ETSI TS 118 103 V2.4.1 (2016-09)

oneM2M;
Security solutions
(oneM2M TS-0003 version 2.4.1 Release 2)

Reference

RTS/oneM2M-000003v200

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 9
Foreword 9
1 Scope 10
2 References 10
2.1 Normative references 10
2.2 Informative references 12
3 Definitions, symbols and abbreviations 13
3.1 Definitions 13
3.2 Symbols 18
3.3 Abbreviations 18
4 Conventions 19
5 Security Architecture 20
5.1 Overview 20
5.1.0 Introduction 20
5.1.1 Identification and Authentication 21
5.1.2 Authorization 21
5.1.3 Identity Management 22
5.2 Security Layers 22
5.2.1 Security Service Layer 22
5.2.2 Secure Environment Abstraction Layer 22
5.3 Integration within overall oneM2M architecture 23
6 Security Services and Interactions 23
6.1 Security Integration in oneM2M flow of events 23
6.1.1 Interactions between layers 23
6.1.2 High level sequence of events 24
6.1.2.1 Enrolment phase 24
6.1.2.2 Operational phase 25
6.1.2.2.1 M2M Service Access 25
6.1.2.2.2 Authorization to access M2M resources 26
6.2 Security Service Layer 26
6.2.1 Access Management 26
6.2.1.1 Authentication 26
6.2.2 Authorization Architecture 27
6.2.3 Security Administration 29
6.2.3.0 Introduction 29
6.2.3.1 Security Pre-Provisioning of SE 29
6.2.3.2 Remote security administration of SE 29
6.2.4 Identity Protection 29
6.2.5 Sensitive Data Handling 29
6.2.5.0 Introduction 29
6.2.5.1 Sensitive Functions 30
6.2.5.2 Secure Storage 30
6.2.6 Trust Enabler security functions 30
6.3 Secure Environment Abstraction Layer Components 31
6.3.1 Secure Environment 31
6.3.2 SE Plug-in 31
6.3.3 Secure Environment Abstraction 31
7 Authorization 32
7.1 Access Control Mechanism 32
7.1.1 General Description 32
7.1.2 Parameters of the Request message 33
7.1.3 Format of *privileges* and *selfPrivileges* Attributes 34
7.1.4 Access Control Decision 36

7.1.5 Description of the Access Decision Algorithm....37
7.2 AE Impersonation Prevention....38
7.2.1 Registrar verification of AE-ID....38
7.2.2 Verification Using End-to-End Security of Primitives (ESPrim)....39
7.3 Dynamic Authorization....40
7.3.1 Purpose of the Dynamic Authorization....40
7.3.2 Dynamic Authorization Stage 2 Details....41
7.3.2.1 Dynamic Authorization Reference Model....41
7.3.2.2 Direct Dynamic Authorization....43
7.3.2.3 Indirect Dynamic Authorization....45
7.3.2.4 Token Structure....48
7.3.2.5 Token Evaluation....49
7.3.2.6 oneM2M JSON Web Tokens (JWTs)....49
7.3.2.6.1 Introduction to oneM2M JWTs....49
7.3.2.6.2 oneM2M JWT Profile....49
7.3.2.6.3 oneM2M JWT Procedures....51
7.4 Role Based Access Control....51
7.4.1 Role Based Access Control Architecture....51
7.4.2 Role Issuing Procedure....53
7.4.2.1 Introduction....53
7.4.2.2 Role Assignment Procedure....53
7.4.2.3 Issuing Token Associated with Role....54
7.4.3 Role Based Access Control Procedure....55

