ETSI TR 103 376 V1.1.1 (2016-10)

SmartM2M;
IoT LSP use cases and standards gaps

Reference
DTR/SmartM2M-103376

Keywords
IoT, M2M

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

IPRs essential or potentially essential to the present document 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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

NOTE: 3GPP™, AllJoyn™, AllSeen™ Alliance™, ASHRAE™, AVNU Alliance™, B2MML™, BACnet™, Bluetooth™, C2C-CC™, DASH7™, DICOM™, EnOcean™, HL7™, IETF™, IIC™, KNX™, LoRa™, LR-WPAN™, LTE™, LTE-Advanced™, LTE-Advanced Pro™, MIPI™, MirrorLink™, OASIS™, OCF™, OGC™, OMA™, OMG™, OPC™, OSGi™, SAE INTERNATIONAL™, SERCOS International™, UMTS™, W3C™, Wi-Fi Alliance™, ZigBee™ and Z-Wave™ are tradenames registered by their respective owners. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of these products and/or associations.

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

Starting from the use case families selected for the IoT Large Scale Pilots (LSPs) the present technical report aim is:

- To provide the collection of all missing functionalities that have been identified in standards bodies (SDOs) to offer solutions addressing the use case requirements.
- To check that there are no omissions in the standardization activity with regard to the use cases. In particular, gaps with respect to the framework as identified by oneM2M should be identified.
- To propose some recommendations to overcome potential gaps. Particular attention will be paid on horizontal application layer standardization and to assure an interworking framework among different vertical industrial segments.

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 103 375: "SmartM2M; IoT Standards landscape and future evolutions".

[i.2] AIOTI WG03: "IoT Large Scale Pilots (LSP) Standard Framework Concepts", Release 2.0, October 2015.

[i.3] AIOTI WG03: "Report on High Level Architecture (HLA)", Release 2.0, October 2015.

[i.4] AIOTI WG08: "Smart City LSP Recommendations Report", October 2015.

[i.5] AIOTI WG05: "Report on Smart Living Environment for Ageing Well", October 2015.

[i.6] AIOTI WG09: "Report on Smart Mobility", October 2015.

[i.7] AIOTI WG07: "Report on Wearables", October 2015.

[i.8] AIOTI WG11: "Report on Smart Manufacturing", October 2015.

[i.9] ISO 37120: "Sustainable development of communities -- Indicators for city services and quality of life".

[i.10] Recommendation ITU-T X.1255: "Framework for discovery of identity management information".

[i.11] AIOTI WG06 Report: "Smart Farming and Food Safety Internet of Things Applications - Challenges for Large Scale Implementations", October 2015.

[i.12] Resolution ITU-R 66: "Studies related to wireless systems and applications for the development of the Internet of Things".

[i.13] IEEE 802.1X-2010™: "IEEE Standard for Local and metropolitan area networks -- Port Based Network Access Control".

3 Definitions and abbreviations

3.1 Definitions

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

SDO: standards developing or standards setting organization

NOTE: In the present document, SDO is used equally for both types of organizations.

standardization gaps: missing or duplicate elements in the IoT standardization landscape

NOTE: Examples of standardization gaps are: missing standards or regulations, missing APIs, technical interoperability profiles that would clarify the use cases, duplications that would require harmonization. They may be technical, societal or business-related.

3.2 Abbreviations

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

3GPP	Third Generation Partnership Project
ACEA	Association des Constructeurs Européens d'Automobiles
AIOTI	Alliance for IoT Innovation
API	Application Programming Interface
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
BAN	Body Area Network
BBF	Broad Band Forum
BSM	Basic Safety Message
C2C-CC	Car 2 Car Communication Consortium
CAM	Cooperative Awareness Message
CCC	Car Connectivity Consortium
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
CiA	CAN in Automation
CoAP	Constrained Application Protocol
CPPS	Cyber-Physical Production System
D2D	Device-to-Device
DDS	Data Distribution Service
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name System
EC	European Commission
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EU	European Union
FIWARE	Future Internet -ware
FMIS	Farm Management Information Systems
GNSS	Global Navigation Satellite System
HF	Human Factors
HGI	Home Gateway Initiative
HL7	Health Level Seven International
HLA	High Level Architecture
HMI	Human Machine Interface
HW	Hardware
IBM	International Business Machines (Corporation)
ICT	Information and Communication Technology

