ETSI TR 118 512 V2.0.0 (2016-09)

TECHNICAL REPORT

oneM2M; End-to-End Security and Group Authentication (oneM2M TR-0012 version 2.0.0)

Reference

DTR/oneM2M-000012

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 Report (TR) has been produced by ETSI Partnership Project oneM2M (oneM2M).

1 Scope

The present document provides options and analyses for the security features and mechanisms providing end-to-end security and group authentication for oneM2M.

The scope of this technical report includes use cases, threat analyses, high level architecture, generic requirements, available options, evaluation of options, and detailed procedures for executing end-to-end security and group authentication.

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.

Not applicable.

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

[i.2] W3C Recommendation: "Canonical XML Version 1.0", 2001.

NOTE: Available at http://www.w3.org/TR/xml-c14n.

[i.3] IETF RFC 7165: "Use Cases and Requirements for JSON Object Signing and Encryption (JOSE)".

[i.4] IETF RFC 5166: "An Interface and Algorithms for Authenticated Encryption", 2008.

[i.5] oneM2M drafting rules.

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

[i.6] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[i.7] ETSI TS 118 102: "oneM2M; Requirements (oneM2M TS-0002)".

[i.8] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003)".

[i.9] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004)".

[i.10] W3C Recommendation "XML Signature Syntax and Processing v1.1", 2013.

NOTE: Available at http://www.w3.org/TR/xmldsig-core1/.

[i.11] W3C Recommendation: "XML Encryption Syntax and Processing v1.1", 2013.

NOTE: Available at http://www.w3.org/TR/xmlenc-core1/.

[i.12] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.13] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[i.14] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[i.15] IETF RFC 4301: "Security Architecture for the Internet Protocol", 2005.

[i.16] IETF RFC 4880: "OpenPGP Message Format", 2007.

[i.17] IETF RFC 5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", 2010.

[i.18] Ferguson, Niels & Schneier, Bruce. "Practical Cryptography". Wiley. p. 333.
ISBN 978-0471223573, 2003.

[i.19] OASIS Standard: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", 2015.

[i.20] OASIS Standard: "Common Alerting Protocol Version 1.2", 2010.

[i.21] IETF RFC 7520: "Examples of Protecting Content using JavaScript Object Signing and Encryption (JOSE)", 2015.

[i.22] IETF RFC 2046: "Multipurpose Internet Mail Extensions, (MIME) Part Two: Media Types", 1996.

[i.23] IANA: "Media Types".

NOTE: Available at http://www.iana.org/assignments/media-types/media-types.xhtml.

[i.24] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", 2014.

[i.25] IETF RFC 7252: "The Constrained Application Protocol (CoAP)", 2014.

[i.26] IANA: "Constrained RESTful Environments (CoRE) Parameters, CoAP Content-Formats".

NOTE: Available at http://www.iana.org/assignments/core-parameters/core-parameters.xhtml#content-formats.

[i.27] OASIS Standard: "MQTT Version 3.1.1", 2014.

NOTE: Available at http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html.

[i.28] IETF RFC 5652: "Cryptographic Message Syntax (CMS)", 2009.

[i.29] Recommendation ITU-T X.680: Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[i.30] Recommendation X.681: "Information technology - Abstract Syntax Notation One (ASN.1): Information object specification".

[i.31] Recommendation X.682: "Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification".

[i.32] Recommendation X.683: "Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications".

[i.33] Recommendation ITU-T X.690: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[i.34] IETF RFC 3156: "MIME Security with OpenPGP", 2001.

[i.35] IANA: "Pretty Good Privacy (PGP)".

NOTE: Available at http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml.

[i.36] W3C XML Security Working Group.

NOTE: Available at http://www.w3.org/2008/xmlsec/.

[i.37] W3C Recommendation: "XML Signature Properties", 2013.

NOTE: Available at http://www.w3.org/TR/xmldsig-properties/.

[i.38] IETF RFC 7518: "JSON Web Algorithms (JWA)", 2015.

[i.39] IETF RFC 7527: "JSON Web Key (JWK)", 2015.

[i.40] IETF RFC 7526: "JSON Web Encryption (JWE)", 2015.

[i.41] IETF RFC 7525: "JSON Web Signature (JWS)", 2015.

[i.42] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[i.43] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[i.44] The Unicode Consortium: "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.1.0, March 2008.