8 Security Frameworks....56
8.1 General Introductions to the Security Frameworks....56
8.1.0 General....56
8.1.1 General Introduction to the Symmetric Key Security Framework....56
8.1.2 General Introduction to the Certificate-Based Security Framework....56
8.1.2.0 Introduction....56
8.1.2.1 Public Key Certificate Flavours....56
8.1.2.2 Certification Path Validation and Certificate Status Verification....57
8.1.2.3 Credential Configuration for Certificate-Based Security Framework....58
8.1.2.4 Information Needed for Certificate Authentication of another Entity....58
8.1.2.5 Certificate Verification....59
8.1.3 General Introduction to the GBA (Generic Bootstrapping Architecture) Framework....60
8.2 Security Association Establishment Frameworks....61
8.2.1 Overview on Security Association Establishment Frameworks....61
8.2.2 Detailed Security Association Establishment Frameworks....65
8.2.2.1 Provisioned Symmetric Key Security Association Establishment Frameworks....65
8.2.2.2 Certificate-Based Security Association Establishment Frameworks....66
8.2.2.3 MAF-Based Symmetric Key Security Association Establishment Frameworks....68
8.3 Remote Security Provisioning Frameworks....71
8.3.1 Overview on Remote Security Provisioning Frameworks....71
8.3.1.1 Purpose of Remote Security Provisioning Frameworks....71
8.3.1.2 Overview on Remote Security Provisioning Frameworks....72
8.3.2 Detailed Remote Security Provisioning Framework....74
8.3.2.1 Pre-Provisioned Symmetric Key Remote Security Provisioning Framework....74
8.3.2.2 Certificate-Based Remote Security Provisioning Framework....79
8.3.2.3 GBA-Based Remote Security Provisioning Framework....80
8.3.3 Common Remote Security Provisioning Framework Procedures....83
8.3.3.1 Certificate Enrolment Procedure call flow....83
8.4 End-to-End Security of Primitives (ESPrim)....83
8.4.1 Purpose of E2E Security of Primitives (ESPrim)....83
8.4.2 End-to-End Security of Primitives (ESPrim) Architecture....84
8.4.3 End-to-End Security of Primitives (ESPrim) Protocol Details....91
8.4.3.1 End-to-End Security of Primitives (ESPrim) Parameter Definitions....91
8.4.3.1.1 originatorESPrimRandObject parameter definition....91
8.4.3.1.2 receiverESPrimRandObject parameter definition....91
8.4.3.1.3 *e2eSecInfo* resource attribute definition....92
8.4.3.2 ESPrim Object formatting and processing using the JWE Compact Serialization....92
8.5 End-to-End Security of Data (ESData)....94

8.5.1 Purpose of ESData ... 94
8.5.2 ESData Architecture ... 95
8.5.2.1 List of ESData Security Classes and ESData Protection Options ... 95
8.5.2.2 Encryption-Only ESData Security Class ... 96
8.5.2.2.1 Encryption-Only ESData Security Class Overview ... 96
8.5.2.2.2 Encryption using Provisioned Symmetric ESData Key ... 97
8.5.2.2.3 Encryption using Trust Enabling Function ... 97
8.5.2.2.4 Encryption using Target End-Point Certificates ... 98
8.5.2.3 Signature-Only ESData Security Class ... 98
8.5.2.3.1 Signature-Only ESData Security Class Overview ... 98
8.5.2.3.2 Digital Signature using Source End-Point Certificate ... 100
8.5.2.4 Nested Sign-then-Encrypt ... 100
8.5.3 End-to-End Security of Data (ESData) Protocol Details ... 101
8.5.3.1 Introduction ... 101
8.5.3.2 Encryption-Only ESData Security Class Protocol Details ... 101
8.5.3.3 Signature-Only ESData Security Class Protocol Details ... 103
8.5.3.4 Nested-Sign-then-Encrypt ESData Security Class Protocol Details ... 104
8.6 Remote Security Frameworks for End-to-End Security ... 104
8.6.1 Overview on Remote Provisioning and Registration of Credentials for End-to-End Security ... 104
8.6.1.1 Introduction ... 104
8.6.1.2 Overall Description of Registration and Remote Provisioning for End-to-End Security ... 104
8.6.2 Remote Security Provisioning Process for End-to-End Security Credentials ... 106
8.6.3 Detailed Description on Source-Generated End-to-End Credentials ... 109
8.7 End-to-End Certificate-based Key Establishment (ESCertKE) ... 111
8.7.1 Purpose of ESCertKE ... 111
8.7.2 ESCertKE Architecture ... 111
8.7.2.1 ESCertKE Reference Model ... 111
8.7.2.2 ESCertKE Procedure Message Flow ... 111
8.8 MAF Security Framework Details ... 114
8.8.1 Introduction to the MAF Security Framework Details ... 114
8.8.2 MAF Security Framework Processing and Information Flows ... 116
8.8.2.1 Introduction ... 116
8.8.2.2 MAF Handshake Procedure ... 116
8.8.2.3 MAF Client Registration Procedure ... 116
8.8.2.4 MAF Client Configuration Retrieval Procedure ... 117
8.8.2.5 MAF Client Registration Update Procedure ... 118
8.8.2.6 MAF Client De-Registration Procedure ... 119
8.8.2.7 MAF Key Registration Procedure ... 120
8.8.2.8 MAF Key Retrieval Procedure ... 122
8.8.2.9 MAF Key Registration Update Procedure ... 123
8.8.2.10 MAF Key De-Registration Procedure ... 124
8.8.3 MAF Client Configuration Details ... 124
8.8.3.1 MAF Client Credential Configuration Details ... 124
8.8.3.2 MAF Client Registration Configuration Details ... 125
8.8.3.3 MAF Key Registration Configuration Details ... 126

