ETSI TR 103 535 V1.1.1 (2019-10)

SmartM2M;
Guidelines for using semantic interoperability in the industry

Reference

DTR/SmartM2M-103535

Keywords

interoperability, IoT, oneM2M, privacy, SAREF, 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

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.

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.1]
- ETSI TR 103 534 [i.2]
- ETSI TR 103 536 [i.3]
- ETSI TR 103 537 [i.4]
- ETSI TR 103 591 [i.5]

1.2 Scope of the present document

Major efforts are on-going in the IoT community regarding the development of semantic interoperability for IoT. This progress has been notably accomplished by the involvement from academic players. However, semantic in IoT is complex, often misunderstood and its benefits are not well perceived by the industrial players.

The main objective of the present document is to push semantic interoperability in IoT forward in raising awareness about its importance in industry in order to unlock the potential economic value of IoT. A major focus is on the development of guidelines on how to use semantic interoperability in the industry.

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".

[i.2] ETSI TR 103 534 (all parts): "SmartM2M; Teaching Material".

[i.3] ETSI TR 103 536: "SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.4] ETSI TR 103 537: "SmartM2M; PlugtestsTM preparation on Semantic Interoperability".

[i.5] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.6] AIOTI Report: "High Level Architecture (HLA) Release 4.0 June 2018".

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

[i.7] IoT-EPI: "IoT Platforms Interoperability Approaches", White Paper, IoT-EPI Platform Interoperability Task Force, 2017 updated in 2018 by "Advancing IoT Platforms Interoperability Book", July 2018, White Paper.

NOTE: Available at http://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf.

[i.8] Inter-IoT project.

NOTE: Available at http://www.inter-iot-project.eu.

[i.9] InterIoT GOIoTP: "Generic Ontology for IoT Platforms".

NOTE: Available at http://docs.inter-iot.eu/ontology.

[i.10] VICINITY project.

NOTE: Available at https://www.vicinity2020.eu.

[i.11] VICINITY Deliverable D1.6: "VICINITY Architectural Design".

NOTE: Available at https://www.vicinity2020.eu/vicinity/content/d16-vicinity-architectural-design.

[i.12] BIG-IoT project.

NOTE: Available at http://big-iot.eu/.

[i.13] Stefan Schmid et al: "An Architecture for Interoperable IoT Ecosystems". 2nd International Workshop on Interoperability & Open Source Solutions for the Internet of Things (InterOSS-IoT 2016) at the 6th International Conference on the Internet of Things (IoT 2016), 7 November 2016, Stuttgart, Germany. Springer, LNCS.

[i.14] A.S. Thuluva et al: Recipes for IoT Applications: "The 7th International Conference on the Internet of Things (IoT 2017)", 22.-25. October 2017, Linz, Austria. ACM.

[i.15] ACTIVEAGE project.

NOTE: Available at http://www.activageproject.eu.

[i.16] ACTIVAGE Deliverable D3.2: "ACTIVAGE Interoperability layer architecture".

[i.17] MONICA project.

NOTE: Available at http://www.monica-project.eu.

[i.18] MONICA Deliverable D3.1: "IoT Enabled Devices and Wearables 2", 2018.

NOTE: Available at https://www.monica-project.eu/sdm_downloads/d3-2-iot-enabled-devices-and-wearables-2/.

[i.19] S. Meiling and al: MONICA in Hamburg: "Towards Large-Scale IoT Deployments in a Smart City".

[i.20] ETSI TS 103 264: "SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping".

NOTE: Available at https://www.etsi.org/standards#page=1&search=TS%20103%20264.

[i.21] ETSI TS 103 410 (all parts): "SmartM2M; Smart Appliances Extension to SAREF".

NOTE: Available at https://www.etsi.org/standards#page=1&search=TS%20103%20410.

[i.22] ETSI TS 118 112: "oneM2M; Base Ontology (oneM2M TS-0012 version 2.0.0 Release 2)".

