ETSI TR 103 533 V1.1.1 (2019-08)

SmartM2M;
Security;
Standards Landscape and best practices

Reference

DTR/SmartM2M-103533

Keywords

cybersecurity, IoT, oneM2M, privacy, 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

Contents

Intellectual Property Rights 6
Foreword 6
Modal verbs terminology 6
1 Scope 7
1.1 Context for the present document 7
1.2 Scope of the present document 7
2 References 8
2.1 Normative references 8
2.2 Informative references 8
3 Definition of terms, symbols and abbreviations 10
3.1 Terms 10
3.2 Symbols 11
3.3 Abbreviations 11
4 Security in the context of IoT 12
4.1 A global approach to IoT Systems 12
4.1.1 Major characteristics of IoT systems 12
4.1.2 The need for an "IoT-centric" view 13
4.1.2.1 Introduction 13
4.1.2.2 Roles 13
4.1.2.3 Reference Architecture(s) 13
4.1.2.4 Guidelines 14
5 Simplified security model for IoT 14
6 Purpose of cyber security as it applies to IoT 15
6.1 Overview 15
6.2 The Security Cycle 16
6.3 The CIA Paradigm 18
6.4 Peculiarities of IoT 19
6.4.1 IoT characteristics 19
6.4.2 Resource limitation 19
6.4.3 Connectivity modes 19
6.4.4 Radio considerations 20
7 Regulatory context of IoT Security 20
7.1 Overview 20
7.2 GDPR 20
7.3 Network Information Security Directive 21
7.3.1 The objectives of the Directive 21
7.3.2 Scope of the NIS Directive 21
7.3.3 Security and incident notification requirements 22
7.3.4 Available security analysis of NIS 23
7.4 Cyber Security package (in development) 24
8 Overview of security standardization ecosystem for IoT 24
8.1 Introduction 24
8.2 Obligation of trust protocols 24
8.3 Identity management and asset discovery 25
8.4 IoT and M2M specific groups 25
8.4.1 ETSI groups 25
8.4.1.1 Overview of ETSI groups active in IoT and M2M 25
8.4.1.2 SmartM2M 25
8.4.1.3 eHealth 25
8.4.1.4 SmartBAN 25
8.4.1.5 ITS - Working group 5 25
8.4.1.6 ERM 26

8.4.2 Other bodies 26
8.4.2.1 oneM2M - Working Group 4 26
8.4.2.2 AIOTI - The Alliance for IoT Innovation 26
8.4.2.3 ITU - International Telecommunication Union 26
8.4.2.4 TCG - Trusted Computing Group® 28
8.4.2.5 OASIS 28
8.5 Other EU and non-EU bodies 28
8.5.1 European Union Agency for Network and Information Security (ENISA) 28
8.5.2 National Institute of Standards and Technology (NIST) 29

9 IoT specific security guidance and best practices 29
9.1 Introduction 29
9.2 Overview 30
9.3 GSMA guidelines 30
9.4 DCMS guidelines and ETSI TS 103 645 31
9.5 ENISA and ECSO 31
9.6 Other industry guidelines 33
9.6.1 Trusted Computing Group 33
9.6.2 Global Platform 33
9.6.3 NIST 33

10 General security guidance and best practices 34
10.1 Overview and introduction to guidance and best practices 34
10.2 Defence in depth 34
10.3 Secure by default 35
10.4 Design for assurance 35
10.5 Privacy by design 35

11 Lessons learned and conclusions 37

Annex A: Best practice security guidelines for implementation, development and operation of IoT 39

Annex B: Change History 40

History 41

List of figures

Figure 1: Generic security model for systems 15
Figure 2: Basic activities of the cyber security ecosystem 17
Figure 3: Mindmap of concepts and functions associated to security 17
Figure 4: Overview of NIS Directive Stakeholders (from [i.14]) 22
Figure 5: Visualization of the relationship of NISD to Cyber-security 23
Figure 6: ETSI's ITS security documents and their relation to each other 26
Figure 7: ITU-T Y-series of recommendations for IoT and Smart Cities 27
Figure 8: ITU-T Y-series recommendations for identification and security 28
Figure 9: Screenshot from ENISA website for references against Authentication practice 32
Figure 10: Role of protection technologies in privacy protection 36
Figure 11: Extending privacy protection to address principles of privacy protection 37

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 Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

1.1 Context for the present document

The design, development and deployment of - potentially large - IoT systems require to address a number of topics - such as security, interoperability or privacy - that are related and should be treated in a concerted manner. In this context, several Technical Reports have been developed that each address a specific facet of IoT systems.

