

ETSI TS 118 103 V2.12.1 (2019-04)



oneM2M; Security solutions (oneM2M TS-0003 version 2.12.1 Release 2A)

ITeH STANDARDS PREVIEW
(standards.iteh.ai)
Full standard available at <https://standards.iteh.ai/catalog/standards/sis/444e-8d85-9a29b87205bd/etsi-ts-118-118-1-2019-04>



Reference

RTS/oneM2M-000003v2A

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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 2019.

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 a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

| | |
|---|----|
| Intellectual Property Rights | 11 |
| Foreword..... | 11 |
| 1 Scope | 12 |
| 2 References | 12 |
| 2.1 Normative references | 12 |
| 2.2 Informative references..... | 14 |
| 3 Definition of terms, symbols and abbreviations..... | 16 |
| 3.1 Terms..... | 16 |
| 3.2 Symbols..... | 21 |
| 3.3 Abbreviations | 21 |
| 4 Conventions..... | 22 |
| 5 Security Architecture..... | 23 |
| 5.1 Overview | 23 |
| 5.1.0 Introduction..... | 23 |
| 5.1.1 Identification and Authentication | 25 |
| 5.1.2 Authorization | 25 |
| 5.1.3 Identity Management | 25 |
| 5.2 Security Layers..... | 25 |
| 5.2.1 Security Service Layer..... | 25 |
| 5.2.2 Secure Environment Abstraction Layer..... | 26 |
| 5.3 Integration within overall oneM2M architecture..... | 26 |
| 6 Security Services and Interactions | 27 |
| 6.1 Security Integration in oneM2M flow of events..... | 27 |
| 6.1.1 Interactions between layers..... | 27 |
| 6.1.2 High level sequence of events..... | 27 |
| 6.1.2.1 Enrolment phase..... | 27 |
| 6.1.2.2 Operational phase..... | 28 |
| 6.1.2.2.1 M2M Service Access..... | 28 |
| 6.1.2.2.2 Authorization to access M2M resources..... | 29 |
| 6.2 Security Service Layer | 29 |
| 6.2.1 Access Management | 29 |
| 6.2.1.1 Authentication..... | 29 |
| 6.2.2 Authorization Architecture | 30 |
| 6.2.3 Security Administration | 32 |
| 6.2.3.0 Introduction..... | 32 |
| 6.2.3.1 Security Pre-Provisioning of SE | 32 |
| 6.2.3.2 Remote security administration of SE..... | 32 |
| 6.2.4 Identity Protection | 32 |
| 6.2.5 Sensitive Data Handling | 32 |
| 6.2.5.0 Introduction..... | 32 |
| 6.2.5.1 Sensitive Functions | 33 |
| 6.2.5.2 Secure Storage..... | 33 |
| 6.2.6 Trust Enabling security functions | 33 |
| 6.3 Secure Environment Abstraction Layer Components | 34 |
| 6.3.1 Secure Environment..... | 34 |
| 6.3.2 SE Plug-in..... | 34 |
| 6.3.3 Secure Environment Abstraction | 34 |
| 7 Authorization..... | 35 |
| 7.1 Access Control Mechanism | 35 |
| 7.1.1 General Description | 35 |
| 7.1.2 Parameters of the Request message | 36 |
| 7.1.3 Format of <i>privileges</i> and <i>selfPrivileges</i> Attributes..... | 37 |
| 7.1.4 Access Control Decision..... | 40 |