[i.23] ETSI SAREF: "SAREF ontology".

NOTE: Available at http://saref.etsi.org. The documentation of SAREF v2.1.1 will be available here soon. The source of the ontology are available as Turtle or RDF/XML Visualize it with VOWL.

[i.24] W3C SSN Editor's Draft: "Semantic Sensor Network Ontology".

NOTE: Available at http://w3c.github.io/sdw/ssn/.

[i.25] W3C Recommendation: "Semantic Sensor Network ontology".

NOTE: Available at https://www.w3.org/TR/vocab-ssn/.

[i.26] ETSI TR 118 507: "oneM2M; Study on Abstraction and Semantics Enablement (oneM2M TR-0007 Release 2)".

[i.27] Moreira, J. L., Daniele, L. M., Ferreira Pires, L., van Sinderen, M. J., Wasielewska, K., Szmeja, P., Paprzycki, M. (2017): "Towards IoT platforms' integration: Semantic Translations between W3C SSN and ETSI SAREF". Paper presented at SEMANTiCS conference 2017, Amsterdam, Netherlands.

[i.28] Mainflux project.

NOTE: Available at https://www.mainflux.com/.

[i.29] Ervin Varga, Draško Drašković, Dejan Mijić: "Scalable Architecture for the Internet of Things", Publisher: O'Reilly Media, Inc., February 2018, ISBN: 9781492024132.

[i.30] ETSI TR 103 545: "SmartM2M; Pilot test definition and guidelines for testing cooperation between oneM2M and Ag equipment standards".

[i.31] ISO 11783: "Tractors and machinery for agriculture and forestry -- Serial control and communications data network".

[i.32] ETSI EN 302 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".

[i.33] IETF RFC 8428: "Sensor Measurement Lists (SenML)", C. Jennings et al. August 2018.

[i.34] Nova: Nova, 2004: "The Ontology Problem: A Definition with Commentary".

[i.35] Jaehun Joo (2011): "Adoption of Semantic Web from the perspective of technology innovation: A grounded theory approach". Int. J. Hum.-Comput. Stud. 69, 3 (March 2011), 139-154.

[i.36] ETSI TS 118 121: "oneM2M; oneM2M and AllJoyn® Interworking (oneM2M TS-0021)".

[i.37] ETSI TS 118 114: "oneM2M; LWM2M Interworking (oneM2M TS-0014)".

[i.38] ETSI TS 118 124: "oneM2M; OIC Interworking (oneM2M TS-0024)".

[i.39] ETSI TR 118 556: "oneM2M; Summary of Differences between Release 2A & Release 3 (oneM2M TR-0056)".

[i.40] ETSI TS 118 133: "Interworking Framework (oneM2M TS-0033 v0.1.1)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

domain ontology: concepts which belong to a part of the world, such as energy, building or Environment

IoT LSP: Internet of Things Large Scale Pilots which are part of the H2020 Work Program 2016-2017

oneM2M: Partnership Project (EPP) on M2M launched by a number of SSOs including ETSI

Open Source Software (OSS): computer software that is available in source code form

NOTE: The source code and certain other rights normally reserved for copyright holders are provided under an open-source license that permits users to study, change, improve and at times also to distribute the software.

source code: any collection of computer instructions written using some human-readable computer language, usually as text

standard: output from a Standards Setting Organization (SSO)

Standards Setting Organization (SSO): any entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting or otherwise maintaining standards that address the interests of a wide base of users outside the standards development organization

NOTE: In the present document, SSO is used equally for both Standards Setting Organization or Standards Developing Organizations (SDO).

upper ontology: also called a top-level ontology or foundation ontology, is an ontology that models very general concepts common across several domains

NOTE: An important function of an upper ontology is to support broad semantic interoperability among a large number of domain-specific ontologies by providing a common starting point for the formulation of definitions.

3.2 Symbols

Void.

