CREATE-IoT

**H2020 Work Programme 2016-2017**

**H202-IoT-02-2016**

Duration: 36 months

European Large-Scale Pilots Programme

## CROSS FERTILISATION THROUGH ALIGNMENT, SYNCHRONISATION AND EXCHANGES FOR IoT

# H2020 – CREATE-IoT Project

# Deliverable 06.07

# Strategy and coordination plan for IoT interoperability and pre-normative and standardisation activities

**Revision:** 1.00

**Due date:** 31-07-2018 (m19)

**Actual submission date:** 30-09-2018

**Lead partner:** ETSI


| Dissemination level | | |
|---|---|---|
| PU | Public | **X** |
| PP | Restricted to other programme participants (including the Commission Services) | |
| RE | Restricted to a group specified by the consortium (including the Commission Services) | |
| CO | Confidential, only for members of the consortium (including the Commission Services) | |

| **Summary** | | | | | |
|---|---|---|---|---|---|
| **No and name** | **D06.07 Strategy and coordination plan for IoT interoperability and pre-normative and standardisation activities.** | | | | |
| **Status** | <Released> | **Due** | m19 | **Date** | 31-07-2017 |
| **Author(s)** | O. Vermesan (SINTEF), R. Bahr (SINTEF), E. Darmois (ETSI), D. Raggett (ERCIM), M. Serrano (NUIG), A. Kung (TL), M. Menon (MI) | | | | |
| **Editor** | E. Darmois (ETSI) | | | | |
| **DoW** | Updated merged document from D06.01 and D06.04 on strategy and coordination for defining IoT interoperability and pre-normative and standardisation activities based on assessment of IoT-EPI and IoT LSPs approaches. | | | | |
| **Comments** | | | | | |

| **Document history** | | | |
|---|---|---|---|
| **Rev.** | **Date** | **Author** | **Description** |
| 0.01 | 15-05-2018 | ETSI | Initial merge of deliverables D06.01 and D06.02. |
| 0.02 | 13-07-2018 | ETSI | First actual merge of deliverables D06.01 and D06.02. |
| 0.03 | 23-07-2018 | ETSI, SINTEF | Integration of some comments |
| 0.04 | 28-07-2018 | SINTEF | Update content |
| 0.05 | 22-09-2018 | SINTEF | Update content |
| 0.06 | 24-09-2018 | ETSI | Some corrections |
| 0.07 | 26-09-2018 | ETSI | Review. |
| 0.08 | 26-09-2018 | SINTEF | Review comments considered. |
| 1.00 | 30-09-2018 | SINTEF | Final version released. |

# Table of contents

# List of Figures



# List of Tables

# 1 EXECUTIVE SUMMARY

## 1.1 Publishable summary

The Internet of Things (IoT) seeks to enable services based upon sensors and actuators that are connected to the Internet. Unlocking the benefits of IoT across many potential application areas, reducing the costs and risks, and providing the confidence needed for sustainable growth of the IoT ecosystem will require that interoperable platforms, standards and technologies be available to the IoT systems designers and developers.

The primary purpose of this document is to outline the basic requirements for a common interoperability and standardisation strategy to be adopted by the IoT Large-Scale Pilots (LSPs). The goal of such a strategy is to ensure that there is an agreement - as large as possible - within the IoT LSPs (and the associated CSAs) about, in particular, the requirements on interoperability, the available and emerging standards, the standards "gaps" and how they should be addressed.

In support of an interoperability and standardisation strategy, the initial elements of a technical framework are described. A first component to this framework is regarding interoperability and how it can be supported by reference architectures, open platforms, etc. Another essential part is regarding the state-of-the-art in standardisation, an overview of the standards currently available and the key role played the "common standards across vertical domains" (aka "horizontal" standards).

In support of the collection of the requirements of both the vertical domains and the LSPs, a survey has been developed in order to collect: i) the requirements of the "vertical domains", i.e. the domains in which the LSPs will principally operate (e.g. Smart Aging, etc.); and ii) the view of the LSP on their approach to standardisation. This initial snapshot on the state-of-the-art of IoT domains and the progress of the LSP provides early views useful for the future set-up of a standardisation strategy and will be further updated and enriched.

Beyond the support of over 300 standards applicable to IoT systems development (amongst which over 40% are "horizontal"), IoT systems designers also have to deal with missing solutions or competing (i.e. non-interoperable) standards. Such "gaps" and "overlaps" - e.g., in standards – are a challenge to the IoT community, in particular the LSPs: the most important ones need to be clearly identified and a strategy for their resolution needs to be defined. In this resolution, Standards Development Organizations are essential, and an overview of their most promising standards is provided as an illustration. As a complement to this work, pre-normative activities gather ideas for use cases, analyse the resulting requirements, and look at how these can be met with existing standards, and where new standards may be needed for the IoT LSPs.

Beyond the initial basis developed in the current document (which is a consolidated merge of deliverables D06.01 "Strategy and coordination plan for IoT interoperability and standard approaches" and D06.04 "Recommendations for commonalities and interoperability profiles of IoT platforms"), complete and operational documents will be developed by CREATE-IoT and the LSP representatives in the IoT LSP Activity Group 2 ("IoT standardisation, architecture and interoperability"), in particular via a number of Workshop addressing the above topics in details.

## 1.2 Non-publishable information

None, the document is classified as public.

# 2 INTRODUCTION

## 2.1 How to use this document

### 2.1.1 Scope and purpose

The primary purpose of this document is to outline the basic requirements for a common interoperability and standardisation strategy to be adopted by the IoT Large-Scale Pilots (LSPs). The goal of such a strategy is to ensure that there is an agreement - as large as possible - within the IoT LSPs (and the associated CSAs) about, in particular, the requirements on interoperability, the available and emerging standards, the standards "gaps" and how they should be addressed.

It is expected that this document, the first in a series of other ones, will be a basic, initial reference in defining and understanding the main issues regarding IoT interoperability and standards. It will be further completed by additional deliverables in the course of development (and maturation) of the IoT LSPs.

Amongst the questions addressed are the following:

- How technical choices regarding interoperability can be made in order to ensure effective implementations within each LSP as well as across LSPs (when necessary). The choices should regard not only interoperability at the communication layer but higher in the IoT system "stack" (e.g. information, business layers) bearing in mind that a unified interface for IoT application development will be a key factor for market adoption of the technology;
- How current standards in the IoT space can be selected and used within LSPs in order to maximise the commonality within a single LSP domain (e.g. smart aging) and across LSPs. It is expected that when common standards are used one or several layers of IoT systems, this will have an immediate benefit in terms of interoperability;
- How missing or overlapping elements in IoT Standardisation – the standardisation "gaps" and "overlaps" – can be addressed by the LSPs in a coordinated manner in order to ensure that common solutions to resolve these gaps can be developed by one or several LSPs, and the promotion of these solutions can be done within the IoT standardisation community with maximum effectiveness;
- How pre-normative activities can be integrated as quickly and efficiently as possible. Pre-normative activities gather ideas for use cases, analyse the resulting requirements, and look at how these can be met with existing standards, and where new standards may be needed for the IoT LSPs.