9 Security Framework Procedures and Parameters ... 126
9.0 Introduction ... 126
9.1 Security Association Establishment Framework Procedures and Parameters ... 127
9.1.1 Credential Configuration Parameters ... 127
9.1.1.0 Introduction ... 127
9.1.1.1 Credential Configuration of Entity A and Entity B ... 127
9.1.1.2 Credential Configuration of M2M Authentication Functions ... 128
9.1.2 Association Configuration Procedures and Parameters ... 128
9.1.2.0 Introduction ... 128
9.1.2.1 Association Configuration of Entity A and Entity B ... 128
9.1.2.1.1 Association Configuration of Entity A ... 128
9.1.2.1.2 Association Configuration of Entity B ... 129
9.1.2.2 Association Configuration of M2M Authentication Functions ... 129
9.2 Remote Security Provisioning Framework Procedures and Parameters ... 130
9.2.1 Bootstrap Credential Configuration Procedures and Parameters ... 130
9.2.1.0 Introduction ... 130

9.2.1.1 Bootstrap Credential Configuration of Enrolee....130
9.2.1.2 Bootstrap Credential Configuration of M2M Enrolment Functions....131
9.2.2 Bootstrap Instruction Configuration Procedures and Parameters....131
9.2.2.0 Introduction....131
9.2.2.1 Bootstrap Instruction Configuration of Enrolees....131
9.2.2.2 Void....132
9.2.2.3 Bootstrap Instruction Configuration of M2M Enrolment Functions....132
9.2.2.4 Bootstrap Instruction Configuration of UNSP Authentication Server....133
9.2.3 End-to-End Credential Configuration Procedures and Parameters....133
9.2.3.0 Introduction....133
9.2.3.1 End-to-End Credential Configuration of Source ESF End-Points and Target ESF End-Points....133
9.2.3.2 End-to-End Credential Configuration at the M2M Trust Enabler Functions....134
9.2.3.3 Configuration parameters for enabling End-to-End Security at Source ESF End-Points and Target ESF End-Points....135

