8

IoT Standards – State-of-the-Art Analysis

Emmanuel Darmois[1], Omar Elloumi[2], Patrick Guillemin[3] and Philippe Moretto[4]

[1]CommLedge, France
[2]Nokia, France
[3]ETSI, France
[4]UNIFY-IoT, ESPRESSO smart cities and Sat4m2m, Germany

8.1 Introduction

The Internet of Things (IoT), as an emerging technology, has the potential to boost innovation in many industrial sectors, as well as to help address many societal challenges including climate change, resource and energy efficiency and ageing.

However, this potential will only materialize if IoT develops as an open platform cutting through the silos, supporting a variety of applications and generating open and sustainable ecosystems. As for any new technology as it begins to emerge, there are many proprietary or semi-closed solutions together a number of existing – and somehow competing – standards, thus re-enforcing the perception that the IoT landscape is fragmented, in particular for standards.

The objective of this chapter is to present the main initiatives that contribute to the analysis of the current status and dynamics of the IoT standardization and to outline their early findings.

The main contributors of this analysis of the IoT standards landscape are the AIOTI WG03, the ETSI Specialist Task Force (STF) 505 and the UNIFY-IoT Coordination and Support Action (CSA).

8.2 Analysing the IoT Standards Landscape

This section introduces three initiatives that target the analysis and understanding of the IoT standards landscape. They are briefly described below and their respective contributions – reference models, identification of Standards Developing Organizations (SDOs), collection of existing standards, and identification of gaps – are further referred to in the rest of the chapter.

8.2.1 AIOTI WG03

Within the Alliance for IoT Innovation (AIOTI, www.aioti.eu), AIOTI WG03 (IoT standardization) is a focus point of European engagement and steering in the standardization process. In collaboration with other AIOTI Working Groups and STFs, WG03 is:

- Maintaining a view on the landscape of IoT standards-relevant activities being driven by SDOs, Consortia, Alliances and OSS projects.
- Providing a forum for analysis, discussion and alignment of strategic, cross-domain, technical themes and shared concerns across landscape activities.
- Developing recommendations and guidelines addressing those concerns.

AIOTI WG03 is engaging the IoT community in disseminating and promoting its results and steering emerging standards. In particular, WG03 is expected to play an important role in conjunction with:

- The upcoming IoT Large Scale Pilots (LSP) (http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/2223-iot-01-2016.html) and the IoT LSP large CSAs.
- Other initiatives and cross alliances that have been prepared and will be launched after the AIOTI General Assembly's approval on 30 May 2016.

AIOTI WG03 has undertaken parallel tasks on 1) IoT Landscaping; 2) IoT High-Level Architecture; 3) IoT Semantic Interoperability; 4) IoT Privacy. A first version of the results of this work has been published in November 2015 together with the other AIOTI WGs reports (http://bit.ly/1GtzJ5I). An updated version of the AIOTI WG03 IoT landscaping report (version 2.6) has been published at the end of May 2016.

8.2.2 ETSI STF 505

STF505 (https://portal.etsi.org/stf.aspx?tbid=595) is a group of experts, funded by the European Commission under the rolling plan on ICT standardization in collaboration with the European Multi-Stakeholder Platform (MSP) and supported by ETSI, commissioned to provide on the one hand an in-depth analysis of the IoT standardization landscape (in particular

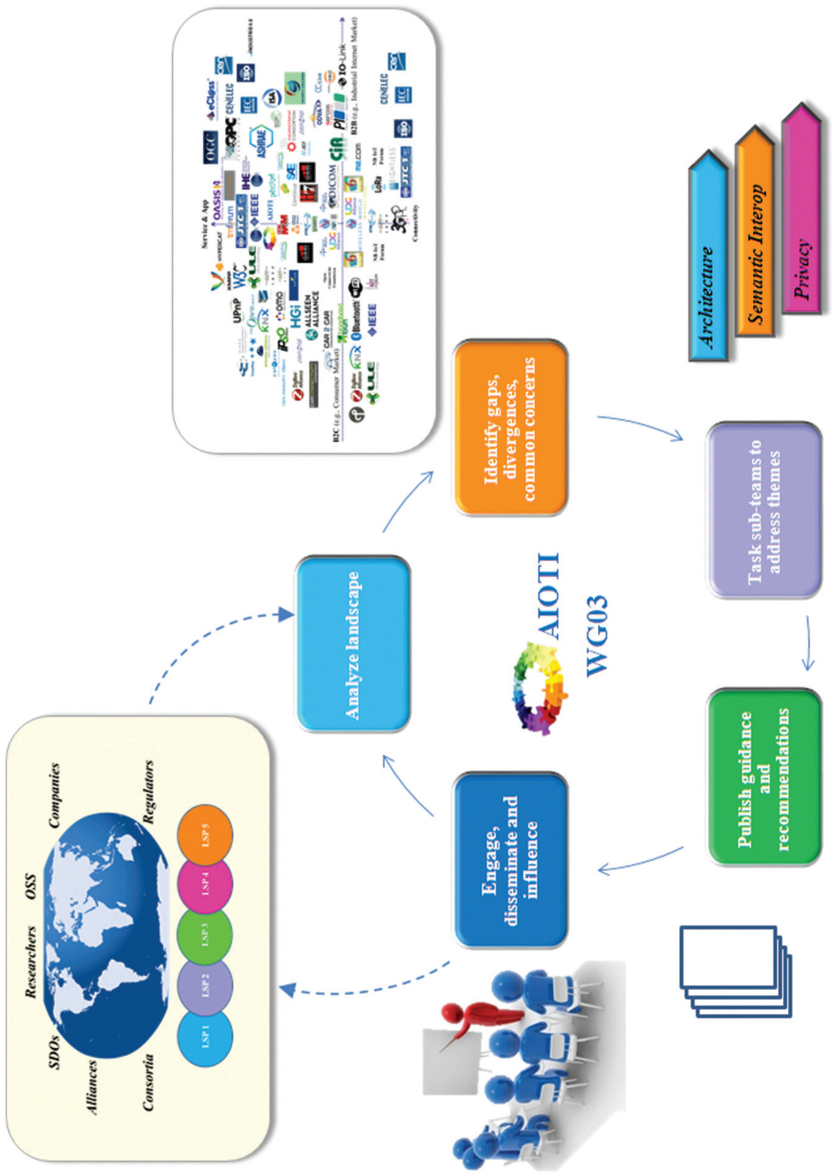


Figure 8.1 AIOTI WG03 and the IoT community.

in conjunction with the AIOTI), and on the other hand, an identification of the IoT standardization gaps.