The definition of a standardisation strategy requires that all concerned stakeholders (e.g., the LSP participants involved in the standardisation activities) have fully defined their requirements, understood the technical ground on which they want to build their implementations, and what are the missing elements that they would like to see coming from the IoT community. The standardisation strategy will not appear overnight and will require that all LSPs have been undertaking this initial work.

This document is, as outlined above, providing a basic set of elements (e.g. concepts, definitions, perceived requirements, existing standards, identified gaps, etc.) to ensure that the future interoperability and standardisation strategy will be built by the stakeholders based on the same bricks.

Beyond the initial basis developed in the current document, more complete and operational documents will be developed by CREATE-IoT and the LSP representatives associated in the IoT LSP Activity Group 2 "IoT standardisation, architecture and interoperability". A summary of the progress of this work will be provided in deliverables D06.02 ("Recommendations for commonalities and interoperability profiles of IoT platforms") and D06.05 ("Initial report on IoT standardisation activities").

### 2.1.2 Target group for this document

The target group for this document is the community of people that have to address the definition of the LSPs from inception to implementation, in particular regarding the main technical choices that have to be made in order to ensure that the implementations will be effective, interoperable and scalable:

- The identification and description of the Use Cases selected by the LSPs;
- The selection of the reference architecture for the description of the interoperability layers and the main building blocks for the implementation of the Use Cases;
- The identification of the main elements of the framework that will be used for the implementation of the selected Use Cases (e.g., development methodology, development environments,
- The selection of the main standards on which the LSP implementation will be based;
- The identification of the standards gaps for which solutions will have to be found, in particular by the cooperation with other LSPs in the context of the IoT standardisation community;
- And more generally with all parties involved in the identification and resolution of technical issues encountered in the course of the LSP implementation.

## 2.2 Contributions of partners

This current deliverable is a consolidated merge of deliverables D06.01 "Strategy and coordination plan for IoT interoperability and standard approaches" and D06.04 "Recommendations for commonalities and interoperability profiles of IoT platforms" which have been developed within CREATE-IoT Work Package 06, in Task 06.01 ("IoT Interoperability, standards approaches, validation and gap analysis") and Task 06.02 ("Pre-normative and standardisation activities").

The list below shows the specific contribution of partners to the current deliverable D06.06. The contribution of partners to deliverables D06.01 and D06.04 can be found in the corresponding documents.

**ETSI:** As Work Package Leader, Task Leader (Task 06.01) and editor of the deliverable ETSI has contributed to all the sections of this document.

**ERCIM:** As Task Leader (Task 06.02) ERCIM has contributed to the definition of the overall content and scope of the deliverable and to the review of the deliverable.

**SINTEF:** SINTEF has contributed to the definition of the overall content and scope of the deliverable and to the review of the deliverable.

## 2.3 Relations to other activities in the project

The interoperability and standardisation strategy outlined in the current document is related – at least for the interoperability part – to the work of CREATE-IoT Work Package 2 ("IoT Large-Scale Pilots Ecosystems Arena for Sharing Common Approaches "), in particular when it comes to open APIs or common methodologies (addressed in Deliverable D02.02).

This deliverable is addressing some of the issues in the scope of Work Package 5 ("IoT Policy Framework - Trusted, Safe and Legal Environment for IoT"). The interoperability and standardisation strategy will be aligned to the needs of Task 05.01 ("Policy framework and trusted IoT environment ") and Task 05.02 ("Data in the context of IoT applications ").

# 3 AN INTEROPERABILITY FRAMEWORK FOR IOT

## 3.1 Background

In its Communication regarding the "ICT Standardisation Priorities for the Digital Single Market" [2], the European Commission outlines the essential role of standards in general and in IoT as well.

Regarding the role of standards, a key emphasis is put on interoperability in general:
***Common standards ensure the interoperability of digital technologies and are the foundation of an effective Digital Single Market.*** *They guarantee that technologies work smoothly and reliably together, provide economies of scale, foster research and innovation and keep markets open. Effective interoperability guarantees that connected devices such as cars, phones, appliances and industrial equipment can communicate seamlessly with each other, regardless of manufacturer, operating system, or other technical components. Open standards ensure such interoperability, and foster innovation and low market entry barriers in the Digital Single Market, including for access to media, cultural and educational content. Differing national standards may significantly slow down innovation and put European businesses at a disadvantage vis-à-vis the rest of the world.* (Outlined by the authors)

Some implications regarding the status and the role of the Standardisation are also drawn, that will be largely addressed in the current document, in particular:

- The increased complexity resulting from the proliferation of standards, that will require standards maps, reference architectures, etc. to clarify the choices;
- The role of standards organisations in ensuring access rights to standards as well as globally applicable solutions.

IoT is clearly outlined as a key domain:
*The EC has identified 5 priority areas:* ***5G communications, cloud computing, the internet of things (IoT), (big) data technologies and cybersecurity****. These are the essential technology building blocks of the Digital Single Market.*

With key challenges to address:
*However, the IoT landscape is currently fragmented because there are so many proprietary or semi- closed solutions alongside a plethora of existing standards. This can limit innovations that span several application areas. Large-scale implementation and validation of cross-cutting solutions and standards is now the key to interoperability, reliability and security in the EU and globally.*

*The European Union needs an open platform approach that supports multiple application domains and cuts across silos to create competitive IoT ecosystems. This requires open standards that support the entire value chain, integrating multiple technologies, based on streamlined international cooperation that build on an IPR framework enabling easy and fair access to standard essential patents (SEPs*).

And a main way-forward:
*Large-scale implementation and validation of cross-cutting solutions and standards is now the key to interoperability, reliability and security in the EU and globally.*

## 3.2 Requirements for IoT interoperability

The way-forward outlined at the end of section 3.1 is a major challenge for IoT. Because IoT is a large domain, spanning across a variety of sectors (e.g., food, health, industry, transportation, etc.):

- Solutions have been developed in application silos where interoperability is limited by the scope of the specific solutions selected and used;

- Many generic solutions (e.g., standards) potentially apply but they have been developed in different sectors (or "vertical domain" or "vertical" as sectors are termed in the present document) and the risk of duplication and fragmentation exists.

### 3.2.1 General requirements

A key objective for a standardisation strategy is to foster interoperability wherever it is needed within or across IoT systems. Interoperability can be seen through various angles: operational behaviour, information exchange, etc. One possible definition can be found in 10.3 (Appendix C).

Though interoperability is often seen as a means for two systems to exchange information at the network layer, there are much more aspects to interoperability. Figure 1 is one of many attempts to describe several layers for interoperability and what is the essential objective for each layer.

