379R01-TS-0003_CR_changing_MEF_bootstrap_classification SEC-2014-0380R01-TS-0003_CR_generalizing_purpose_of_MEF_bootstrap_scenario SEC-2014-0384-TS-0003_CR_Clause_617_cleanup SEC-2014-0385R03-Integrated_introductory_clause_from_0359_0382_0371 SEC-2014-0386R03-TS-0003_Clause_3_Updated_Definitions_CR SEC-2014-0387R01-TS-0003_Clause_8_2_etc_Security_Association_Cleanup_CR SEC-2014-0388R02-TS-0003_Clause_8_3_etc_Remote_Provisioning_Cleanup_CR SEC-2014-0389R02-TS-0003_Clause_9_1_cleanup_CR SEC-2014-0390R03-TS-0003_Clause_9_2_cleanup_CR SEC-2014-0393R02-TS-0003_Clause_10_3_Remote_Provisioning_Details_CR

© OneM2MPartners

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 76

AT&T BLOWS AWAY CONNECTED DEVICE NUMBERS IN Q3

October 22, 2014 Kathryn Lawhon

BY JAMES BREHM & KATHRYN LAWHON

The machine-to-machine connections that AT&T added this quarter will make your jaw drop. This afternoon, AT&T released that 1.275 million connected devices have been added to their overall number, making them stand out among many carriers. We believe that this is the first million-device quarter outside of China.

This marks a watershed moment in the IoT space as the number of new connected devices outgrew the 1.2 million new postpaid mobile smartphones that were added. A huge portion of this can be attributed to AT&T's strategy around the connected car with over 500,000 net additions. This number points to a host of other connected devices, creating new possibilities in the Internet of Things.

We believe that this number from AT&T is three or four times that of the competition. AT&T takes the cake this quarter- no questions asked.

Copyright 2014 / All Rights Reserved

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 77

AT&T increases business velocity with machine-to-machine solutions

SERVICES MANAGEMENT

1 Farming Site
- Preventative maintenance
- Firmware upgrades
- Precision planting
- Irrigation management

2 Construction
- Job site connectivity (hot spot with heavy machinery)
- Tracking/location of assets
- Job site connectivity: workers/mobile devices
- Heavy machinery maintenance
- Field data collection

3 HVAC System
- Predictive maintenance
- Remote monitoring and control
- Manage temperature, environmental factors
- Automate service ticket generation
- Consumables management

4 Chemical Tanks
- Monitor tank levels (liquid, solid, gas)
- Mesh networks
- Automatic refill
- Fleet integration
- Flow, level, proximity sensors
- Waste flow disposal

TRANSPORTATION

1 Railroad (freight and passenger)
- Positive Train Control
- Wayside Track Monitoring
- Locomotive Telemetry
- Maintenance of Way
- eTicketing
- Passenger Information Systems
- Safety and Security

2 Automotive telematics
- Safety and Security
- Vehicle Maintenance History
- Trouble Code Notices
- Usage Based Insurance
- Location of Vehicles
- Driver behavior
- Idle-time management

3 Fleet Management
- Fleet Monitoring of location and delivery scheduling
- Improve regulatory compliance
- Improve Drive efficiencies
- Dynamic routing
- Driver Behavior scoring

CONNECTED MEDICAL DEVICES

1 Large Asset Management
Medical asset status and management
- Reduced downtime/ Improved customer satisfaction
- Proactive /preventative maintenance
- Reduced field service trips

Improved efficiency in Consumables replenishment
Infrastructure independence for faster installations; avoid hospital/clinic WAN integration issues; facilitate post-sale diagnostics and maintenance.

2 Small Portable Connected Medical Devices
Post acute care monitoring of surgical patients to proactively detect problems that could lead to costly readmission.

3 Chronic Disease Management
Monitoring of patients with chronic diseases
- Increased compliance
- Improved clinical outcomes
- Reduce likelihood of disease state becoming more acute

4 Aging In Place
Helping aging population to have independence but still be connected to care providers
- Fall detection
- Wandering prevention

ASSET MANAGEMENT

1 Agriculture
- Machine maintenance reporting
- Yield production information
- Grain Silo levels
- Precision planting
- Irrigation management

2 Well-head Pressure Monitoring
- Oil flow
- Well pressure
- Status of pump
- Remote Maintenance
- Environmental systems integration
- Pipeline/flow monitoring
- Tool/inventory status

3 Global Asset Tracking/Management
- Vehicle Fleet management
- Tracking of high value assets
- Tracking/location of all assets (small, medium, large)
- Monitor asset fuel consumption, maintenance, diagnostics
- Asset Optimization
- Remote Monitoring and Control
- High Value Cargo Security
- Real Time Asset Visibility

4 Construction
- Tracking/location of assets
- Fleet Management
- Job site connectivity: workers/mobile devices
- Heavy machinery maintenance
- Monitor assets - location, fuel consumption, maintenance
- Field data collection

5 Real Time Container Data Collection
- Management of pallets and containers
- Notification of container condition (seeds emptied, has been moved)
- Dry Boxes
- Refrigerator Boxes
- Global Tracking
- Global Geofencing
- Intermodal Transport Logistics
- Environmental Monitoring of Cargo
- Security Sensors and Breach Alerts
- Logistics Service Provider Integration

REMOTE MONITORING

1 Industrial Equipment
- Monitor environmental constraints
- Manage equipment configuration
- Automate service ticket generation
- Monitor warranty compliance
- Software and firmware distribution
- SCADA

2 Building Automation
- Adjust lighting, temperature, alarm activation
- Meter reading/management
- Link office and safety equipment
- Alarm/fire panel integration
- Weather integration
- Smart grid integration
- Smart meters
- Demand response

3 Smart Vending
- Consumables replenishment
- Point of Sale integration
- Integration with Digital Signage
- Interaction with consumer applications
- Remote visual monitoring of system malfunctions

4 Computer Storage Arrays, Telecommunication Equipment, Power Supplies
- Automate software delivery
- Manage power/heat consumption
- Predictive service analytics
- Manage equipment configuration
- Usage billing

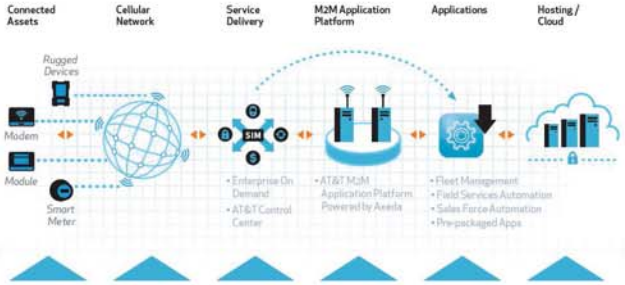
5 ATM
- Remotely validate system configuration
- Automate consumable replenishment
- Remote login
- Software version control
- Predictive maintenance
- Vandalism detection and alarm management
- Payment system integration

6 Digital Signage
- Manage digital displays remotely
- In-store marketing
- Video/image capture
- Capture images based on equipment and environmental thresholds
- Control power consumption

Rethink Possible AT&T

AT&T Machine to Machine

Increase productivity through the deployment of fully integrated mobile solutions.



Provide professional services to design, integrate, deploy and manage across all areas of the solution.

Connected Assets
- Certified Modules
- Embedded Computing
- Sensors
- Modems
- Certified Devices

Cellular Network
- Over 13.3 million M2M Connections
- Coverage in >200 Countries
- Global SIM

Service Delivery
- Billing
- Provisioning
- Diagnostics
- Business Rules

M2M Application Platform
- M2M Application Services
- Rules Engine, Data Model
- Agents, Device Protocol Adapters
- Connected Product Management Applications

Applications
- Vertical Applications
- Custom Applications
- Enterprise Application Integration
- Integration Framework

Hosting / Cloud
- Scalable
- Secure

AT&T M2M Benefits

Real-time Container Tracking
Global information on location, environmental factors, tampering, humidity and temperature conditions, reducing costs and increasing service reliability, improved regulatory compliance.

Fleet Management
Increase productivity, lower fuel costs, reduce vehicle wear and tear, improved vehicle up-time, strengthened compliance reporting, improved worker safety.

Industrial Automation
Maximize machine uptime, reduce power consumption, minimize meantime to repair (MTTR), improved product quality.

Farming
Improved decisions on harvesting, irrigation, seeding, reduced frequency of field visits saving time and money, improved prices for crops.

Well Head Monitoring
Eliminates expenses for extensive cabling, reduces costs by minimizing on-site visits, lessens environmental issues, potential avoidance of catastrophic events, improved regulatory reporting.

Digital Signage
Compliance logging and reporting, interactive content that can improve sales, proper equipment usage with real-time instructions, maximize usage of equipment (displaying ads when digital signage device is not in use).

Building Automation
Reduced energy costs, future proof building management systems, communications between disparate systems.

Connected Medical Devices
Reduce costly readmissions, improve patient independence, maximize regulatory compliance, improve patient outcomes, reduce equipment downtime, reduce replenishable inventory costs.

Any Connected Asset
Track and trace, sense and respond to events, collect and analyze key data to deliver and accelerate business value.

Hardware	Chipsets, Modules, Sensors, Environmental Specs, Certification (FCC/PTCRB/Carrier Testing)
Connectivity	Wireless, Wireline, Satellite, WiFi, etc.
Service Delivery	SIM Provisioning, Billing, Troubleshooting, Device Management
Applications	M2M Application Platform, Custom Application Development, Industry Applications, Remote Service Applications
Infrastructure	Data Centers, Back-end Systems, Cloud Computing
Professional Services	Consulting, App Development, Integration, Deployment Services
Managed Services	Lifecycle Services, HelpDesk, Hosting

To learn more about AT&T solutions for Machine to Machine, go to ***att.com/m2m***

©2012 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

AT&T Service: Coverage not available in all areas. Compatible device and wireless service plan required. Additional collections, associated services or features, hardware and/or network connections may be required. Subject to the applicable AT&T agreement, rate plan brochure(s) and coverage map(s). Additional terms and restrictions apply. Offer subject to change.

©2012 Dachis Group

AB-2640

Rethink Possible®

AT&T Solutions to Enhance

Machine to Machine Solutions

AT&T increases business velocity with machine-to-machine 360. Whether it is adding features to a product or service to improve the customer experience such as tracking and gaining valuable performance information from valuable assets, or transforming an entire industry such as healthcare by reducing costs and providing a better patient experience, AT&T can assist from the design stages through full implementation.