10 Protocol and Algorithm Details....136
10.1 Certificate-Based Security Framework Details....136
10.1.1 Certificate Profiles....136
10.1.1.0 General....136
10.1.1.1 Common Certificate Details....136
10.1.1.2 Raw Public Key Certificate Profile....136
10.1.1.3 Details Common to Certificates with Certificate Chains....136
10.1.1.4 Profile for Device Certificates and their Certificate Chains....136
10.1.1.4.1 Profile for Device Certificates....136
10.1.1.4.2 Profile for Certificate Authority Certificates for Device Certificates....137
10.1.1.5 Profile for AE-ID Certificates and their Certificate Chains....137
10.1.1.6 Profile for FQDN Certificates and their Certificate Chains....137
10.1.1.7 Profile for CSE-ID Certificates and their Certificate Chains....137
10.1.2 Public Key Identifiers....138
10.1.3 Support Requirements for each Public Key Certificate Flavour....138
10.2 TLS and DTLS Details....138
10.2.1 TLS and DTLS Versions....138
10.2.2 TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks....139
10.2.3 TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks....139
10.3 Key Export and Key Derivation Details....140
10.3.1 TLS Key Export Details....140
10.3.2 Derivation of Master Credential from Enrolment Key....140
10.3.3 Derivation of Provisioned Secure Connection Key from Enrolment Key....141
10.3.4 Generating KeID....141
10.3.5 Generating Key Identifier for the MAF Security Framework....141
10.3.6 Derivation of End-to-End Master Key from Provisioned Secure Connection Key....141
10.3.6.1 Introduction....141
10.3.6.2 Key Extraction and Expansion of End-to-End Master Key....142
10.3.7 Derivation of Usage-Constrained Symmetric Keys from Enrolment Key....142
10.3.8 sessionESPrimKey Derivation Algorithms....143
10.3.8.1 Introduction....143
10.3.8.2 HMAC-SHA256 sessionESPrimKey Derivation Algorithm....143
10.4 Credential-ID Details....143
10.5 KpsaID....144
10.6 KmID Format....144
10.7 Enrolment Expiry....144

11 Privacy Protection Architecture using Privacy Policy Manager（PPM）....144
11.1 Introduction....144
11.2 Relationship between components of PPM and oneM2M....145
11.3 Privacy Policy Management in oneM2M Architecture....145
11.3.1 Introduction....145
11.3.2 Involved Entities....145
11.3.3 Management Flow in PPM Architecture....146
11.3.3.0 Introduction....146
11.3.3.1 Joining an IN-CSE....146
11.3.3.2 Subscription to a service by IN-AE....147

11.3.3.3 Request for personal data to the IN-CSE 149
11.4 Privacy Policy Manager Implementation Models 151
11.4.1 Using Terms and Conditions Mark-up Language 151
11.4.1.0 Introduction 151
11.4.1.1 Registration of Application Service Provider Privacy Policy 152
11.4.1.2 Registration of End User Privacy Preferences 153
11.4.1.3 Creating a customized Privacy Policy for each end user 153

12 Security-Specific oneM2M Data Type Definitions 154
12.1 Introduction 154
12.2 Simple Security-Specific oneM2M Data Types 154
12.3 Enumerated Security-Specific oneM2M Data Types 154
12.3.1 Introduction 154
12.3.2 Enumeration type definitions 154
12.3.2.1 sec:credIDTypeID 154
12.4 Complex Security-Specific oneM2M Data Types 155
12.4.1 sec:tefClientCfg 155
12.4.2 sec:tefClientRegCfg 156
12.4.3 sec:tefKeyRegCfg 156

Annex A (informative): Mapping of 3GPP GBA terminology 157

Annex B (informative): General Mutual Authentication Mechanism 158

B.0 Introduction 158

B.1 Group Authentication 159

Annex C (normative): Security protocols associated to specific SE technologies 160

C.0 Introduction 160

C.1 UICC 160

C.2 Other secure element and embedded secure element with ISO 7816 interface 160

C.3 Trusted Execution Environment 160

C.4 SE to CSE binding 160

Annex D (normative): UICC security framework to support oneM2M Services 161

D.0 Introduction 161

D.1 Access Network UICC-based oneM2M Service Framework 162
D.1.1 Access Network UICC-based oneM2M Service Framework characteristics 162
D.1.2 M2M Service Framework discovery for Access Network UICC 162
D.1.3 Content of files at the DF_{1M2M} level 163
D.1.3.0 Introduction 163
D.1.3.1 EF_{1M2MST} (oneM2M Service Table) 163
D.1.3.2 $EF_{1M2MSID}$ (oneM2M Subscription Identifier) 165
D.1.3.3 $EF_{1M2MSPID}$ (oneM2M Service Provider Identifier) 165
D.1.3.4 EF_{M2MNID} (M2M Node Identifier) 166
D.1.3.5 EF_{CSEID} (local CSE Identifier) 166
D.1.3.6 $EF_{M2MAE-ID}$ (M2M Application Identifiers list) 166
D.1.3.7 $EF_{INCSEIDS}$ (M2M IN-CSE IDs list) 167
D.1.3.8 $EF_{MAFFQDN}$ (MAF-FQDN) 167
D.1.3.9 EF_{MEFID} (M2M Enrolment Function Identifier) 168