The study considers "vertical" functionalities (standards and protocols) in specific application domains, i.e., a single vertical industry, such as home automation, smart mobility and wearable medical devices, etc. and "horizontal" functionalities that are not specific to any particular domain but aim to provide common standards, protocols and solutions applicable to as many vertical industries as possible.

The essential objectives are:

- To analyse the status of current IoT standardization.
- To leverage liaisons between SDOs, SSOs, and industrial alliances, which allows:
    - To assess the industry and vertical market fragmentation vis-à-vis standardization
    - To point towards actions that can increase the effectiveness of IoT standardization, to improve interoperability, and to allow for the building of IoT ecosystems.
- To foster dissemination work for the sustainable development of a global community of stakeholders involved in the standardization of IoT.

This STF is developing a set of deliverables that will include recommendations aimed at supporting material for the IoT Large-Scale Pilots (LSPs), in particular:

1. A technical report (TR) on standards landscape for IoT (who does what, what are the next milestones) and identification of potential frameworks for interoperability (e.g. oneM2M). The methodology for drafting the TR on "IoT standards landscaping" is to collect and analyse SDOs and industry standards, to evaluate their stability and maturity, to analyse complementarities/antagonism with open source development, and to provide recommendations.
2. A technical report on identification of gaps and proposals on how to address them in standardization. The methodology for drafting the TR on "IoT European LSP gap analysis" is to systematically analyse the SDOs standards and roadmaps with the support of a survey, to map the LSPs use cases and lifecycle on the related standards, and to identify gaps in standard support;
3. A thematic workshop on Smart Home covering different LSP application domains such as Smart Living, eHealth, Wearables and Smart Cities;

4. An extended delivery workshop centred on the presentation of the STF results and their application by the winning LSP proposals.

8.2.3 UNIFY-IoT CSA

The objectives of UNIFY-IoT (www.unify-iot.eu) are to stimulate the collaboration between IoT projects, between the potential IoT platforms (http://iot-epi.eu/) and to support them in sustaining the IoT ecosystems developed by focusing on complementary actions. The overall goal is to foster and stimulate acceptance of IoT technology as well as the means to understand and overcome obstacles for deployment and value creation.

The UNIFY-IoT CSA is aiming to be a "working partner" of AIOTI and the IoT European Research Cluster (IERC) by coordinating and supporting the activities on innovation ecosystems, IoT standardization, policy issues, research and innovation, and goes beyond the classical workshops and conferences.

The cooperation framework consists of six dedicated Tasks Forces: Innovation, Platforms interoperability, IoT accelerators, IoT business models, Educational platforms and International cooperation.

UNIFY-IoT will also establish links with the selected H2020 IoT-01-2016 LSPs and IoT-02-2016 CSAs when they will start to operate at the beginning of 2017.

8.3 A Framework to Analyse IoT Standardization

In order to ensure a sound and safe methodology to capture the standards landscape and to identify the standardization gaps, some elements have been used as a framework for the analysis of the IoT landscape and are described in this section. Some of them come from the AIOTI WG03 work or from the STF 505 work and some are a refinement of the AIOTI WG03 work made by the STF 505.

8.3.1 Horizontal and Vertical Domains

The AIOTI WG03 has defined a way to graphically represent the "IoT SDOs and Alliances landscape (vertical and horizontal domains)" by highlighting the main activity of SDOs and Alliances with respect to two dimensions:

- The IoT application domains represented as "verticals"
- The IoT telecommunication infrastructure domain represented as "horizontal/telecommunication".

8.3.1.1 Vertical Domains

The vertical domains are those that are addressed by the IoT LSPs as described below:

- ***Smart cities***. The modern cities need to evolve and become structured and interconnected places where all components (energy, mobility, buildings, water management, lighting, waste management, environment, etc.) are working together for the benefit of humans. By using IoT technologies, 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.
- ***Smart living environments for ageing well*** (e.g. smart home). It is expected that the IoT will support the continuously growing population of elderly people in living longer, staying active, non-dependent and out of institutional care settings, together with reducing the costs for care systems and providing a better quality of life. This should be achieved in particular with IoT for smart home and home automation supporting technologies.
- ***Smart farming and food security***. The application of IoT technologies to the overall farming value chain will enable to produce more with less resources and negative environmental impacts and will improve at the same time food safety. Technologies such as data gathering, processing and analytics as well as orchestrated automation technologies supported by IoT are expected to achieve this.
- ***Wearables***. The integration of intelligent systems to bring new functionalities into clothes, fabrics, patches, aids, watches and other body-mounted devices will provide new opportunities and applications. Basic technologies such as nano-electronics, organic electronics, sensing, actuating, localization, communication, etc. will be offered to the end-user, with an associated range of problems such as acceptability, ease of use, privacy, security or dependability.
- ***Smart mobility (smart transport systems/smart vehicles/connected cars)***. The IoT applied to the mobility domain may create the potential for major innovations across a wide variety of market sectors, with mobility applications such as self-driving and connected vehicles, multi-modal transport systems and "intelligent" transportation infrastructure from roads or sea ports to parking garages.
- ***Smart environment (smart water management)***. IoT will be a key building block to solutions for vertical applications such as environmental monitoring and control that will use sensors to assist in environmental

protection by monitoring air, water quality, atmospheric or soil conditions and noise pollution.

