ETSI TS 118 132 V2.0.2 (2017-11)

MAF and MEF Interface Specification
(oneM2M TS-0032 version 2.0.2 Release 2A)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/669e7731-848c-4d1e-9d7c-4dc1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11

Reference

DTS/oneM2M-000032V2A

Keywords

IoT, M2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/...-2017-11

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2017.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/c6680731-b48c-441e-9d7c-4dc1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/e6680731-848c-4d1e-9d7c-4dc1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Partnership Project oneM2M (oneM2M).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/c6680731-848c-4d1e-9d7c-4dc1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11

1 Scope

The present document specifies communication between the M2M Authentication Function (MAF) and MAF clients on the reference point Mmaf and between the M2M Enrolment Function (MEF) and MEF clients on the reference point Mmef.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[1] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[2] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003)".

[3] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004)".

[4] ETSI TS 118 108: "oneM2M; CoAP Protocol Binding (oneM2M TS-0008)".

[5] ETSI TS 118 109: "oneM2M; HTTP Protocol Binding (oneM2M TS-0009)".

[6] ETSI TS 118 110: "oneM2M; MQTT Protocol Binding (oneM2M TS-0010)".

[7] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[8] ETSI TS 118 120: "oneM2M; WebSocket Protocol Binding (oneM2M TS-0020)".

[9] ETSI TS 118 122: "oneM2M; Field Device Configuration (oneM2M TS-0022)".

iTeh STANDARD PREVIEW (standards.iteh.ai)

2.2 Informative references

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[i.1] oneM2M Drafting Rules.

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 118 111 [7], ETSI TS 118 103 [2] and the following apply:

MAF Client: functionality for performing MAF procedures on behalf of an associated CSE or AE, or on behalf of CSE or AE(s) present on an associated Node

MAF interface: communication interface between a MAF and a MAF Client identified by reference point Mmaf

MEF Client: functionality for performing MEF procedures on behalf of an associated CSE or AE, or on behalf of CSE or AE(s) present on an associated Node, or an associated MAF

MEF interface: communication interface between a MEF and a MEF Client identified by reference point Mmef

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 118 111 [7], ETSI TS 118 103 [2] and the following apply:

ADN	Application Dedicated Node
AE	Application Entity
AE-ID	Application Entity Identifier
API	Application Programming Interface
ASN	Application Service Node
BBF	Broadband Forum
CDT	Common Data Types
CRUD	Create, Retrieve, Update, Delete (operation)
CSE	Common Services Entity
CSE-ID	Common Services Entity Identifier
DM	Device Management
DTLS	Datagram Transport Layer Security
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IN	Infrastructure Node
MAF	M2M Authentication Function
MEF	M2M Enrolment Function
MN	Middle Node
MQTT	Message Queue Telemetry Transport
MTE	M2M Trust Enabler
NP	Not Present
RSPF	Remote Security Provisioning Framework
RO	Read-Only
RW	Read-Write
SEC	Security
SP	Service Provider
SP-ID	Service Provider Identifier
SUID	Security Usage Identifier
TLS	Transport Layer Security
WO	Write-Only
XML	eXtensible Markup Language

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/c6680731-848c-4d1e-ed7c-4d1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in the present document are to be interpreted as described in the oneM2M Drafting Rules [i.1].

5 General Description

5.1 MAF Interface

5.1.1 Introduction

The MAF Interface is a simple variant of the Mcc/Mca reference points specifying the interaction of MAF Clients with a M2M Authentication Function (MAF), acting on behalf of an *administrating stakeholder* such as an M2M SP or third party M2M Trust Enabler (MTE). The present document does not specify the operation and management of the MAF required to support these procedures.

A MAF Client interacts with the MAF on behalf of a Node (ADN, ASN, IN or MN), or a CSE or an AE.

Figure 5.1.1-1 defines the reference point Mmaf between MAF clients and a MAF.