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IIC	Industrial Internet Consortium
IMT	International Mobile Telecommunications
IoT	Internet of Things
IP	Internet Protocol
IPSO	Internet Protocol for Smart Object
ISO	International Organization for Standardization
ISO/IEC JTC1	ISO/IEC joint technical committee
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Sector
KA	Knowledge Area
KNX	KoNneX
LAN	Local Area Network
LE	Low Energy
LON	Local Operator Network
LSP	Large Scale Pilot
M2M	Machine-to-Machine
MAC	Media Access Control
MAN	Metropolitan Area Network
MES	Manufacturing Execution System
MESA	Manufacturing Enterprise Solutions Association International
MQTT	MQ Telemetry Transport
NFC	Near Field Communication
NWK	NetWorK
OAA	Open Automotive Alliance
OAGi	Open Applications Group
OASIS	Advancing Open Standards for the Information Society
OCF	Open Connectivity Foundation
ODVA	Open DeviceNet Vendor Association
OGC	Open Geospatial Consortium
OMA	Open Mobile Alliance
OMG	Object Management Group
OPC	Open Platform Communications
OSGi	Open Services Gateway initiative
PAN	Personal Area Network
PHD	Personal Health Device
PHY	PHYsical layer
PII	Personally Identifiable Information
PLC	Power Line Communication
PLC	Programmable Logic Controller
PSA	Protocol Standards Association
QoS	Quality of Service
ROI	Rate Of Interest
ROLL	Routing Over Low power and Lossy networks
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Developing Organization
SERCOS	SErial Real-time COmmunication System
SES	Satellite Earth Stations and Systems
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprise
SSO	Standards Setting Organization
TC	Technical Committee
TCP	Transmission Control Protocol
TIM	Transducer Interface Module
TR	Technical Report
ULE	Ultra Low Energy

US	United States
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
W3C	Worldwide Web Consortium
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
XMPP	eXtensible Messaging and Presence Protocol

4 General Considerations

4.1 Introduction

4.1.1 Defining gaps

In ETSI TR 103 375 [i.1], an inventory of the current IoT standardization has been performed. Its objective is to assess the degree of industry and vertical market fragmentation; and to point towards actions that can increase the effectiveness of IoT standardization, to improve interoperability, and to allow for the building of IoT ecosystems. ETSI TR 103 375 [i.1] identifies a number of standards that are available, i.e. that have reached a final stage in a Standards Developing Organization by the time of writing the report, and can be used for the work of the IoT Large Scale Pilots (LSP).

However, the coverage of the IoT landscape - and the possibility to develop large-scale interoperable solutions - is not fully guaranteed since some elements in this landscape may be missing. These missing elements are referred to as "gaps" in the remainder of the present document. Gaps may also be identified when harmonization or interoperability between a large number of potential solutions is missing.

These "gaps" are the main point of interest of the present document. Three categories of gaps will be addressed:

- Technology gaps. Some examples in this category are communications paradigms, data models or ontologies, software availability.
- Societal gaps. Some examples in this category are privacy, energy consumption, ease of use.
- Business gaps. Some examples in this category are siloed applications, value chain, and investment.

In the reminder of the present document, the identification of gaps will be specially made in view of ensuring that they will be further understood, handled and closed within the IoT community (and possibly beyond). This identification of gaps will rely on an approach that allows for:

- The characterization of gaps, in particular by understanding the type of gaps (see above), the scope of the gap, the difficulties it generates, and other appropriate descriptions.
- The mapping of the gaps on an architectural framework (see clause 4.1.3) that allows for the mapping of the gaps on a reference that can be understood by the IoT community and, in particular, that can be related to other frameworks e.g. those developed in other organizations, for instance in Standards Setting Organizations.

This characterization and mapping are made with the objective to ensure that - whenever possible - these gaps may be handled, and hopefully closed, by one or more organizations in the IoT community.

The present document does not have the aim to undertake the resolution of the gaps that is left to the proper organizations of the IoT community. However, its objective is also to provide recommendations for the future standard framework.

4.1.2 Identifying gaps: user survey

A critical part of the identification of gaps is the collection of those missing elements. Since they can be of very different nature (see clause 4.1.1) and may have been detected by very different actors of the IoT community, there needs to be a mechanism to collect the largest possible information. To this extent, a survey has been built in order to identify as many gaps as possible with the help of the IoT community, in particular the IoT standardization community.