- ***Smart manufacturing***. In support of the European manufacturing industry and of the Factories of the Future, all forms of competitive industries will have to massively incorporate more intelligence, that will rely in particular on IoT through advanced connected objects providing sensing, measurement, control, power management and communication, both wired and wireless.

The vertical domains are further used for the classification of the identified standards and standardization gaps.

Note: After the final definition of STF 505, AIOTI has included two new Working Groups on "Smart Buildings and Architecture" and "Smart Energy" that should be included in the future extensions of the scope of the IoT Gap Analysis.

8.3.1.2 IoT SDOs and Alliance Landscape

The "IoT SDOs and Alliances landscape (vertical and horizontal domains)" representation generated by the AIOTI WG03 is illustrated in Figure 8.2 below, in its release 2.6.

This representation captures the SDOs and Alliances that are active in the horizontal and vertical domains.

It should be noted that this representation includes not only SDOs (that develop standards for the IoT) but also alliances that very often serve different purposes such as marketing, promotion, solution profiling, etc.

8.3.2 Knowledge Areas

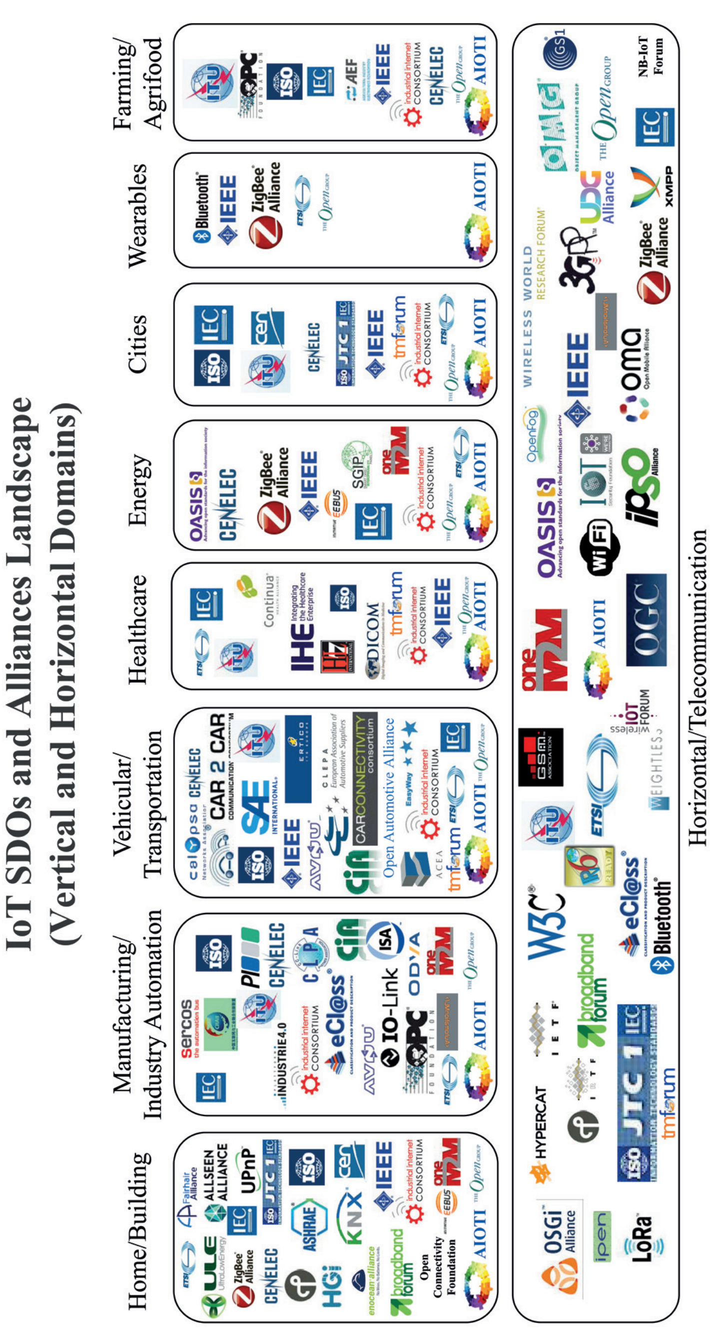
The AIOTI WG03 has defined Knowledge Areas (KAs) that are further used for the classification of Standards in the subsequent sections of this chapter. The definition of the AIOTI WG03 KAs is reminded below (with minor adaptations made by the STF 505):

Communication and Connectivity

This KA covers mainly specification of communication protocols at all layers, e.g., PHY, MAC, NWK, Transport, Service, and Application layers. It includes the management associated with the KA.

Integration/Interoperability

This KA covers mainly specification of common IoT features required to provide integration (assembly of sub-systems) and interoperability (interoperation of heterogeneous sub-systems).



Source: AIOTI WG3 (IoT Standardisation) – Release 2.6

Figure 8.2 IoT SDOs and alliance landscape by domains.

Applications

This KA covers the support of the applications lifecycle. This includes development tools, application models, deployment, monitoring and management of the applications.

Note: The application level protocols, APIs, data models, ontologies, etc. are part of the "Communication and Connectivity" KA.

Infrastructure

This KA covers the design, deployment, and management of computational platforms and infrastructures (e.g. network elements, servers, etc.) that support IoT-based usage scenarios.

IoT Architecture

It covers the specification of complete IoT systems, with a focus on architecture descriptions.

Devices and sensor technology

This KA covers mainly device and sensor lifecycle management.

Note: The communication protocols between devices and other elements are covered in the "Communication/Connectivity" KA.

Security and Privacy

This KA covers all security and privacy topics.

8.3.3 High Level Architecture (HLA)

8.3.3.1 The AIOTI HLA

The AIOTI WG03 has developed the AIOTI High Level Architecture for IoT (AIOTI HLA), a standard framework or architecture for IoT that should be applicable to IoT LSPs. The HLA is meant to be the basis for further discussion with the LSP WGs in order to promote architectural convergence among the WGs.

The AIOTI HLA is similar or can be mapped to other frameworks such as those developed by ITU-T, oneM2M or IIC. An example of such a mapping is provided in the next sub-section.