Turn the page to learn how we can provide a total solution to potentially provide new revenue streams, reduce costs, and to provide real-time information to increase business velocity.

©2012 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners.

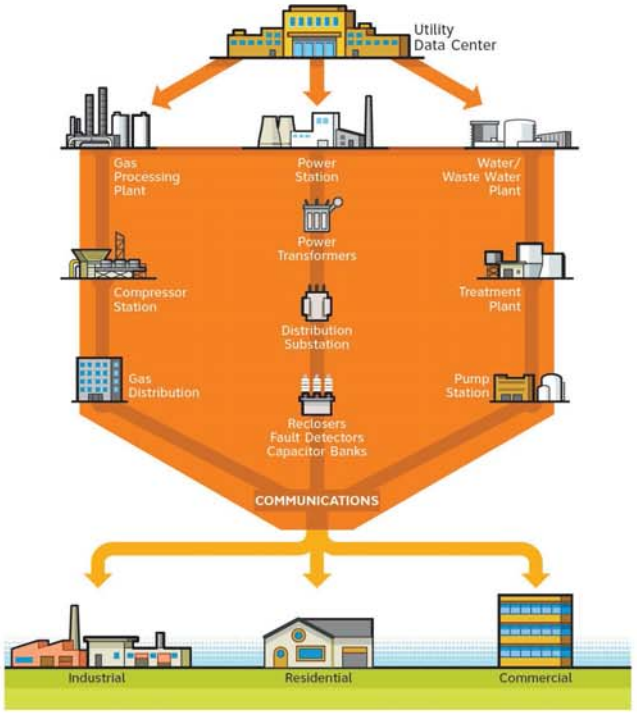
Rethink Possible®

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 78

End-to-end communications

AT&T helps utilities grow by extending their footprint, strengthening their network infrastructure, making their internal business operations more efficient and complementing their existing infrastructure with added application services. We also bring value to utilities by providing a utility-focused and experienced team of consultants, a team of industry veterans well versed in the wide array of communication and information needs of the utility industry.



AT&T Differentiators

Enterprise Resources for Utilities

- Enterprise resources; wireline & wireless products and services supporting business continuity and disaster recovery requirements
- Converged wireless and wireline offers
- Comprehensive consulting and delivery services
- Dedicated corporate security team supporting the wireline and wireless networks. Approximately 18 petabytes of data are handled on AT&T's networks on an average business day
- Utility specific security task force
- End user platforms dedicated to managing activations and devices
- Custom design, engineering and application services
- AT&T Consulting practitioners and AT&T Labs researchers to participate in the evolution of the smart grid and the evolving energy utility

Utilities Ecosystem Leadership

- Leadership position for national AMI and Smart Grid initiatives
- Our External Affairs department actively campaigns and educates federal and local regulatory committees on Smart Grid communications requirements
- Custom pricing developed to support various deployment models for AMI and Smart Grid solutions. Point-To-Point and Mesh

Vendor Alliances

- Large ecosystem of vendors focused on AMI & Smart Grid solutions
- Large number of vendors to support your enterprise: software, hardware, and consulting vendors focused on AMI & Smart Grid solutions

GSM & MPLS Network

- GSM global standard for forward and backward compatibility
- Commitment to longevity
- MPLS backbone for end-to-end, all IP communications for energy assets

Spectrum

- One of the broadest, highest-quality and most efficient spectrum portfolios in the industry.
- AT&T's strong spectrum holdings will help us to enhance further the quality and reliability of existing wireless broadband and voice services, and to set the foundation for new-generation wireless broadband technologies and services

Memberships

- EEI
- Grid Wise Alliance
- IEEE
- UTC
- Zigbee Alliance

EEI EDISON ELECTRIC INSTITUTE · GRIDWISE ALLIANCE · ASSOCIATE MEMBER UTC UTILITIES TELECOM COUNCIL · ZigBee Member

©2010 AT&T Intellectual Property. All rights reserved.
AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies.

AT&T Service: Coverage not available in all areas. Compatible device and wireless service plan required. Additional software, associated services or features, hardware and/or network connections may be required. Subject to the applicable AT&T agreement, rate plan brochure(s) and coverage map(s). Additional terms and restrictions apply. Offer subject to change.

XPLANATIONS™ by XPLANE™
©XPLANE 2010

AB-1823

Energy and Utilities
Are you ready for tomorrow?

AT&T knows what these questions mean to your organization. We can help you build your strategy.

Look inside to find out more:

at&t Your world. Delivered.

TOMORROW'S INTELLIGENT UTILITY

Brought to you by AT&T

Here's a comprehensive look at AT&T's end-to-end utility solution.

AT&T's SMART UTILITY

We assembled our Smart Utility solutions using comprehensive enterprise resources, corporate leadership in Smart Utility initiatives, and a large ecosystem of allied vendors. AT&T's Smart Utility solutions can give you control, monitoring, data analysis and smart metering.

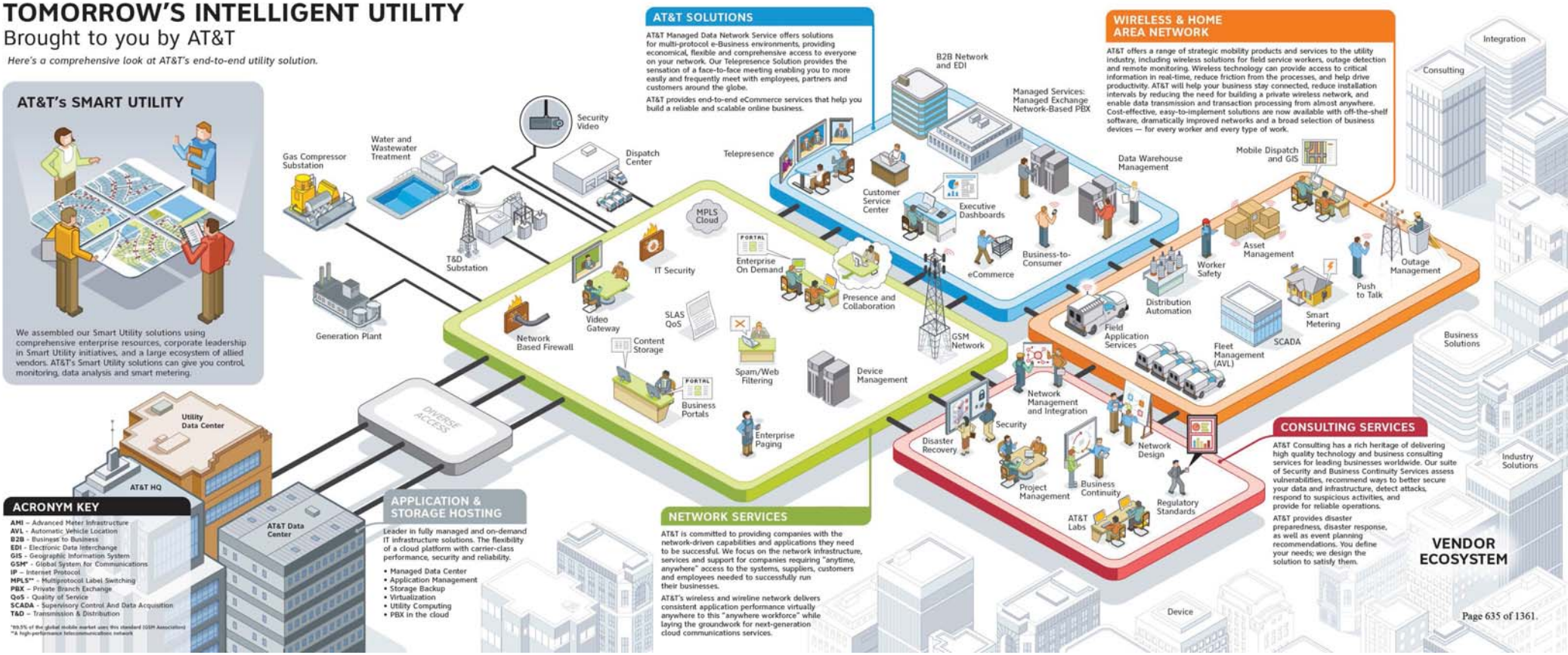
AT&T SOLUTIONS

AT&T Managed Data Network Service offers solutions for multi-protocol e-Business environments, providing economical, flexible and comprehensive access to everyone on your network. Our Telepresence Solution provides the sensation of a face-to-face meeting enabling you to more easily and frequently meet with employees, partners and customers around the globe.

AT&T provides end-to-end eCommerce services that help you build a reliable and scalable online business.

WIRELESS & HOME AREA NETWORK

AT&T offers a range of strategic mobility products and services to the utility industry, including wireless solutions for field service workers, outage detection and remote monitoring. Wireless technology can provide access to critical information in real-time, reduce friction from the processes, and help drive productivity. AT&T will help your business stay connected, reduce installation intervals by reducing the need for building a private wireless network, and enable data transmission and transaction processing from almost anywhere. Cost-effective, easy-to-implement solutions are now available with off-the-shelf software, dramatically improved networks and a broad selection of business devices — for every worker and every type of work.



CONSULTING SERVICES

AT&T Consulting has a rich heritage of delivering high quality technology and business consulting services for leading businesses worldwide. Our suite of Security and Business Continuity Services assess vulnerabilities, recommend ways to better secure your data and infrastructure, detect attacks, respond to suspicious activities, and provide for reliable operations.

AT&T provides disaster preparedness, disaster response, as well as event planning recommendations. You define your needs; we design the solution to satisfy them.

VENDOR ECOSYSTEM

ACRONYM KEY

AMI – Advanced Meter Infrastructure
AVL - Automatic Vehicle Location
B2B - Business to Business
EDI - Electronic Data Interchange
GIS - Geographic Information System
GSM* - Global System for Communications
IP – Internet Protocol
MPLS** - Multiprotocol Label Switching
PBX – Private Branch Exchange
QoS - Quality of Service
SCADA - Supervisory Control And Data Acquisition
T&D – Transmission & Distribution

*89.5% of the global mobile market uses this standard (GSM Association)
**A high-performance telecommunications network

APPLICATION & STORAGE HOSTING

Leader in fully managed and on-demand IT infrastructure solutions. The flexibility of a cloud platform with carrier-class performance, security and reliability.

- Managed Data Center
- Application Management
- Storage Backup
- Virtualization
- Utility Computing
- PBX in the cloud

NETWORK SERVICES

AT&T is committed to providing companies with the network-driven capabilities and applications they need to be successful. We focus on the network infrastructure, services and support for companies requiring "anytime, anywhere" access to the systems, suppliers, customers and employees needed to successfuly run their businesses.