| | | |
|-----------|--|----|
| 7.1.5 | Description of the Access Decision Algorithm..... | 40 |
| 7.2 | AE Impersonation Prevention | 43 |
| 7.2.1 | Registrar verification of AE-ID | 43 |
| 7.2.2 | Verification Using End-to-End Security of Primitives (ESPrim) | 44 |
| 7.3 | Dynamic Authorization | 45 |
| 7.3.1 | Purpose of the Dynamic Authorization..... | 45 |
| 7.3.2 | Dynamic Authorization Stage 2 Details..... | 45 |
| 7.3.2.1 | Dynamic Authorization Reference Model | 45 |
| 7.3.2.2 | Direct Dynamic Authorization | 47 |
| 7.3.2.3 | Indirect Dynamic Authorization..... | 50 |
| 7.3.2.4 | Token Structure | 52 |
| 7.3.2.5 | Token Evaluation | 53 |
| 7.3.2.6 | oneM2M JSON Web Tokens (JWTs) | 54 |
| 7.3.2.6.1 | Introduction to oneM2M JWTs | 54 |
| 7.3.2.6.2 | oneM2M JWT Profile..... | 54 |
| 7.3.2.6.3 | oneM2M JWT Procedures..... | 55 |
| 7.4 | Role Based Access Control | 56 |
| 7.4.1 | Role Based Access Control Architecture..... | 56 |
| 7.4.2 | Role Issuing Procedure | 57 |
| 7.4.2.1 | Introduction | 57 |
| 7.4.2.2 | Role Assignment Procedure | 57 |
| 7.4.2.3 | Issuing Token Associated with Role | 58 |
| 7.4.3 | Role Based Access Control Procedure..... | 60 |
| 8 | Security Frameworks..... | 61 |
| 8.1 | General Introductions to the Security Frameworks | 61 |
| 8.1.0 | General..... | 61 |
| 8.1.1 | General Introduction to the Symmetric Key Security Frameworks | 61 |
| 8.1.2 | General Introduction to the Certificate-Based Security Frameworks | 61 |
| 8.1.2.0 | Introduction..... | 61 |
| 8.1.2.1 | Public Key Certificate Flavours | 61 |
| 8.1.2.2 | Certification Path Validation and Certificate Status Verification | 62 |
| 8.1.2.3 | Credential Configuration for Certificate-Based Security Framework | 63 |
| 8.1.2.4 | Information Needed for Certificate Authentication of another Entity..... | 63 |
| 8.1.2.5 | Certificate Verification..... | 64 |
| 8.1.3 | General Introduction to the GBA (Generic Bootstrapping Architecture) Framework | 65 |
| 8.2 | Security Association Establishment Frameworks | 66 |
| 8.2.1 | Overview on Security Association Establishment Frameworks | 66 |
| 8.2.2 | Detailed Security Association Establishment Frameworks | 70 |
| 8.2.2.1 | Provisioned Symmetric Key Security Association Establishment Frameworks | 70 |
| 8.2.2.2 | Certificate-Based Security Association Establishment Frameworks | 72 |
| 8.2.2.3 | MAF-Based Symmetric Key Security Association Establishment Frameworks..... | 74 |
| 8.3 | Remote Security Provisioning Frameworks | 77 |
| 8.3.1 | Overview on Remote Security Provisioning Frameworks | 77 |
| 8.3.1.1 | Purpose of Remote Security Provisioning Frameworks..... | 77 |
| 8.3.1.2 | High Level Flow | 78 |
| 8.3.2 | Detailed Remote Security Provisioning Framework..... | 81 |
| 8.3.2.1 | Pre-Provisioned Symmetric Key Remote Security Provisioning Framework..... | 81 |
| 8.3.2.2 | Certificate-Based Remote Security Provisioning Framework..... | 86 |
| 8.3.2.3 | GBA-Based Remote Security Provisioning Framework | 87 |
| 8.3.3 | Void | 90 |
| 8.3.4 | Enrolment Exchange | 90 |
| 8.3.4.1 | Enrolment Exchange Procedures | 90 |
| 8.3.4.2 | MEF Client Registration | 90 |
| 8.3.4.3 | Symmetric Key Provisioning | 90 |
| 8.3.4.4 | Certificate Provisioning | 91 |
| 8.3.4.5 | Device Configuration | 91 |
| 8.3.4.6 | MEF Client Command | 91 |
| 8.3.5 | Symmetric Key Provisioning Details..... | 93 |
| 8.3.5.1 | Introduction | 93 |
| 8.3.5.2 | MEF Security Framework Processing and Information Flows | 94 |
| 8.3.5.2.1 | Introduction | 94 |