The purpose of AIOTI HLA (and of the other frameworks) is in particular to support interoperability in complex IoT systems and to provide means of identifying and defining interworking standards with reduced complexity. This framework also supports the characterization of standards gaps and is used by the STF 505 to this extent. A functional model of the AIOTI HLA is depicted in the Figure 8.3 below.

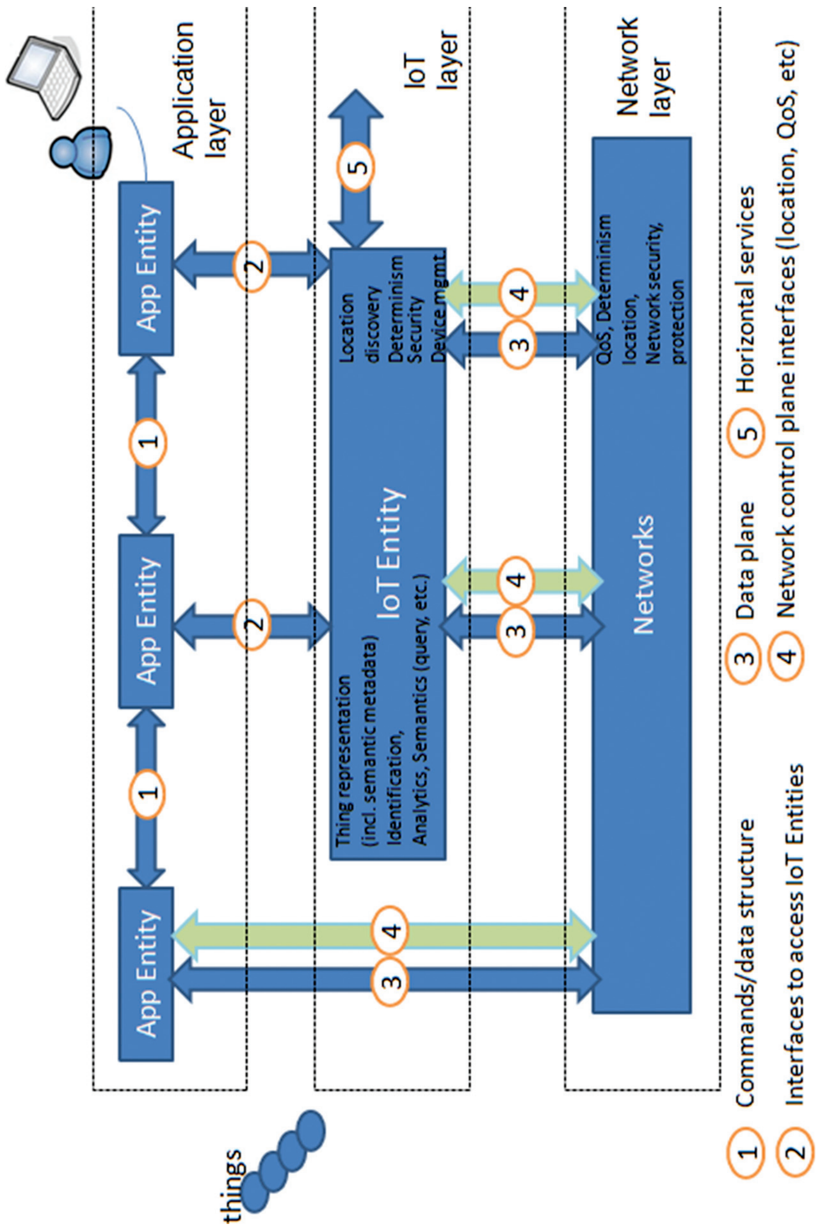


Figure 8.3 Functional model of AIOTI HLA.

The role of the interfaces is to:

- 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.
- Enables access to services exposed by an IoT entity to e.g. register/subscribe for notifications, expose/consume data, etc.
- Enables the sending/receiving of data across the networks to other entities.
- Enables the requesting of network control plane services such as: device triggering (similar to "wake on LAN" in IEEE 802), location (including subscriptions) of a device, QoS bearers, deterministic delivery for a flow, etc.
- 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.

8.3.3.2 Mapping of the HLA: The Example of oneM2M

This fragmented nature of the M2M and IoT market has led to the creation of oneM2M, an alliance of standards organisations looking to develop a single horizontal platform for the exchange and sharing of data among all applications.

oneM2M is creating a distributed software layer, like an operating system, which is facilitating that unification by providing a framework for interworking with different technologies, e.g. OMA LWM2M, OCF (previously OIC) and AllSeen (providing standards for proximity networks). oneM2M enables interoperability across IoT applications regardless of the underlying technology used.

oneM2M defines a Common Services Layer which is a software layer that sits between the network and applications, be it in the wide area network domain or in the filed domain (where devices and gateways are generally deployed). The functions in the Common Services Layer include: device management, data collection, protocol conversion and interworking, group management, security, etc. Those functions are exposed to applications (in the cloud, gateway or devices) via Restful APIs.

The functional oneM2M architecture is depicted in Figure 8.4. The reference points defined by oneM2M are:

- **Mca**: is a Restful API to expose functions in the common service layer to applications running in the devices, gateways or in the cloud.
- **Mcc**: is the reference point that allows, among other features, to register a device or gateway, perform discovery, and exchange IoT data on behalf of the applications. Mcc is also used to perform device management that allows managing the lifecycle of the devices. Device management functions include: software and firmware upgrade, configuration management and performance management.
- **Mcn**: is the reference point that allows to access network services, on behalf of IoT applications, such as device triggering (for sleeping devices), network location or request quality of service connections for IoT services that need specific guarantees.

The Figure 8.5 provides a mapping between oneM2M and the AIOTI HLA functional model.