AT&T's wireless and wireline network delivers consistent application performance virtually anywhere to this "anywhere workforce" while laying the groundwork for next-generation cloud communications services.

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 79

ONEM2M TECHNICAL SPECIFICATION	
Document Number	oneM2M-TS-0002-V-0.6.2
Document Name:	oneM2M Requirements Technical Specification
Date:	< 2013-10-17>
Abstract:	This present document contains an informative functional role model and normative technical requirements for oneM2M.

This Specification is provided for future development work within oneM2M only. The Partners accept no liability for any use of this Specification.

The present document has not been subject to any approval process by the oneM2M Partners Type 1. Published oneM2M specifications and reports for implementation should be obtained via the oneM2M Partners' Publications Offices.

About oneM2M

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

More information about oneM2M may be found at: http//www.oneM2M.org

Copyright Notification

No part of this document may be reproduced, in an electronic retrieval system or otherwise, except as authorized by written permission.

The copyright and the foregoing restriction extend to reproduction in all media.

© 2013, oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC).

All rights reserved.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. NO oneM2M PARTNER TYPE 1 SHALL BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY THAT PARTNER FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL oneM2M BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. oneM2M EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

Contents

Contents 3
1 Scope 4
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions and acronyms 6
3.1 Definitions 6
3.2 Acronyms 6
4 Conventions 8
5 Introduction to the M2M ecosystem 9
5.1 Functional roles description 9
6 Functional Requirements 11
6.1 Overall System Requirements 11
6.2 Management Requirements 16
6.3 Abstraction & Semantics Requirements 17
6.3.1 Abstraction Requirements 17
6.3.2 Semantics Requirements 18
6.4 Security Requirements 18
6.5 Charging Requirements 20
6.6 Operational Requirements 21
6.7 Communication Request Processing Requirements 21
7 Non-Functional Requirements (non-normative) 22
History 23

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

1 Scope

This present document contains an informative functional role model and normative technical requirements for oneM2M.

© oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC)
This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

2 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 referenced document (including any amendments) applies.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] oneM2M TR0004, “oneM2M Definitions and Acronyms”

[2] 3GPP TS 22.368, "Service Requirements for Machine-Type Communications (MTC); Stage 1"

[3] oneM2M TS0003, “oneM2M Security Solutions”

2.2 Informative references

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

(http://member.onem2m.org/Static_pages/Others/Rules_Pages/oneM2M-Drafting-Rules-V1_0.doc)

[i.2] ETSI TS102 689 V1.1.1, Machine-to-Machine communications (M2M);M2M service requirements

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

3 Definitions and acronyms

3.1 Definitions

For the purposes of the present document, the terms and definitions given in "oneM2M Definitions and Acronyms" [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in [1].

Dynamic Device/Gateway Context: see definition in [1].

Event: see definition in [1].

Event Categories: see definition in [1].

Infrastructure Domain: see definition in [1].

Information Model: see definition in [1].

M2M Application: see definition in [1].

M2M Application Service: see definition in [1].

M2M Application Service Provider: see definition in [1].

M2M Area Network: see definition in [1].

M2M Common Services: see definition in [1].

M2M Device: see definition in [1].

M2M Service: see definition in [1].

M2M Service Administrative State of a M2M Device: see definition in [1].

M2M Service Operational Status of a M2M Device: see definition in [1].

M2M Service Provider: see definition in [1].

M2M Service Subscription: see definition in [1].

M2M Session: see definition in [1].

M2M System: see definition in [1].

Network Operator: see definition in [1].

Static Device/Gateway Context: see definition in [1].

Underlying Network: see definition in [1].

User: see definition in [1].

3.2 Acronyms

For the purposes of the present document, the following abbreviations apply:

CHA: Continua Health Alliance

GSMA: Global System for Mobile Communications Association

HSM : Hardware Security Module

OMA : Open Mobile Alliance

Qos: Quality of Service

SMS : Short Message Service

USSD : Unstructured Supplementary Service Data

WAN: Wide Area Network

© oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC)
This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

4 Conventions

The key words “shall”, “shall not”, “should”, “should not”, “may”, “need not” in this document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

© oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC) Page 6 of 23
This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

5 Introduction to the M2M ecosystem

5.1 Functional roles description

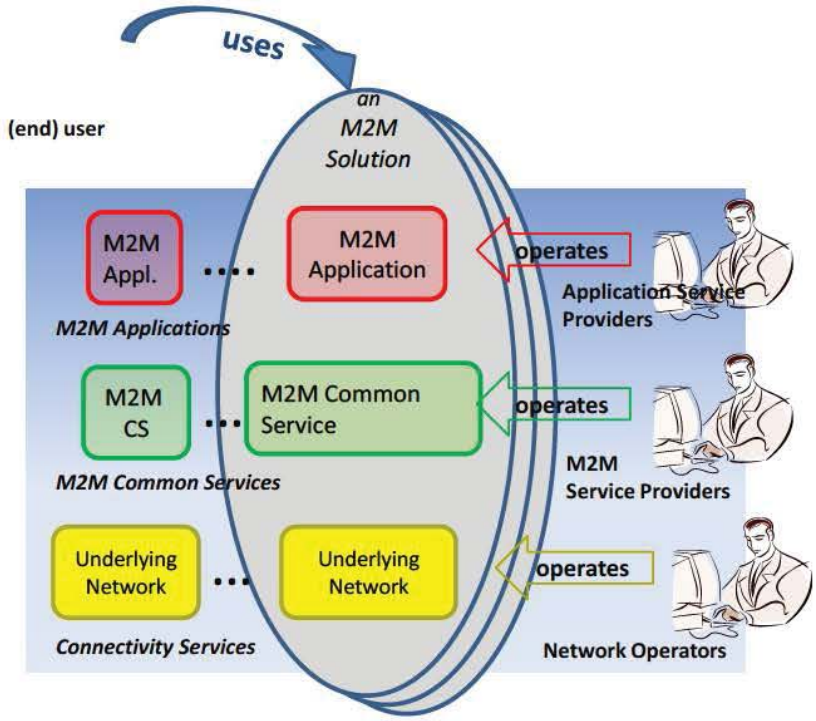


Figure 1: Functional Roles in the M2M Ecosystem

1. The ***User*** (individual or company – aka: end-user)
   fulfils all of the following criteria

   - Uses an ***M2M solution***

2. The ***Application Service Provider***
   fulfils all of the following criteria

   - Provides an ***M2M Application Service***
   - Operates ***M2M Applications***

3. The ***M2M Service Provider***
   fulfils all of the following criteria

   - Provides ***M2M Services*** to ***Application Service Providers***
   - Operates ***M2M Common Services***

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

4. The ***Network Operator***
fulfils all of the following criteria

- Provides ***Connectivity*** and related services for ***M2M Service Providers***
- Operates an ***Underlying Network***. Such an Underlying Network could e.g. be a telecom network.

Any of the above functional roles may coincide with any of the other roles. These functional roles do not imply business roles or architectural assumptions.

© oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC) Page 6 of 48
This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

6 Functional Requirements

6.1 Overall System Requirements

Requirement ID	Description	Release
OSR-001	The M2M System shall be able to allow communication between M2M Applications by using multiple communication means based on IP Access.	
OSR-002	The M2M System shall support communication means that can accommodate devices with constrained computing (e.g. small CPU, memory, battery) or communication capabilities (e.g. 2G wireless modem, certain WLAN node) as well as rich computing (e.g. large CPU, memory) or communication (e.g. 3/4G wireless modem, wireline) capabilities.	
OSR-003	The M2M System shall support the ability to maintain M2M Session in coordination with application session for those M2M Applications that require it.	
OSR-004	M2M System shall support the ability to support session-less application communications for those M2M Applications that require it.	
OSR-005	The M2M System shall be able to expose the services offered by telecommunications networks to M2M Applications (e.g. SMS, USSD, localization, subscription configuration, authentication (e.g. Generic Bootstrapping Architecture), etc),subject to restriction based on Network Operator's policy.	
OSR-006	The M2M System shall be able to reuse the services offered by Underlying Networks to M2M Applications and/or M2M Services by means of open access models (e.g. OMA, GSMA OneAPI framework).Examples of available services are: • IP Multimedia communications • Messaging • Location • Charging and billing services • Device information and profiles • Configuration and management of devices • Triggering, monitoring of devices • Small data transmission • Group management Note: The set of features or APIs to be supported depends on the M2M Common Services and access to available APIs.	
OSR-007	The M2M System shall provide a mechanism for M2M Applications to interact with the Applications and data/information managed by a different M2M Service Provider, subject to permissions as appropriate.	
OSR-008	The M2M System shall provide the capability for M2M Applications to communicate with an M2M Device (i.e. application in the device) without the need for the M2M Applications to be aware of the network technology and the specific communication protocol of the M2M Device.	
OSR-009	The M2M System shall support the ability for single or multiple M2M Applications to interact with a single or multiple M2M Devices/Gateways	

	(application in the device/gateway). Note: The relation M2M Network Application to M2M Device/Gateway may be 1:1, 1:n, n:1 and/or n:m.	
OSR-010	The M2M System shall support mechanisms for confirmed delivery of a message to its addressee to those M2M Applications requesting reliable delivery to dectect failure of message within a given time interval.	
OSR-011	The M2M System shall be able to request different communication paths, from the Underlying Network based on Underlying Network Operator and/or M2M Service Provider policies, routing mechanisms for transmission failures or request from M2M Applications.	
OSR-012	The M2M System shall support communications between M2M Applications and Devices supporting M2M Services by means of continuous or non-continuous connectivity.	
OSR-013	The M2M System shall be aware of the delay tolerance acceptable by the M2M Application and shall schedule the communication accordingly or request the Underlying Network to do it, based on policies criteria.	
OSR-014	The M2M System shall be able to communicate with M2M Devices, behind an M2M Gateway that supports heterogeneous M2M Area Networks.	
OSR-015	The M2M System shall support different communication patterns including infrequent communications, small data transfer, large file transfer, streamed communication.	
OSR-016	The M2M System shall provide the capability to notify M2M Applications of the availability of, and changes to, available M2M Application/management information on the M2M Device/Gateway, including changes to the M2M Area Network.	
OSR-017	The M2M System shall be able to offer access to different sets of M2M Services to M2M Application Providers. The minimum set of services are: • Connectivity management • Device management (service level management) • Application Data management In order to enable different deployment scenarios, these services shall be made available by the M2M System, individually, as a subset or as a complete set of services.	
OSR-018	The M2M System shall be able to offer M2M Services to M2M Devices roaming across cellular Underlying Networks,subject to restriction based on Network Operator's policy. Note:No roaming on M2M Service level is assumed by this requirement.	
OSR-019	The M2M System shall support the capabilities for data repository (i.e. to collect/store) and for data transfer from one or more M2M Devices or M2M Gateways, for delivery to one or more M2M Gateways, M2M Services Infrastructure, or M2M Application Infrastructure, in ways requested by the M2M Application Infrastructure as listed below: • action initiated either by an M2M Device, M2M Gateway, M2M Services Infrastructure, or M2M Application Infrastructure • when triggered by schedule or event;	