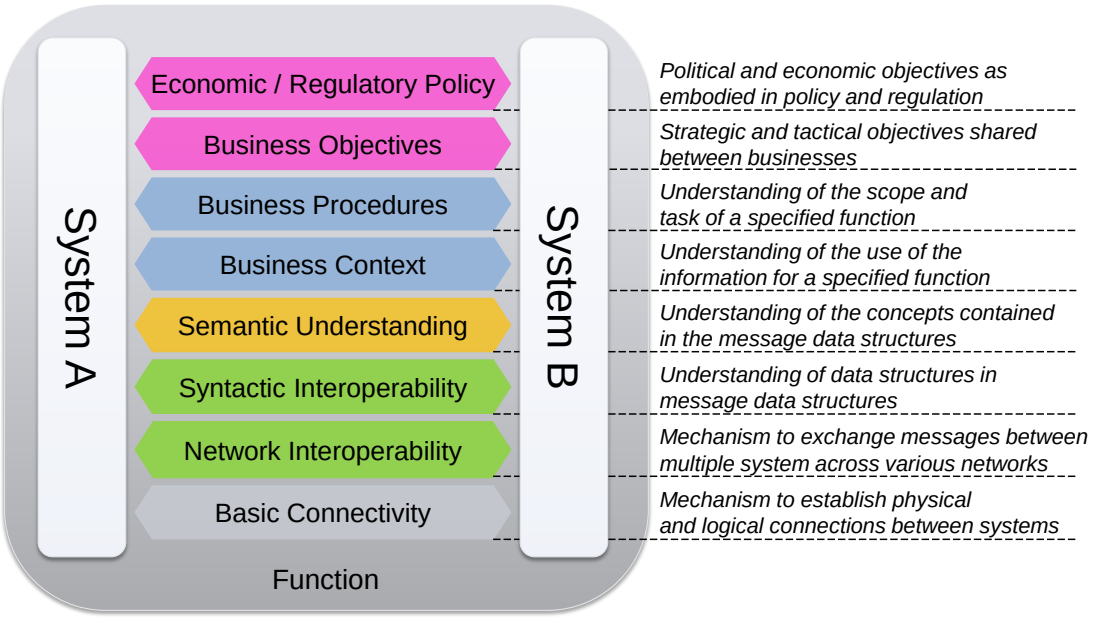


*Figure 1: Interoperability Categories (from the GWAC Stack [3])*

In the context of the present document (in particular the survey presented in section 6.1), the levels of interoperability addressed will not be as detailed as above, but will concern essentially the following layers: business process (encompassing all the business layers), semantic, syntactic and network.

Examples of standards applicable at some of the interoperability layers are:

- Semantic: SAREF and the SSN ontology;
- Syntactic: OCF and oneM2M;
- Network: protocols like CoAP, HTTP and MQTT.

As described in [5], the most important requirements for IoT interoperability are:

- Interoperability between the different IoT systems and testbeds. Previous attempts for IoT frameworks resulted on standalone systems because they were designed for specific applications. This led to a scarcity in the IoT world, since each system had a different framework, architecture and interface. In order to fully exploit the benefits of IoT, we have to break the silos and enable the interoperability between the different systems. This means that the IoT systems must be compatible or interoperable exploiting open interfaces or following the same standards in order to allow easy, flexible, and secure exchange of data between each other.
- Scalable sharing, integration and deployment of distributed resources. There should be an easy, efficient and flexible way for the different IoT systems to share data and information between them in an interoperable manner. To enable cross domain applications there is a need to integrate information from various IoT systems, which most of the time is not homogeneous

and is stored in distributed databases. To address this issue, we have to create mechanisms to allow the secure exchange of information between heterogeneous systems.

- Interoperability applied on services and applications. IoT services or applications are mainly designed and developed according to the specific requirements of each IoT system they are running on and these systems have usually their own interfaces towards the application layer. This results in applications or services that can't exploit data from various IoT systems or applications that can't be ported easily to or even communicate seamlessly with other systems, thus minimizing their efficiency and reusability. To fulfil the main requirement for integration of IoT systems, the IoT applications and services must be interoperable. This means that the IoT systems should share same or similar interfaces with the application layer, so that applications developed for one system can easily get data from other systems, extending the possibility to produce more generic knowledge. Furthermore, availability of a unified interface for IoT application development could greatly accelerate adoption of the technology across all industry segments.

### 3.2.2 Application and domain specific requirements

In many cases, the requirements originate from the needs of a "vertical" domain and the corresponding IoT systems will developed in a "silo" mode (i.e. by adopting solely the solutions, including standards, from the domain itself). But the IoT comes with the possibility to associate in an IoT systems a variety of elements that have been developed in different "verticals" which will require cross domain interoperability.

Two examples of such requirements are:

- In the case of a smart home in the area of Active and Healthy Ageing, there is a prominent need of interoperability due to the fact that it needs to integrate a diverse set of heterogeneous systems in order to provide the maximum level of efficiency for the sake of the patient. For example, an AHA system should combine information from systems such as home automation (for automatically opening doors and windows for disabled people), home environmental monitoring (for monitoring the air quality and the temperature/humidity levels), health monitoring of the patient (i.e. through wearables and other on-body sensors) and communication with the doctor or the hospital for real-time information or emergency notification. These systems are usually silos running separate applications that are incompatible with each other. Thus, to provide a more generic AHA application, there is a need to design a framework to integrate efficiently and effectively the silo systems, ensuring the secure and reliable interoperability between these separate systems.
- In the same example as above, the measurements captured throughout the day don't need to be transmitted if there is not an emergency but need to be stored, preferably to a database easily accessible from the sensors near to the patient. On the other hand, the doctor responsible for the patient should have access to the information of the patient on demand. Thus, there is the need of a service with the ability to have access to the patient's database and to interpret the information to the format asked by the doctor. This shows the need for scalable sharing, integration and deployment of distributed resources.

These requirements will be very often requiring that interoperability is not only handled at Network level, but often more importantly at Syntactic, Semantic and even Business levels.

## 3.3 Main elements of an IoT interoperability framework

### 3.3.1 Introduction

Interoperability requires agreements between elements of a system that may be of very different nature. For the LSPs (as well as other actors in the IoT community), coming to a common understanding and to the possibility to adopt similar solutions, some elements have to be elicited

that allow the expression and the comparison of the proposed solutions: they are the components of a framework for IoT Interoperability.

The main elements of such a framework addressed in this section are reference architectures, platforms and standards. On top of these, pre-normative activities are also touched upon: they are the basis from which new framework elements will emerge to provide new solutions to current challenges.

### 3.3.2 Reference Architectures

In order to achieve standardization, a lot of elements such as models, definitions or well-defined set of vocabularies need to be agreed upon by the IoT stakeholders in order to ensure a common understanding of the concepts. Moreover, given the need to be able to deal with a potential very large variety of IoT systems architecture, it is also necessary to create high level reference architectures (HLA) like the ones defined by AIOTI.

The AIOTI High-Level Architecture for IoT (AIOTI HLA) is a standard framework or architecture for IoT. The AIOTI functional model shown in Figure 2 describes functions and interfaces between functions of the IoT system.

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.