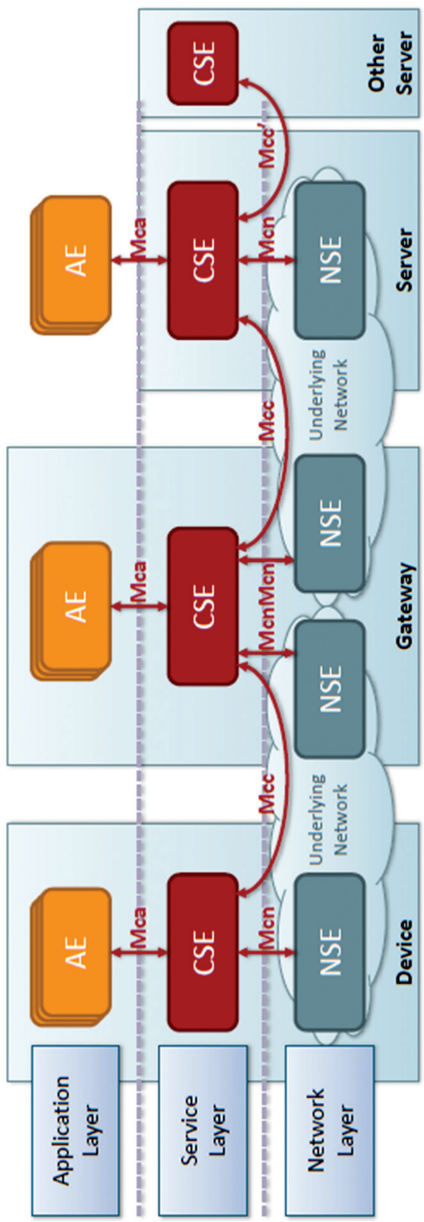
oneM2M has specified all interfaces depicted in Figure 8.4 to a level that allows for interoperability. Three protocols binding have been specified, so far, for Mcc and Mca reference points: CoAP, MQTT and HTTP. As regards the Mcn reference point, normative references have been made to interfaces specified by 3GPP and 3GPP2 in particular.

However, oneM2M does not specify vertical specific data formats for exchange between App Entities according to AIOTI HLA interface 1. This can however be achieved by interworking with other technologies such as ZigBee, AllSeen, etc.

8.3.3.3 The STF 505 Enterprise IoT Framework

The STF 505 has defined an Enterprise IoT Framework in order to put a global structure on the framework used for the analysis of the SDO landscape. Such a framework has to deal not just with the technology, but also with other relevant area to be taken into consideration such as include the stakeholder views, the regulatory aspects (e.g. for a city): all these make up an enterprise view.

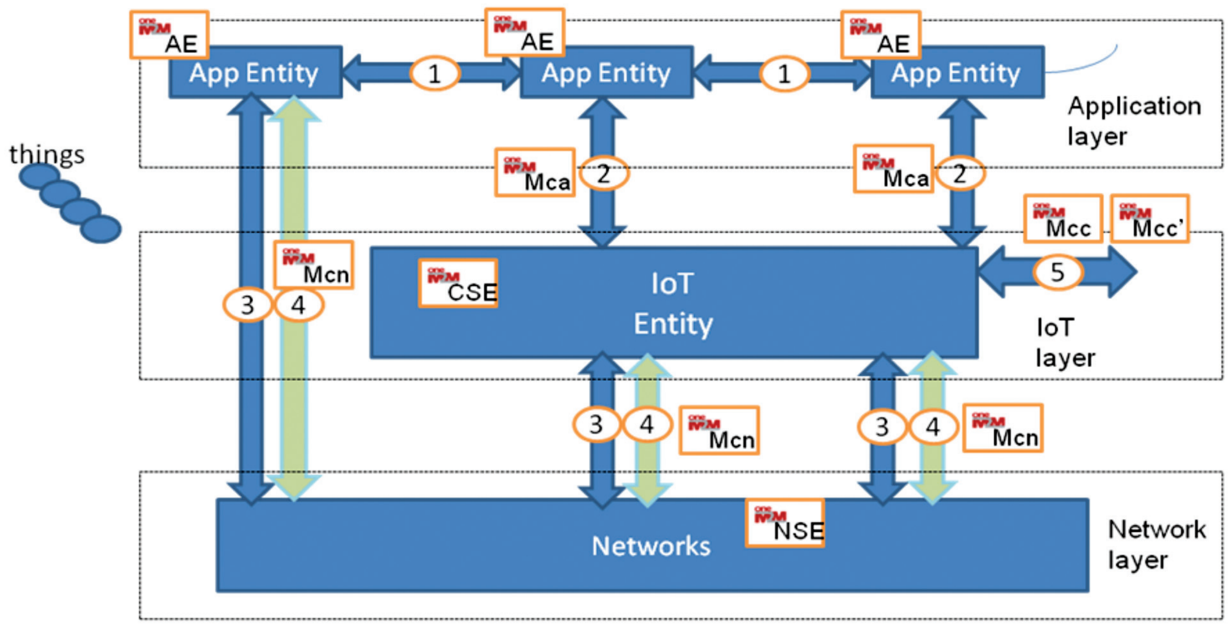
The AIOTI WG03 reports point out that part of the complexity of IoT comes from its intention to support a number of different applications covering a wide array of disciplines that are not all part of the ICT domain: taking an overview of all these elements can be overwhelming without a structural view. The STF 505 approach is to view the IoT framework as an Enterprise Architecture (in line with the TOGAF model for Enterprise Architecture).



Entities AE (Application Entity), CSE (Common Services Entity) and NSE (Network Services Entity)

Reference Point One or more interfaces - Mca, Mcn, Mcc and Mcc'

Figure 8.4 oneM2M functional architecture.



CSE: Common Services Entity - **NSE**: Network Services Entity - **AE**: Application Entity
Mcn: reference point between a CSE and the Network Services Entity (NSE), enable a CSE to use network services such as location and QoS
Mcc/Mcc': reference point between a CSE and a CSE. It allows registration, security, data exchange, subscribe/notify, etc.
Mca: API to Application Entities that expose functions of the CSE.
oneM2M CSE functions include: device management, registration, discovery, group management, data management and repository, etc.