	• for specified data	
OSR-020	The M2M System shall be able to support policies and their management regarding the aspects of storage and retrieval of data/information.	
OSR-021	The M2M System shall be able to provide mechanisms to enable sharing of data among multiple M2M Applications.	
OSR-022	When some of the components of M2M System are not available (e.g. WAN connection lost), the M2M System shall be able to support the normal operation of components of the M2M System that are available.	
OSR-023	The M2M System shall be able to identify the M2M Services to be used by M2M Service Subscriptions. Note: M2M Service Subscriptions are not Application subscriptions (e.g., Home Energy Management).	
OSR-024	The M2M System shall be able to identify the M2M Devices used by M2M Service Subscriptions.	
OSR-025	The M2M System shall be able to identify the M2M Applications used by M2M Service Subscriptions.	
OSR-026	If provided by the Underlying Network, the M2M System shall be able to associate the M2M Device used by M2M Service Subscriptions with the device identifiers offered by the Underlying Network and the device.	
OSR-027	The M2M System shall provide a generic mechanism to support transparent exchange of information between the M2M Application and the Underlying Network, subject to restriction based on M2M Service Provider's policy and/or Network Operator 's policy. Note: Transparent exchange of information implies information that is mainly interpreted by the M2M Application and the Underlying Network Provider.	
OSR-028	The M2M System shall be able to trigger a series of commands to actuators on behalf of M2M Applications.	
OSR-029	The M2M System shall be able to support sending common command(s) to each actuator or sensor via a group.	
OSR-030	The M2M System shall be able to support the management (i.e. addition, removal, retrieval and update) of the membership of a group.	
OSR-031	The M2M System shall be able to support a group as a member of another group.	
OSR-032	The M2M System shall be able to support Event Categories (e.g., normal, urgency) associated with data for M2M Applications when collecting, storing and reporting that data. Note: Based on the Event Categories and via interworking with Underlying Networks, the M2M System can support differentiated services (by providing Quality-of-Service) requested by M2M Applications.	
OSR-033	Based on the Dynamic Device/Gateway Context of the M2M Gateway and/or Device and the defined Event Categories, the M2M System shall provide the capability to dynamically adjust the scheduling of reporting and notification of the M2M Device/Gateway.	

	Note: For example, if the battery of Gateway is remained only 10% or below, the Gateway notifies the M2M service platform of the status. The M2M Application in the Infrastructure node will adjust the scheduling of reporting and notification based on the Event Categories associated with each message. Consequently, the M2M Gateway operates longer.	
OSR-034	The M2M System shall support seamless replacement of M2M Devices as well as M2M Gateways (e.g., redirecting traffic, connection, recovery, etc.).	
OSR-035	The M2M System shall support the exchange of non-M2M Application related relevant information (e.g. Device/Gateway classes) between M2M Device/Gateway and M2M Service Infrastructure for the purpose of efficient communication facilitation. This includes the capability for an M2M Device to report its device class to M2M Service Infrastructure and for the M2M Service Infrastructure to inform M2M Device of the M2M Service Infrastruture capabilities.	
OSR-036	The M2M System should provide mechanisms to accept requests from M2M Application Service Providers for compute/analytics services.	
OSR-037	The M2M System shall enable an M2M Application to request to send data, in a manner independent of the Underlying Network, to the M2M Applications of a group of M2M Devices and M2M Gateways in geographic areas that are specified by the M2M Application.	
OSR-038	The M2M System shall support the inclusion of M2M Application's QoS preference in service requests to Underlying Networks.	
OSR-039	The M2M System shall be able to authorize service requests with QoS preference at service level, but shall pass M2M Application's QoS preference in service requests to Underlying Network for authorization and granting or negotiation of the service QoS requests.	
OSR-040	The M2M System shall be able to leverage multiple communication mechanisms (such as USSD or SMS) when available in the Underlying Networks.	
OSR-041	The M2M System shall provide a mechanism, which supports the addition of new M2M Services without impact to M2M interface interoperability	
OSR-042	The M2M System shall be able to support different QoS-levels specifying parameters, such as guaranteed bitrate, delay, delay variation, loss ratio and error rate, etc.	
OSR-043	The M2M System shall be able to verify that members of a group support a common set of functions.	
OSR-044	The M2M System shall support communication with M2M Devices which are reachable based on defined time schedules (e.g. periodic) as well as M2M Devices which are reachable in an unpredictable and spontaneous manner.	
OSR-045	The M2M System shall be able to be aware of the reachability status and to utilize reachability schedules generated by either the M2M Device or the Infrastructure Domain.	
OSR-046	The M2M System shall be able to support capability for the M2M Application to select communication protocol acknowledgment mechanisms.	
OSR-047	The M2M System shall be able to support mechanism for the M2M Devices and/or Gateways to report their geographical location information to M2M	

	Applications. Note: Geographical location information can be more than simply longitude and latitude.	
OSR-048	The M2M System shall provide an M2M Service that allows M2M Devices and/or Gateways to share their own or other M2M Devices' geographical location information. Note: Geographical location information can be more than simply longitude and latitude.	
OSR-049	The M2M System shall be able to provide the capability for an M2M Application to selectively share data (e.g. access control) among applications.	
OSR-050	If communication over one communication channel provided by the Underlying Network can only be triggered by one side (Infrastructure Domain or Field Domain), and alternative channel(s) is (are) available in the other direction, the M2M System shall be able to use the alternative channel(s) to trigger bidirectional communication on the first channel.	
OSR-051	Depending on availability of suitable interfaces provided by the Underlying Network the M2M System shall be able to request the Underlying Network to broadcast / multicast data to a group of M2M Devices in a specified area.	
OSR-052	The M2M System shall be able to select an appropriate Underlying Network to broadcast or multicast data depending on the network's broadcast/multicast support and the connectivity supported by the targeted group of M2M Devices/Gateways.	
OSR-053	The M2M System shall provide a means that enables the interoperability of interfaces among different releases. Note: "means" above does not imply only technical mechanisms.	
OSR-054	The M2M System shall be able to support an M2M Application, M2M Device, or M2M Gateway to obtain access to resources of another M2M Application, M2M Device, or M2M Gateway.	
OSR-055	The M2M System shall be able to provide the capability of M2M Applications to exchange data with one or more authorized M2M Applications which are not known.	
OSR-056	The M2M System shall enable discovery of usable M2M Applications on an M2M Gateway or at an M2M Device .	
OSR-057	The M2M System shall enable discovery of M2M Gateways and M2M Devices available to an M2M Application for data exchange.	
OSR-058	The M2M System shall be able to provide time stamps as needed by common service functions.	
OSR-059	The M2M System shall be able to support Role-based access control based on M2M Service Subscriptions.	
OSR-060	The M2M System should support time synchronization with an external clock source.	
OSR-061	M2M Devices and M2M Gateways may support time synchronization within the M2M System.	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

OSR-062	The M2M System shall enable means of testing the connectivity towards a set of M2M Applications.	
OSR-063	The M2M System shall be able to manage the scheduling of M2M Service Layer connectivity and messaging between the Infrastructure Domain and M2M Devices/Gateways.	
OSR-064	The M2M System shall be able to aggregate messages depending on message delay tolerance and/or category.	
OSR-065	The M2M System shall be able to provide mechanisms to accept M2M Applications for distribution, from M2M Application Service Providers.	
OSR-066	The M2M System shall be able to support the placement and operation of M2M Applications in selected M2M nodes per criteria requested by M2M Application Service Providers, subject to access rights.	
OSR-067	The M2M System shall be able to take operational and management action as requested by M2M Applications.	
OSR-068	When available from an Underlying Network, the M2M System shall be able to provide the capability to retrieve and report the information regarding whether an M2M Device is authorized to access Underlying Network services.	
OSR-069	When available from the Underlying Network, the M2M System shall be able to maintain the M2M Service Operational Status of a M2M Device and update it when the Underlying Network connectivity service status changes.	
OSR-070	The M2M System shall be able to provide the capability to notify an authorized M2M Application when the M2M Service Administrative State or M2M Service Operational Status of an M2M Device changes, if that M2M Application has subscribed for such notifications.	
OSR-071	The M2M System shall be able to enable an authorized M2M Application to set the M2M Service Administrative State of a M2M Device.	
OSR-072	The M2M System shall be able to initiate a set of well-defined actions (e.g. trigger upon a threshold, compare a value …) to one or more M2M Application(s) on behalf of another M2M Application.	

Table 1 Overall System Requirements

6.2 Management Requirements

Requirement ID	Description	Release
MGR-001	The M2M System shall be able to support management and configuration of M2M Gateways/ Devices including resource constrained M2M Devices.	
MGR-002	The M2M System shall provide the capability to discover the M2M Area Networks including information about devices on those networks and the parameters (e.g. topology, protocol) of those networks..	
MGR-003	The M2M System shall be able to provide the capability to maintain and describe the management information model of devices and parameters (e.g. topology, protocol) of M2M Area Networks.	