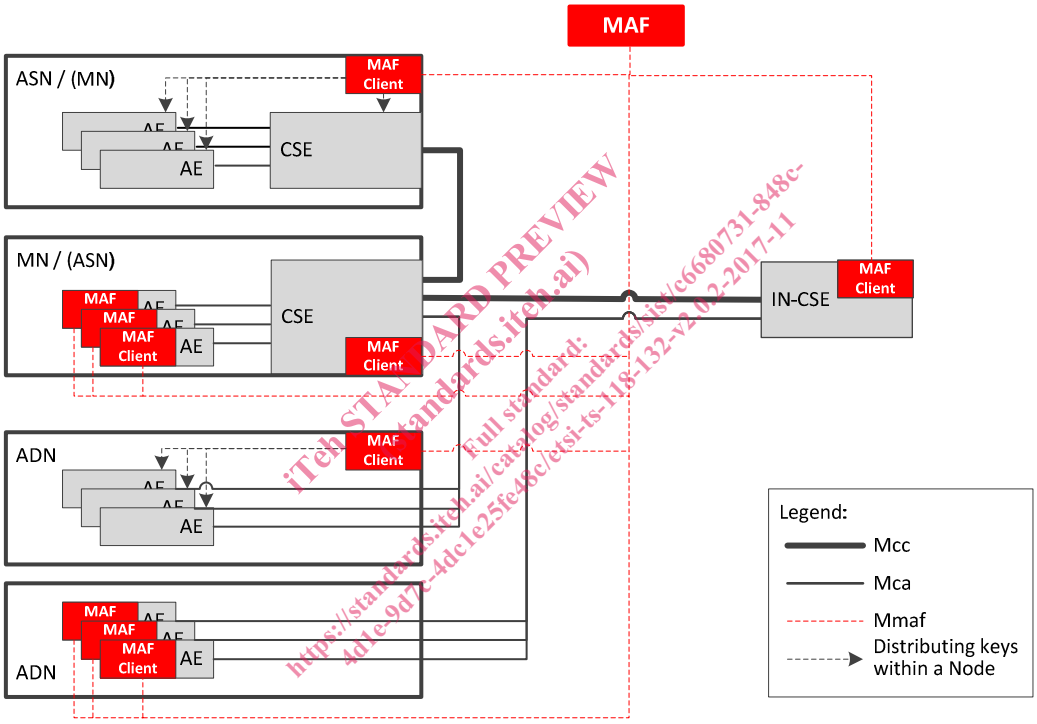

Figure 5.1.1-1: Reference Architecture for MAF

The administrating stakeholder authorizes the MAF's services to MAF clients, and oversees authorizing the distribution of symmetric keys. A MAF may provide its services on behalf of multiple administrating stakeholders. A MAF Client may be associated with multiple administrating stakeholders, each administrating the use of the MAF within a different scope.

NOTE 1: The administrating stakeholder could be an M2M SP administrating the registration and distribution of credentials used for SAEFs and ESPrim within the M2M SP's Domain.

NOTE 2: The administrating stakeholder could be an MTE administrating the registration and distribution of credentials for ESPrim and ESData to MAF Clients belonging to a particular Application Service Provider, where the MAF Clients could be distributed over multiple M2M SP domains.

iTeh STANDARD PREVIEW (iteh-standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/c6680731-848c-4d1e-9d72-4dc1e25fe46c/etsi-ts-118-132-v2.0.2-2017-11

The present document has no impact on the specifications in ETSI TS 118 101 [1] and ETSI TS 118 104 [3]. However, the MAF Interface uses much of the specification in ETSI TS 118 104 [3] and in particular allows use of the HTTP binding in ETSI TS 118 108 [4], the CoAP binding in ETSI TS 118 109 [5] and the WebSocket binding in ETSI TS 118 120 [8].

NOTE 3: The MQTT binding in ETSI TS 118 110 [6] is not suitable for the MAF Interface, because the MAF Interface assumes a TLS or DTLS connection from the MAF Client to the MAF - which is not possible using the MQTT binding.

The MAF Interface incorporates the following concepts from the Mcc/Mca reference points:

- The concept of operations acting on resources.
- The resource addressing from Mcc/Mca is used.
- The universal attributes and some common attributes of resources.

The MAF Interface differs from Mcc/Mca in the following ways:

- The MAF Client can only communicate directly with the MAF - there are no transited CSEs. Only Blocking Mode communication method is supported.
- None of the resource types applicable on Mcc/Mca are used:
    - Access control decisions use simple access control list for Retrieve access, and <*accessControlPolicy*> resources are not used for resources hosted by the MAF. A consequence of this is that the accessControlPolicyIDs attributes are not needed in the resources hosted by the MAF.
    - The <*subscription*> resource and NOTIFY operations are not supported.
    - There is no AE registration or CSE registration, but a similar process where a MAF Client creates a <*mafClientReg*> (MAF Client registration record) resource on the MAF.
    - There are no announced resources.

The hierarchy of resources hosted by a MAF shall be as follows:

- <*MAFBase*> resource type is the structural root for all the resources that are residing on a MAF. This resource is implicitly created by the MAF and uses the fixed resource name "maf" and contains following child resources:
    - <*mafClientReg*> resource. It confirms the MAF Client's registration to an administrating stakeholder, and can contain configuration information to be returned to the MAF Client.
    - <*symmKeyReg*> resources. It is created by the MAF Client, and contains symmetric keys for retrieval by another MAF Client.

5.1.2 MAF Interface Overview

This MAF Interface overview is based on the specification in clause 6 of ETSI TS 118 104 [3].

Identifiers such as M2M-SP-ID, AE-ID and CSE-ID as defined in clause 6.2.3 of ETSI TS 118 104 [3] also apply to the MAF Interface. M2M Trust Enablers (MTEs) are identified using an M2M-SP-ID.

Resources are addressed as specified in clause 6.2.4 in ETSI TS 118 104 [3].