Figure 8.5 Mapping oneM2M to AIOTI HLA.

The main elements of this framework shown in Figure 8.6 are the following:

- An architecture reference model which consists of an IoT architecture integrating all components that make up an IoT system;
- An IoT domain which holds the view of what makes up an IoT system;
- A standards information database which is the main object of study of the IoT standards landscaping, aiming to hold all relevant standards that can be used;
- A reference library which holds any re-useable information that can be used across the IoT LSP pilots;
- A governance repository that houses all policies, regulations that applies to any LSP.

The Standards Information Database

Standards are published documents that establish specifications and procedures designed to ensure the reliability of the materials, products, methods, and/or services people use every day. The Standards Information Base (SIB) collects the standards with which new architectures must comply, which may include industry standards.

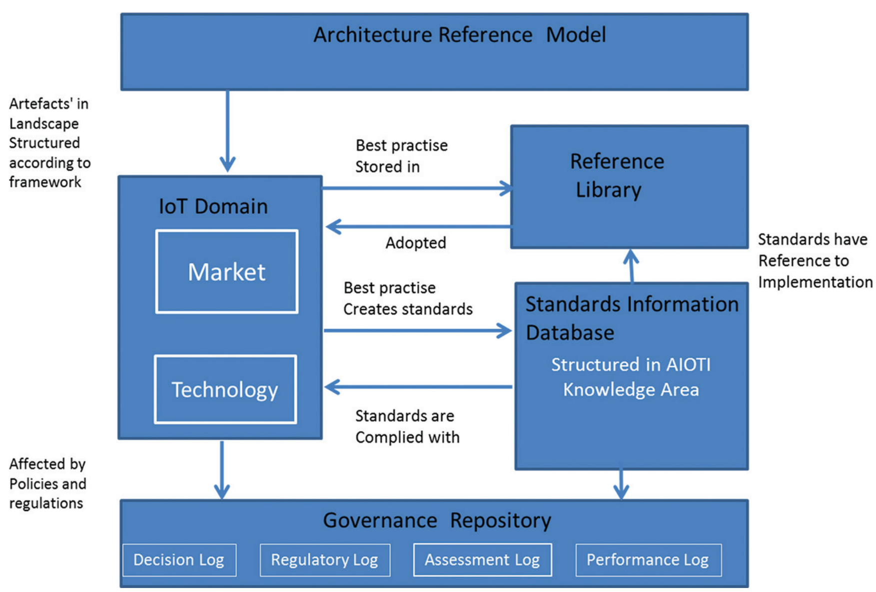


Figure 8.6 The IoT enterprise framework.

AIOTI have come up with a set of standards that are relevant to the LSPs. Some of the standards are common across the LSPs, while some are specific for a LSP. In order to better represent the standards landscape across the various technology areas, AIOTI have come up with the concept of "knowledge area" that has been used a classification scheme for the standards information base.

Standards and Knowledge Areas

Considering the KAs defined above, it may be appropriate to clarify the kind of standards that can be expected in a given KA. Some examples are given below. STF 505 has used this approach for the classification of existing standards.

Communication and Connectivity

Examples of the type of standards that can apply to this KA are:

- Connectivity at physical and link layer
- Network layer
- Service level and application enablers
- Application level API, data models and ontologies
- Management of the protocols

Integration/Interoperability

Examples of the type of standards that can apply to this KA are:

- Profiles
- Certification

Applications

Examples of the type of standards that can apply to this KA are:

- Flexible remote management
- Support methods for installing, starting, updating applications

Infrastructure

Examples of the type of standards that can apply to this KA are:

- Virtualization
- Mobile-edge computing
- Network management
- Network dimensioning, network planning

IoT Architecture

Examples of the type of standards that can apply to this KA are:

- Reference architecture

Devices and Sensor Technology
Examples of the type of standards that can apply to this KA are:

- Device monitoring
- Sensor/actuators virtualization
- Configuration management

Security and Privacy
Examples of the type of standards that can apply to this KA are:

- Communications security and integrity
- Access control
- Authorization, authentication, identity management
- PII (Personally Identifiable Information) management

8.3.4 Status of Standardization in IoT

The IoT has generated the development of standards in order to allow heterogeneous devices to communicate and to leverage common software applications. Interoperability is a great challenge for IoT and standards are the best approach to address it.

Several standardization initiatives currently co-exist, in individual SDOs or in partnerships (e.g. ETSI SmartM2M, ITU-T, ISO, IEC, ISO/IEC JTC 1, oneM2M, W3C, IEEE, OASIS, IETF, etc.) and also in conjunction with a number of industrial initiatives (e.g. AllSeen Alliance, Industrial Internet Consortium (IIC), Open Connectivity Foundation (OCF), Thread protocol, Platform Industrie 4.0, etc.).

In addition to Figure 8.2 where SDO and Alliances were mapped by using two axis representing horizontal and vertical domains, the AIOTI WG03 report on "IoT LSP Standard Framework Concepts" has introduced also two other dimensions: an horizontal axis that represents the market type and a vertical axis that represents the technology that these initiatives cover and focus on. This is displayed in Figure 8.7.

Both of these two figures convey the visual idea of a multiplicity of actors (not to mention the additional multiplicity of standards these actors can produce). It is why the analysis of the IoT standards landscape can give a more precise answer to the question of the proliferation of standards or of the fragmentation of the IoT SDO landscape. This analysis will therefore have several objectives:

- Clarify the issue of SDO landscape fragmentation;
- Identify generic standards that can apply to several vertical domains. These standards can be corresponding to the "horizontal" domain as defined by the AIOTI WG03 but also to cross-domain standards;

Source: AIOTI WG03 (IoT Standardisation) – Release 2.6

Figure 8.7 IoT SDOs and alliances: market and technology.

- Identify standards that are specific to a vertical domain;
- Identify standards gaps.