MGR-004	The M2M System shall support common means to manage devices enabled by different management technologies (e.g. OMA DM, BBF TR069).	
MGR-005	The M2M System shall provide the capability to manage multiple devices in a grouped manner.	
MGR-006	The M2M System shall provide the capability for provisioning and configuration of devices in M2M Area Networks .	
MGR-007	The M2M System shall provide the capability for monitoring and diagnostics of M2M Gateways/Devices in M2M Area Networks .	
MGR-008	The M2M System shall provide the capability for software management of devices in M2M Area Networks.	
MGR-009	The M2M System shall provide the capability for rebooting and/or resetting of M2M Gateways/Devices and other devices in M2M Area Networks.	
MGR-010	The M2M System shall provide the capability for authorizing devices to access M2M Area Networks.	
MGR-011	The M2M System shall provide the capability for modifying the topology of devices in M2M Area Networks,subject to restriction based on management policy of M2M Area Network.	
MGR-012	Upon detection of a new device the M2M Gateway shall be able to be provisioned by the M2M Service Infrastructure with an appropriate configuration which is required to handle the detected device.	
MGR-013	The M2M System shall be able to identify and manage M2M Service status of M2M Devices.	
MGR-014	The M2M System shall be able to retrieve events and information logged by M2M Gateways/ Devices and other devices in M2M Area Networks.	
MGR-015	The M2M System shall be able to support firmware management (e.g. update) of M2M Gateways/ Devices and other devices in M2M Area Networks.	
MGR-016	The M2M System shall be able to retrieve information related to the Static and Dynamic Device/Gateway Context for M2M Gateways/Devices as well as Device Context for other devices in M2M Area Networks.	
MGR-017	The M2M System shall support the capability to map M2M service subscription role(s) to roles used within technology specific Device Management protocols.	

Table 2 Management Requirements

6.3 Abstraction & Semantics Requirements

6.3.1 Abstraction Requirements

Requirement ID	Description	Release
ABR-001	The M2M System shall provide a generic structure for data representation.	

ABR-002	The M2M System shall be able to provide translation mechanisms between Information Models used by M2M Applications, M2M Devices/Gateways, and other devices.	
ABR-003	The M2M System shall provide capabilities to represent Virtual Devices and Things, (which are not necessarily physical devices.)	

Table 3 Abstraction Requirements

6.3.2 Semantics Requirements

Requirement ID	Description	Release
SMR-001	The M2M System shall provide capabilities to manage semantic descriptions of resources and M2M Applications, e.g, create, retrieve, update, delete, associate/link.	
SMR-002	The M2M System shall support a common modeling language for semantic descriptions (including relationships between Things) in order to make them available to M2M Applications.	
SMR-003	The M2M System shall be able to provide interworking capabilities between different modeling languages for semantic descriptions.	
SMR-004	The M2M System shall provide capabilities to discover M2M Resources based on semantic descriptions.	
SMR-005	The M2M System shall support the capability to access semantic descriptions which are outside of the M2M System.	
SMR-006	The M2M System shall be able to support capabilities for performing M2M data Analytics based on semantic descriptions from M2M Applications and /or from the M2M System.	
SMR-007	The M2M System shall be able to provide capabilities for performing Semantic Mash-up using M2M data from M2M Applications and/or from the M2M System (e.g. to create Virtual Devices, offer new M2M Services, etc.)	

Table 4 Semantics Requirements

6.4 Security Requirements

Requirement ID	Description	Release
SER-001	The M2M System shall incorporate protection against threats to its availability such as Denial of Service attacks.	
SER-002	The M2M System shall be able to ensure the confidentiality of data.	
SER-003	The M2M System shall be able to ensure the integrity of data.	
SER-004	In case where the M2M Devices support USIM / UICC and the Underlying Networks support network layer security, the M2M System shall be able to leverage device's USIM / UICC credentials and network's security capability	

	e.g. 3GPP GBA for establishing the M2M Services and Applications level security through interfaces to Underlying Network.	
SER-005	In case where the M2M Devices support USIM/UICC and the Underlying Networks support network layer security, and when the M2M System is aware of Underlying Network's bootstrapping capability e.g. 3GPP GBA, the M2M System shall be able to expose this capability to M2M Services and Applications through API.	
SER-006	In case where the M2M Devices support USIM / UICC and the Underlying Networks support network layer security, the M2M System shall be able to leverage device's USIM / UICC credentials when available to bootstrap M2M security association.	
SER-007	When some of the components of an M2M Solution are not available (e.g. WAN connection lost), the M2M System shall be able to support the confidentiality and the integrity of data between authorized components of the M2M Solution that are available.	
SER-008	The M2M System shall support countermeasures against unauthorized access to M2M Services and M2M Application Services.	
SER-009	The M2M System shall be able to support mutual authentication for interaction with Underlying Networks, M2M Services and M2M Application Services.	
SER-010	The M2M System shall be able to support mechanisms for protection against misuse, cloning, replacement or theft of security credentials.	
SER-011	The M2M System shall protect the use of the identity of an M2M Stakeholder within the M2M System against discovery and misuse by other stakeholders.	
SER-012	The M2M System shall be able to support countermeasures against Impersonation attacks and Replay attacks.	
SER-013	The M2M System shall be able to provide the mechanism for integrity-checking on boot, periodically on run-time, and on software upgrades for software/hardware/firmware component(s) on M2M Device(s).	
SER-014	The M2M System shall be able to provide configuration data to an authenticated and authorized M2M Application in the M2M Gateway/Device.	
SER-015	The M2M System shall be able to support mechanisms to provide Subscriber identity to authorized and authenticated M2M Applications when the M2M System has the Subscriber's consent.	
SER-016	The M2M System shall be able to support non repudiation within the M2M service layer and in its authorized interactions with the network and application layers.	
SER-017	The M2M System shall be able to mitigate threats identified in TS-0003[3].	
SER-018	The M2M System shall enable an M2M Stakeholder to use a resource or service and be accountable for that use without exposing its identity to other stakeholders.	
SER-019	The M2M System shall be able to use service-level credentials present inside the M2M device for establishing the M2M Services and Applications level security.	

SER-020	The M2M System shall enable legitimate M2M Service Providers to provision their own credentials into the M2M Devices/Gateways.	
SER-021	The M2M System shall be able to remotely and securely provision M2M security credentials in M2M Devices and/or M2M Gateways.	
SER-022	The M2M System shall enable M2M Application Service Providers to authorize interactions involving their M2M Applications on supporting entities (e.g. Devices/ Gateways/ Service infrastructure).	
SER-023	If a Hardware Security Module (HSM) is supported, the M2M Device shall be able to use the HSM to support security.	
SER-024	The M2M System shall enable M2M Applications to use different and segregated security environments.	
SER-025	The M2M System shall be able to prevent unauthorized M2M Stakeholders from identifying and/or observing the actions of other M2M Stakeholders in the M2M System, e.g. access to resources and services. Note: The above requirement does not cover whatever is outside of the M2M System, e.g. Underlying Networks.	
SER-026	The M2M System shall be able to provide mechanism for the protection of confidentiality of the geographical location information. Note: Geographical location information can be more than simply longitude and latitude.	

Table 5 Security Requirements

6.5 Charging Requirements

Requirement ID	Description	Release
CHG-001	The M2M System shall support collection of charging specific information related to the individual services facilitated by the M2M System (e.g. Data Management, Device Management and/or Connectivity Management). Collection of charging specific information shall be possible concurrent with the resource usage.The format of the recorded information shall be fully specified including mandatory and optional elements.	
CHG-002	The M2M System shall support mechanisms to facilitate correlation of charging information (e.g. of a User) collected for M2M Services, M2M Application Services and services provided by underlying network operators.	
CHG-003	The M2M System shall provide means to coordinate charging data records for data usages with differentiated QoS from the Underlying Network.	
CHG-004	The M2M System shall be able to reuse existing charging mechanisms of Underlying Networks.	
CHG-005	The M2M System shall support transfer of the charging information records to the Billing Domain of the M2M Service Provider, for the purpose of: • subscriber billing • inter-provider billing	

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

	• provider-to-subscriber accounting including additional functions like statistics.	
CHG-006	The M2M System should support generation of charging events for the purpose of requesting resource usage authorization from the real time credit control system where the subscriber account is located. The information contained in the charging events and the relevant chargeable events shall be fully specified including mandatory and optional elements. Note: A chargeable event is any activity, a provider may want to charge for that utilizes the resources and related M2M Services offered by such provider. A charging event is the set of charging information needed by the credit control system for resource authorization.	

Table 6 Charging Requirements

6.6 Operational Requirements

Requirement ID	Description	Release
OPR-001	The M2M System shall provide the capability for monitoring and diagnostics of M2M Applications.	
OPR-002	The M2M System shall provide the capability for software management of M2M Applications.	
OPR-003	The M2M System shall be able to configure the execution state an M2M Application (start, stop, restart).	
OPR-004	When suitable interfaces are provided by the Underlying Network, the M2M System shall have the ability to schedule traffic via the Underlying Network based on instructions received from the Underlying Network.	
OPR-005	The M2M System shall be able to exchange information with M2M Applications related to usage and traffic characteristics of M2M Devices or M2M Gateways by the M2M Application. This information includes the following features for an M2M Device: • Time controlled for devices to send or receive data only during defined time intervals. Note: "Time controlled" is equivalent to the MTC Features specified in [2] (section 7.2 of 3GPP TS 22.368)	
OPR-006	Depending on availability of suitable interfaces provided by the Underlying Network the M2M System shall be able to provide information related to usage and traffic characteristics of M2M Devices or M2M Gateways to the Underlying Network.	

Table 7 Charging Requirements

6.7 Communication Request Processing Requirements

Requirement ID	Description	Release
CRPR-001	The M2M System shall be able to support M2M Gateways and M2M Devices	

	that offer communication services to M2M Application to buffer incoming messages for communicating data to another M2M Gateway/Device/Infrastructure Domain.	
CRPR-002	The M2M System shall be able to support forwarding buffered messages depending on communication policies and based on service preference associated with the buffered messages.	
CRPR-003	The M2M System shall enable an M2M Application to send a communication request with the following service preference: • QoS parameters, including delay tolerance, for initiating the delivery of data • categorizing communication requests into different levels of priority or QoS classes	
CRPR-004	The M2M System shall be able to support concurrent processing of messages within M2M Gateways and/or M2M Devices from different sources with awareness for the service preference associated with the messages while observing the provisioned communication policies.	
CRPR-005	The M2M System shall be able to maintain context associated with M2M sessions (e.g. security context or network connectivity context during the interruption of the session).	

Table 8 Communication Request Processing Requirements

7 Non-Functional Requirements (non-normative)

This section is intended to gather high-level principles and guidelines that shall govern the design of the oneM2M System. Such principles and guidelines are fundamental to the design of the M2M System. But as they cannot necessarily be expressed as requirements per se, they shall be introduced and expressed in this section.

Requirement ID	Description	Release
NFR-001	Continua Health Alliance is incorporating a RESTful approach to its design. To support CHA, oneM2M should consider RESTful styles and approaches while designing the M2M architecture.	
NFR-002	The M2M System should communicate using protocols that are efficient in terms of amount of exchanged information over amount of exchanged data measured in bytes.	