| | | |
|------------|--|-----|
| 8.3.5.2.2 | MEF Handshake Procedure | 94 |
| 8.3.5.2.3 | MEF Client Registration Procedure..... | 95 |
| 8.3.5.2.4 | MEF Client Configuration Retrieval Procedure | 96 |
| 8.3.5.2.5 | MEF Client Registration Update Procedure | 97 |
| 8.3.5.2.6 | MEF Client De-Registration Procedure..... | 97 |
| 8.3.5.2.7 | MEF Key Registration Procedure..... | 98 |
| 8.3.5.2.8 | MEF Key Retrieval Procedure | 100 |
| 8.3.5.2.9 | MEF Key Registration Update Procedure | 101 |
| 8.3.5.2.10 | MEF Key De-Registration Procedure..... | 102 |
| 8.3.5.3 | Mapping to Protocol in ETSI TS 118 132..... | 102 |
| 8.3.6 | Certificate Provisioning Procedure Details..... | 102 |
| 8.3.6.1 | Introduction..... | 102 |
| 8.3.6.2 | Certificate Provisioning procedures using EST | 103 |
| 8.3.6.2.1 | Introduction | 103 |
| 8.3.6.2.2 | Initial Certificate Provisioning procedure using EST | 104 |
| 8.3.6.2.3 | Certificate Re-Provisioning procedure using EST..... | 105 |
| 8.3.6.3 | Certificate Provisioning procedures using SCEP | 106 |
| 8.3.6.3.1 | Introduction | 106 |
| 8.3.6.3.2 | Details of Certificate Provisioning procedures using SCEP | 106 |
| 8.3.7 | MEF Client Configuration Details..... | 107 |
| 8.3.7.1 | MEF Client Credential Configuration Details..... | 107 |
| 8.3.7.2 | MEF Client Registration Configuration Details..... | 108 |
| 8.3.7.3 | MEF Key Registration Configuration Details..... | 109 |
| 8.3.8 | Profile for Device Configuration within an Enrolment Exchange | 109 |
| 8.3.9 | MEF Client Command Processing..... | 110 |
| 8.3.9.1 | Introduction..... | 110 |
| 8.3.9.2 | MEF Client Command Retrieve Procedure..... | 110 |
| 8.3.9.3 | MEF Client Command Update procedure..... | 112 |
| 8.3.9.4 | The cmdDescription element | 112 |
| 8.3.9.5 | The cmdStatusCode element | 113 |
| 8.3.9.5.1 | Introduction | 113 |
| 8.3.9.5.2 | cmdStatusCode MEF_CLIENT_CMD_ISSUED..... | 113 |
| 8.3.9.5.3 | cmdStatusCode MEF_CLIENT_CMD_REISSUED..... | 113 |
| 8.3.9.5.4 | cmdStatusCode MEF_CLIENT_CMD_OK..... | 114 |
| 8.3.9.5.5 | cmdStatusCode MEF_CLIENT_CMD_REPEATED_CMD_ID | 114 |