8.3.5 Overview of IoT Standards Landscape

Regarding IoT landscaping, the work of STF 505 has been focused on the identification and classification of existing standards emanating from SDOs. At the time of this writing, the STF has produced a draft Technical Report than will soon be submitted to public review. In this draft report, two types of standards have been identified:

- "Generic" standards that are common to several vertical domains. A standard is considered as generic when it is used in at least three of the vertical domains;
- "Specific" standards that apply to only one vertical domain.

At this stage, the report (and the standards identified) is under review and cannot be presented globally in this paper. The publication of the final reports of the STF 505 is expected in November 2016, making available the full list of standards that have been analysed.

8.3.5.1 Generic Cross Domain Standards

A number of the standards identified in the IoT landscape are used in several of the analysed vertical domains. Those standards are listed in tables, classified by KAs

- Communication and connectivity
- Integration/interoperability
- Application
- Infrastructure
- IoT architecture
- Device and sensor technology
- Security and privacy

An example of such table with one standard is provided in Table 8.1 where:

- The first column is the short name of the SDO;
- The second column is a short description of the standard;
- The third column provides a description and short analysis of the scope of the standard;

Table 8.1 Example of a generic cross-domain standard

SDO	Standards	Description/Analysis	SC	SL	SF	W	Smo	SE	Sma
Bluetooth	Bluetooth BR/EDR (basic rate/ enhanced data rate) Bluetooth Low Energy (BLE)	Bluetooth is a global wireless communication standard that connects devices. Communication between Bluetooth devices happens over short-range, ad hoc networks known as piconets. The network ranges from two to eight connected devices. When a network is established, one device takes the role of the master while all the other devices act as slaves. Piconets are established dynamically and automatically as Bluetooth devices enter and leave radio proximity. There are different versions of the core specification of Bluetooth. The most common are Bluetooth BR/EDR (basic rate/enhanced data rate) and Bluetooth with low energy functionality. http://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics		X	X	X	X	X	

- The seven rightmost columns correspond to the different vertical domains and the meaning of an "X" in a cell is that the Standard(s) described in the row apply to the vertical in the column:
  - SC: Smart Cities
  - SL: Smart Living
  - SF: Smart Farming
  - W: Wearables
  - Smo: Smart Mobility
  - SE: Smart Environment
  - Sma: Smart Manufacturing

The number of currently identified standards per KA and per each vertical domain are displayed in Table 8.2:

As a conclusion, a large number of standards (a total of 70 standards in the above table) may apply to several IoT vertical domains. This set of generic solutions has the potential to provide a common ground to the developers of IoT solutions, irrespective of the specific domain in which they may be applied.

However, this potential will only materialize if the development of IoT standards in vertical domains is making effective use of those standards rather than reinventing similar but not compliant ones, thus increasing the fragmentation of the IoT standards landscape.

8.3.5.2 Domain Specific Standards

Each of the vertical domains has a number of specific standards listed in tables (sometimes empty, in particular when the "generic" standards fully apply), classified by KAs.

An example of such table with one standard is provided in Table 8.3.

Table 8.2 Current STF 505 identified standards per KA and vertical domains

Knowledge Area	3 Vertic.	4 Vertic.	5 Vertic.	6 Vertic.	7 Vertic.	Total
Communication and Connectivity	4	4	4	5		17
Integration/ interoperability	2	3	3	1		9
Application	1	1	1			3
Infrastructure	1	1	2	3	2	9
IoT Architecture		1	3	1	2	6
Device and Sensor technology	1	1		10	4	16
Security and Privacy	1		1	5	3	10

Table 8.3 Example of domain specific standards per vertical domain

SDO	Standards	Description	Analysis
ASHRAE	ISO 16484-5: BACnet – A Data Communication Protocol for Building Automation and Control Networks ISO 16484-6: Method of Test for Conformance to BACnet	BACnet is a data communication protocol for building automation and control.	BACnet provides a standard way of representing the functions of any device, as long as it has these functions, as collections of related information called "objects," each of which has a set of "properties" that further describe it. One of the object's most important properties is its identifier. As devices have common appearances on the network in terms of their objects and properties, messages can manipulate this information in a standard way. It makes possible the interconnection of different vendors' equipment that uses the BACnet protocol http://www.bacnet.org/Overview/index.html

8.3.6 Identifying IoT Standards Gaps

8.3.6.1 Defining Gaps

The work done by the STF 505 on standards identification (described in the previous section) has shown that a number of standards are available, i.e. have reached a final stage (Technical standard (TS) or TR, etc.) in a SDO by the time of writing the report, and can be used for the work of the IoT LSPs.

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 are missing. These missing elements are referred to as "gaps" in this paper. Gaps may also be identified when harmonization or interoperability between a large numbers of potential solutions is missing.

These "gaps" are the main point of interest of the second STF 505 report. 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.

The identification of gaps has been 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 relies 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 STF 505 work does not have the aim to undertake the resolution of the gaps that is left to the proper organizations of the IoT community.

8.3.6.2 Identify Gaps: A 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 and may have been detected by very different actors of the IoT community, a mechanism is needed 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;
- Clarifying the respondent objectives and main area of work;
- Defining up to three gaps of all three types described above.

The survey has been largely distributed. At the time of writing this paper, over 190 answers have been collected.

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.

8.3.6.3 Example of Gaps

The gaps have been analysed for each of the vertical domains. The sources for the gaps come from both:

- The analysis of the IoT requirements for the vertical domain, based on a variety of sources. These requirements are matched with the list of standards identified in the IoT standards landscaping report and a gaps is identified when no standard seems to match the requirement;
- The analysis of the results of the survey regarding the vertical domain. In this case, the gap has been identified by the respondent and is further analysed.

An example of gaps analysis regarding the Connectivity at Network Layer in the Smart cities domain is shown in Table 8.4.

An example of societal gap identified in the survey in the Smart Cities domain is shown in Table 8.5.

