ETSI TR 103 534-2 V1.1.1 (2019-10)

SmartM2M;
Teaching material;
Part 2: Privacy

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/40172c58-c498-4ced-81d6-d11ffc82d680/etsi-tr-103-534-2-v1.1.1-2019-10

Reference

DTR/SMARTM2M-103534-2

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/[illegible]/etsi-tr-103-534-2-v1.1.1-2019-10

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/40172c58-c498-8fd6-d1ffc32d680e/etsi-tr-103-534-2-v1.1.1-2019-10

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/40172c58-c498-4ced-81d6-d11ffc82d680/etsi-tr-103-534-2-v1.1.1-2019-10

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 is to focus on producing teaching material on privacy and to direct the reader to other materials that are available in order to gain a basic understanding on what the privacy concept relates to that is particularly relevant, also, for the IoT environment. The present document is based on the Privacy Report ETSI TR 103 591 [i.1].

Taking into account the main gaps result of the STF 505 (https://portal.etsi.org/STF/STFs/STFHomePages/STF505) in relation to privacy and security as captured under ETSI TR 103 376 [i.13], the document starts by introducing the target audience to whom the present document is addressed to base on the assumption that the future reader has no knowledge on the issue of privacy. To this end and in view of achieving the maximum of the learning outcome, the document will address key aspects of privacy by raising a set of relevant questions. In line with the educational purpose envisioned, the document will be largely based on the use of examples.

In addition, the present document provides for other sources available for learners. In particular and in line with the approach taken under STF 515 (https://portal.etsi.org/STF/STFs/STFHomePages/STF515), a set of quizzes will allow the learner to verify the knowledge gained. Similarly, a set of slides will allow the learner to easily gain access to the contents of the present document. Both the quizzes and the slides are integrated in annex B of the present document.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/40172c58-c498-4ced-81d6-c11fc6e1d6c0/etsi-tr-103-534-2-v1.1.1-2019-10

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 privacy, 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 a 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:

ETSI TR 103 533 [i.14]

ETSI TR 103 534-1 [i.7]

ETSI TR 103 534-2 (the present document)

ETSI TR 103 535 [i.15]

ETSI TR 103 536 [i.16]

ETSI TR 103 537 [i.17]

ETSI TR 103 591 [i.1]

1.2 Scope of the present document

The focus of the present document is to present a summary of the teaching material to help in acquiring knowledge on IoT Privacy. The teaching slides are in annex B of the present document. The present document is to support the IoT Technical Report (TR) and it will re-enforce the knowledge in the TR such that reader can acquire basic knowledge to apply IoT privacy in their area of engagement or at least know where to obtain that information. The present document does not address IoT security, although closely linked but this is being addressed in a separate report which is ETSI TR 103 534-1 [i.7].

Learning Objective: Considering that the overarching objective of this teaching material is to provide learners with the necessary information, so as to gain basic knowledge on how the concept of privacy applies in the IoT environment. Allowing them to make decisions and act accordingly.

This teaching material is addressed to learners holding different functions in the supply chain. To this end, it provides for actors such as device manufacturers, software developers, and users benefiting from the delivery of service through the IoT supply chain.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/40172c58-c498-4ced-81dd-dffe2d80/etsi-tr-103-534-2-v1.1.1-2019-10

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 103 591 (V1.1.1): "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.2] European Data Protection Supervisor: "Glossary".

NOTE: Available at https://edps.europa.eu/data-protection/data-protection/glossary_en.

[i.3] Cloud Service Level Agreement Standardisation Guidelines.

NOTE: Available at https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines.

[i.4] 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.5] 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.6] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.7] ETSI TR 103 534-1 (V1.1.1): "SmartM2M; Teaching Material; Part 1: Security".

[i.8] Protecting Privacy and Data in the Internet of Things: "Considerations and techniques for big data, machine learning and analytics February 2019 GSMA".

NOTE: Available at www.gsma.com.

[i.9] European Data Protection Supervisor: "Preliminary Opinion on privacy by design", 31 May 2018.

[i.10] Noto La Diega Guido and Walden Ian: "Contracting for the 'Internet of Things': Looking into the Nest" (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016.

[i.11] Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, adopted on 16 September 2014.

[i.12] ICO: "Privacy in Mobile Apps Guidance for app developers".

NOTE: Available at https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf.

[i.13] ETSI TR 103 376 (V1.1.1) (2016-10): "SmartM2M; IoT LSP use cases and standards gaps".

ITeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/401...c58-c498-...-10
ced-11fc82...etsi-tr-103-534-2-v1.1.1-2019-10

[i.14] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.15] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.16] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.17] ETSI TR 103 537: "SmartM2M; Plugtests™ preparation on Semantic Interoperability".

[i.18] Proposal for a Regulation of the European Parliament and of the Council on ENISA, theof the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation.

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

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.18]

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

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/40172-58c498-4c4d-8f56-d1f6c82d680/etsi-tr-103534-2-v1.1.1-2019-10

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

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: bility 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 protection: The employment of technical, organisational and legal measures in order to achieve the goals of data security (confidentiality, integrity and availability), transparency, intervenability and portability, as well as compliance with the relevant legal framework.

NOTE: In the context of the present report, data protection refers to the protection of personal data. It is largely technically feasible that non-personal data become personal data.

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

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

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

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

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

The following terms are taken from [i.2]:

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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

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. 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 have to purchase and install them in their computers) or be built into the architecture of information system.

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
API	Application Programming Interface
CCTV	Closed Circuit TV
CIPM	Certified Information Privacy Manager
CIPP	Certified Information Privacy Professional
CIPP/E	Certified Information Privacy Professional/Europe
CIPT	Certified Information Privacy Technologist
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
HLA	High Level Architecture
IAPP	International Association of Privacy Professionals
IoT	Internet of Things
IT	Information Technology
MAC	Media Access Control
OTP	One Time Password
TR	Technical Report
TV	Television
WIFI	Wireless Networking

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/40172c58-c498-4ced-81dc-d11ffc82d680/etsi-tr-103-534-2-v1.1.1-2019-10

4 What is privacy?

4.1 Outline

This clause will introduce the learner to the concept of privacy, also, by using examples. It considers the related definitions from the EDPS glossary [i.2].

4.2 Privacy and data protection

Privacy is a concept used across different disciplines. From a legal standpoint its ability of an individual to be left alone, out of public view, and in control of information about oneself. As, also, illustrated under clause 3.1, 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 latter relates to what is known as personal data protection under EU law. In other terms, privacy is considered to be the underlying value of personal data protection. Note that for the purposes of the present document, privacy is conceived as personal data protection.

As further discussed under ETSI TR 103 591 [i.1] privacy is closely linked to security. Although, privacy and security are separate concepts in the sense, for example, that privacy can be perceived independently of security, yet, they are complementary, given that in reality security is an enabler of privacy. It can be stressed that security is a basic requirement for the effective protection of privacy.

4.3 The General Data Protection Regulation (GDPR)

4.3.1 Introduction

General Data Protection Regulation (GDPR) [i.4] provides exclusively for the protection of personal data in EU. The EU Institutions decided to repeal the Data Protection Directive [i.5] that provided for the protection of personal data at EU level as of 1995 by adopting a legislative instrument in the form of Regulation. The GDPR became applicable on the 25 May 2018 and it is directly applicable across all EU Member States.

The GDPR defines [i.4] the key concepts and the role of the main actors, as follows:

Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by 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.

Note that the GDPR provides separately for special categories of data, namely, genetic data, biometric data and data concerning health.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject: an 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.

Data Controller: Determines the purposes and means of the processing of personal data. The controller exercises control over the why and how of a data processing activity. Can be a person, Public authority, agency, organization, alone or jointly.

Data Protection Officer (DPO): A person who is formally tasked with ensuring that the organization is aware of and complies with its data protection responsibilities and obligations according to GDPR. The DPO, someone of expert knowledge on data protection law and practices. According to the GDPR, the DPO has an independent position and is not, therefore, assigned with tasks and duties that result in a conflict of interest.

Data Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller; Processor has to comply with instructions of the controller, Processors will now need to:

- Keep records of processing.
- Interact and assist supervisory authorities in the performance of their tasks.
- Implement appropriate technical and organizational measures ensure data security (now a legal obligation and will be exposed to fines for non-compliance).
- Notify any data breach to the controller without undue delay.
- Appoint a DPO where undertaking the following on a large scale: processing sensitive personal data or undertaking systematic monitoring of data subjects.

Third Party: natural or legal person, public authority, agency or body acting who are authorized to process personal data under the direct authority of the controller or processor.

Supervisory Authorities: they are independent public authorities their main responsibility is to monitor the application of GDPR with the aim to protect the fundamental rights and freedom of natural persons in relation to processing of data linking to them. Public authorities also promote public awareness and facilitate organizations' compliance by issuing guidance on actual implementation of the regulatory framework.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/401...-4ce6...-tr-103-534-2-v1.1.1-2019-10