ETSI TR 103 537 V1.1.1 (2019-09)

TECHNICAL REPORT

SmartM2M;
Plugtests™ preparation on Semantic Interoperability

Reference

DTR/SmartM2M-103537

Keywords

interoperability, IoT, oneM2M, privacy, SAREF,
semantic, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

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

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

- ETSI TR 103 533 [i.12]: "SmartM2M; Security; Standards Landscape and best practices".
- ETSI TR 103 534 [i.13]: "SmartM2M; Teaching Material: Part 1: IoT Security and SmartM2M; Teaching Material; Part 2: IoT Privacy".
- ETSI TR 103 535 [i.1]: "SmartM2M; Guidelines for using semantic interoperability in the industry".
- ETSI TR 103 536 [i.9]: "SmartM2M; Strategic/technical approach on how to acheive interoperability/interworking of existing IoT Platforms".
- ETSI TR 103 591 [i.14]: "SmartM2M; Privacy study report; Standards Landscape and best practices".

1.2 Scope of the present document

The present document intends to define and prepare the organization of a Plugtests™ event on Semantic Interoperability based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing to demonstrate a more practical/industrial use. This work includes test configurations and scenarios as well as guidelines for the test organization and reporting.

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 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.2] "Advancing IoT Platforms Interoperability", IoT European Platforms Initiative (IoT-EPI), River Publishers, 2018.

[i.3] "Semantic Interoperability", AIOTI WG03, Release 2.0, 2015.

[i.4] "Semantic Interoperability as Key to IoT Platform Federation", M. Jacoby, A. Antonic, K. Kreiner, R. Lapacz and J. Pielorz, 2017.

[i.5] ETSI TS 103 264 (V2.1.1): "SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping".

[i.6] ETSI TS 118 133: "oneM2M; Interworking Framework (oneM2M TS-0033)".

[i.7] ETSI TS 118 112: "oneM2M; Base Ontology (oneM2M TS-0012)".

[i.8] ETSI TS 118 113: "oneM2M; Interoperability Testing (oneM2M TS-0013)".

[i.9] ETSI TR 103 536: "SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.10] ETSI TS 118 115: "oneM2M; Testing Framework (oneM2M TS-0015)".

[i.11] "High Level Architecture (HLA)", AIOTI WG03, Release 4.0, 2018.

[i.12] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.13] ETSI TR 103 534 (all parts): "SmartM2M; Teaching Material (Part 1: IoT Security and Part 2: IoT Privacy)".

[i.14] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.15] ETSI TS 118 123: "oneM2M; Home Appliances Information Model and Mapping (oneM2M TS-0023)".

[i.16] ETSI TS 118 121: "oneM2M; oneM2M and AllJoyn® Interworking (oneM2M TS-0021)".

[i.17] ETSI TS 118 114: "oneM2M; LWM2M Interworking (oneM2M TS-0014)".

[i.18] ETSI TS 118 124: "oneM2M; OCF nterworking (oneM2M TS-0024)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

ontology: formal specification of a system, defining its components as objects with their main concepts, properties, attributes and relationships versus other components (derived from ETSI TS 118 112 [i.7])

semantics: meta-data describing the content and meaning of a data structure that relates it to the real system it describes

semantic interoperability: ability of IoT devices and platforms to exchange data with unambiguous, shared meaning (derived from Wikipedia)

semantic interoperability testing: validating that a data source and sink are compatible and have the same semantics for a specific data structure

semantic interworking: ability of IoT devices and platforms to exchange data by the means of intermediate components responsible for the mapping of data

semantic-unaware platform: IoT platform which does not support semantics

3.2 Symbols

Void.

3.3 Abbreviations

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

AIOTI	Alliance for IoT Innovation
BO	Base Ontology
CFG	Configuration
CIM	Core Information Model
CSE	Common Services Entity
CTI	Centre for Testing and Interoperability
DUL	DOLCE Ultra Lite
EPI	European Platforms Initiative
ERP	Enterprise Resource Planning
ETSI	European Telecommunication Standards Institute
EU	European Union
HMI	Human Machine Interface
HPA	High Pressure Alarm
ICT	Information and Communication Technology
IoT	Internet of Things
IoT-EPI	IoT European Platforms Initiative
IP	Internet Protocol
ISA	International Society of Automation
IT	Information Technology
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
LSP	Large Scale Pilot
LWM2M	Lightweight M2M
M2M	Machine-to-Machine
Mcc	Reference Point for M2M Communication with CSE
OCF	Open Connectivity Foundation
OWL	Web Ontology Language
PT	Pressure Transmitter
PV	Pressure Value
RDF	Resource Description Framework
SAREF	Smart Applications REFerence ontology
SDT	Smart Device Template
SI	Semantic Interoperability
SSN	Semantic Sensor Network
TC	Technical Committee
TR	Technical Report
TS	Technical Specification
V	Vessel
W3C	World Wide Web Consortium
WG	Working Group
WiFi	Wireless Fidelity
WoT	Web of Things
XML	eXtensible Markup Language

4 Semantic Interoperability Plugtests™ 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 a focus on the technical solutions, which may lead to suboptimal or even ineffective systems. In the case of IoT systems, a very large variety of potential stakeholders are involved, each coming with specific - and potentially conflicting - requirements and expectations. 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.