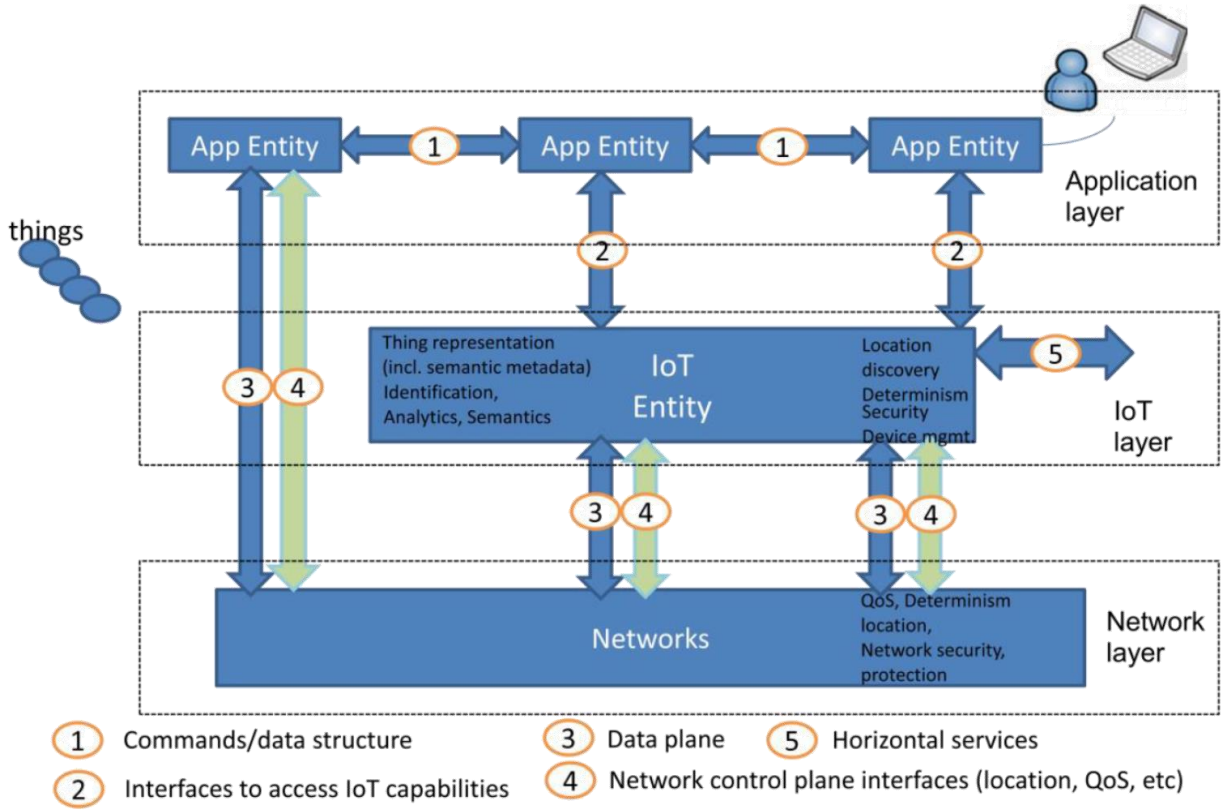


*Figure 2: AIOTI Functional Model*

The AIOTI HLA is similar or can be mapped to other frameworks such as those developed by ITU-T, oneM2M or IIC.

### 3.3.3 Platforms

There are hundreds of IoT platforms available for the development of IoT systems. The question of a choice of platform(s) by IoT system designers is complex. Some dimensions have to be considered:

- Scope and Breadth. Some of the existing IoT platforms may address a specific problem or a limited technical environment, offering a point solution addressing a part of the IoT stacks. On the other hand, some platforms can be very general purpose and integrate the IoT system in a larger (enterprise) system.
- Maturity and ownership. The available platforms may have different development status, technical readiness levels and user adoption level. Moreover, they can be proprietary as well as opened (e.g., open source).
- Standards support. They available platforms can also have very different support to interoperability and to the standards in support of it.

Some general considerations when evaluating IoT platforms are as follows:

*Table 1: General considerations regarding evaluation of IoT platforms*

| Topic | Considerations |
|---|---|
| Location | Is the platform suitable for the network edge, the fog, the cloud or some form of distributed peer to peer architecture? |
| Pluggable protocol support | Does the platform support an extensible range of protocols? These can be further divided into IoT communication technologies and Internet backhaul protocols. |
| IoT standards support | Does the platform support an extensible range if IoT standards, e.g. oneM2M, OCF, OPC-UA, and so forth |
| Security and trust | What security capabilities are supported and how well do they scale with the number of connected devices? Some factors include the kinds of identifiers for devices, services, people, companies, etc., support for data integrity and encryption, access control, third party attestations, and means for bootstrapping trust? |
| Safety | Does the platform comply with relevant safety regulations? |
| Resilience | Is there support for policy-based control of system behaviour in the presence of faults and cyber-attacks? Does the system provide for defence in depth? Can you use machine learning to monitor behaviour and signal anomalous conditions? |
| Provisioning and device management | What support is there for managing large collections of devices? Does this provide automated control of software updates? |
| Analytics and business intelligence | Which support for value middleware capabilities? |
| Context management | What support is there for storing and reasoning with information describing the context? |
| Semantic interoperability | Is there support for declarative descriptions of devices with both interaction models and semantic models that can be used to enable service providers and service consumers to know that the meaning of the data they exchange? |
| Privacy | Does the platform support the new EU General Data Protection Regulation (GDPR), which is intended to intend to strengthen and unify data protection for all individuals within the European Union? |

| | |
|---|---|
| B2B | Does the platform enable business to business services? This relates to the need for service level agreements, and the potential for automated negotiation of terms and conditions, and where appropriate payment mechanisms. |

Amongst the many IoT platforms in use, with a very diverse scope of functionality, the IoT Service Platform plays an important role since its main objective is to provide an abstraction layer between the applications and the IoT devices and to provide a built-in support for a very large number of standards (existing or forthcoming).

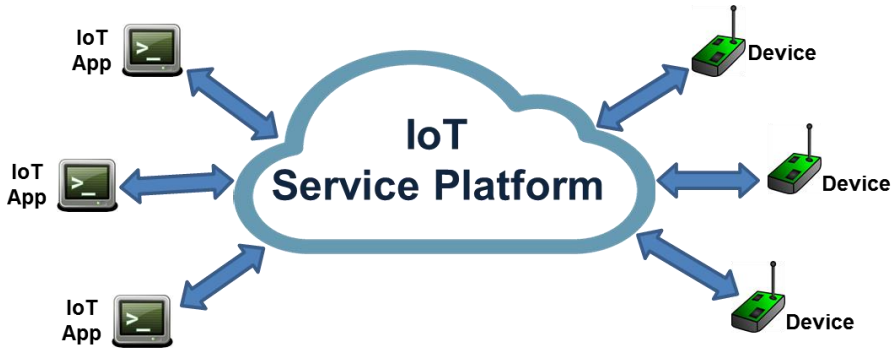


*Figure 3: The IoT Service Platform*

An IoT Service Platform is essentially:

- An Intelligent layer between applications, networks and devices;
- Offering a coherent set of standardized functionalities;
- And an enabler for communication and data interoperability.

The IoT service platform is the actual implementation/deployment of an abstract IoT architecture (entities and interfaces) like the ones outlined in the previous section.

### 3.3.4 Standards

In lieu of the meaning of standards, ISO mentions that "an International Standard provides rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include: test methods, codes of practice, guideline standards and management systems standards". As such, standards are essential to modern business, providing certainty for customers compared to the risks of proprietary solutions. Likewise, standards reduce the risks for investors and through re-use, the costs for developers themselves. In combination with the network effect, this can dramatically expand the market size for hardware, software and services. Therefore, understanding the role of standards in the creation of conditions for sustainable growth of the IoT ecosystem is essential. This potential for growth can be hindered both by fragmentation due to a plethora of non-interoperable platforms, standards and technologies and by the lack of standard-based solutions to address some of the most pressing challenges for IoT, such as interoperability or security.

