# ETSI TR 103 591 V1.1.1 (2019-10)

TECHNICAL REPORT

# SmartM2M;
# Privacy study report;
# Standards Landscape and best practices

Reference

DTR/SmartM2M-103591

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

# List of Figures

# 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.

# Introduction

The present document focuses on privacy, which is particularly relevant within the IoT environment due to a series of emerging challenges resulting from hyper-connectivity. The approach adopted builds on the fundamental assumption that even though it is generally considered that privacy and security are separate concepts, they are actually interconnected, and they should therefore be treated in practice in a coordinated manner. Security constitutes a prerequisite for the effective protection of privacy, as it has also been confirmed by the General Data Protection Regulation (GDPR).

NOTE: See also the Preamble of the Regulation (EU) 2016/679 [i.16] 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) [i.23].

# 1 Scope

## 1.1 Context of the present document

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 (see below) with the objective to ensure that the particularities of the IoT systems are properly addressed and that the overall results are coherent and complementary.

In this context, the present document has been built with this common approach also applied in all of the other documents listed below:

- ETSI TR 103 533 [i.2]
- ETSI TR 103 534 (part 1 and 2) [i.28]
- ETSI TR 103 535 [i.33]
- ETSI TR 103 536 [i.34]
- ETSI TR 103 537 [i.35]
- ETSI TR 103 591 (the present document)

## 1.2 Scope of the present document

The present document elaborates on how to ensure effective protection of individuals' privacy in the IoT environment. It acknowledges the challenges for privacy and data protection and stresses the necessity for a human centred approach.

To this end, the present document will:

- highlight the role of social values in the design of IoT systems;
- discuss the role of standards under the GDPR and the proposed ePrivacy Regulation;
- outline the role of the individual, also, through a set of use cases drawn from an ongoing EU project and further adapted for the needs of the present document;
- produce an overview of the main privacy and data protection challenges emerging in the IoT environment;
- review the privacy standardization gaps identified in ETSI TR 103 376 [i.1] and how some of these gaps have been resolved since the completion of the work if at all;
- illustrate current best practices across industrial and other organizations in the processing of personal information to meet, and in some cases exceed, the minimum requirements for compliance in view of maximizing the protection of personal information;
- point at the fundamental shifts taking place in relation to privacy under EU Law, including the shift from rule-based frameworks to principle-based frameworks, the necessity to go beyond mere compliance to meaningful accountability and the implementation of impact-based measures.

For reasons explained below under clause 7.3, the development of new standards falls outside the scope and the objectives of the present document.

Notably, the present document is addressed to the entire set of stakeholders with a role in the IoT environment and it complements ETSI TR 103 533 [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 103 376: "SmartM2M; IoT LSP use cases and standards gaps".

[i.2] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.3] European Commission: "Cloud Service Level Agreement Standardisation Guidelines".

[i.4] European Data Protection Supervisor: "Glossary".

NOTE: Available at https://edps.europa.eu/node/3110#privacy.

[i.5] GHOST Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control: "D3.9: Trials use case specification and report ($1^{rst}$ release).

NOTE: Available at https://www.ghost-iot.eu/results-documents.

[i.6] ISO/IEC 20547-3: "Information technology - Big data reference architecture - Part 3: Reference architecture".

[i.7] ISO/IEC 20547-4: "Information technology - Big data reference architecture. Part 4: Security and privacy fabric".

[i.8] ISO/IEC TR 27550: "Information technology - Security techniques - Privacy engineering [Draft]".

[i.9] ISO/IEC 27552: "Information technology - Security techniques - Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management - Requirements and guidelines [Draft]".

[i.10] ISO/IEC CD 3014: "Internet of Things Reference Architecture (IoT RA)".

[i.11] ISO/IEC 29100:2011: "Information technology - Security techniques - Privacy framework".

[i.12] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Interinstitutional File: 2017/0003(COD), Brussels.

[i.13] 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 303/59.

[i.14] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

[i.15] European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01.

[i.16] 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.17] 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.

[i.18] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 13.9.2017.

[i.19] 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.

[i.20] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[i.21] Council of the European Union (2018) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Interinstitutional File: 2017/0003(COD), Brussels.

[i.22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[i.23] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

[i.24] European Data Protection Supervisor: Preliminary Opinion on privacy by design, 31 May 2018.

[i.25] "IoT LSP Standards Framework Concepts", Release 2.8, White Paper, AIOTI, 2017.

[i.26] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

[i.27] ETSI TS 118 103: "oneM2M; Security solutions".

[i.28] ETSI TR 103 534 (part 1 and 2): SmartM2M; Teaching Material; Part 1:Security and Part 2: Privacy.

[i.29] ISO/IEC 27030: "Information technology - Security techniques - Guidelines for security and privacy in Internet of Things".

[i.30] Directive 2010/40/EU: of the European Parliament and of the council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[i.31] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 19 October 2018.

[i.32] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 15 February 2019.

[i.33] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.34] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.35] ETSI TR 103 537: "SmartM2M; Plugtests$^{\text{TM}}$ preparation on Semantic Interoperability".

[i.36] ISO/IEC 29151:2017: "Information technology - Security techniques - Code of practice for personally identifiable information protection".

[i.37] ISO/IEC 29134: "Information technology - Security techniques - Guidelines for privacy impact assessment".

[i.38] ISO 27018: "Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors".