Table 9 Non-Functional Requirements

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

History

This clause shall be the last one in the document and list the main phases (all additional information will be removed at the publication stage).

Publication history		
V1.1.1	<dd-Mmm-yyyy>	<Milestone>

Draft history (to be removed on publication)		
V.0.0.1	11 Mar 2013	Rapporteur Input – Skeleton Draft
V.0.0.2	11 Mar 2013	Implement the agreed contributions until TP#3: oneM2M-REQ-2012-0054R07 oneM2M-REQ-2013-0180R03 oneM2M-REQ-2013-0195R01 oneM2M-REQ-2013-0143R02 oneM2M-REQ-2013-0154R03 oneM2M-REQ-2013-0155R03 oneM2M-REQ-2013-0228R02 oneM2M-REQ-2013-0198R03 oneM2M-REQ-2013-0162R02 oneM2M-REQ-2013-0170R04 oneM2M-REQ-2013-0134R02

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.0.3	24 Apr 2013	Implement the agreed contributions: oneM2M-REQ-2013-0174R05 oneM2M-REQ-2013-0187R07 oneM2M-REQ-2013-0269R02 oneM2M-REQ-2013-0148R04 oneM2M-REQ-2013-0149R03 Note: no changes are required by 149R03. It only states that the current charging requirements covers the overlapped proposals. oneM2M-REQ-2013-0247 Note: Operational Section was added oneM2M-REQ-2013-0252R02 oneM2M-REQ-2013-0268R01 oneM2M-REQ-2013-0285R02 oneM2M-REQ-2013-0310R01 oneM2M-REQ-2013-0271R02 oneM2M-REQ-2013-0291R03 oneM2M-REQ-2013-0280R02
V0.1.0	20 May 2013	Implement the agreed contributions: oneM2M-REQ-2013-0179R08
V0.2.0	03 Jun 2013	Implement the agreed contributions: oneM2M-REQ-2013-0297R04 oneM2M-REQ-2013-0274R01 oneM2M-REQ-2013-0273R02
V0.3.0	17 Jun 2013	Implement the agreed contributions: oneM2M-REQ-2013-0274R02

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.4.0	24 Jun 2013	Implement the agreed contributions: oneM2M-REQ-2013-0157R06 oneM2M-REQ-2013-0368R01 oneM2M-REQ-2013-0267R05 oneM2M-REQ-2013-0275R03 oneM2M-REQ-2013-0320R02 oneM2M-REQ-2013-0287R05 oneM2M-REQ-2013-0329R01 oneM2M-REQ-2013-0189R08 oneM2M-REQ-2013-0311R02 oneM2M-REQ-2013-0331R02 oneM2M-REQ-2013-0341R01 oneM2M-REQ-2013-0343R04 oneM2M-REQ-2013-0344R05 oneM2M-REQ-2013-0363R02 oneM2M-REQ-2013-0372R01 oneM2M-REQ-2013-0376R01 oneM2M-REQ-2013-0173R05 oneM2M-REQ-2013-0313R02 oneM2M-REQ-2013-0375 oneM2M-REQ-2013-0345R01

This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

V0.5.0	09 Aug 2013	Implement the agreed contributions: oneM2M-REQ-2013-0357R05 oneM2M-REQ-2013-0358R01 oneM2M-REQ-2013-0359R04 oneM2M-REQ-2013-0335R03 oneM2M-REQ-2013-0366R02 oneM2M-REQ-2013-0371R01 oneM2M-REQ-2013-0138R05 oneM2M-REQ-2013-0316R03 oneM2M-REQ-2013-0333R03 oneM2M-REQ-2013-0337R05 oneM2M-REQ-2013-0338R02 oneM2M-REQ-2013-0349R02 oneM2M-REQ-2013-0350R05 oneM2M-REQ-2013-0373R03 oneM2M-REQ-2013-0374R02 oneM2M-REQ-2013-0378R01 oneM2M-REQ-2013-0381R03 oneM2M-REQ-2013-0392R01 oneM2M-REQ-2013-0394R02 oneM2M-REQ-2013-0397R01 oneM2M-REQ-2013-0384R03 oneM2M-REQ-2013-0360R03 oneM2M-REQ-2013-0403R01 oneM2M-REQ-2013-0404R01
V0.5.1	22 Aug 2013	1. Modify the text of Abstract. 2. Chang “OneM2M” to “oneM2M”.

V0.5.2	16 Oct 2013	1. Create new section 6.7 Communication Request Processing Requirements. 2. Move OSR-042, OSR-043, OSR-044 and OSR-045 from section 6.1 to section 6.7. 3. Implement the agreed contributions at TP#7: oneM2M-REQ-2013-0340R04 Definition of Event Categorization oneM2M-REQ-2013-0413R05-Requirements_cleanup oneM2M-REQ-2013-0418R02-CR_on_SER-015 oneM2M-REQ-2013-0419R02 Proposed clean-up of some unclear requirements in TS-0002 oneM2M-REQ-2013-0421R02 Security Requirements Modification
V0.6.0	17 Oct 2013	Do some changes to keep consistent with oneM2M-Template-TS-20130923.
V0.6.1	17 Oct 2013	Editorial changes
V0.6.2	17 Oct 2013	Editorial changes

© oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TTA, TTC) Page 28 of 28
This is a draft oneM2M document and should not be relied upon; the final version, if any, will be made available by oneM2M Partners Type 1.

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 80

Sierra Wireless AirPrime® Embedded Wireless Modules AR Series

Easy Wireless Integration for Automotive Solutions

The Sierra Wireless AirPrime® AR Series modules offer powerful, robust and reliable in-vehicle connectivity that reduces time-to-market, product, and development costs. These automotive grade modules stand up to demanding environments and have been designed specifically to meet the needs of automotive OEMs.

SIMPLE, SCALABLE, SECURE

AirPrime AR Series modules are equipped with a powerful multicore architecture with a dedicated application processor, an open-source embedded platform, and built-in connectivity to secure cloud services. AR Series modules reduce system complexity to help embedded software developers get products to market faster.

SIMPLIFY APPLICATION DEVELOPMENT WITH AN OPEN, FLEXIBLE PLATFORM

AirPrime AR Series modules come with Legato™, an open source embedded platform built on Linux. Made up of a tightly integrated application framework, Linux distribution, and feature-rich development environment, the Legato platform comes ready to run, build, and connect out-of-the-box.

SEAMLESSLY CONNECT TO THE CLOUD

Reduce effort and cost to develop, deploy, and operate innovative new M2M solutions with built-in connectivity to the AirVantage® M2M cloud. The AirVantage M2M Cloud simplifies device management and delivers machine information wherever you need it.

GLOBAL COVERAGE

Available with frequency band groupings, AirPrime AR Series minimizes design effort for automotive manufacturers operating in North America, EMEA, and APAC.

DESIGNED FOR AUTOMOTIVE

The Sierra Wireless AirPrime AR Series modules are designed and tested to real world automotive scenarios, offering:

- Automotive-grade manufacturing (TS-16949 certified)
- Automotive quality processes (PPAP, 8D, FA) & low target ppm rates
- Tolerance to extreme operating environments including thermal shock cycles
- Extended operating temperature range from -40°C to +85°C

AIRPRIME AR755X

Built on a Qualcomm Gobi™ 9x15 chipset, these 3G/4G LTE modules can host the most robust customer applications. A powerful dedicated application core, high speed interfaces, and GNSS deliver time-to-market advantage to design next generation in-vehicle telematics solutions.

KEY BENEFITS

- Automotive-grade manufacturing and quality processes
- GNSS for precise location information
- 4G for high bandwidth telematics solutions
- Reduced design effort for global projects
- High quality, reliable performance over the life of the vehicle

Automotive

SIERRA WIRELESS | AirPrime

Sierra Wireless AirPrime®
Embedded Wireless Modules
AR Series

	AR755x
CHIPSET	
	Qualcomm MDM9x15™
CORES	
Application core	ARM® Cortex™-A5 (550MHz)
Telecom core	Dual QDSP6 (600MHz)
AIR INTERFACES	
	LTE/HSPA+/EV-DO/EDGE/GPRS/GSM
APPROVALS	
Regulatory	GCF, PTRCB, FCC, IC, R&TTE*
Carrier	AR7550: Verizon, AR7552: AT&T* AR7558: Sprint
FREQUENCY BAND	
LTE (cat 3, 100/50 Mbps)	AR7550: 700/1700/2600 (NA:Verizon) AR7552: 700/850/1700/1900/2600 (NA:AT&T) AR7554: 800/900/1800/2100/2600 (EMEA/APAC) AR7558: 850/1700/1900/2600 (NA: Sprint/Rogers)
EV-DO Rev A/ CDMA 1x	AR7550 BC0 800/BC1 1900 AR7558 BC0/BC10 800/BC1 1900
HSPA+	AR7550, AR7552: 850/1900 AR7554: 850/900/2100 AR7558: 850/ 1900
GSM/GPRS/EDGE	AR7552, AR7554: 850/900/1800/1900 AR7558: 850/1900
FOOTPRINT	
	STAR LGA
DIMENSIONS	
	32 x 37 x 3.6mm
INTERFACES AND VOLTAGE	
Link	USB OTG, HSIC
Digital	SPI, I2C, 11xGPIOs, Int, SDIO
Audio	PCM, Analog
Analog	3xADC, 2xSIM, 1.8V out
Input voltage	3.4V - 4.2V
GPS/GLONASS	
	✓
EMBEDDED SOFTWARE ENVIRONMENT	
	Legato (Linux)
CLOUD SERVICES	
AirVantage Management Service	✓
AirVantage Enterprise Platform	✓
TEMP RANGE	
	- 40°C to + 85°C

* Target

About Sierra Wireless

Sierra Wireless is the global leader in machine-to-machine (M2M) devices and cloud services, delivering intelligent wireless solutions that simplify the connected world. Our solutions are **simple**, **scalable**, and **secure**, and enable customers to get their connected products and services to market faster.

For further company and product information, please visit www.sierrawireless.com.

Sierra Wireless, the Sierra Wireless logo, AirPrime, AirVantage, Legato, and the red wave design are trademarks of Sierra Wireless. Other registered trademarks that appear on this brochure are the property of the respective owners.
© 2014 Sierra Wireless, Inc. www.sierrawireless.com

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 81

Sierra Wireless AirPrime® Embedded Wireless Modules WP Series

An Entire M2M Ecosystem on a Module

The Sierra Wireless AirPrime® WP Series delivers processing and connectivity in a single device optimized for industrial machine-to-machine (M2M) applications. Designed to reduce the complexity of integrating embedded wireless communications, the WP Series provides an entire M2M ecosystem on a module.