Examples of such roles to be characterized and analysed are:

- System Designer
- System Developer
- System Deployer
- Device Manufacturer
- Interoperability test organizer
- Interoperability test technical expert

More roles can be defined but the present document will focalise on the ones above.

4.1.2.3 Reference Architecture(s)

In order to better achieve interoperability, many elements (e.g. vocabularies, definitions, models) have to be defined, agreed and shared by the IoT stakeholders. This can ensure a common understanding across them of the concepts used for the IoT system definition. They also are a preamble to standardization. Moreover, the need to be able to deal with a great variety of IoT systems architectures, it is also necessary to adopt Reference Architectures, in particular Functional Architectures. An example of such architecture is the AIOTI High Level Architecture, described in [i.11].

4.1.2.4 Guidelines

The very large span of requirements, use cases and roles within an IoT system make it difficult to provide prototypical solutions applicable to all of the various issues addressed. The approach taken in the present document is to outline some solutions but also to provide guidelines on how they can be used depending on the target audience. Such guidelines are associated to the relevant roles and provide support for the decision-making.

4.2 Main objectives of the present document

As part of its activities towards platforms interoperability, the present document aims at preparing a Plugtests^{TM} event on Semantic Interoperability. For this Plugtests^{TM} event, the interoperability will be based on AIOTI High Level Architecture, oneM2M base ontology (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing, with the objective to demonstrate a more practical/industrial use. The present document will include test requirements, configurations and test descriptions in preparation of the event. This work is expected to be developed in close collaboration with the ETSI Centre for Testing and Interoperability (CTI) and will deliver examples of test scenarios and testing organization.

4.3 Purpose and target group

The purpose of the present document is described in clause 1.2.

The target group of readers for the present document is described in clause 4.1.2.2, "Roles".

4.4 Content of the document

The first part of the present document intends to identify the testing requirements from the semantic interoperability standards, especially those collected in ETSI TR 103 535 [i.1] and ETSI TR 103 536 [i.9].

In a next step, the present document focuses on the test configurations and additional elements involved such as components, protocols, data models when appropriate.

Then, the present document defines a set of related interoperability test scenarios based on results in these Technical Reports, but also use case documents from AIOTI, oneM2M, SmartM2M, W3C, etc. Scenarios showing interworking of semantic-unaware systems with systems supporting semantic interoperability are included as well. The scenarios are described from a user point of view, following the ETSI methodology as defined in ETSI Testing Framework [i.10].

Each scenario description clarifies the different actors involved in the test, the pre-conditions, trigger, main and alternative operational flows, as well as post-conditions and test sequence.

Finally, the present document identifies and describes the event preparation requirements like infrastructure, IT and related tools. In this step, it provides guidelines/cook-book on requirements for anonymous reporting of the Plugtests™ outcomes and results.

The organization (logistics/administration), detailed test description and the conduction of the event including the support to participants, are outside the scope of the present document.

5 Requirements for testing semantic interoperability

5.1 Approaches for Semantic Interoperability (SI)

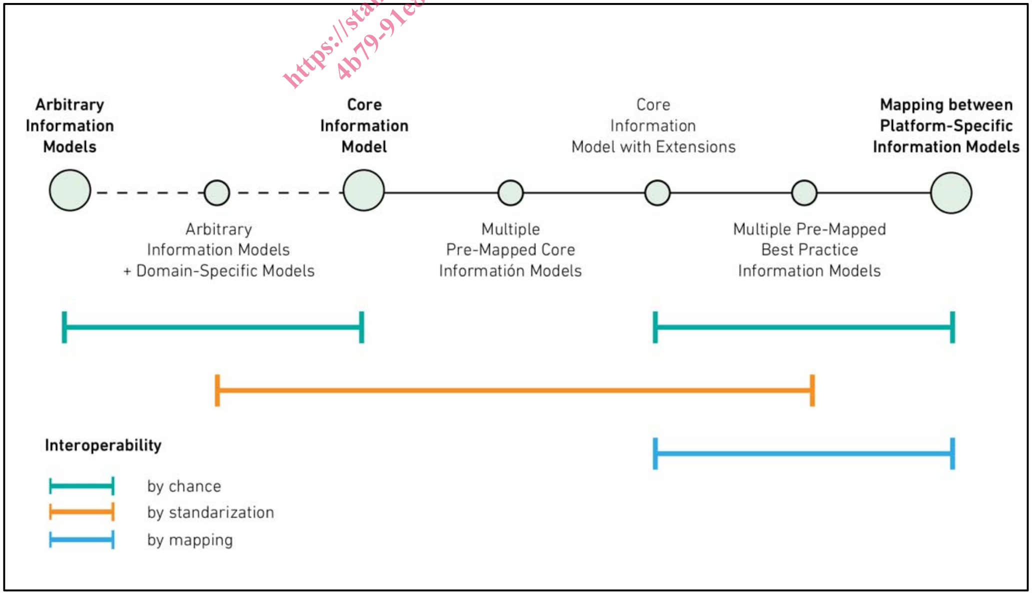
5.1.1 Possible approaches

The main expectation of semantic interoperability is to provide an unambiguous meaning of what the "things" are that two (or more) platforms may share and agree upon, thus bridging the potential semantic gap coming from different description and implementations of the "thing" under concern. The challenge of semantic interoperability is in general a cross-platform issue, though it can be also met with two components on the same platform.