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

[i.45] IETF RFC 2014: "HMAC: Keyed-Hashing for Message Authentication".

[i.46] IETF RFC 5869: "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", 2010.

[i.47] W. Diffie and M. Hellman: "New directions in cryptography", IEEE Transactions on Information Theory 22 (6): 644-654, 1976.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 118 111 [i.1] and the following apply:

authenticated encryption with associated data: An algorithm providing confidentiality for the plaintext and a way to check its integrity and authenticity while providing the ability to check the integrity and authenticity of some associated data. In this context: plaintext refers to data that is authenticated and encrypted; and associated data refers to data that is authenticated, but not encrypted. See IETF RFC 5166 [i.4] for further details.

canonical: unique and unambiguous representation of data [i.2].

canonicalization: process of converting a legal representation of data into its canonical form

End-to-End Authentication: provides an entity with the ability to validate another entity's identity that was supplied as part of the message

NOTE: The communicating entities can be multiple hops away.

End-to-End Data Confidentiality Protection: provides the ability for an entity to provide for confidentiality protection of data

NOTE: The confidentiality protected data can be transported over multiple hops consisting of trusted or untrusted communication entities. Only authorized entities can decrypt the confidentiality protected data. Such a protection mechanism would ensure that the data is confidentiality protected "at-rest" and "in-transit" even when handled by intermediate nodes.

End-to-End Data Integrity Protection: provides the ability for an entity to integrity protect data

NOTE: The integrity protected data can be transported over multiple hops consisting of trusted or untrusted communication entities. An authorized consumer of the data is able to verify the integrity of data and is also able to verify the originator of the data. Such a protection mechanism would ensure that the data is integrity protected "at-rest" and "in-transit" even when handled by intermediate nodes.

End-to-End Security: provides for securing messages that can traverse multiple hops between communication entities

NOTE: Securing of messages involves mutually authenticating the end entities. Securing of messages also involves providing confidentiality and integrity protection of messages in order that end entities are assured that the messages have not been altered or eavesdropped by un-authorized entities (including intermediary nodes involved in the transmission)

group authentication: provides an entity (authenticator) with the ability to validate the identities of all entities which belong to a group [i.6]

NOTE 1: Confidentiality and integrity of communication between the authenticator and each individual entity in the group is protected from exploit by other entities in the group and any middle node.

NOTE 2: This may contain additional information.

M2M Trust Enabler Function (TEF): trusted third-party entity that can provide services such as credential generation, registration and provisioning in order to enable secure data protection and access

object-based security: technology that embeds application data within a secure object that can be safely handled by untrusted entities [i.3]

3.2 Symbols

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

||	Concatenation

3.3 Abbreviations

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

AMI	Advanced Metering Infrastructure
AEAD	Authenticated Encryption with Associated Data
DAP	Data Aggregation Point
IdAx	Identifier for entity Ax
IdAy	Identifier for entity Ay
IdB	Identifier for entity B
IdC	Identifier for entity C
Kpsa	Provisioned Credential for M2M Security Association Establishment
KpsaId	Provisioned Credential for M2M Security Association Establishment Identifier
Ks	M2M Group Secure Connection Key
KsId	M2M Group Secure Connection Key Identifier
Rand	Random Number Generated by the Infrastructure Node
MN	Middle Node
IN	Infrastructure Node

4 Conventions

The key words "Shall", "Shall not", "May", "Need not", "Should", "Should not" in this document are to be interpreted as described in the oneM2M Drafting Rules [i.5].

5 Use Cases

5.1 Use Case of End-to-End Authentication in Key Distribution

5.1.1 Description

An oneM2M system may need to transfer sensitive data that should not be exposed to any intermediate nodes or even the application programs in the end nodes, i.e. these data should only be handled, stored and used in secure environments. One example is to distribute secret keys to the members of a group so that the group members can communicate to each other confidentially. In this case the hop-by-hop security mechanisms cannot meet the required security level, and an end-to-end security mechanism should be adopted.

The use case in the following clauses shows how an end-to-end mechanism could be used to deploy group credentials. For more information about using group credentials seeing clause 5.4.

5.1.2 Actors

The entities involved in this use case are shown in the Figure 5.1.2-1 and described as follows:

M2M Server: It represents an infrastructure equipment that is responsible for creating groups, generating group credentials and transferring group credentials to group members.