| 8.3.9.5.6 | cmdStatusCode MEF_CLIENT_CMD_CLASS_NOT_SUPPORTED..... | 114 |
| 8.3.9.5.7 | cmdStatusCode MEF_CLIENT_CMD_BAD_ARGUMENTS | 114 |
| 8.3.9.5.8 | cmdStatusCode MEF_CLIENT_CMD_UNACCEPTABLE_ARGUMENTS | 114 |
| 8.3.9.5.9 | cmdStatusCode MEF_CLIENT_CMD_CERT_PROV_SERVER_ERROR..... | 114 |
| 8.3.9.5.10 | cmdStatusCode MEF_CLIENT_CMD_CERT_PROV_CLIENT_ERROR..... | 114 |
| 8.3.9.5.11 | cmdStatusCode MEF_CLIENT_CMD_DEV_CFG_SERVER_ERROR..... | 114 |
| 8.3.9.5.12 | cmdStatusCode MEF_CLIENT_CMD_DEV_CFG_CLIENT_ERROR..... | 114 |
| 8.3.9.5.13 | cmdStatusCode MEF_CLIENT_CMD_MO_NODE_NOT_FOUND..... | 114 |
| 8.3.9.5.14 | cmdStatusCode MEF_CLIENT_CMD_MO_NODE_TYPE_CONFLICT | 114 |
| 8.3.9.5.15 | cmdStatusCode MEF_CLIENT_CMD_MO_NODE_BAD_ARGS..... | 115 |
| 8.3.9.5.16 | cmdStatusCode MEF_CLIENT_CMD_MO_NODE_UNACCEPTABLE_ARGS..... | 115 |
| 8.3.9.5.17 | cmdStatusCode MEF_CLIENT_CMD_MO_NODE_INCONSISTENT_CONFIG | 115 |
| 8.3.9.5.18 | cmdStatusCode MEF_CLIENT_CMD_MO_NODE_PROCESSING_FAILED | 115 |
| 8.3.9.6 | NO_MORE_COMMANDS MEF Client Command Class-specific Processes | 115 |
| 8.3.9.7 | CERT_PROV MEF Client Command Class-specific Processes..... | 116 |
| 8.3.9.8 | DEV_CFG MEF Client Command Class-specific Processes..... | 117 |
| 8.3.9.9 | MO_NODE MEF Client Command Class-specific Processes | 118 |
| 8.3.9.9.1 | Generic MO_NODE Processes..... | 118 |
| 8.3.9.9.2 | [authenticationProfile]-specific Processes | 119 |
| 8.3.9.9.3 | Process [authenticationProfile] MO Node with pre-provisioned symmetric key..... | 121 |
| 8.3.9.9.4 | Process [authenticationProfile] MO Node with MEF-established symmetric key..... | 122 |
| 8.3.9.9.5 | Process [authenticationProfile] MO Node with MAF-established symmetric key | 123 |
| 8.3.9.9.6 | Process [authenticationProfile] MO Node with Certificate | 124 |
| 8.3.9.9.7 | [trustAnchorCred]-specific Processes | 124 |
| 8.3.9.9.8 | [MAFClientRegCfg]-specific Processes | 125 |
| 8.4 | End-to-End Security of Primitives (ESPrim) | 126 |
| 8.4.1 | Purpose of E2E Security of Primitives (ESPrim) | 126 |