The IoT European Platforms Initiative (IoT-EPI) has addressed this issue (see [i.2]) in a global manner with a model that is depicted in Figure 1. There are two dimensions in their analysis:

- The main approaches related to the technical solution that can range from a single Core Information Model (CIM) that every platform should comply to (irrespective of the domain or sector) up to the possibility to define the models that a platform considers as appropriate, while ensuring that these models can be aligned by using a semantic mapping that can be shared across platforms.

- The type of interoperability that can be expected: "by chance" (where a platform will interoperate with another one only if their models happen to be the same), "by standardization" (where platforms agree on whole or part of a common standardized model) or "by mapping" (where some translation "logic" is applied between different models).


Arbitrary Information Models
Core Information Model
Core Information Model with Extensions
Mapping between Platform-Specific Information Models
Arbitrary Information Models + Domain-Specific Models
Multiple Pre-Mapped Core Information Models
Multiple Pre-Mapped Best Practice Information Models
Interoperability
by chance
by standarization
by mapping

NOTE: Source: IoT-EPI Task Force, [i.2], based on [i.4].

Figure 1: Possible approaches to semantic interoperability

The preparation and undertaking of semantic interoperability Plugtests™ will address the validation of interoperability "by standardization" or "by mapping" and will focus on the approaches ranging from Core Information Model (CIM) to Multiple Pre-Mapped Best Practice Information Models (as described in Figure 1). A similar approach would apply for the case of multiple ontologies, as described in clause 6.

More information on and examples of these approaches can be found in the companion ETSI TR 103 535 [i.1]. Some are also described in clause 5.1.3 of the present document.

5.1.2 Commonalities and differences between SI approaches

The most common way to achieve semantic interoperability is via "ontologies" that are an explicit specification of a shared "understanding" that can be processed automatically by machines. Recent standardization efforts have produced a number of IoT-specific ontologies, such as SAREF, oneM2M Base Ontology (BO), SSN Ontology and others (see the AIOTI WG03 analysis in [i.3]).

The IoT ontologies will in general offer different perspectives on (parts of) the IoT system and describe a way to model the central part of an IoT system. However, standardized IoT ontologies may result from different approaches: high-level abstraction (e.g. oneM2M BO), deep taxonomies (e.g. SSN that extends a top-level ontology DUL), or deployment orientation (e.g. Open-IoT weather station model).

IoT ontologies often need to be extended (e.g. Core ontologies) or customized before being used in a concrete application thus creating the need for careful validation of different implementations which is the purpose of the Plugtests^{TM}.

5.1.3 Examples of different approaches

5.1.3.1 SAREF

The Smart Appliances/Applications REFerence ontology (SAREF) is the result of an EU initiative launched in 2013 with the support of ETSI in order to create a shared semantic model based on consensus to enable the missing interoperability among smart appliances. SAREF can be considered as an addition to existing communication protocols to enable the translation of information coming from existing (and future) protocols to and from all other protocols that are referenced to SAREF. For example, a home gateway enriched by SAREF can associate devices in a home with each other and with different service providers.

The initial focus was on the optimization of energy management in smart buildings. The first resulting semantic model - SAREF - was standardized by ETSI in November 2015 (ETSI TS 103 264 [i.5]). SAREF is a first ontology standard in the IoT ecosystem and sets a template and a base for the development of similar standards for other verticals.

Since its first release, SAREF continues to evolve systematically into a modular network of standardized semantic models, with additional extensions such as SAREF for Energy, SAREF for Environment and SAREF for Buildings. More work is on-going in a number of other domains such as Smart Cities, Smart AgriFood, Smart Industry and Manufacturing, Automotive, eHealth/Ageing-well and Wearables. The objective is to make SAREF a "Smart Application REFerence ontology", which enables better integration of semantic data from various vertical domains.

5.1.3.2 oneM2M semantic interoperability approaches

The oneM2M standard supports different approaches for semantic interoperability requiring a before agreement between applications and devices to share data between them (see [i.6]).

The main approaches are:

1) Pure ontology-based solution (RDF/OWL serialization format): oneM2M base ontology extended with a domain-specific ontology e.g. SAREF.
See: "oneM2M TS-0012 oneM2M Base Ontology" (ETSI TS 118 112 [i.7]).

2) Common vocabulary (basic serialization format XML or JSON): Smart Device Template (SDT) for the home domain.
See: "oneM2M TS-0023 Home Appliances Information Model and Mapping" (ETSI TS 118 123 [i.15]).