The survey aims at:

- Identifying the domain of activity of the respondent.
- Understanding what his/her objectives and main area of work are.
- Defining up to three gaps of all three types as defined in clause 4.1.1.

The detailed text of the survey can be found in annex B.

The survey has been largely distributed. At the time of writing the final version of the present document, 215 answers have been collected and the survey is closed. A few statistics on the responders and answers received can be found in clause B.2.

In a second step, these answers have been analysed with the objective to identify commonalities (i.e. related missing functionalities that can be considered as one gap) and associated interoperability frameworks.

The answers received have been tentatively classified in the different clauses of the present document. Clauses 5.3, 6.3, 7.3, 8.3, 9.3, 10.3 and 11.3 provide the answers which are related to a defined vertical sector. Clause 12.1 gives the answers which apply to the horizontal domain or are more generic. However, it should be noted that the answers received are generally not applicable to one specific vertical sector. For example, readers willing to cover all answers applicable to the wearable vertical sector should refer to the clauses related to Smart Living, Smart Wearables as well as clause 12.1. The matrix provided in table 0 gives guidance in that direction.

Table 0: Cross-domain reading of the survey answers

Answers in [vertical or horizontal domain on the right] may be shared with the [vertical domain below]	Horizontal (clause 12.1)	Smart Cities (clause 5.3)	Smart Living (clause 6.3)	Smart Farming (clause 7.3)	Smart Wearables (clause 8.3)	Smart Mobility (clause 9.3)	Smart Manufacturing (clause 10.3)	Smart Environment (clause 11.3)
Smart Cities	X	X	X			X		
Smart Living	X	X	X		X			
Smart Farming	X			X			X	X
Smart Wearables	X		X		X			
Smart Mobility	X	X				X		X
Smart Manufacturing	X			X			X	
Smart Environment	X			X		X		X

4.1.3 Identifying gaps: requirements analysis

The present clause explains the methodology implemented by the editors of the present document to identify technological requirements for each of the vertical areas and tentatively map them to organizations that provide standards related to these requirements.

This study has been executed in parallel and independently from the user survey described in clause 4.1.2.

For each vertical sector, the main technological requirements are extracted from the vertical-specific AIOTI reports and other available documentation describing that vertical sector. In a second step, the listed requirements are classified according to the knowledge areas to which they belong. They are shown in the left column of the tables. For more accuracy, the Communication and connectivity knowledge area is divided according to the main usual communication layers:

- Connectivity at physical and link layer.
- Network layer.
- Service level and application enablers.
- Application level API, data models and ontologies.

The next step identifies which SDOs/Alliances address the target requirement. The standards found are not listed directly in the present document, since this list maybe complex in some cases (it may be provided however in a revised version of the present document). The reader is rather referred to the partner TR, ETSI TR 103 375 [i.1], as the reference where existing concrete standards for each SDO/Alliance that address the specific requirement in the target vertical domain and knowledge area can be found.

In the case where no standard could be identified for a specific requirement, the requirement is declared as a potential standardization gap.

4.1.4 Mapping gaps

Before mentioning gaps, and in particular standards gaps that an LSP may have to address in the achievement of its objectives, one first needs to have a target framework in mind. The AIOTI WG03 has developed a standard framework or architecture for IoT which is similar or can be mapped to other frameworks such as ITU, oneM2M, IIC. The one thing that the frameworks have in common is the fact that interoperability must be achived amongst the various elements of the IoT. Interoperability means having interworking standards with less complexity. With a target model in mind and an idea of what the current landscape looks like, which are the objectives of the ETSI TR 103 375 [i.1], it is now possible to identify which are the remaining gaps to achieve IoT. The focus of the present document is to look at such gaps in the standard that will be needed to achieve the various LSP and make recommendation on going forward.

The landscape analysed in ETSI TR 103 375 [i.1] has described the IoT standards from the view point of the elements or knowledge areas that make up the IoT framework. The present document adopts a similar structure by looking at the gaps based on the knowledge areas but it also defines the main requirements specific to each vertical sector, analyses how they are covered and what the gaps that have been identified are.

Figure 1 shows the AIOTI High Level Target Architecture for IoT (AIOTI HLA).