The default approach to standardisation is to first collect representative use cases, analyse them to obtain the requirements, identify relevant technical approaches, check for matching standards, identify gaps where new standards are needed, create proof of concept implementations, build a coalition of parties with an interest in creating the missing standards, submit the work to a new or existing standards activity. Work to mature the specifications, identify testable assertions, assess market support for the proposed standard, put in place certification for conformance to the new standard, collect errata and apply corrections, and identify gaps/improvements for the next version of the standard.
Many of the requirements for standards are the same across different application domains, e.g. communication technologies, protocols, and generic frameworks for metadata.

The IoT landscape [3] developed by the AIOTI Work Group 3 on Standardisation has used the distinction between the horizontal and vertical domains for the classification of the organisations that are active in IoT standardisation.

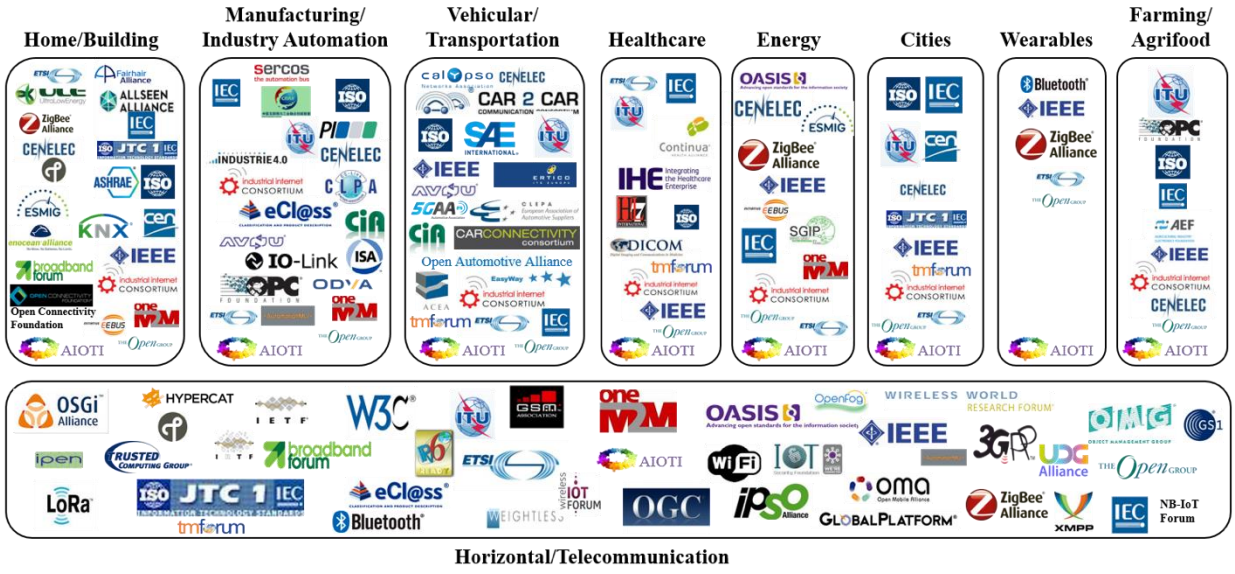


*Figure 4: IoT SDOs and Alliances Landscape*

The classification of IoT standardisation organisations is done along two dimensions:

- Vertical domains (or "verticals") that represent 8 sectors where IoT systems are developed and deployed. These vertical domains include all those that the LSPs are currently addressing;
- A "horizontal" layer that groups standards that span across vertical domains, in particular regarding telecommunications.

The great number of actors in this landscape is suggesting, as already outlined, the risk of fragmentation. In order to have a more precise view of this potential risk, the identification of existing standards and of perceived gaps and overlaps is key. Another aspect is the characterisation of the most promising activities undertaken by the actors in the standardisation landscape. Both aspects are analysed in more details in the following sections. They are key to any decision regarding a possible standardisation strategy.

### 3.3.5 Pre-normative activities

Pre-normative activities explore promising directions, and just as importantly, attempt to present these in ways that are easy to explain to other communities, thereby helping to build a shared understanding on what new standards are needed.

Pre-normative activities need to examine where existing standards are inadequate, and to look at promising approaches to fill the gaps. Some potential examples include: platform independent approaches to identifying security principles, and to describing their trust relationships; work on platform and programming agnostic approaches to describing interaction models for things; or scalable solutions for semantic models and their application to smart services for adaptation to devices from different vendors and offering different capabilities.

Promising ideas include the means to use programming language independent means to describe the interaction model for things exposed to applications as objects in the same execution space as the applications. Semantic models are also needed to enable communicating parties to agree on a shared meaning for the data they exchange. Here, the challenge is that different communities will produce different semantic models, raising barriers for services that need to span communities. This could be likened to having toll gates as each road passes through a village or town, resulting in barriers to free trade and a reduction in the overall economy.

# 4 IoT STANDARDS AND GAP ANALYSIS IDENTIFICATION

## 4.1 Introduction

The objective of this section is twofold. A first objective is to make an overview of the current state-of-the-art in standardisation, in particular regarding the new approaches that are currently addressed by standards organisations and that will rapidly enlarge the scope of current standards.

The second objective is to address the gaps and overlaps, in particular the standards gaps and overlaps: the missing elements of the IoT landscape, mostly due to the complexity of the IoT landscape, that need to be identified before they may be resolved in the near future.

## 4.2 The Current IoT Standardisation Landscape

The IoT community has recognized long ago the importance of IoT standardisation and started to work in many directions, adapting general purpose standards to the IoT context or developing new IoT specific standards. There is now a large number of standards that can be used by those who want to develop and deploy IoT systems. This section will address the current state-of-the-art, evaluate the number of available standards and suggest ways to classify them.

Two complementary dimensions (outlined in the next subsections) are considered by the IoT standardisation community:

- Expansion of the reach of "horizontal layers" standards versus "verticals"-specific standards;
- Specialisation of general- purpose standards for application to more complex and demanding domains. This is in particular the case with the convergence of IT (Information Technology) and OT (Operation Technology) in the industrial domain.

### 4.2.1 Horizontal IoT standardisation activities

A key requirement for LSPs is cross-domain interoperability. To achieve this, the standards used in the development of IoT systems should be generic (not "domain" related) which in turn will foster a large usage. The identification of these “Common Standards across vertical domains” – also termed "horizontal in the current document – is a key enabler.

In order to give an indication of the relative importance of "horizontal" versus "vertical" standards, the ETSI Specialist Task Force (STF) 505 report on the IoT Landscape [7] has identified 329 standards that apply to IoT systems. Those standards have been further classified in:

- 150 "Horizontal" standards, mostly addressing communication and connectivity, integration/interoperability and IoT architecture.
- 179 "Vertical" standards, mostly identified in the Smart Mobility, Smart Living and Smart Manufacturing domains.