In order to provide a global and coherent view of all the topics addressed, a common approach has been outlined across the Technical Reports concerned with the objective to ensure that the requirements and specificities of the IoT systems are properly addressed and that the overall results are coherent and complementary.

The present document has been built with this common approach also applied in all of the other documents listed below (the present document is highlighted in *italic* script in the list):

ETSI TR 103 533 (the present document)

ETSI TR 103 534-1 [i.43]

ETSI TR 103 535 [i.45]

ETSI TR 103 536 [i.46]

ETSI TR 103 537 [i.47]

ETSI TR 103 591 [i.2]

1.2 Scope of the present document

The present document provides an overview of the Standards Landscape and best practices for the application of security technology to the IoT.

Existing work in mapping the landscape of security standards and best practices has been published by ETSI in both formal ETSI publications and in the review of security activity presented in the annual white paper, by ENISA through the IoT Security Expert Group (in [i.3] and [i.4]), and others but have often not addressed the particularities of IoT for the general case. In this regard the present document builds on the content of ETSI TR 103 306 [i.1] which addresses IT Security in general with a specific view to the IoT and extends and builds on the previously published work in the field.

The present document is structured as follows:

- Clause 5 provides a simplified security model of IoT.
- Clause 6 presents an introduction to the security purposes of IoT as a specialization of the generic cyber-security domain and introduces some of the paradigms used in security analysis, design, and implementation.
- Clause 7 presents an overview of the regulatory domain as it impacts IoT security.
- Clause 8 presents an overview of the security ecosystem and identifies the stakeholders in standards development and development of best practices.
- Clause 9 presents a review of the security best practices and development guidance arising from the stakeholders identified in clause 4.
- Clause 10 presents an overview of the specific technologies of security that may apply to IoT.
- Clause 11 provides a summary of the findings of the present document.
- Annex A collates a set of best practice guidelines for non-consumer IoT.

The present document complements the overview of the Standards Landscape and best practice for privacy to be found in ETSI TR 103 591 [i.2].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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 TR 103 306: "CYBER; Global Cyber Security Ecosystem".

[i.2] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.3] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", ISBN: 978-92-9204-236-3, doi: 10.2824/03228.

[i.4] ENISA: "Security and Resilience of Smart Home Environments: Good practices and recommendations", ISBN: 978-92-9204-141-0 | doi:10.2824/360120.

[i.5] Recommendation ITU-T Y.4806. "Security capabilities supporting safety of the Internet of things".

[i.6] ENISA: "Security Recommendations for IoT".

[i.7] European Data Protection Supervisor: "EDPS formal comments in response to the Çybersecurity Package' adopted by the Commission".

NOTE: Available from https://edps.europa.eu/sites/edp/files/publication/17-12-15_formal_comments_2017-0810_en.pdf.

[i.8] UK Department of Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report".

NOTE: Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf?_ga=2.246964045.819894548.1566555869-1475373752.1566555869.

[i.9] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

NOTE: Available from https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[i.10] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.11] FIPS 197: "Federal Information Processing Standards Publication 197; Advanced Encryption Standard (AES)", issued by the National Institute of Standards and Technology (NIST), November 26, 2001".

[i.12] European Commission, Special Eurobarometer 460: "Attitudes towards the impact of digitisation and automation on daily life", 2017.

NOTE: Available from http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/78998.

[i.13] European Commission, Special Eurobarometer 464a: "Europeans' attitudes towards cyber security", 2017.

NOTE: Available from http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79735.

[i.14] European Commission Cross Fertilisation Through Alignment, Synchronisation and Exchanges for IoT: "Legal IoT Framework (Initial)", Deliverable 05.05 2017.

NOTE: Available from https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf.

[i.15] ETSI TR 103 167: "Machine to Machine (M2M); Threat analysis and counter measures to M2M service layer".

[i.16] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.17] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

[i.18] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.19] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[i.20] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.21] GDPR: "General Data Protection Regulation (GDPR) (EU) 2016/679".

[i.22] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

[i.23] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.24] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.25] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.26] ETSI TR 103 305 (all parts): "CYBER; Critical Security Controls for Effective Cyber Defence".

[i.27] European Commission: "Communication from the Commission to the European Parliament and the Council: Making the most of NIS - towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", 4 October 2017.

NOTE: Available from https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-ANNEX-1-PART-1.PDF.

[i.28] ENISA: "Good Practices for Security of Internet of Things in the context of Smart Manufacturing".

[i.29] ENISA: "Towards secure convergence of Cloud and IoT".

[i.30] TCG: "Architect's Guide: IoT Security".

NOTE: Available from https://trustedcomputinggroup.org/wp-content/uploads/TCG-Architects-Guide_2018_FC01_web.pdf.

[i.31] TCG: "IoT Security Infographic, Securing the Internet of Things".