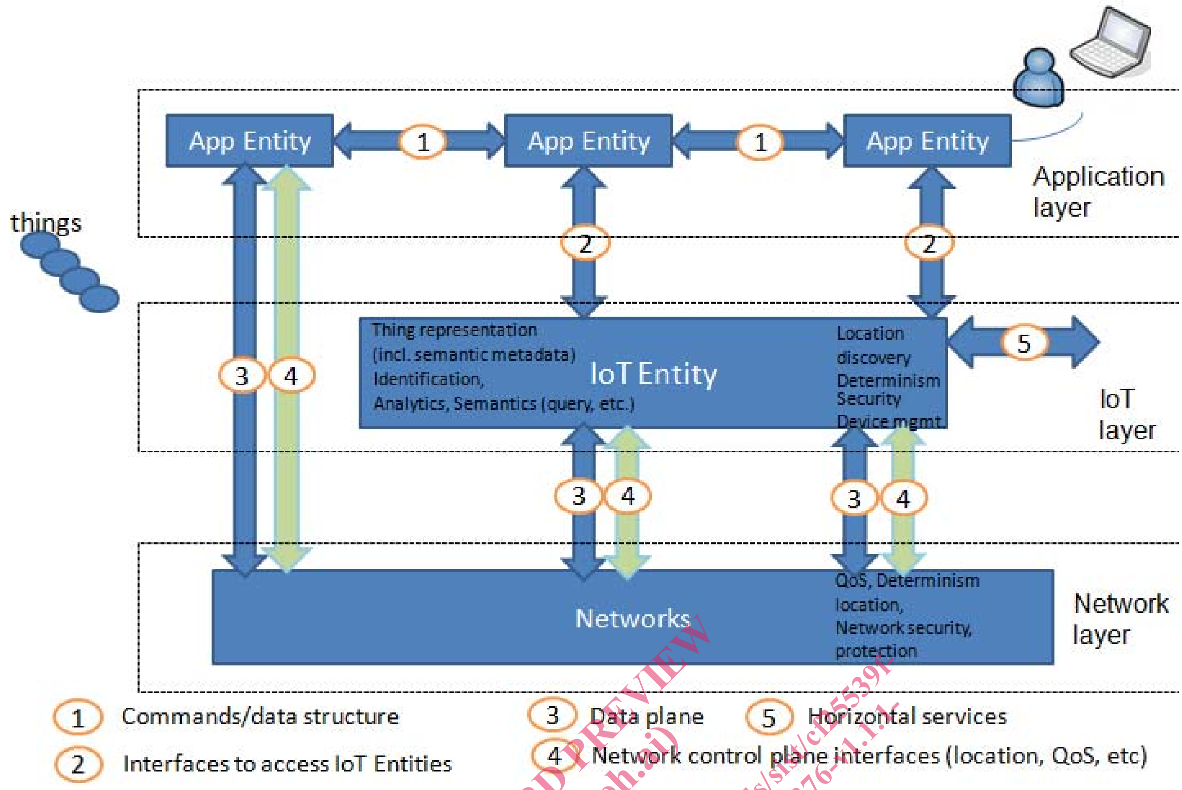

Figure 1: AIOTI high level architecture for IoT (from [i.3])

Interfaces above are:

1: Defines the structure of the data exchanged between App Entities (the connectivity for exchanged data on this interface is provided by the underlying Networks). Typical examples of the data exchanged across this interface are: authentication and authorization, commands, measurements, etc.

2: This interface enables access to services exposed by an IoT Entity to e.g. register/subscribe for notifications, expose/consume data, etc.

3: Enables the sending/receiving of data across the Networks to other entities.

4: Enables the requesting of network control plane services such as: device triggering (similar to "wake on LAN" in IEEE 802.1X [i.13]), location (including subscriptions) of a device, QoS bearers, deterministic delivery for a flow, etc.

5: Enables the exposing/requesting services to/from other IoT Entities. Examples of the usage of this interface are to allow a gateway to upload data to a cloud server, retrieve software image of a gateway or a device, etc.

4.2 Vertical domains covered

As a support for the IoT Large Scale Pilot, the vertical domains that are addressed in the present document are those where such LSP will be defined and, for some, selected and undertaken. These domains are the following:

- Smart Cities. The modern cities need to evolve and become structured, interconnected ecosystems where all components (energy, mobility, buildings, water management, lighting, waste management, environment, etc.) are working together in support of humans. By using the IoT technology, the cities are expected to achieve this transition while maintaining security and privacy, reducing negative environmental impact and doing it in a reliable, future proof and scalable manner.