M2M Gateway: It represents a gateway that is responsible for forwarding the messages exchanging between M2M Server and target M2M Devices. It also acts as a group agent that is responsible for controlling the entities in the Group-1, Group-2 and Group-3, and broadcasting control commands to these entities.

M2M Device: It represents a device that is responsible for accumulating data from fire sensors, controlling fire doors or fire extinguishing equipments which are attached to this M2M Device.

Group-1: It contains a set of M2M Devices which are responsible for accumulating data from attached fire sensors.

Group-2: It contains a set of M2M Devices which are responsible for controlling attached fire doors.

Group-3: It contains a set of M2M Devices which are responsible for controlling attached fire extinguishing equipments.

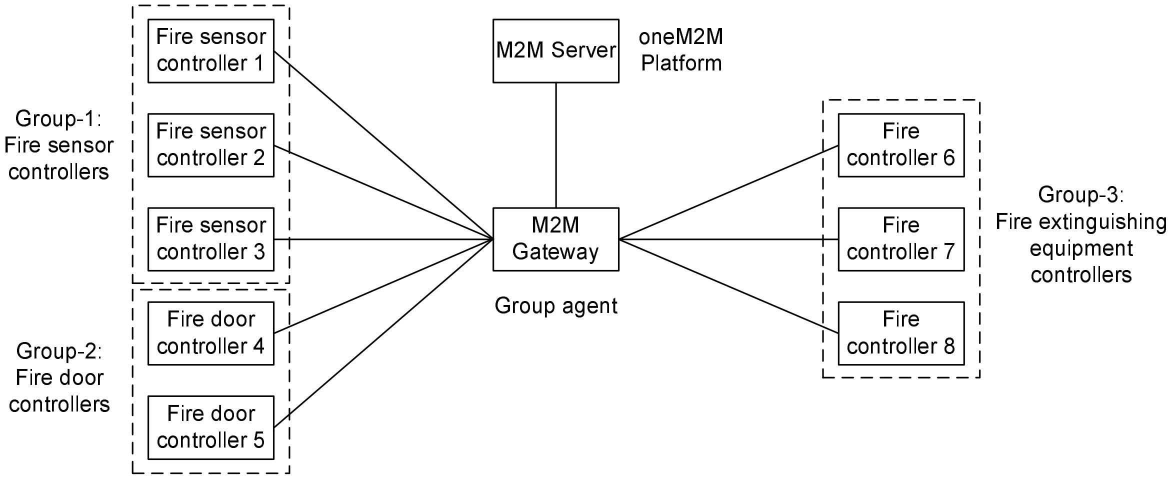

Figure 5.1.2-1: Group credential distribution use case

5.1.3 Pre-conditions

M2M Server, M2M Gateway and M2M Devices are all pre-provisioned with credential(s) that can be used for authentication, data integrity protection and data confidentiality protection.

M2M Devices register to the M2M Gateway in order to communicate with the M2M Server.

5.1.4 Normal Flow

Group credentials distribution procedure:

1) M2M Server creates group resources for the M2M Devices according to their functionality. Group-1 is used for grouping all the M2M Devices that are responsible for accumulating the data from the fire sensors. Group-2 is used for grouping all the M2M Devices that are responsible for controlling the fire doors. Group-3 is used for grouping all the M2M Devices that are responsible for controlling the fire extinguishing equipments.

2) The M2M Server generates group credentials for each group separately.

3) The M2M Server performs an end-to-end authentication with both the M2M Gateway and a target M2M Device with their pre-provisioned credentials. After that a security mechanism used to transfer group credentials is negotiated.

4) The M2M Server encrypts the group credentials using the pre-provisioned credentials shared with the M2M Device and the security method selected in step 3, encapsulates it into a message, and then sends this message to the M2M Gateway.

5) The M2M Gateway forwards the message further to the target M2M Device.

6) The target M2M Device extracts the encrypted content from the message, and then decrypts the encrypted content to get the group credentials.

5.1.5 Potential requirements

1) M2M System should support end-to-end security providing mutual authentication, security association establishment and remote security provisioning.

2) M2M System should support establishment of end-to-end security using pre-provisioned credentials.

3) The information exchanged between end entities should not be exposed to the intermediate nodes.