D.2 oneM2M Service Module application for symmetric credentials on UICC (1M2MSM) 169
D.2.0 Introduction 169
D.2.1 oneM2M Service Module application file structure 169
D.2.1.0 Introduction 169
D.2.1.1 Content of UICC files at the Master File (MF) level 169
D.2.1.2 Content of files at the 1M2MSM ADF (Application DF) level 169
D.2.2 oneM2M Subscription related procedures for M2M Service 170

D.2.2.0 Introduction....170
D.2.2.1 Initialization - 1M2MSM Application selection....170
D.2.2.2 1M2MSM session termination....170
D.2.2.3 oneM2M Service discovery procedure....170
D.2.2.4 oneM2M Service provisioning procedures....170
D.2.2.5 oneM2M Application Identifiers provisioning procedure....171
D.2.2.6 oneM2M Secure provisioning related procedures....171
D.2.2.7 oneM2M Security Association related procedures....171

Annex E (informative): Precisions for the UICC framework to support M2M Services....172

E.0 Introduction....172

E.1 Suggested content of the EFs at pre-personalization....172

E.2 EF changes via Data Download or CAT applications....172

E.3 List of SFI values at the ADF_{M2MSM} or DF_{M2M} level....173

E.4 UICC related tags defined in annex J....173

Annex F (normative): Acquisition of Location Information for Location based Access Control....174

F.0 Introduction....174

F.1 Description of Region....174
F.1.1 Circular Description....174
F.1.2 Country Description....174

F.2 Acquisition of Location Information....174
F.2.0 Introduction....174
F.2.1 Circular Description....175
F.2.2 Country Description....176

Annex G (informative): Access Control Decision Request....177

Annex H (informative): Implementation Guidance and index of solutions....178

Annex I (informative): Bibliography....179

Annex J (normative): List of Privacy Attributes....180

Annex K (informative): Terms and Conditions Mark-up Language implementation rules....189

History....191

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+) (GSM); 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] Void.

[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.

[48] IETF RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF).

[49] IETF RFC 7518 (2015): "JSON Web Algorithms (JWA)".

[50] IETF RFC 7516: "JSON Web Encryption (JWE)", 2015.

[51] IETF RFC 7515: "JSON Web Signature (JWS)", 2015.

[52] W3C Recommendation: "XML Signature Syntax and Processing v1.1", 2013.

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

[53] IETF RFC 7519: "JSON Web Token (JWT)", 2015.

[54] OpenID Foundation: "OpenID Connect Core 1.0", 2014.

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

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

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

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.

[i.2] Void.

[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.

[i.13] Void.

[i.14] Void.

[i.15] ETSI TR 118 519: "oneM2M Dynamic Authorization for IoT".

[i.16] ETSI TR 118 512: "oneM2M End-to-End Security and Group Authentication (oneM2M TR-0012)".

[i.17] ETSI TR 118 501: "oneM2M Use Case collection".

[i.18] IANA JSON Web Token (JWT) registry.

NOTE: Available at http://www.iana.org/assignments/jwt/jwt.xhtml.

[i.19] IETF RFC 6455: "The Web Socket Protocol", December 2011.

[i.20] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[i.21] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

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 [2] and the following apply:

additional authenticated data [14]: Refers to data that is authenticated, but not encrypted by an authenticated encryption with associated data algorithm.

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

authenticated encryption with associated data [14]: 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 additional authenticated data. In this context plaintext refers to data that is authenticated and encrypted