Common data types applicable to the MAF Interface are inherited from clause 6.3 of ETSI TS 118 104 [3].

Tables 5.1.2-1 and 5.1.2-2 list the request and response primitive parameters inherited from clauses 6.4.1 and 6.4.2 in ETSI TS 118 104 [3], respectively; the data types of these parameters are unchanged. The ***From*** parameter shall include the MAF client ID which can be a Node-ID, AE-ID or CSE-ID, depending on whether the client acts on behalf of a node, AE or CSE. Note that this is in contrast to primitives on the Mca and Mcc interface, where the ***From*** primitive parameter cannot include a Node-ID.

NOTE: All other optional request and response primitive parameters defined in clause 6.4.1 of ETSI TS 118 104 [3] are not used on the MAF Interface.

Table 5.1.2-1: MAF Interface request primitive parameters

Parameter	Multiplicity	Notes
Operation	1	
To	1	
From	0..1	If not present, the MAF internally assigns ***From*** to be the identity of the Node, CSE or AE associated with the credential used for the MAF Handshake procedure.
Request Identifier	1	
Resource Type	0..1	
Content	0..1	
Result Content	0..1	

Table 5.1.2-2: MAF Interface response primitive parameters

Parameter	Multiplicity	Notes
Response Status Code	1	
Request Identifier	1	
Content	0..1	

Data types associated with resources applicable to the MAF Interface are defined in clause 7.

Table 5.1.2-3 lists the response status codes from clause 6.6 of ETSI TS 118 104 [3] which are supported by the MAF Interface.

Table 5.1.2-3: Response status codes supported by the MAF Interface

Response status codes	Interpretation
2000	OK
2001	CREATED
2002	DELETED
2004	UPDATED
4000	BAD_REQUEST
4004	NOT_FOUND
4005	OPERATION_NOT_ALLOWED
4103	ACCESS_DENIED
5000	INTERNAL_SERVER_ERROR

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/c66e0731-948c-4d1e-9d7c-4dc1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11

The MIME media types defined on clause 6.7 of ETSI TS 118 104 [3] shall be supported on the MAF interface. The notification related Media types vnd.onem2m-ntfy+json, vnd.onem2m-ntfy+cbor, vnd.onem2m-preq+xml do not apply to the MAF interface.

Virtual resources (clause 6.8 of ETSI TS 118 104 [3]) are not supported by the MAF Interface.

5.2 MEF Interface

5.2.1 Introduction

The M2M Enrolment Function (MEF) is an essential part of the oneM2M Remote Security Provisioning architecture.

Clause 6.1.2.1 of ETSI TS 118 103 [2] defines the following three variants of Remote Security Provisioning Frameworks (RSPF):

- Pre-Provisioned Symmetric Key RSPF,
- Certificate-Based RSPF,

- GBA-based RSPF.

The MEF interface defined in the present specification applies to Pre-Provisioned Symmetric Key RSPF and Certificate-Based RSPF only. For interfaces and procedures applicable to GBA-based RSPF, see clause 8.3.2.3 of ETSI TS 118 103 [2].

When using Pre-Provisioned Symmetric Enrolee Key RSPF or Certificate-Based RSPF, the MEF serves a number of different use cases which are summarized as follows:

1) The MEF provisions an Enrolee to perform MAF Security Framework procedures with a MAF as defined in clause 8.8.2 of ETSI TS 118 103 [2].

2) The MEF provisions an Entity A and an Entity B to perform Security Association Establishment as defined in clauses 8.2.2.1 and 8.2.2.2 of ETSI TS 118 103 [2].

3) The MEF provisions an originator and a receiver of a primitive with credentials to enable End-to-End Security of Primitives (ESPRIM) with security credentials as specified in clause 8.4 of ETSI TS 118 103 [2].

4) The MEF provisions the source and target endpoints of End-to-End Security of Data (ESDATA) as specified in clause 8.5 of ETSI TS 118 103 [2].

The present document defines messages and procedures for the above listed MEF use cases.

NOTE 1: A MEF may also be implemented as a Device Management server using device management protocols such as OMA DM, OMA LwM2M and BBF TR-069. Such procedures are defined in ETSI TS 118 103 [2] and ETSI TS 118 122 [9].

Like the Mmaf Interface, the Mmef Interface is a simple variant of the Mcc/Mca reference points specifying the interaction of MEF Clients with a M2M Enrolment Function (MEF), managing symmetric keys on behalf of an *administrating stakeholder* such as an M2M SP or third party M2M Trust Enabler (MTE). The present document does not specify the operation and management of the MEF required to support these procedures.

A MEF Client interacts with the MEF on behalf of a Node (ADN, ASN, IN or MN), or a CSE or an AE for use case 1 and 2 in the above list. Figure 5.2.1-1 defines the reference point Mmef between MEF clients and a MEF, and between MEF and MAF.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/9d7c4dc1-8486-4d1e-9d7c-4dc1e25fe48c/etsi-ts-118-132-v2.0.2-2017-11