ETSI SR 003 680 V1.1.1 (2020-03)

SmartM2M;
Guidelines for Security, Privacy and Interoperability in IoT System Definition;
A Concrete Approach

Reference

DSR/SmartM2M-003680

Keywords

interoperability, IoT, IoT platforms, oneM2M
privacy, SAREF, security, semantic

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

Contents

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 Special Report (SR) 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.

Executive summary

IoT systems are often seen as an extension to existing systems created by the (potentially massive) addition of networked devices to an existing system to enlarge its capabilities. However, in a growing number of ICT systems, the IoT part becomes the core of the overall system and the place where a large part of the value is created.

Though many of the characteristics of IoT systems may be found in other ICT-based systems, the main challenge with IoT systems is that they should address simultaneously a number of high-level issues like e.g. stakeholders' involvement, technology choices, deployment model, and integration with/of legacy.

The complexity of these challenges for IoT raises a very large range of questions that should be addressed across the whole lifecycle of any IoT system (from its inception to its development, deployment and even de-commissioning). The approach to IoT systems specification, development and deployment taken in the present document is based on the analysis of typical examples (Use Cases) which have been selected in order to cover a broad panel of sectors and to answer some of the most pressing questions of the readers from a strategy, management and technology perspective.

The present document focuses on questions related to privacy, security, platforms interoperability and semantic interoperability that are addressed from different angles and not just from a simple technical perspective. Tables present "Frequently Asked Questions" with the intent to illustrate major questions in IoT, and their solutions in an easily digestible form.

The present document offers some strategic, operational and technical guidelines, which intend to fix the issues addressed in it.

Annexes of the present document contain representative Use Cases (eHealth, Smart Buildings, Industrial IoT, IoT-based Mission Critical Communications) relating to the issues addressed in the present document and contain material and references for further reading as short descriptions of the Technical Reports already produced by ETSI, technical material and others.

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.

- ETSI TR 103 533: "Security; Standards Landscape and best practices" [i.1].
- ETSI TR 103 534: "Teaching Material: Part 1 (Security) [i.2] and Part 2 (Privacy)" [i.3].
- ETSI TR 103 535: "Guidelines for semantic interoperability in the industry" [i.4].
- ETSI TR 103 536: "Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms" [i.5].
- ETSI TR 103 537: "Plugtests™ preparation on Semantic Interoperability" [i.6].
- ETSI TR 103 591: "Privacy study report; Standards Landscape and best practices" [i.7].

In order to provide a global and coherent view of all the topics addressed, a common approach has been outlined across the above Technical Reports (TRs) 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 TRs listed above.

1.2 Scope of the present document

The present document intends to be a high-level document for the general public and is not specifically addressing a technical audience (e.g. designers, developers, etc.). It is introducing, in a relatively non-technical manner, to some of the main issues that individuals and organizations should address when they face the development of an IoT system. A strong emphasis is put on interoperability, security, privacy and standards in support.

Based on the analysis of representative Use Cases (eHealth, Smart Buildings, Industrial IoT, IoT-based Mission Critical Communications), which are documented in Annex A, and relating to (and updating) the guidelines developed in the TRs listed in clause 1.1, it provides guidelines for Security, Privacy and Interoperability in IoT System Definition.

The present document is structured as follows:

- Clauses 1 to 3 set the scene and provide references as well as definition of terms, symbols and abbreviations, which are used in the document on hand.
- Clause 4 explains the approach to IoT systems specification, development and deployment taken in the present document. This approach is based on the analysis of typical examples (also termed as Use Cases) which have been selected in order to cover a broad panel of sectors (e.g. eHealth or Smart Buildings) and to answer some of the most pressing questions of the readers from a strategy, management and technology perspective. The clause also suggests how the rest of the document should be read in order to maximize the findings for the readers.
- Clause 5 focuses on questions related to **privacy, security and interoperability (platforms interoperability and semantic interoperability)** that are addressed from different angles and not just from a simple technical perspective. The text in this clause is mostly presented in the form of a "Frequently Asked Questions" (FAQ) information sheet with the intent to illustrate major questions in IoT, and their solutions, in an easily digestible form. The questions also refer to the associated Technical Reports (detailed in Annex B) and the use case examples (detailed in Annex A).
- Clause 6 offers some strategic, operational and technical guidelines, which intend to fix the issues addressed in clause 5.
- Clause 7 provides observations and lessons learned from the addressed issues and analysis of Use Cases.

- Annex A documents representative Use Cases (eHealth, Smart Buildings, Industrial IoT, IoT-based Mission Critical Communications) relating to the issues addressed in clause 5 and guidelines provided in clause 6.
- Annex B contains short descriptions of the Technical Reports listed in clause 1.1, as well as technical material and others for further reading.

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 103 533: "SmartM2M; Security; Standards Landscape and best practices".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103533/01.01.01_60/tr_103533v010101p.pdf.

[i.2] ETSI TR 103 534-1: "SmartM2M; Teaching material; Part 1: Security".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf.