REDUCE TOTAL SYSTEM COSTS AND TIME TO MARKET

AirPrime WP Series modules are equipped with a powerful multicore architecture offering a dedicated application processor, an open-source embedded platform, and built-in connectivity to secure cloud services. Their advanced technology reduces system complexity to help embedded software developers get products to market faster.

SIMPLIFY APPLICATION DEVELOPMENT WITH AN OPEN, FLEXIBLE PLATFORM

AirPrime WP Series modules come with Legato™, an open source embedded platform built on Linux. Made up of a tightly integrated application framework, Linux distribution, and feature-rich development environment, the Legato platform comes ready to run, build, and connect out-of-the-box.

SEAMLESSLY CONNECT TO THE CLOUD

Reduce effort and cost to develop, deploy, and operate innovative new M2M solutions with built-in connectivity to the cloud. AirVantage® M2M Cloud simplifies device management and delivers machine information wherever you need it.

DESIGNED FOR INDUSTRIAL M2M

The Sierra Wireless AirPrime WP Series modules are designed to meet the needs of industrial M2M solutions:

- Support for a comprehensive set of industrial interfaces
- Tolerance for difficult operating environments
- Easy design and automated manufacturing with STAR LGA form factor

AIRPRIME WP810X AND WP710X

Built on a Qualcomm Gobi™ 9x15 chipset, these 3G/4G LTE modules can host the most robust customer M2M applications. A powerful dedicated application core, high speed and industrial interfaces, and GNSS deliver time-to-market advantage to OEMs designing feature-rich next generation M2M solutions.

KEY BENEFITS

- Optimize performance and total system costs
- Simplify application development with an open source, flexible platform and secure cloud services
- Easily scale to millions of devices, from 3G to 4G
- Reduce effort and cost to develop, deploy and operate new M2M solutions

Smart

SIERRA WIRELESS | AirPrime®

Sierra Wireless AirPrime®
Embedded Wireless Modules
WP Series

	WP710x	WP810x*
CHIPSET		
	Qualcomm MDM9x15™	Qualcomm MDM8215™
CORES		
Application core	ARM® Cortex™-A5 (550MHz)	ARM® Cortex™-A5 (550MHz)
Telecom core	Dual QDSP6 (600MHz)	Dual QDSP6 (600MHz)
AIR INTERFACES		
	LTE/HSPA+/EV-DO/EDGE/GPRS/GSM	HSPA+/EDGE/GPRS /GSM
APPROVALS*		
Regulatory	GCF-CC, PTCRB FCC/IC, R&TTE	GCF-CC, PTCRB FCC/IC, R&TTE
Carrier	WP7100 : Verizon WP7102 : AT&T WP7104: Telstra	AT&T
FREQUENCY BAND		
LTE (cat 3, 100/50 Mbps)	WP7100 : 700/1700/2600 (NA : Verizon) WP7102 : 700/850/1700/1900/2600 (NA : AT&T) WP7104 : 800/900/1800/2100/2600 (EMEA, APAC)	
EV-DO Rev A/ CDMA 1x	WP7100 : BC0 800/BC1 1900	
HSPA+	WP7100, WP7102 : 850/1900 WP7104 : 850/900/2100	850/1900 800/850/900/2100 MHz
GSM/GPRS/EDGE	WP7102, WP7104 : 850/900/1800/1900	
FOOTPRINT		
	STAR LGA	STAR LGA
DIMENSION		
	32 x 37 x 3.6mm	32 x 37 x 3,6 mm
INTERFACES AND VOLTAGE		
Link	USB OTG, HSIC	USB OTG, 2 x UART, HSIC
Digital	SPI, I2C, 10xGPIOs, SDIO	SPI, I2C, 10xGPIOs, SDIO SPI, I2C, 11xGPIOs, Int, SDIO
Audio	PCM, I2S	3xI2S, PCM
Analog	2xADC, 2xSIM, 1.8V out	2xADC, 2xSIM, Int SON8, 1,8V out
Input voltage	3.4V - 4.2V	3.4b – 4.6V
GPS/GLONASS		
	✓	✓
EMBEDDED SOFTWARE ENVIRONMENT		
	Legato (Linux)	Legato (Linux)
CLOUD SERVICES		
AirVantage Management Service	✓	✓
AirVantage Enterprise Platform	✓	✓
TEMP RANGE (CLASS B)		
	-40°C to + 85°C	-40°C to + 85°C

* Planned

About Sierra Wireless

Sierra Wireless is the global leader in machine-to-machine (M2M) devices and cloud services, delivering intelligent wireless solutions that simplify the connected world. Our solutions are **simple**, **scalable**, and **secure**, and enable customers to get their connected products and services to market faster.

For further company and product information, please visit www.sierrawireless.com.

Sierra Wireless, the Sierra Wireless logo, AirPrime, and the red wave design are trademarks of Sierra Wireless.
Other registered trademarks that appear on this brochure are the property of the respective owners.
© 2014 Sierra Wireless, Inc. www.sierrawireless.com

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 82

Sierra Wireless Legato™ Platform

Open source embedded platform built on Linux designed to simplify M2M application development.

The Legato™ platform gives embedded M2M development a head start and is ready to run, build, and connect out-of-the-box. Made up of a tightly integrated application framework, fully tested Linux distribution, and feature-rich development environment, the open source Legato platform accelerates application level development of connected devices.

READY-TO-RUN

Start developing immediately with the Legato platform that has been integrated, tested, and validated. The Linux distribution supports next generation AirPrime® WP and AR Series of smart modules, so Legato comes ready-to-run without any porting.

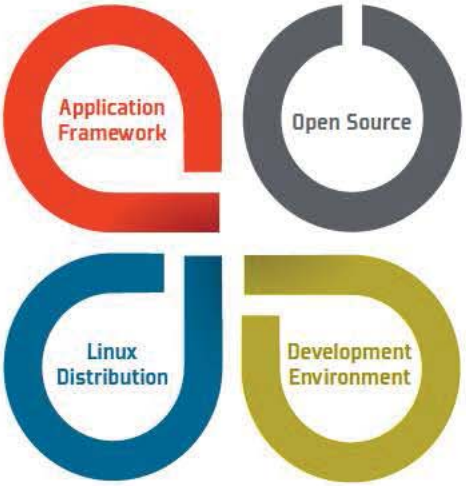
READY-TO-BUILD

Available in open source, Legato future-proofs software investments by easily porting the stack to any module or application processor as product requirements evolve. With security and connectivity built in and customizable middleware components, the platform simplifies development by enabling OEMs to just focus on the value-add applications.

READY-TO-CONNECT

Designed for connected products, the Legato platform makes it easy to get device data to the enterprise thanks to seamless integration with the AirVantage® M2M Cloud. For devices, Legato provides access to device peripherals like USB or Ethernet out-of-the-box. And robust API's make it easy to connect to any cloud or network – whether mobile, wired, or personal.

Legato™



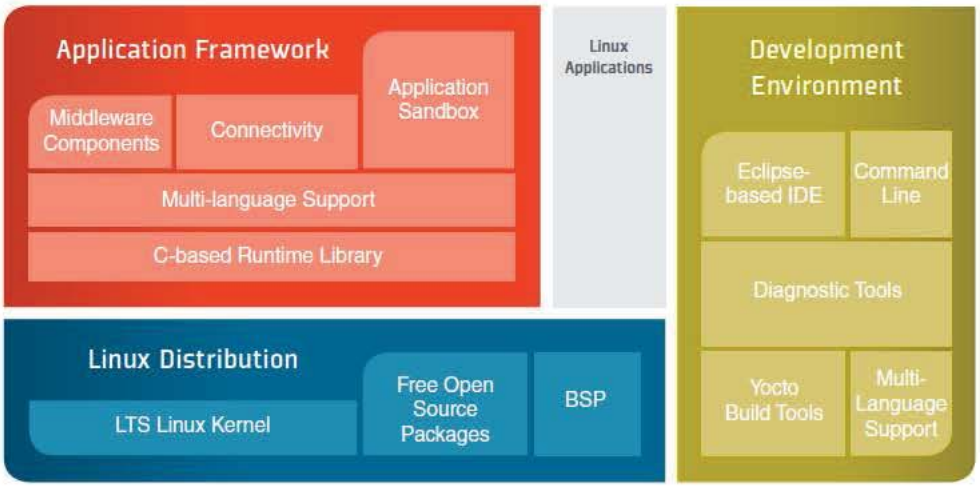
WHY WOULD YOU WANT TO START YOUR EMBEDDED PROJECT WITH ANYTHING ELSE?

- Get started immediately with Legato pre-loaded on AirPrime AR and WP smart modules.
- Future-proof software investments and access existing open source packages common to M2M.
- Utilize existing software and skillsets with multi-language support and customizable components.
- Integrate valuable device data to the enterprise with the AirVantage M2M Cloud.
- Connect to any WWAN, WLAN, PAN, or HAN without any wireless expertise.
- Access hardware interfaces via USB, UART, I2C, SPI, Ethernet, GPIO, ADC, and audio out-of-the box.

SIERRA WIRELESS | AirPrime®

Sierra Wireless Legato™ Platform

APPLICATION FRAMEWORK, LINUX DISTRIBUTION, AND DEVELOPMENT ENVIRONMENT GIVES EMBEDDED M2M DEVELOPMENT A HEAD START.



APPLICATION FRAMEWORK | DESIGNED WITH SECURITY & CONNECTIVITY IN MIND

- Application Sandbox - secure environment to run and control multiple applications
- Robust Connectivity APIs - access cloud and network services such as voice calls, SMS, data, radio controls
- Customizable middleware components - select building blocks such as configuration, DB, resource arbitration, secure IPC
- Multi-language support – utilize embedded applications in different programming languages
- C-based runtime library – fast, efficient system designed to maximize processing power and user application space

LINUX DISTRIBUTION | CUSTOMIZABLE WITH BUILT-IN M2M FEATURES

- Free open source packages - validated by the Linux Foundation that include BusyBox, OpenSSL, DHCP, PPP, and OpenSSH
- Long-term supported Linux kernel (LTSI) - hosted by the Linux Foundation and maintained by the embedded systems industry
- Board support package (BSP) - enables hardware interfaces and power management, validated on AirPrime WP and AR smart modules

DEVELOPMENT ENVIRONMENT | FLEXIBLE TO SIMPLIFY APPLICATION LEVEL DEVELOPMENT

- Eclipse-based integrated development environment (IDE) - extensible and familiar toolset with built-in API awareness
- Command Line - automate builds and integrate into any tool chain
- Robust diagnostic tools - local and remote debugging, troubleshooting, monitoring, and profiling
- Yocto build tools - rebuild and tailor the Linux distribution for any project
- Multi-language support - code using your favorite programming language

About Sierra Wireless

Sierra Wireless is the global leader in machine-to-machine (M2M) devices and cloud services, delivering intelligent wireless solutions that simplify the connected world. Our solutions are **simple**, **scalable**, and **secure**, and enable customers to get their connected products and services to market faster.