8.3.6.4 Status of Gaps Identification

At this stage, the standard gaps identified are under review and they cannot be presented globally in this paper. The publication of the final reports of the

Table 8.4 Example of gap analysis for connectivity in smart cities

Requirements	Organizations Providing Related Standards
Support of local and remote access to infrastructure services	3GPP, ETSI TETRA, IEEE 802.x, LoRa alliance, ITU, IETF,
Support of point-to-point communications	3GPP, ETSI TETRA, IEEE 802.x, ITU, EnOcean Alliance, DASH7 Alliance,
Support of point-to-multipoint communications	ETSI TETRA, IEEE 802.x, ITU
Support of routing continuity across different network technologies	IETF 6lo
Support of device unique identification	This is a potential gap

Table 8.5 Example of societal gap identified in smart cities by the STF 505 survey

Nature of the Gap	Knowledge Area	Criticality	How Can Standardization or Regulation Improve this?
Privacy and security aspects not sufficiently covered, developed and not real, mature models/solutions seem to be available. This could limit IoT adoption Another social gap is that many decision makers does not have a real understanding of practical potentialities IoT can provide and a dissemination campaign would be useful addressing mainly Public administration.	Communication and Connectivity (network and service levels); Integration/ Interoperability; IoT Architecture; Security and Privacy	3	IoT and big data pose new challenges to an acceptable model of privacy and security management and rules (in terms of civil rights and “industrial privacy/security” guarantees: it is necessary to find out new models/ approaches

STF 505 is expected in November 2016. The full list of the identified standard gaps will then be available.

8.3.7 Conclusions and Further Challenges

The work on IoT standards landscaping and IoT standards gaps analysis is an on-going task that will continue over time. At this stage, the actors involved have established a solid framework and started to collect the results regarding the actual standards and gaps.

The work done by the STF 505 will provide a list of standards and a list of identified gaps. In particular, these gaps will have to be handled, a task that is not in the scope of the STF.

It is expected that it will be the role of AIOTI WG03 and of the IoT LSP and the Coordination and Support Actions (CSA) starting in 2017.

AIOTI WG03 is addressing three key challenges as displayed in Table 8.6 and specific challenges as displayed in Table 8.7 derived from the landscape analysis with collaborations of contributors based on consensus, providing guidance and recommendations on specific technical themes, and around an understanding of how that guidance will be disseminated in an effective way.

This will help to achieve the overall goals as set by the European Commission, and promote the use of open standards that:

- Support the entire value chain,
- Apply within IoT domains and cross-IoT domains.
- Are integrating multiple technologies, based on streamlined international cooperation and which enables easy and fair access to standard essential patents (SEPs).

Table 8.6 Key challenges AIOTI WG03

1	*Architecture*	Guidelines and recommendations, which contribute to the consolidation of architectural frameworks, reference architectures, and architectural styles in the IoT space.
2	*Semantic Interoperability*	Guidelines and recommendations, which contribute to the consolidation of semantic interoperability approaches in the IoT space.
3	*Privacy*	Guidelines and recommendations regarding personal data and personal data protection to the various categories of stakeholders in the IoT space.

Table 8.7 Challenges for AIOTI WG03

	Timeframe	
Specific Challenges	Before 2020	2020 and Beyond
Recommendations of reference architectures, both for experimentation and deployments within IoT domains and cross – IoT domains	X	
Identification of missing (semantic) interoperability standards and technologies within IoT domains and cross – IoT domains and recommendations on solving them	X	
Recommendations and guidelines on solving protocol and interface gaps needed to support new IoT features within IoT domains and cross – IoT domains. In particular, promote the uptake of IoT standards in public procurement to avoid lock-in	X	X
Promoting the use and development of Open Reference Vocabularies and Open Application Programming Interfaces to allow for flexible ad-hoc communication and interaction between different actors within IoT domains and cross – IoT domains	X	X
Provide guidelines on how to translate the Digital Rights Management recommendations within IoT domains and cross – IoT domains	X	
Recommendation of an interoperable IoT numbering space that transcends geographical limits, and an open system for object identification and authentication, which can be applied within IoT domains and cross – IoT domains	X	

Acknowledgments

The content of this chapter is largely relying on the many contributions of the IoT standardization community. The authors would like in particular to thank:

- The reviewers: Georgios Karagiannis, Patrick Wetterwald
- The STF 505 members: Emmanuel Darmois, Joachim Koss, Samir Medjiah, Jumoke Ogunbekun, and Michelle Wetterwald.
- The contributors to the three AIOTI WG03 reports, in particular the report on “IoT LSP Standard Framework Concepts”: Howard Benn, Werner Berns, Angel Boveda, Marco Carugi, Pablo Chacin, John Davies, Thierry Demol, Jean-Pierre Desbenoit, Zeta Dooly, Omar Elloumi, Patrick Guillemin, Georgios Karagiannis, Levent Gurgen, Juergen Heiles, Sharadha Kariyawasam, Jochen Kilian, Guenter Kleindl, Paul

Murdock, Thomas Paral, Nigel Rix, Friedhelm Rodermund, Mohammad-Reza Tazari, Martin Serrano, Carlos Ralli Ucendo, Ovidiu Vermesan, Alexander Vey, Patrick Wetterwald.

Bibliography

[1] AIOTI WG03 Report: "IoT LSP Standard Framework Concepts Release 2.0", November 2015. http://bit.ly/1GtzJ5I
Note: the most recent version (Release 2.6 on 30 May 2016) can be found at https://docbox.etsi.org/SmartM2M/Open/AIOTI/

[2] AIOTI WG03 Report: "High Level Architecture (HLA) Release 2.0" November 2015. http://bit.ly/1GtzJ5I
Note: the most recent version (Release 2.1 on 30 May 2016) at https://docbox.etsi.org/SmartM2M/ Open/AIOTI/

[3] AIOTI WG03 Report: "Semantic Interoperability Release 2.0" November 2015. http://bit.ly/1GtzJ5I

[4] STF 505 Draft TR 103 375 "SmartM2M IoT Standards landscape and future evolution", June 2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

[5] STF 505 Draft TR 103 376 "SmartM2M; IoT LSP use cases and standards gaps", June 2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505