3.3 Abbreviations

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

AD	Automated Driving
ADN	Application Dedicated Node
AE	Application Entity
AEF	Agricultural Industry Electronics Foundation
AIOTI	Alliance for the Internet of Things Innovation
API	Application Programming Interface
ASN	Application Service Node
BLE	Bluetooth Low Energy
CBOR	Concise Binary Object Representation
CEN	European Committee for Standardization
CIM	Core Information Model

CSE	Common Service Entity
DATEX	Data Exchange format For Exchanging Traffic Information
DL	Description Logic
DMAG	Data Modelling Activity Group
DSF	Demand-side Flexibility
EC	European Commission
EPI	European Platforms Initiative
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
ETL	Extract, Transform and Load
ETSI	European Telecommunications Standards Institute
EXI	Efficient XML Interchange
GPS	Global Positioning System
HGI	Home Gateway Initiative
ICT	Information and Communication Technology
IIoT	Industrial IoT
IoT	Internet of Things
IoT-EPI	IoT European Platform Initiative
iPaaS	Integration Platform as a Service
ISG	Industry Specification Group
ISO	International Organization for Standardization
ITS	Intelligent Transport System
JSON	JavaScript Object Notation
LSP	Large Scale Pilot
M2M	Machine-to-Machine
MN	Middle Node
MQTT	Message Queuing Telemetry Transport
NGSI	Next Generation Service Interface
OGC	Open Geospatial Consortium
OIC	Open Interconnect Consortium
OPC	Open Platform Communications
OPC-UA	OPC Unified Architecture
OSS	Open Source Software
OWL	OntologyWeb Language
P2P	Point-to-Point
PIM	Platform-Specific Information Model
RDF	Resource Description Framework
SAREF	Smart Applications REFerence ontology
SDO	Standard Development Organization
SDT	Smart Device Template
SEAS	Smart Energy Aware Systems
SIL	Semantic Interoperability Layer
SOSA	Sensor, Observation, Sampler and Actuator
SPINE	Smart Premises Interoperable Neutral-message Exchange
SSN	Semantic Sensor Network
SSO	Standards Setting Organization
TC	Technical Committee
UA	Unified Architecture
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WoT	Web of Things
XML	eXtensible Markup Language

4 Semantic interoperability 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.

Most of the above-mentioned essential characteristics may be found in other ICT-based systems. However, the main difference with IoT systems is that they all have to be dealt with simultaneously. The most essential ones are:

- **Stakeholders.** There is a large variety of potential stakeholders with a wide range of roles that shape the way each of them can be considered in the IoT system. Moreover, none of them can be ignored.
- **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.
- **Interoperability.** There are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc.
- **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.
- **Technologies.** By nature, all IoT systems have to integrate potentially very diverse technologies, very often for the same purpose (with a risk of overlap). The balance between proprietary and standardized solutions has to be carefully managed, with a lot of potential implications on the choice of the supporting platforms.
- **Deployment.** 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 have to deal with the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.
- **Legacy.** Many IoT systems have to deal with legacy (e.g. existing connectivity, back-end ERP systems). The challenge is to deal with these requirements without compromising the "IoT centric" approach.

4.1.2 The need for an "IoT-centric" view

4.1.2.1 Introduction

In support of an "IoT-centric" approach, some elements have been used in the present document in order to:

- support the analysis of the requirements, use cases and technology choices (in particular related to interoperability);
- ensure that the target audience can benefit from recommendations adapted to their needs.

4.1.2.2 Roles

A drawback of many current approaches to system development is an exclusive focus on the technical solutions without considering the individual in these multiple capacities (e.g. user of an IoT device, professional) which may lead to suboptimal or even ineffective systems that hinder maximizing the benefits of IoT. In the case of IoT systems, a very large variety of potential stakeholders are involved, each coming with specific - and potentially conflicting - requirements, expectations and, possibly, vested interests. Their elicitation requires that the precise definition of roles that can be related to in the analysis of the requirements, of the use cases, etc.