[i.3] ETSI TR 103 534-2: "SmartM2M; Teaching material; Part 2: Privacy".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf.

[i.4] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf.

[i.5] ETSI TR 103 536: "SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf.

[i.6] ETSI TR 103 537: "SmartM2M; Plugtests™ preparation on Semantic Interoperability".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103537/01.01.01_60/tr_103537v010101p.pdf.

[i.7] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103591/01.01.01_60/tr_103591v010101p.pdf.

[i.8] ETSI TR 103 582: "EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf.

[i.9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[i.10] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303.

[i.11] Directive 2011/24/EU Of The European Parliament And Of The Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88.

[i.12] 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).

[i.13] AIOTI WG03 Release 4.0, 2018: "High Level Architecture (HLA)".

NOTE: Available at https://aioti.eu/wp-content/uploads/2018/06/AIOTI-HLA-R4.0.7.1-Final.pdf.

[i.14] ETSI TS 118 112: "oneM2M; Base Ontology (oneM2M TS-0012)".

[i.15] GDPR & Public Safety, EENA and Bird & Bird, August 2019.

NOTE: Available at https://eena.org/document/gdpr-public-safety/.

[i.16] ISO/IEC 29147: "Vulnerability Disclosure".

[i.17] ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.18] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.19] ETSI TS 118 103: "oneM2M; Security Solutions (oneM2M TS-003)".

[i.20] "Privacy Code of Conduct on mobile health apps".

NOTE: Available at https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

[i.21] ETSI TR 103 305 (all parts): "CYBER; Critical Security Controls for Effective Cyber Defence".

[i.22] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.23] ISO/IEC 27000:2018: "Information technology -- Security techniques -- Information security management systems".

[i.24] BS 10012:2017: "Data protection - Specification for a personal information management system".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

denial of service type attacks: cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
AIOTI	Alliance for the Internet of Things Innovation
API	Application Programming Interface
BMS	Building Management System
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CTI	Centre for Testing and Interoperability
CTO	Chief Technical Officer
CXO	Chief eXperience Officer
DCMS	Department of Culture, Media and Sport (a UK Government body)
ECSO	European Cyber Security Organization
ENISA	European Network Information Security Agency
ER	Emergency Room
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GSMA	GSM Association (a trade body)
HMI	Human Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communications Technology
IEA	International Energy Agency
IIoT	Industrial IoT
IoT	Internet of Things
IoT-EPI	IoT-European Platforms Initiative
JSON	Java Script Object Notation
NIS	Network Information Security
NIST	National Institute of Standards and Technology
OCF	Open Connectivity Foundation
PoC	Proof-of-Concepts
PPM	oneM2M Privacy Policy Manager
PSAP	Public Safety Answering Point
SAREF	Smart Applications REFerence ontology
SIM	Subscriber Identity Module
SSN	Semantic Sensor Network
TCG	Trusted Computing Group
TR	Technical Report
TVRA	Threat Vulnerability Risk Analysis
UML	Unified Modelling Language
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

4 Role based analysis of IoT systems

4.1 Challenges

IoT systems are often seen as an extension to existing systems created by the (potentially massive) addition of networked devices to an existing system to enlarge its capabilities. However, in a growing number of ICT systems, the IoT part becomes the core of the overall system and the place where a large part of the value is created.

Though many of the characteristics of IoT systems may be found in other ICT-based systems, the main challenge with IoT systems is that they are required to address simultaneously a number of high-level issues amongst which:

- **Stakeholders involvement:** during the life-cycle (e.g. definition, design, development, deployment) of an IoT system, a large variety of stakeholders with a wide range of roles should be associated in order to ensure that their - potentially conflicting - requirements (regarding e.g. economics, technology, usage) can be considered, discussed and resolved in a concerted manner.

- **Technology choices:** by nature, all IoT systems should integrate potentially very diverse technologies, very often for the same purpose (e.g. communication protocols) with a risk of overlap. A critical aspect is the balance between proprietary and standardized solutions which should be carefully managed, with a lot of potential implications on the choice of the supporting platforms.

- **Deployment model:** a key aspect of IoT systems is that they emerge at the very same time where Cloud Computing and Edge Computing have become mainstream technologies. All IoT systems are facing the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.

- **Integration with/of Legacy:** many IoT systems are requested to deal with legacy (e.g. existing connectivity, back-end ERP systems). The challenge is to deal with the requirements of the legacy part without compromising an "IoT centric" approach which may, as much as possible, favour the demands of the IoT part.

4.2 Issues to address

Given the complexity of the challenges outlined in clause 4.1, a very large span of issues needs to be addressed during the whole lifecycle of an IoT system (from its inception, to its development, deployment and de-commissioning). The present document is addressing issues such as:

- **Interoperability:** there are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc. These requirements also have an impact on the selection of the platform(s) that are expected to concretely support and implement them.

- **Privacy:** in the case of IoT systems that deal with critical data in critical applications (e.g. e-Health, Intelligent Transport, Food, Industrial systems), privacy becomes a make or break property.