One important way to ensure that "interoperability, reliability and security" aspects (outlined above as key by the EC report [1]) are handled more efficiently is to make sure that "horizontal" standards are chosen over "vertical" ones whenever possible. A "horizontal" standard is likely to be developed to serve general-purpose requirements and better address interoperability.

### 4.2.2 Vertical sectors IoT standardisation activities

The standardisation activities within a "vertical" domain (or sector) are largely related to the issues that the actors have to deal with (a field bus in Agriculture has different requirements than a field bus in Manufacturing), the kind of information they have to exchange (hence the possibly very different requirements on interoperability), the complexity of the legacy systems, the maturity of the business domains, etc.

The IoT brings a new dimension to standardisation with two main subjects of concern regarding which the progress of standardisation in the "verticals" will be a trade-off:

- The expected benefits of the "vertical" stakeholder regarding he adoption of IoT:
- The complexity, specialisation and lack of openness (i.e. the silos) of the legacy.

One point to note is not only the split of standards between "horizontal" and "verticals" but also the split of the "verticals" across the various domains as shown in Figure 1 (note that some of the domains mentioned in the figure are not dealt with by the LSPs).

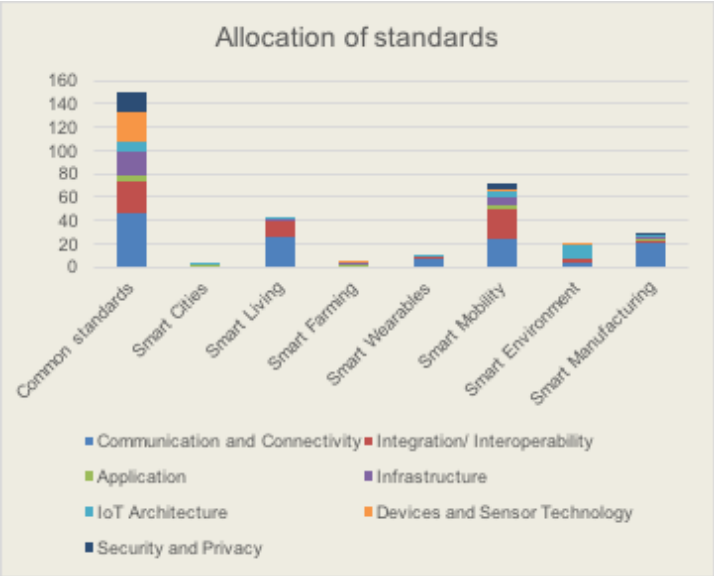


*Figure 5: Horizontal and vertical-specific IoT Standards (source ETSI STF 505)*

## 4.3 IoT Gaps and overlaps Identification

Despite many available standards on which to build IoT systems, the development of large-scale interoperable solutions may not be fully guaranteed, when some elements in the IoT standards landscape are missing or conflicting standards may be selected. Such elements, commonly referred to as "gaps" and "overlaps", are subject of several analyses that aims at identifying them with the intent to ensure that their resolution can be handled by the IoT community, the standardization community. The work of standardisation never stops whichever domain is concerned, IoT being no different. At any moment, new issues arise that cannot be dealt with given the status of (in particular technical) standardisation. The emergence of these gaps, and the initiatives taken for their resolution, define the evolution of the roadmap of standardisation organisations.

### 4.3.1 Identifying IoT Standards gaps and overlaps

Though the gaps related to missing technologies are the most commonly thought of, several categories of gaps can be identified and need to be equally addressed. In the work of ETSI STF 505 [9], three categories of gaps have been addressed:

- *Technology* gaps and overlaps with examples such as communications paradigms, data models or ontologies, or software availability.
- *Societal* gaps with examples such as privacy, energy consumption, or ease of use.
- *Business* gaps with examples such as siloed applications, incomplete value chains, or missing investment.

The perceived criticality of the gaps may be different depending on the role of an actor in standardisation. The Table 2 below is listing some of the major gaps identified in [9]. In addition to their nature and type, it also provides a view of their criticality that comes from an early evaluation by the LSPs reported from the survey described in 6.2. This evaluation is one possible view, and it may differ if the opinion of other actors (e.g., users, service providers) is requested.

*Table 2: Some standards gaps and overlaps and their perceived criticality*

| Nature of the gap | Type | Criticality |
|---|---|---|
| Competing communications and networking technologies | Technical | Medium |
| Easy standard translation mechanisms for data interoperability | Technical | Med |
| Standards to interpret the sensor data in an identical manner across heterogeneous platforms | Technical | High |
| APIs to support application portability among devices/terminals | Technical | Medium |
| Fragmentation due to competitive platforms | Business | Medium |
| Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms | Technical | High |
| Easy accessibility and usage to a large non-technical public | Societal | High |
| Standardized methods to distribute software components to devices across a network | Technical | Medium |
| Unified model/tools for deployment and management of large-scale distributed networks of devices | Technical | Medium |
| Global reference for unique and secured naming mechanisms | Technical | Medium |
| Multiplicity of IoT HLAs, platforms and discovery mechanisms | Technical | Medium |
| Certification mechanisms defining “classes of devices” | Technical | Medium |
| Data rights management (ownership, storage, sharing, selling, etc.) | Technical | Medium |
| Risk Management Framework and Methodology | Societal | Medium |

The characterization of gaps and overlaps, in particular their type, their scope, the difficulties they create, and other appropriate descriptions is a first step. No listing of gaps is final, and their identification will remain a work-in-progress in the IoT Standardisation community.

### 4.3.2 Mapping IoT Standards gaps

The AIOTI has developed the High-Level Architecture (HLA) [6] that defines three layers (as depicted in Figure 6 below) and provides more complete ways to characterise and classify the applicable standards.

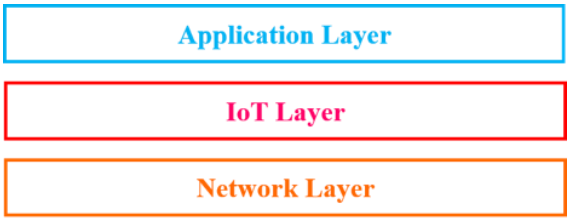


*Figure 6: AIOTI three layers' functional model.*

The three layers are one way to structure an IoT with the following characteristics:

- The Application layer contains the information exchange and interface methods used in process-to-process communications;

- The IoT layer groups IoT specific functions, such as data storage and sharing, and exposes those to the application layer via Application Programming Interfaces (APIs). The IoT Layer makes use of the Network layer's services;
- The Network layer services can be grouped into data plane services, providing short- and long-range connectivity and data transport between entities, and control plane services such as location, device triggering, QoS or determinism.

It may be useful to characterise how the gaps and overlaps outlined in the section above can be mapped on the AIOTI HLA. It is a possible way to outline, amongst others:

- What are the implications in terms of interoperability? When a layer is identified, the scope of the interoperability solution may be more narrowed down. Interoperability at Network layer will require different solutions than interoperability at IoT or Application layer;
- What are the possible routes to standardisation that the resolution of the gaps and overlaps may suggest in order to identify relevant and efficient partners for such resolution?

