ETSI TS 118 103 V1.1.0 (2016-03)

TECHNICAL SPECIFICATION

oneM2M;
Security solutions
(oneM2M TS-0003 version 1.4.2 Release 1)

Reference

RTS/oneM2M-000003v110

Keywords

IoT, M2M, security

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

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

Contents

Intellectual Property Rights

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.

Foreword

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

1 Scope

The present document defines security solutions applicable within the M2M system.

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 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[3] Void.

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

[5] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[6] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[7] ETSI TS 102 225 (V11.0.0): "Smart Cards; Secured packet structure for UICC based applications (Release 11)".

[8] ETSI TS 102 226 (V11.0.0): "Smart Cards; Remote APDU structure for UICC based applications (Release 11)".

[9] ETSI TS 131 115 (V10.1.1): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (3GPP TS 31.115 version 10.1.1 Release 10)".

[10] ETSI TS 131 116 (V10.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Remote APDU Structure for (U)SIM Toolkit applications (3GPP TS 31.116 version 10.2.0 Release 10)".

[11] 3GPP2 C.S0078-0 (V1.0): "Secured packet structure for CDMA Card Application Toolkit (CCAT) applications".

[12] 3GPP2 C.S0079-0 (V1.0): "Remote APDU Structure for CDMA Card Application Toolkit (CCAT) applications".

[13] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".

[14] 3GPP2 S.S0109-A: "Generic Bootstrapping Architecture (GBA) Framework".

[15] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[16] Void.

[17] Void.

[18] IETF RFC 5705: "Keying Material Exporters for Transport Layer Security (TLS)".

[19] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[20] "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.1.0, March 2008.

NOTE: Available at http://www.unicode.org.

[21] GlobalPlatform Device Technology TEE Administration framework, DRAFT.

[22] GlobalPlatform Device Technology TEE System Architecture, Version 1.0.

[23] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[24] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[25] ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[26] ISO/IEC 7816-4: "Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange".

[27] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[28] Void.

[29] Void.

[30] Void.

[31] IETF RFC 6655: "AES-CCM Cipher Suites for Transport Layer Security (TLS)".

[32] IETF RFC 5289: "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)".

[33] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[34] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[35] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[36] IETF RFC 6961: "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension".

[37] IETF RFC 7250: "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)".

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

[39] National Institute of Standards and Technology (July 1999): "Recommended Elliptic Curves for Federal Government user".

NOTE: Available at http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf.

[40] IETF RFC 6920: "Naming Things with Hashes".

[41] IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings".

[42] IETF RFC 5487: "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode".

[43] IETF RFC 4492: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[44] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[45] IETF RFC 7251: "AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[46] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

[47] GlobalPlatform Device Technology Secure Element Remote Application Management v1.0 GPD_SPE_008.

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

[i.2] oneM2M TR-0004: "Definitions and Acronyms".

[i.3] Void.

[i.4] ETSI TR 118 508: "Analysis of Security Solutions for the oneM2M System".

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

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

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

[i.8] Void.

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

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

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

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

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

AE-ID Certificate: certificate with a certificate chain to a trust anchor certificate and containing an AE-ID in the subjectAltName extension

NOTE: An AE_ID certificate can be used to verify that an entity has been assigned the AE-ID in the certificate.

association configuration: phase of a Security Association Establishment Framework in which the entity establishing the Security Association (and the Central Key Distribution Server, in the case of Centralized Security Frameworks), are provided with identities (and any other relevant credentials) to ensure that the security association is established between the intended entities

association security handshake: phase of a Security Association Framework in which the security association endpoints perform mutual authentication

bootstrap credential: pre-provisioned credential enabling mutual authentication of the Enrolee and the M2M Enrolment function

bootstrap credential configuration: phase of a Security Bootstrap Framework in which the Bootstrap Credentials are pre-provisioned to the Enrolee and the M2M Enrolment function

bootstrap enrolment handshake: phase of a Security Bootstrap Framework in which the Enrolee and M2M Enrolment Function perform mutual authentication

bootstrap instruction configuration: phase of a Security Bootstrap Framework in which the Enrolee and M2M Enrolment Function are provided with identities (and any other relevant credentials) to enable the M2M Enrolment function to establish a Master Credential between the intended Enrolee and M2M Authentication Function

bootstrap server function [13]: BSF is hosted in a network element under the control of a Mobile Network Operator. BSF, HSS, and UEs participate in GBA in which a shared secret is established between the network and a UE by running the bootstrapping procedure

NOTE: The shared secret can be used between NAFs and UEs, for example, for authentication purposes.

bootstrapping transaction identifier [13]: bootstrapping transaction identifier (B-TID) is used to bind the subscriber identity to the keying material in GBA reference points Ua, Ub and Zn

CA-Certificate [i.6]: certificate created by one certification authority (CA) certifying the public key of another CA

certificate: See Public Key Certificate.

certificate chain: sequence of one or more CA-certificates, where: the Public Verification Key in each CA-certificate is certified in the previous CA-certificate; and the public key of the first CA-Certificate is trusted *a priori*

NOTE: Trust in the public key in each CA-certificate can be based on trust in the previous CA-Certificate.

certificate name: unique identifier in a name field of a Certificate (e.g. in the X.509 "Subject" or "Subject Alternative Name" attribute)

certificate verification: process necessary to trust an entity's Certificate

certification authority [i.6]: responsible for establishing and vouching for the authenticity of public keys

NOTE: This includes binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and certificate revocation.

credential configuration: phase of a Security Association Establishment Framework in which the Credentials necessary for the Security Association Establishment Framework are configured to the relevant entities and functions

Credential-ID type-ID: portion of a Credential-ID indicating the type of credential being identified