| | | |
|-----------|---|-----|
| 8.4.2 | End-to-End Security of Primitives (ESPrim) Architecture | 126 |
| 8.4.3 | End-to-End Security of Primitives (ESPrim) Protocol Details | 134 |
| 8.4.3.1 | End-to-End Security of Primitives (ESPrim) Parameter Definitions | 134 |
| 8.4.3.1.1 | originatorESPrimRandObject parameter definition..... | 134 |
| 8.4.3.1.2 | receiverESPrimRandObject parameter definition..... | 135 |
| 8.4.3.1.3 | <i>e2eSecInfo</i> resource attribute definition | 135 |
| 8.4.3.2 | ESPrim Object formatting and processing using the JWE Compact Serialization..... | 135 |
| 8.5 | End-to-End Security of Data (ESData) | 138 |
| 8.5.1 | Purpose of ESData..... | 138 |
| 8.5.2 | ESData Architecture | 138 |
| 8.5.2.1 | List of ESData Security Classes and ESData Protection Options | 138 |
| 8.5.2.2 | Encryption-Only ESData Security Class..... | 139 |
| 8.5.2.2.1 | Encryption-Only ESData Security Class Overview | 139 |
| 8.5.2.2.2 | Encryption using Provisioned Symmetric ESData Key..... | 141 |
| 8.5.2.2.3 | Encryption using Trust Enabling Function..... | 141 |
| 8.5.2.2.4 | Encryption using Target End-Point Certificates..... | 141 |
| 8.5.2.3 | Signature-Only ESData Security Class | 142 |
| 8.5.2.3.1 | Signature-Only ESData Security Class Overview | 142 |
| 8.5.2.3.2 | Digital Signature using Source End-Point Certificate | 143 |
| 8.5.2.4 | Nested Sign-then-Encrypt | 144 |
| 8.5.3 | End-to-End Security of Data (ESData) Protocol Details | 144 |
| 8.5.3.1 | Introduction | 144 |
| 8.5.3.2 | Encryption-Only ESData Security Class Protocol Details | 145 |
| 8.5.3.3 | Signature-Only ESData Security Class Protocol Details | 146 |
| 8.5.3.4 | Nested-Sign-then-Encrypt ESData Security Class Protocol Details | 147 |
| 8.6 | Remote Security Frameworks for End-to-End Security | 147 |
| 8.6.1 | Overview on Remote Provisioning and Registration of Credentials for End-to-End Security | 147 |
| 8.6.1.1 | Introduction | 147 |
| 8.6.1.2 | Overall Description of Registration and Remote Provisioning for End-to-End Security | 148 |
| 8.6.2 | Remote Security Provisioning Process for End-to-End Security Credentials..... | 150 |
| 8.6.3 | Detailed Description on Source-Generated End-to-End Credentials | 153 |
| 8.7 | End-to-End Certificate-based Key Establishment (ESCertKE)..... | 155 |
| 8.7.1 | Purpose of ESCertKE | 155 |
| 8.7.2 | ESCertKE Architecture..... | 155 |
| 8.7.2.1 | ESCertKE Reference Model | 155 |
| 8.7.2.2 | ESCertKE Procedure Message Flow..... | 155 |
| 8.8 | MAF Security Framework Details | 158 |
| 8.8.1 | Introduction to the MAF Security Framework Details | 158 |
| 8.8.2 | MAF Security Framework Processing and Information Flows | 160 |
| 8.8.2.1 | Introduction | 160 |
| 8.8.2.2 | MAF Handshake Procedure | 160 |
| 8.8.2.3 | MAF Client Registration Procedure..... | 160 |
| 8.8.2.4 | MAF Client Configuration Retrieval Procedure | 161 |
| 8.8.2.5 | MAF Client Registration Update Procedure | 162 |
| 8.8.2.6 | MAF Client De-Registration Procedure..... | 163 |
| 8.8.2.7 | MAF Key Registration Procedure..... | 163 |
| 8.8.2.8 | MAF Key Retrieval Procedure..... | 165 |
| 8.8.2.9 | MAF Key Registration Update Procedure | 166 |
| 8.8.2.10 | MAF Key De-Registration Procedure..... | 167 |
| 8.8.3 | MAF Client Configuration Details | 168 |
| 8.8.3.1 | MAF Client Credential Configuration Details | 168 |
| 8.8.3.2 | MAF Client Registration Configuration Details | 168 |
| 8.8.3.3 | MAF Key Registration Configuration Details | 169 |
| 9 | Security Framework Procedures and Parameters | 170 |
| 9.0 | Introduction | 170 |
| 9.1 | Security Association Establishment Framework Procedures and Parameters | 170 |
| 9.1.1 | Credential Configuration Parameters..... | 170 |
| 9.1.1.0 | Introduction | 170 |
| 9.1.1.1 | Credential Configuration of Entity A and Entity B | 170 |
| 9.1.1.2 | Credential Configuration of M2M Authentication Functions | 171 |
| 9.1.2 | Association Configuration Procedures and Parameters | 171 |