This is the purpose of the Table 3 below

*Table 3: IoT gaps mapped on the AIOTI HLA*

| Gap | Impact |
|---|---|
| Competing communications and networking technologies | Network layer |
| Easy standard translation mechanisms for data interoperability | IoT and application layers |
| Standards to interpret the sensor data in an identical manner across heterogeneous platforms | IoT layer |
| APIs to support application portability among devices/terminals | IoT layer |
| Fragmentation due to competitive platforms | Not specific to HLA |
| Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms | Mostly IoT layer, also Appl. and Network |
| Easy accessibility and usage to a large non-technical public | Not specific to HLA |
| Standardized methods to distribute software components to devices across a network | IoT and network layers |
| Unified model/tools for deployment and management of large-scale distributed networks of devices | All layers; critical in IoT layer |
| Global reference for unique and secured naming mechanisms | All layers |
| Multiplicity of IoT HLAs, platforms and discovery mechanisms | Addressed by HLA |
| Certification mechanisms defining "classes of devices" | Network layer |
| Data rights management (ownership, storage, sharing, selling, etc.) | All layers |
| Risk Management Framework and Methodology | All layers; interface definition |

The gaps will be addressed later in section 6.3 when dealing with the objectives of the LSPs.

## 4.4 Existing and emerging IoT standards activities

### 4.4.1 Addressing gaps and fragmentation

With different organisations working independently on IoT standards, it is inevitable that they will come up with different approaches even when they are addressing similar use cases. One example of this is for smart homes, where OCF, oneM2M, ETSI SAREF and the Japanese ECHOnet

consortium all differ in the details for the capabilities they selected for home appliances. Furthermore, individual vendors seek to differentiate their products from their competitors via different product capabilities. This makes it impractical to impose a single ontology.

A more effective approach is to design ontologies for each standards suite (e.g. OCF, oneM2M, ECHOnet) and to relate them via a bridging ontology. This approach is being investigated by the W3C Web of Things Interest Group. Another idea is to work on defining best practices for modular ontologies to make it easier for vendors to describe their particular products' capabilities in a standard way.

When it comes to mapping between ontologies, the most appropriate mapping may depend on the context, i.e. the value of the data and the context in which it is situated. A way to express such context dependent mappings would be an advance in the state of the art.

The next level down of importance covers gaps concerning standards for management of services, devices, technologies and platforms; usability by non-technical experts, and data rights management (ownership, storage, sharing, selling, etc.). This points to the need for pre-normative activities that pool experience, gather use cases and best practices, and prepare the way for further standardisation.

### 4.4.2 Some SDO Activities

As already outlined in section 4.2, there are many organisations working in the IoT Standardisation landscape. In the rest of this section, some of them – in particular SDOs – are presented with some of the IoT applicable standards they have already developed and some of their on-going activities that will become standards in the short to medium-term.

More on the topic can be found in the ETSI report [7] that introduces 329 standards applying to IoT and the organisations that produce and maintain them.

#### 4.4.2.1 ETSI

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies.

ETSI SmartM2M, started in Jan 2009, has developed two releases of IOT/M2M specifications R1 (2011) and R2 (2012). It is the initial promoter of the oneM2M Partnership Project (PP). With the publication of oneM2M Release 1 (2015 - data sharing and communication framework) and Release 2 (2016 - semantic support), the transfer of its core technical work t oneM2M has been completed.

ETSI Smart M2M is currently focalized on:

- Lead the ETSI participation and contribution to the EU initiatives in the M2M and IoT areas (Smart Metering, Smart Grid, Smart Cities, etc.);
- Standardize a framework for an open ontology (SAREF) to that enables information sharing among IoT devices and servers using different technologies. The scope of SAREF is starting from Smart Appliances and extending it to other domains like Energy, Buildings, Cities, Agriculture, etc.
- Support to AIOTI Initiative, in particular the WG3 (standardization) with landscape analysis & architectural gap analysis;
- Support the Industry Specification Group (ISG) CIM to develop a complementary and integrated component to oneM2M, to avoid CIM overlap with oneM2M.

In addition to the current work done in Technical Committees (e.g., SmartM2M, 3GPP, ITS or DECT), several expanding or emerging ETSI activities are expected to provide important contributions to IoT:

- The SAREF specification within TC SmartM2M. The objective of SAREF (Smart Appliances REFerence ontology), launched in 2014 and standardised in 2015, is to create a shared semantic model of consensus to enable the missing interoperability among smart appliances. SAREF is to 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. SAREF has gradually grown into a modular network of standardized semantic models that continues to evolve with already standardised extensions in Energy, Environment and Buildings. Others ae on the roadmap for Smart Cities, Smart AgriFood, Smart Industry and Manufacturing, Automotive, eHealth/Ageing-well and Wearables.
- TC SmartBAN is developing standards for use in Body Area Network (BAN) in order to enable the use of small, low power wireless devices which can be carried or embedded inside or on the body. The work involves items such as: low complexity Medium Access Control (MAC) and routing requirements for SmartBANs; an ultra-low power Physical Layer for on-body communications between a hub and sensor nodes; a distributed multi-agent based IoT reference architecture; and a system description, including an overview and use cases
- The ISG CIM on Context Information Management. This Industry Specification Group (ISG) has been created in order to develop technical specifications and reports to enable multiple organisations to develop interoperable software implementations of a cross-cutting Context Information Management (CIM) Layer and bridge the gap between abstract standards and concrete implementations. The CIM Layer enables applications to update, manage, and access context information from many different sources, as well as publishing that information through interoperable data publication platforms.

Other ETSI activities related to IoT, in particular by providing "horizontal" standards for Network interoperability:

- ETSI is a partner of 3GPP which develops IoT radio access technologies such as NB-IOT, a new radio added to the LTE platform optimized for the low end of the market.
- TC DECT provides an IoT European radio access DECT / ULE (Ultra-Low Energy), an evolution of DECT for the IoT;
- IoT is also addressed in TC SmartBAN (Body Area Networks), TC ITS (Intelligent Transport Systems), TC ERM TG28 (Short Range Devices and LTN/LPWA) and TG34 (RFID).

#### 4.4.2.2 IEEE

The IEEE Standards Association, a standards-setting body within IEEE, develops standards through a process that brings together a broad stakeholder community. IEEE standards set specifications and best practices based on current scientific and technological knowledge. These standards span wired and wireless connectivity, encryption, data security, etc.

IEEE P2413 is working with a top down approach and follows the recommendations for architecture descriptions defined in ISO/IEC/IEEE 42010 ("Systems and software engineering - Architecture description", 2011) which:

- Provides a core ontology for the description of architectures
- Specifies provisions that enforce desired properties of architecture frameworks
- Can be used to establish a coherent practice for developing architecture frameworks
- Can be used to assess conformance of an architecture framework

#### 4.4.2.3 IETF

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

IETF supports IoT support since 2005 when it started with 6LoWPAN (IPv6 over Low-power WPAN). IETF has now an IoT Directorate, i.e. an advisory group of experts that coordinate within

IETF IoT groups and increase IETF IoT standards visibility to external SDOs, alliances, and other organizations. IoT related IETF WGs:

- 6Lo (IPv6 over Networks of Resource-constrained Nodes);
- ROLL (Routing Over Low-power and Lossy networks);
- CORE (Constrained RESTful Environments);
- ACE (Authentication and Authorization for Constrained Environments) (ACE);
- CBOR (Concise Binary Object Representation Maintenance and Extensions);
- 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e)
- IPWAVE (IP Wireless Access in Vehicular Environments);
- IPWAN (IPv6 over Low Power Wide-Area Networks);
- Detnet (Deterministic Networking);
- LWIG (Light-weight Implementation Guide)

It should also be noted that - on a more long-term and pre-normative scope - the Internet Research Task Force (IRTF) has the IoT-related Research Group T2TRG on Thing 2 Thing.