CSE-ID certificate: certificate with a certificate chain to a root of trust and containing a CSE-ID in the subjectAltName extension

NOTE: A CSE_ID certificate can be used to verify that an entity has been assigned the CSE-ID in the certificate.

device certificate: certificate with a certificate chain to a root of trust and containing at least one globally unique hardware instance identifier in the subjectAltName extension

NOTE: A device certificate can be used to verify that an entity is executing on the identified hardware instance.

digital signature [i.7]: information is signed by appending to it an enciphered summary of the information

NOTE: The summary is produced by means of a one-way hash function, while the enciphering is carried out using the private key of the signer.

enrolee: AE or CSE that requires remote provisioning of a symmetric key to be shared with an enrolment target

enrolment key: symmetric key established between an Enrolee and M2M Enrolment Function following successful mutual authentication

NOTE: A symmetric key to be shared by the Enrolee and an Enrolment Target may be derived (at the Enrolee and M2M Enrolment Function) from the currently valid Enrolment Key, and the M2M Enrolment Function subsequently securely delivers the symmetric key to the Enrolment Target.

enrolment key generation: phase of remote security provisioning Framework in which the Enrolee and M2M Enrolment function establish an Enrolment Key and Enrolment Key identifier

enrolment phase: step in the lifecycle of an M2M equipment where it becomes provisioned for operation with a specific M2M Service Provider

enrolment target: M2M Authentication Function, CSE, or AE with whom an Enrolee wishes to establish a symmetric key (master credential or pre-provisioned secure connection key) using remote security provisioning

entity identifier: CSE-ID (or AE-ID respectively) of a CSE (or AE respectively)

FQDN certificate: certificate with a certificate chain to a root of trust and containing an FQDN

generic bootstrap architecture: set of 3GPP and 3GPP2 specifications providing security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP and 3GPP2 underlying network authentication mechanisms

message integrity code: tag computed from a message and a symmetric key, and attached to a message

NOTE 1: The purpose of a messages integrity code is to facilitate, without the use of any additional mechanisms, assurances regarding both the source of a message and its integrity.

NOTE 2: A Message Integrity Code is sometimes called a "Message Authentication Code" - "Message Integrity Code" has been used since the abbreviation of "Message Authentication Code" (MAC) might be misunderstood to refer to "Media Access Control". The definition is based on text from [i.6] (p323).

M2M secure connection key: key shared between two CSEs of M2M Nodes (e.g. ASN/MN-CSE and IN-CSE) in order to secure the communication between those two entities

NOTE: This M2M Secure Connection Key results from a successful M2M Security Association Establishment procedure.

MAF handshake: phase of a Security Association Establishment Framework in which an entity and the MAF perform mutual authentication and generate a Symmetric Key which can then be used in the Association Security Handshake for mutual authentication between that entity and other entities

master credentials: credentials used to mutually authenticate between an ASN/MN-CSE and the MAF. This is done to secure access to the infrastructure of an M2M Service Provider

NOTE: The Master Credentials are either pre-provisioned or remotely provisioned (without relying on those credentials).

Online Certificate Status Protocol: protocol for requesting a report on the status of one or more X.509 certificates (IETF RFC 6960 [35])

operational phase: period in the lifecycle of an M2M equipment where it is actually used for providing M2M services

policy decision point [i.5]: system entity that evaluates applicable policy and renders an authorization decision

policy enforcement point [i.5]: system entity that performs access control, by making decision requests and enforcing authorization decisions

policy information point [i.5]: system entity that acts as a source of attribute values

policy retrieval point: system entity that retrieves applicable policy or policy set

pre-provisioned secure connection key: Symmetric Key that is pre-provisioned to two entities (which may be AEs or CSEs) to be used for mutual authentication of those entities in Security Association Establishment

pre-provisioned secure connection key identifier: Identifier for a Pre-Provisioned Secure Connection Key

pre-provisioned symmetric enrolee key: Symmetric Key that is pre-provisioned to the Enrolee and M2M Enrolment Function

pre-provisioned symmetric enrolee key identifier: Identifier for a Pre-Provisioned Symmetric Enrolee Key

private signing key: secret key that can generate signatures that can be verified using a corresponding Public Verification Key

public key certificate: electronic document that uses a digital signature to bind a public key with an identity

NOTE: [i.6] A *public-key certificate* is a data structure consisting of a data part and a signature part. The data part contains cleartext data including, as a minimum, a public [verification] key and a string identifying the part (subject entity) to be associated therewith. The signature part consists of the digital signature of a certification authority over the data part, thereby binding the subject entity's identity to the specified public key.

public key certificate flavour: name describing the usage of a public key certificate within the scope of oneM2M

public key infrastructure: set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke Public Key Certificates

NOTE: For more details, see [i.6].

public verification key: credential that can verify digital signatures generated by a corresponding Private Signing Key, but which cannot be used to generate digital signatures

raw public key certificate: certificate comprising only the SubjectPublicKeyInfo structure of an X.509 certificate that carries the parameters necessary to describe the public key [37]

relative enrolment key identifier: part of the enrolment key identifier that is unique within the context of a M2M Enrolment Function

security association establishment: sequential processing of credential configuration, association configuration and association security handshake between two entities

NOTE: Credential configuration and/or association configuration can not be performed if those steps have already been executed before.

security association establishment framework: Security Framework for Security Association Establishment

security bootstrap framework: Security Framework for Remote security provisioning: a mechanism for remotely provisioning a Master Credential and Master Credential Identifier to a Enrolee and an M2M Authentication Function

secure environment: a logical entity that protects Sensitive Data and Sensitive Functions from tampering, unauthorized monitoring or execution and that provides access to these Sensitive Data and Sensitive Functions to authorized oneM2M entities

security framework: set of procedures providing Security Association Establishment or Remote security provisioning