| | | |
|------------|---|-----|
| 9.1.2.0 | Introduction..... | 171 |
| 9.1.2.1 | Association Configuration of Entity A and Entity B..... | 171 |
| 9.1.2.1.1 | Association Configuration of Entity A..... | 171 |
| 9.1.2.1.2 | Association Configuration of Entity B..... | 172 |
| 9.1.2.2 | Association Configuration of M2M Authentication Functions..... | 172 |
| 9.2 | Remote Security Provisioning Framework Procedures and Parameters..... | 173 |
| 9.2.1 | Bootstrap Credential Configuration Procedures and Parameters..... | 173 |
| 9.2.1.0 | Introduction..... | 173 |
| 9.2.1.1 | Bootstrap Credential Configuration of Enrollee..... | 173 |
| 9.2.1.2 | Bootstrap Credential Configuration of M2M Enrolment Functions..... | 174 |
| 9.2.2 | Bootstrap Instruction Configuration Procedures and Parameters..... | 174 |
| 9.2.2.0 | Introduction..... | 174 |
| 9.2.2.1 | Bootstrap Instruction Configuration of Enrolees..... | 174 |
| 9.2.2.2 | Void..... | 175 |
| 9.2.2.3 | Bootstrap Instruction Configuration of M2M Enrolment Functions..... | 175 |
| 9.2.2.4 | Bootstrap Instruction Configuration of UNSP Authentication Server..... | 175 |
| 9.2.3 | End-to-End Credential Configuration Procedures and Parameters..... | 176 |
| 9.2.3.0 | Introduction..... | 176 |
| 9.2.3.1 | End-to-End Credential Configuration of Source ESF End-Points and Target ESF End-Points..... | 176 |
| 9.2.3.2 | End-to-End Credential Configuration at the M2M Trust Enabling Functions..... | 177 |
| 9.2.3.3 | Configuration parameters for enabling End-to-End Security at Source ESF End-Points and Target ESF End-Points..... | 177 |
| 10 | Protocol and Algorithm Details..... | 178 |
| 10.1 | Certificate-Based Security Framework Details..... | 178 |
| 10.1.1 | Certificate Profiles..... | 178 |
| 10.1.1.0 | General..... | 178 |
| 10.1.1.1 | Common Certificate Details..... | 178 |
| 10.1.1.2 | Raw Public Key Certificate Profile..... | 179 |
| 10.1.1.3 | Details Common to Certificates with Certificate Chains..... | 179 |
| 10.1.1.4 | Profile for Device Certificates and their Certificate Chains..... | 179 |
| 10.1.1.4.1 | Profile for Device Certificates..... | 179 |
| 10.1.1.4.2 | Profile for Certificate Authority Certificates for Device Certificates..... | 179 |
| 10.1.1.5 | Profile for AE-ID Certificates and their Certificate Chains..... | 180 |
| 10.1.1.6 | Profile for FQDN Certificates and their Certificate Chains..... | 180 |
| 10.1.1.7 | Profile for CSE-ID Certificates and their Certificate Chains..... | 180 |
| 10.1.1.8 | Profile for Node-ID Certificates and their Certificate Chains..... | 180 |
| 10.1.2 | Public Key Identifiers..... | 180 |
| 10.1.3 | Support Requirements for each Public Key Certificate Flavour..... | 181 |
| 10.1.4 | Certificate Signing Request Profile..... | 181 |
| 10.2 | TLS and DTLS Details..... | 181 |
| 10.2.1 | TLS and DTLS Versions..... | 181 |
| 10.2.2 | TLS and DTLS Ciphersuites for TLS-PSK-Based Security Frameworks..... | 182 |
| 10.2.3 | TLS and DTLS Ciphersuites for Certificate-Based Security Frameworks..... | 182 |
| 10.3 | Key Export and Key Derivation Details..... | 183 |
| 10.3.1 | TLS Key Export Details..... | 183 |
| 10.3.2 | Derivation of Master Credential from Enrolment Key..... | 183 |
| 10.3.3 | Derivation of Provisioned Secure Connection Key from Enrolment Key..... | 183 |
| 10.3.4 | Generating KeID..... | 184 |
| 10.3.5 | Generating Key Identifier for the MAF Security Framework..... | 184 |
| 10.3.6 | Derivation of End-to-End Master Key from Provisioned Secure Connection Key..... | 184 |
| 10.3.6.1 | Introduction..... | 184 |
| 10.3.6.2 | Key Extraction and Expansion of End-to-End Master Key..... | 184 |
| 10.3.7 | Derivation of Usage-Constrained Symmetric Keys from Enrolment Key..... | 185 |
| 10.3.8 | sessionESPrimKey Derivation Algorithms..... | 186 |
| 10.3.8.1 | Introduction..... | 186 |
| 10.3.8.2 | HMAC-SHA256 sessionESPrimKey Derivation Algorithm..... | 186 |
| 10.4 | Credential-ID Details..... | 186 |
| 10.5 | KpsaID..... | 186 |
| 10.6 | KmID Format..... | 187 |
| 10.7 | Enrolment Expiry..... | 187 |