[i.39] ISO/IEC 27000: "Information Technology - Security Techniques - Information Security Management Systems - Overview And Vocabulary".

[i.40] ISO/IEC 27001: "Information Security Management".

[i.41] ISO/IEC 27002: "Information Technology - Security Techniques - Code Of Practice For Information Security Controls".

[i.42] BS 10012:2017: "Data protection. Specification for a personal information management system. Specification for a personal information management system".

[i.43] Recommendation ITU-T X.1231:"Supplement on guidance to assist in countering spam for mobile phone developers".

[i.44] Recommendation ITU-T X.1155: "Guidelines on local linkable anonymous authentication for electronic services.

[i.45] Recommendation ITU-T TD 733-PLEN: "Technical framework of PII (Personally Identifiable Information) handling system in IoT environment".

[i.46] Recommendation ITU-T TD 731-PLEN: "Security guidelines for smart metering service in smart grids".

[i.47] Recommendation ITU-T TD 962-PLEN: "Security Requirements and Framework for Big Data Analytics in mobile Internet services".

[i.48] British Information Commissioner's Office (ICO) Guidance to Privacy in mobile apps.

[i.49] British Code of Practice for consumer IoT security UK Gov: Dept of Digital, Culture, Media & Sport.

[i.50] GSMA Report on Protecting Privacy and Data in the Internet of Things.

[i.51] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC OJ L 337/35.

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

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

**biometric data:** personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data [i.16]

**cyber security (or cybersecurity):** comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats [i.18]

NOTE: There are multiple definitions on cybersecurity each of which pertains to a specific domain. The definition above has been considered appropriate for the purpose of the present document.

**data concerning health:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status [i.16]

**data protection:** protection of data relating to an identified or identifiable natural person. In the context of the present report, data protection refers to personal data protection.  Notably, it is largely technically feasible that non-personal data become personal data

**genetic data:** personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

The following terms are taken from [i.3] and [i.4]:

**authentication:** verification of the claimed identity of an entity

**availability:** property of being accessible and usable upon demand by an authorized entity

**data:** data of any form, nature or structure, that can be created, uploaded, inserted in, collected or derived from or with cloud services and/or cloud computing, including without limitation proprietary and non-proprietary data, confidential and non-confidential data, non-personal and personal data, as well as other human readable or machine-readable data

**data controller:** natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

**data integrity:** property of protecting the accuracy and completeness of assets

**data portability:** ability to easily transfer data from one system to another without being required to re-enter data

**data processor:** natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller

**data retention period:** length of time which the cloud service provider will retain backup copies of the cloud service customer data during the termination process (in case of problems with the retrieval process or for legal purposes); this period may be subject to legal or regulatory requirements, which can place lower or upper bounds on the length of time that the provider can retain copies of cloud service customer data

**data subject:** identified or identifiable natural person, being an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

**information security:** preservation of confidentiality, integrity and availability of information

**personal data:** 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

**privacy:** ability of an individual to be left alone, out of public view, and in control of information about oneself

NOTE: One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy"). The concept of privacy therefore overlaps, but does not coincide, with the concept of data protection. The right to privacy is enshrined in the Universal Declaration of Human rights (Article 12) as well as in the European Convention of Human Rights (Article 8). (Also, see the definition in [i.4]). The concept of privacy within the context of data protection entails that personal data is entrusted to the data controller and/or data processor. The data controller and/or data processor are responsible to keep the data as "private" as possible, in the sense that data needs to be protected, as if it was not disclosed.

**privacy by design:** 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

NOTE: It is considered that a wider spectrum of approaches may be taken into account for the objective of privacy by design which includes a visionary and ethical dimension, consistent with the principles and values enshrined in the EU Charter of Fundamental Rights of the EU [i.24]. In practice, organizations often confuse privacy by design with data protection; privacy by design forms the broader concept, part of which is data protection.

**privacy enhancing technologies (PETs):** coherent system of information and communication technology (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system

NOTE: The use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules. It should result in making breaches of certain data protection rules more difficult and/or helping to detect them. PETs can be stand-alone tools requiring positive action by consumers (who does purchase and install them in their computers) or be built into the very architecture of information system.

**processing purposes:** list of processing purposes (if any) which are beyond those requested by the customer acting as a controller

**recital:** part of a legal document that sets out the reasons for the contents of the enacting terms (i.e. the articles) of an article

**vulnerability:** weakness of an asset or group of assets, e.g. software or hardware related, that can be exploited by one or more threats

## 3.2 Symbols

Void

## 3.3 Abbreviations

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

| | |
|---|---|
| AIOTI | Alliance for the Internet of Things Innovation |
| BS | British Standard |
| CCTV | Closed Circuit Television |
| DCMS | Digital, Culture, Media and Sport |
| DPIA | Data Protection Impact Assessment |
| EC | European Commission |
| EDPS | European Data Protection Supervisor |
| EEA | European Economic Area |
| ERP | Enterprise-Resource-Planning |
| ETSI | European Telecommunication Standards Institute |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| GSMA | Global System for Mobile Communications Association |
| ICO | Information Commissioner's Office |
| ICT | Information and Communication Technology |
| IEC | International Electrotechnical Commission |
| IoT | Internet of Things |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITS | Intelligent Transport System |
| ITU | International Telecommunications Union |
| ITU-T | ITU Telecom sector |
| LIBE | committee on civil Liberties, Justice and Home Affairs |