For further company and product information, please visit www.sierrawireless.com.

Sierra Wireless, the Sierra Wireless logo, Legato, AirPrime, and the red wave design are trademarks of Sierra Wireless. Other registered trademarks that appear on this brochure are the property of the respective owners.
© 2014 Sierra Wireless, Inc. **www.sierrawireless.com**

SIERRA WIRELESS | AirPrime®

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 83

Sierra Wireless Open AT Application Framework

Integrate Wireless Connectivity Easily

Powering millions of devices operating worldwide, the Sierra Wireless Open AT application framework is the world's first complete software package for M2M application development.

Available for 2G and 3G, it offers a range of readily available building blocks to accelerate the application development process and reduce total cost.

LESS EFFORT ON INTEGRATION, MORE TIME FOR INNOVATION

The Open AT application framework makes it easier and faster to deploy M2M solutions. It allows you to use a 10-year track record technology that is already widely deployed, to provide the foundation for the wireless connectivity. Save time on integration to focus on the unique value you are bringing to the market.

> "Working with Sierra Wireless allowed us to focus on our own core strengths – we didn't need to become wireless experts to integrate the connectivity we needed and get our router to market quickly." Helmut Ratzenhofer, CEO, GÖRLITZ Austria GmbH

KEY BENEFITS:

- Focus on innovation, not integration
- Accelerate application development
- Reduce cost
- Effortlessly deploy one application on global 2G and 3G networks

A Complete Software Package

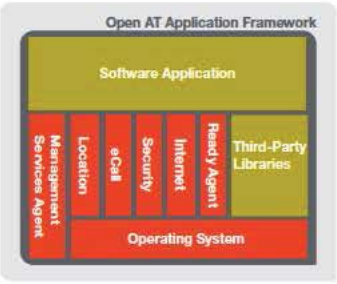
OPERATING SYSTEM

Open AT includes the world's only operating system designed specifically for M2M. It allows you to easily write embedded applications in standard ANSI C/C++.

LIBRARIES

A wide choice of libraries provide extra features and protocols to facilitate software development.

- **Internet:** Manages file transfer (FTP), email (POP3, SMTP), web services (HTTP) and MMS. IP routing with DHCP server, port forwarding, DNS proxy and NAT provide.
- **Security:** Protects your transactions and data through SSL, a cryptographic engine and jamming detection.
- **Location:** Facilitates GPS integration with a power management feature, fast TTFF and Assisted-GPS capability.



The Open AT Application Framework includes an operating system and libraries to ease the integration of your software.

- **eCall InBand Modem:** Brings emergency call capability,standardized by 3GPP, to in-vehicle systems.
- **Ready Agent:** Connects to the AirVantage M2M Cloud Platform.

DEVELOPER STUDIO

Developer Studio is an easy-to-use development tool based on Eclipse™ which makes the application development experience more streamlined and efficient.

SIERRA WIRELESS | AirPrime

Sierra Wireless Open AT Application Framework

Key Features

Operating system	
Real time, preemptive and multitask Timer and captures services Bus services: GPIO, USB, UART, I2C and SPI, ADC and DAC Interruption management RTC	Watchdog Fail safe file system, Flash storage Update service for firmware and application Application trace capabilities and error management
Programming language	
ANSI C/C++	
Compiler compatibility	
GCC and ARM RVDS	
Wireless connectivity management	
SIM management: PhoneBook, open SIM access, SIM toolkit Call, GPRS, SMS and MMS services GSM stack services: PLMN scan, cell information, TX burst indication Network Scan	
Power down management	
Ability to completely turn off radio interface Ability to dynamically Up/Down CPU processing speed	Configurable alarm and external interrupts to leave low power modes
Audio management	
DTMF coder and decoder Tone player Audio player and recorder	Echo cancelation and noise reduction PCM audio stream control
AT Commands management	
Standard and extended command set Incoming / outgoing AT command control	Custom AT commands capability AT commands filtering
IP Connectivity	
TCP and UDP sockets Email: POP and SMTP Ping, DNS resolution, SNMP Client	Web service: HTTP File transfer: FTP
IP routing	
Gateway capabilities: DHCP server, DNS Proxy, port forwarding, NAT	
Security	
SSL (Secure Sockets, HTTPS), Crypto engine	Jamming detection
Location services	
GPS capability, NMEA frame, fast TTFF, Assisted-GPS, jamming removal	
eCall service	
3GPP compliant, MSD PUSH and PULL modes, PSAP Test Server	

Test Open AT Application Framework Today

- **Download the installer:**
  http://developer.sierrawireless.com/OpenAT/download
- **Join our developer community:**
  http://developer.sierrawireless.com

Device Management

AirPrime™ Management Services is a cloud-based device management solution which enables you to remotely monitor and upgrade Open AT applications and AirPrime embedded modules firmware in the field through a web portal.

REMOTE DEVICE MONITORING & CONFIGURATION

The user interface includes the possibility to create dashboards in order to easily manage devices in the field:

- Monitor key parameters and communication traffic
- Configure devices
- Remotely send AT commands

REMOTE SOFTWARE AND FIRMWARE UPGRADES

AirPrime Management Services enables application software and firmware upgrades over-the-air, including the following features:

- Delta generation (download only the code that has changed for faster downloads and reduced data volume)
- Upgrade for multiple devices
- Reports

Easy to deploy, secure and scalable, AirPrime Management Services are based on industry standards: OMA-DM and full IP architecture.

Sierra Wireless, the Sierra Wireless logo, AirPrime, and the red wave design are trademarks of Sierra Wireless.
Other registered trademarks that appear on this brochure are the property of the respective owners.
© 2012 Sierra Wireless, Inc. www.sierrawireless.com

EXHIBIT 1 TO FELDMAN REPLY DECLARATION

DOCUMENT 125

Prepare

Mapping out your program – making sure you know all of your steps. From target Business Models through Distribution there are a lot of decisions to make. Even choosing the optimum network for your product must be defined.

Business Models
Distribution
Network
Platforms

Business Models

AT&T has the flexibility to support a wide spectrum of business and functional support models, ensuring that you are ready to support the needs of your product, customers, and business. Device certification and wireless transport are two core-competencies that AT&T offers, but you can also utilize services related to end-user support, end-user billing, or branding that will shape the partnership into an AT&T retail model.

A business model's position is defined by the level of ownership and control both service elements and the customer.

Flexibility

A business model's position on the spectrum is defined by the level of ownership and control of both service elements and the customer. Partners who have a mature infrastructure may be best served by a traditional wholesale model. For those partners wishing to focus on their devices and platforms, AT&T can deliver a retail experience.

Next Topic: Distribution

Wholesale Use Case

Partner provides device and value-added service/technology. AT&T provides the network and certification. The Partner and/or AT&T may provide distribution, branding, customer support and billing.

OWNERSHIP & CONTROL LEVEL

- AT&T certifies the device to ensure optimal performance on the network.
- AT&T can establish a dedicated APN to ensure that SIMs access only partner-defined sites.
- Partner purchases data network access from AT&T for a simple out-of-the-box customer experience.
- Partner creates pricing models which meet the needs of the customer experience.
- Partner bills the customer directly for content and/or access to the network.

Previous 1 / 3 Next

Ownership & Control Level

WHOLESALE Learn More

RETAIL Learn More

HYBRID Learn More

Flexibility

A business model's position on the spectrum is defined by the level of ownership and control of both service elements and the customer. Partners who have a mature infrastructure may be best served by a traditional wholesale model. For those partners wishing to focus on their devices and platforms, AT&T can deliver a retail experience.

Next Topic: Distribution

Retail Use Case

Partner provides the device, AT&T provides network, certification, distribution, branding, end - user support, and customer billing.

- AT&T certifies the device to ensure optimal performance on the network.
- Customer purchases a data plan which includes AT&T 3G and Wi-Fi access.
- Customers can subscribe to monthly or pay-as-you-go service at the point of sale.
- Device utilizes the AT&T Connection Manager to simplify use of Wi-Fi and the wireless network for the customer.
- Partner works with AT&T and national retailers to sell and activate devices.

OWNERSHIP & CONTROL LEVEL

Previous 2 / 3 Next

Ownership & Control Level

WHOLESALE Learn More

RETAIL Learn More

HYBRID Learn More

Flexibility

A business model's position on the spectrum is defined by the level of ownership and control of both service elements and the customer. Partners who have a mature infrastructure may be best served by a traditional wholesale model. For those partners wishing to focus on their devices and platforms, AT&T can deliver a retail experience.

Next Topic: Distribution

Hybrid Use Case

Partner provides device and value-added service/technology. AT&T provides the network and certification. The Partner and/or AT&T may provide distribution, branding, customer support, and billing.

- AT&T certifies the device to ensure optimal performance on the network.
- AT&T and Partner determine the economic relationship to provide mutual benefit and the best customer experience.
- Customers can subscribe to recurring or prepaid data service plans. Partner will work with AT&T and National Retailers on distribution.

PARTNERS AT&T

OWNERSHIP & CONTROL LEVEL

Previous 3 / 3 Next

Ownership & Control Level

Learn More Learn More Learn More

Flexibility

A business model's position on the spectrum is defined by the level of ownership and control of both service elements and the customer. Partners who have a mature infrastructure may be best served by a traditional wholesale model. For those partners wishing to focus on their devices and platforms, AT&T can deliver a retail experience.

Next Topic: Distribution

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENTS 84 THROUGH 85

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

PUBLIC VERSION

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 84

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 85

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 85

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 85

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 85

HIGHLY CONFIDENTIAL MATERIALS OMITTED

EXHIBIT 2 TO FELDMAN REPLY DECLARATION

DOCUMENT 85