| | | |
|-------------------------------|---|------------|
| 11 | Privacy Protection Architecture using Privacy Policy Manager (PPM)..... | 187 |
| 11.1 | Introduction | 187 |
| 11.2 | Relationship between components of PPM and oneM2M..... | 187 |
| 11.3 | Privacy Policy Management in oneM2M Architecture | 188 |
| 11.3.1 | Introduction..... | 188 |
| 11.3.2 | Involved Entities..... | 188 |
| 11.3.3 | Management Flow in PPM Architecture | 189 |
| 11.3.3.0 | Introduction..... | 189 |
| 11.3.3.1 | Joining an IN-CSE | 189 |
| 11.3.3.2 | Subscription to a service by IN-AE..... | 190 |
| 11.3.3.3 | Request for personal data to the IN-CSE | 191 |
| 11.4 | Privacy Policy Manager Implementation Models | 194 |
| 11.4.1 | Using Terms and Conditions Mark-up Language..... | 194 |
| 11.4.1.0 | Introduction..... | 194 |
| 11.4.1.1 | Registration of Application Service Provider Privacy Policy | 195 |
| 11.4.1.2 | Registration of End User Privacy Preferences | 196 |
| 11.4.1.3 | Creating a customized Privacy Policy for each end user..... | 196 |
| 12 | Security-Specific oneM2M Data Type Definitions..... | 197 |
| 12.1 | Introduction | 197 |
| 12.2 | Simple Security-Specific oneM2M Data Types | 197 |
| 12.3 | Enumerated Security-Specific oneM2M Data Types | 197 |
| 12.3.1 | Introduction..... | 197 |
| 12.3.2 | Enumeration type definitions..... | 197 |
| 12.3.2.1 | sec:credIDTypeID | 197 |
| 12.3.2.2 | sec:devMgmtID..... | 198 |
| 12.3.2.3 | sec:cmdClassID..... | 198 |
| 12.3.2.4 | sec:cmdStatusCode | 199 |
| 12.3.2.5 | sec:certProvProtocolID | 199 |
| 12.3.2.6 | sec:certSubjectType | 199 |
| 12.3.2.7 | sec:objectTypeID | 200 |
| 12.4 | Complex Security-Specific oneM2M Data Types..... | 200 |
| 12.4.1 | MAF and MEF client configuration data..... | 200 |
| 12.4.2 | sec:clientRegCfg..... | 200 |
| 12.4.3 | sec:keyRegCfg..... | 201 |
| 12.4.4 | sec:cmdDescription..... | 201 |
| 12.4.5 | sec:cmdArgs | 201 |
| 12.4.6 | sec:noMoreCmdArgs..... | 201 |
| 12.4.7 | sec:certProvCmdArgs | 202 |
| 12.4.8 | sec:devCfgCmdArgs..... | 202 |
| 12.4.9 | sec:MONodeCmdArgs..... | 202 |
| 12.4.10 | sec:authProfileMONodeArgs..... | 202 |
| Annex A (informative): | Mapping of 3GPP GBA terminology | 203 |
| Annex B (informative): | General Mutual Authentication Mechanism..... | 204 |
| B.0 | Introduction | 204 |
| B.1 | Group Authentication..... | 205 |
| Annex C (normative): | Security protocols associated to specific SE technologies..... | 206 |
| C.0 | Introduction | 206 |
| C.1 | UICC | 206 |
| C.2 | Other secure element and embedded secure element with ISO 7816 interface..... | 206 |
| C.3 | Trusted Execution Environment..... | 206 |
| C.4 | SE to CSE binding..... | 206 |
| Annex D (normative): | UICC security framework to support oneM2M Services..... | 207 |