- **Security:** as an essential enabling property for Trust, security is a key feature of all IoT systems and needs to be dealt with in a global manner. One key challenge is that it is involving a variety of users in a variety of Use Cases.

Though these issues are rather technology-oriented in nature, they raise questions that cannot be resolved from a simple technical perspective.

4.3 Guidelines

Based on the identified set of issues, the present document is proposing **guidelines** regarding strategy (e.g. how to make choices that globally impact the structure in charge of the IoT system), technology (e.g. what are the main choices to guaranty the development and evolution of the IoT system) and operations (e.g. how to ensure that the choices made can be supported by the structure and the stakeholders involved).

These guidelines are generic in nature. They have been developed by using two complementary sets of information:

- The guidelines developed in the associated set of Technical Reports developed concurrently with the present document (listed in clause 1.1) and relating to the following topics:
    - Privacy Standards and Best Practices
    - Security Standards and Best Practices
    - Teaching Material for Security
    - Teaching Material for Privacy

- Guidelines for using Semantic Interoperability in the Industry
- Preparation of Plugtests™ on Semantic Interoperability
- Interoperability and interworking of existing IoT Platforms

- The generalization of the guidelines and recommendations coming from a set of detailed examples.

4.4 Stakeholders and roles

The present document intends to provide support to a large variety of "stakeholders" involved across the IoT system lifecycle, not only those with a technical role. Examples of the stakeholders concerned by the guidelines are:

- CXOs (e.g. CEO, CTO) involved in the high-level choices related to the IoT system inception;
- System Designer, System Developer, System Deployer;
- End-user;
- Device Manufacturer.

4.5 Detailed examples

Examples from different sectors have been chosen to illustrate the generic (cross-sector) guidelines. The sectors chosen are illustrative of the large span of situations: eHealth, Smart Building, Industrial IoT and Critical Communications.

The analysis made in the detailed examples allows not only to illustrate the generic guidelines in a specific context, but reversely - when significant - to explain how the view from a specific sector can highlight the relevance of a guideline: for example, the privacy aspects are an important element for all use cases, and the analysis of the eHealth example will bring a very important clarification whichever is the reader's sector of interest.

5 Questions to address

5.1 Introduction

The complexity of the challenges for IoT (outlined in clause 4.1) raises a very large range of questions that should be addressed across the whole lifecycle of any IoT system (from its inception to its development, deployment and even de-commissioning). The present document focuses on questions related to **privacy, security and interoperability (platforms interoperability and semantic interoperability)** that are addressed from different angles and not just from a simple technical perspective.

The text in this clause is mostly presented in the form of a "Frequently Asked Questions" (FAQ) information sheet with the intent to illustrate major questions in IoT, and their solutions, in an easily digestible form. The questions also refer to the associated Technical Reports (detailed in Annex B) and the use case examples (detailed in Annex A).

5.2 Privacy

Two associated Technical Reports (ETSI TR 103 591 [i.7] and ETSI TR 103 534-2 [i.3]) and a set of teaching slides have addressed privacy within IoT. The key aspects are that there should be a clear allocation of responsibilities regarding the protection of personal data between the series of entities involved in the provisioning of IoT services.

Table 1 provides examples of possible questions and answers from interested stakeholders.

Table 1: Questions and answers for privacy

Question	Answer	Reference for further information
What are the main challenges facing Privacy in IoT?	The key challenges for privacy in IoT can be summarized as follows: • the high risk of profiling, for example, of a user of an IoT device or for a resident of a smart home; • the lack of transparency resulting from hyper-connectivity hindering individuals to exercise their rights; • increased dependencies raise concerns on the acquisition of a *freely* given and well-informed consent Overall, it seems less likely for the individual to be able to exercise control over the information concerning him and to be able to retain his anonymity within an IoT environment, while the large amounts of data collected create stakes not only at an individual but also at a societal level.	ETSI TR 103 591 [i.7]
Is IoT privacy different from existing privacy concept?	In general, the concept of privacy is broader than privacy in IoT. Privacy in IoT should be rather perceived as closer to the concepts of informational privacy and data protection.	ETSI TR 103 591 [i.7] ETSI TR 103 534-2 [i.3] (Teaching material)
Are there any existing examples of implementation of privacy for IoT systems?	A relevant example of practical implementation of Privacy policy for IoT is the oneM2M Privacy Policy Manager (PPM) architecture. This simple architecture describes the implementation of GDPR principle for IoT.	ETSI TR 103 591 [i.7] ETSI TS 118 103 [i.19]
What is the most important concept to consider when considering Privacy for an IoT system?	Privacy by design is an approach that aims to build privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.	ETSI TR 103 591 [i.7]
Which data are affected by privacy?	The concept of privacy refers to personal data. Under EU law personal data are defined as: "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."	ETSI TR 103 591 [i.7] ETSI TR 103 534-2 [i.3] (Teaching material)
Does GDPR apply to IoT systems?	GDPR applies to all processing of personal data, irrespective of the technology used. It, therefore, applies to IoT systems.	ETSI TR 103 591 [i.7]