NOTE: Available from https://trustedcomputinggroup.org/wp-content/uploads/INFOGRAPHIC-TCG-IoT-FINAL.pdf.

[i.32] AIOTI: "IoT LSP Standards Framework Concepts", Release 2.8, White Paper, 2017.

[i.33] Recommendation ITU-T X.1205: "Overview of cybersecurity".

[i.34] ISO/IEC 27032: "Information technology -- Security techniques -- Guidelines for cybersecurity".

[i.35] NIST SP800-183: "Networks of 'Things'".

[i.36] ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.37] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003)".

[i.38] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.39] ETSI TR 103 369: "CYBER; Design requirements ecosystem".

[i.40] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.41] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.42] ETSI TR 103 304: "CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services".

[i.43] ETSI TR 103 534-1: "SmartM2M; Teaching Material; Part 1: Security".

[i.44] ETSI TR 103 534-2: "SmartM2M; Teaching Material; Part 2: Privacy".

[i.45] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.46] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.47] ETSI TR 103 537: "SmartM2M; Plugtests preparation on Semantic Interoperability".

[i.48] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.49] IEEE 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.50] IEEE 802.15.4™: "IEEE Standard for Low-Rate Wireless Networks".

[i.51] National Security Agency (NSA): "Defense in Deph".

NOTE: Available from https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 103 306 [i.1] and the following apply:

centre of excellence: educational or research & development organization recognized as a leader in accomplishing its cyber security mission

Consumer IoT: This includes consumer purchased 'off the shelf' IoT devices; IoT devices used and installed 'in the home' and the associated services linked to these devices.

NOTE: Definition from [i.8].

cyber environment: users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks

NOTE: Definition from Recommendation ITU-T X.1205 [i.33].

cyber security (or cybersecurity): collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets

NOTE: Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality, Recommendation ITU-T X.1205 [i.33].

Also,

cybersecurity: preservation of confidentiality, integrity and availability of information in the Cyberspace

NOTE: Definition from ETSI TR 103 591 [i.2].

cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

NOTE: Definition from ETSI TR 103 591 [i.2].

Internet connected services: Allowing devices to communicate with other devices over a broad network. These connections usually involve a link occurring between devices and systems and the collection of data (definition from [i.8]).

Internet of Things (IoT): The totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

NOTE: Definition from [i.8].

Secure by Design: A design-stage focus on ensuring that security is in-built within consumer IoT products and connected services.

NOTE: Definition from [i.8].

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
AIOTI	Alliance for Internet of Things Innovation
ANT+™	Advanced and Adaptive Network Technology

NOTE: Trademark of Garmin.

BSIMM	Building Security in Maturity Model
CCRA	Common Criteria Recognition Agreement
CIA	Confidentiality Integrity Availability
cPP	co-operative Protection Profile
DCMS	Department of Culture, Media and Sport (a UK Government body)

ECSO	European Cyber Security Organisation
EDPS	European Data Protection Supervisor
ENISA	European Network Information Security Agency
EP	ETSI Project
ERP	Enterprise Resource Planning
ES	ETSI Standard
EU	European Union
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
GSMA	GSM Association (a trade body)
HSM	Hardware Security Module
ICT	Information and Communications Technology
IoT	Internet of Things
ISM	Industrial Scientific Medical
IT	Information Technology
ITS	Intelligent Transport System
LAN	Local Area Network
M2M	Machine to Machine
NCSC	National Cyber Security Centre (a UK Government body)
NFV	Network Function Virtualisation
NIS	Network Information Security
NISD	Network Information Security Directive
NoT	Network of Things
NSA	National Security Agency
OASIS	Organization for the Advancement of Structured Information Standards
OES	Operators of Essential Services
OoT	Obligation of Trust
PII	Personal Identifying Information
RDSP	Relevant Digital Service Providers
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
SAML	Security Assertion Markup Language
SAMM	Open Software Assurance Maturity Model
SCP	Smart Card Platform
SDL	(Microsoft) Security Development Lifecycle
SE	Secure Element
SSDL	Software Security Development Lifecycle
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TSS	TPM Software Stack
TVRA	Threat Vulnerability Risk Analysis
UICC	Universal Integrated Circuit Card
XACML	eXtensible Access Control Markup Language

4 Security in the context of IoT

4.1 A global approach to IoT Systems

4.1.1 Major characteristics of IoT systems

IoT systems are often seen as an extension to existing systems needed because of the (potentially massive) addition of networked devices. However, this approach does not take stock of a set of essential characteristics of IoT systems that push for an alternative approach where the IoT system is at the centre of attention of those who want to make them happen. This advocates for an "IoT-centric" view.