| | | |
|-------------------------------|--|------------|
| D.0 | Introduction | 207 |
| D.1 | Access Network UICC-based oneM2M Service Framework..... | 208 |
| D.1.1 | Access Network UICC-based oneM2M Service Framework characteristics | 208 |
| D.1.2 | M2M Service Framework discovery for Access Network UICC | 208 |
| D.1.3 | Content of files at the DF _{1M2M} level | 209 |
| D.1.3.0 | Introduction..... | 209 |
| D.1.3.1 | EF _{1M2MST} (oneM2M Service Table) | 209 |
| D.1.3.2 | EF _{1M2MSID} (oneM2M Subscription Identifier) | 211 |
| D.1.3.3 | EF _{1M2MSPID} (oneM2M Service Provider Identifier) | 211 |
| D.1.3.4 | EF _{M2MNID} (M2M Node Identifier) | 212 |
| D.1.3.5 | EF _{CSEID} (local CSE Identifier)..... | 212 |
| D.1.3.6 | EF _{M2MAE-ID} (M2M Application Identifiers list) | 213 |
| D.1.3.7 | EF _{INCSEIDS} (M2M IN-CSE IDs list)..... | 213 |
| D.1.3.8 | EF _{MAFFQDN} (MAF-FQDN)..... | 214 |
| D.1.3.9 | EF _{MEFID} (M2M Enrolment Function Identifier) | 214 |
| D.2 | oneM2M Service Module application for symmetric credentials on UICC (1M2MSM) | 215 |
| D.2.0 | Introduction | 215 |
| D.2.1 | oneM2M Service Module application file structure | 215 |
| D.2.1.0 | Introduction..... | 215 |
| D.2.1.1 | Content of UICC files at the Master File (MF) level | 215 |
| D.2.1.2 | Content of files at the 1M2MSM ADF (Application DF) level | 215 |
| D.2.2 | oneM2M Subscription related procedures for M2M Service | 216 |
| D.2.2.0 | Introduction..... | 216 |
| D.2.2.1 | Initialization - 1M2MSM Application selection..... | 216 |
| D.2.2.2 | 1M2MSM session termination..... | 216 |
| D.2.2.3 | oneM2M Service discovery procedure | 217 |
| D.2.2.4 | oneM2M Service provisioning procedures | 217 |
| D.2.2.5 | oneM2M Application Identifiers provisioning procedure | 217 |
| D.2.2.6 | oneM2M Secure provisioning related procedures | 217 |
| D.2.2.7 | oneM2M Security Association related procedures | 217 |
| Annex E (informative): | Precisions for the UICC framework to support M2M Services | 219 |
| E.0 | Introduction | 219 |
| E.1 | Suggested content of the EFs at pre-personalization..... | 219 |
| E.2 | EF changes via Data Download or CAT applications..... | 219 |
| E.3 | List of SFI values at the ADF _{M2MSM} or DF _{M2M} level | 220 |
| E.4 | UICC related tags defined in annex J | 220 |
| Annex F (normative): | Acquisition of Location Information for Location based Access Control..... | 221 |
| F.0 | Introduction | 221 |
| F.1 | Description of Region | 221 |
| F.1.1 | Circular Description | 221 |
| F.1.2 | Country Description | 221 |
| F.2 | Acquisition of Location Information..... | 221 |
| F.2.0 | Introduction | 221 |
| F.2.1 | Circular Description | 222 |
| F.2.2 | Country Description | 223 |
| Annex G (informative): | Access Control Decision Request..... | 224 |
| Annex H (informative): | Implementation Guidance and index of solutions..... | 225 |
| Annex I: | Void | 226 |
| Annex J (normative): | List of Privacy Attributes..... | 227 |

Annex K (informative): Terms and Conditions Mark-up Language implementation rules.....235

Annex L (informative): Example SCEP implementation237

L.1 Introduction237

L.2 Certificate Provisioning procedures using SCEP237

History241

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/fb256d09-9498-464e-8d85-9a29b87205bd/etsi-ts-118-103-v2.12.1-2019-04>

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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).

ETSI STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/118-103-v2.12.1-2019-04/44e-8d85-9a29b87205bd/etsi-ts-118-103-v2.12.1-2019-04>

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] 3GPP TS 31.115 (V10.1.0): "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications (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.S0109-0: "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, January 2008.
- NOTE: Available at <http://unicode.org/reports/tr15/>.
- [21] GlobalPlatform® Device Technology TEE Management Framework (TMF) Version 1.
- [22] GlobalPlatform® Device Technology TEE System Architecture, Version 1.1.
- [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] Federal Information Processing Standard (FIPS) 186-4: "Digital Signature Standard (DSS)".
- NOTE: Available at <https://csrc.nist.gov/publications/detail/fips/186/4/final>.
- [40] IETF RFC 6920: "Naming Things with Hashes".
- [41] IETF RFC 4648: "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 TLS".