#### 4.4.2.4 ISO/IEC

ISO and IEC have a joint technical committee called JTC 1. JTC 1 established a Special Working Group (WG10) on IoT in 2012 that was changed into a formal WG in 2015 and transitioned to a formal Sub Committee in 2017, JTC 1/SC 41, “Internet of Things and related technologies” that will take over the work of WG10 and WG7, "Sensor networks". Current work items in JTC1/WG10:

- ISO/IEC 30141, Internet of Things Reference Architecture: System characteristics, conceptual model, reference model and architecture views for IoT. Draft International Standard by Oct 2017
- ISO/IEC 20924, Definition and vocabulary. A terminology foundation for the Internet of Things. 2nd Committee Draft by March 2017
- ISO/IEC 21823-1, Interoperability for Internet of Things Systems, Part 1: Framework. An overview of interoperable IoT systems and framework for interoperability to ensure information exchanges supporting peer-to-peer interoperability of IoT systems and seamless communication among IoT system entities. 1st CD by June 2017
- ISO/IEC PDTR 22417, IoT Use cases. Identification of IoT scenarios and use cases based on real-world applications and requirements. To be published by June 2017

Under consideration are two additional activities:

- 21823-2 on Network connectivity;
- 21823-3 on Semantic interoperability.

Additional activities related to IoT in ISO are listed below:

- *ISO activities on Smart Cities* - Smart cities standardisation activities are taking place in ISO/IEC JTC1/WG11 and in ISO/IEC JTC1/SC27 on privacy. WG11 deals with framework standards such as ISO 30145-1 (Smart city business framework), ISO 30145-1 (Smart city business framework), ISO 30145-3 (Smart city engineering framework) or ISO 30146 (Business indicators). SC27/WG5 is carrying a study period on privacy in smart cities.
- *ISO activities on Big Data* - Smart cities standardisation activities are taking place in ISO/IEC JTC1/WG9 and in ISO/IEC JTC1/SC27 on privacy and security. WG9 deals with framework standards such is ISO Big Data - Definition and Vocabulary, and ISO 20547 Big data - Reference architecture. SC27/WG4 and SC27/WG5 focus on ISO 20547 Part 4 (Big data – Reference architecture – security and privacy fabric).
- *ISO activities on security-by-design and privacy-by design* - These activities are taking place in ISO/IEC JTC1 SC27. All major standards on security of information systems come from this subcommittee, for instance ISO 27001 (ISMS requirements), ISO 27002 (ISMS Code of

practice for information security controls), or ISO 27005 (Information security risk management). All major standards on privacy also come from this subcommittee, for instance ISO 29100 (Privacy framework), ISO 29134 (Privacy impact assessment guidelines), ISO 29151 (Code of practice for PII protection), ISO 27550 (Privacy engineering), ISO 27551 (Enhancement to ISO/IEC 27001 for privacy management - Requirements).

#### 4.4.2.5 ITU-T

ITU-T develops international standards which act as defining elements in the global infrastructure of information and communication technologies (ICTs). ITU standardisation activities are managed in Study Groups (SG), two of them of particular interest: SG17 on security and SG20 on IoT Smart Cities.

SG17 on security is working closely with ISO SC27, for instance ISO 29151 is a joint SG17 – SC27 standard. During the SC27 meeting in April 2017, it was agreed to explore the possibility to start a new standard on privacy preference management. The focus proposed by ITU was on IoT and oneM2M. As a result, a study period on privacy preference management has been established. CREATE-IoT will be active in this study period.

The ITU-T Study Group was established in June 2015. Since its inception, it established in June 2015, is the leading SG on IoT and its applications, SC&C (smart cities and communities) and IoT identification. SG20 responsibilities include (among others): roadmaps for coordinated development of IoT (and IoT standards database maintenance); big data aspects and intelligent control; use cases and applications (verticals); requirements and capabilities; architectural framework and end-to-end architectures; security, privacy and trust of IoT and SC&C; middleware aspects and platforms; interoperability across verticals; evaluation and assessment of SC&C (guidelines, methodologies, best practices); supervision of JCA (Joint Coordination Activity) on IoT and SC&C [high level coordination within ITU-T & with other SDOs and organisations. To further its work in the domain of data management for IoT architectures, ITU-T SG20 has created the Focus Group on Data Processing and Management to support IoT and Smart Cities. This Focus Group has over 16 deliverables on various topics associated with data management framework for IoT and Smart Cities along with the privacy management for IoT infrastructures. These deliverables will be transferred to the ITU-T SG20 after their approval by the FG-DPM participants, for their approval as international standards within ITU-T.

#### 4.4.2.6 oneM2M

oneM2M is an alliance of regional telecom SDOs (ETSI, TIA, ATIS, ARIB, TTC, TTA, CCSA and TSDSI), associated with industry forums such as OMA, BBF or GlobalPlatform, that operates similarly as 3GPP but with IoT as its focus. The purpose and goal of oneM2M is to develop technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software and relied upon to connect the myriad of devices in the field with M2M application servers worldwide.

oneM2M is an M2M services platform built upon devices, gateways, and servers. It allows end-to-end communication between data source and applications. OneM2M is network centric. It allows interoperability between devices and application through the use of uniform interfaces and APIs. OneM2M reaches to achieve interoperability through different standardisation efforts. The different working groups produce specifications for a reference architecture (ARC WG), a messaging protocol (PRO WG), a data management, abstraction and semantics (MAS WG), but also interoperability testing (TST WG).

The TS 0001 ("Functional Architecture") and TS 0002 ("Requirements") standards define the oneM2M architecture and support the deployment of IoT infrastructures, using service platforms that provide multi-domain support and interoperability with a middleware offering e.g., identification and naming of devices and applications.

#### 4.4.2.7 W3C

The World Wide Web Consortium (W3C) is an international member funded community focussing on defining Web technology standards. Many of these are applicable to Web browsers, e.g. HTML, CSS, SVG, MathML, and a suite of standards for browser APIs. Others relate to Linked Data and the Semantic Web, e.g. the Resource Description Framework (RDF), SPARQL, OWL and so forth. A third area involves the extensible markup language (XML), XML Schema, and standards for using XML for messaging (Web Services). W3C recently started work on standards relating to the Internet of Things, starting with a Workshop in 2014, followed by launching a Web of Things Interest Group in early 2015 and a Working Group in 2017. W3C has a strong commitment to accessibility (one Web for all), internationalisation and security.

All of these areas are relevant to the Internet of Things. Web browsers are available for a very broad range of devices and provide a basis for rich user interaction with distributed services. Linked Data provides a lingua franca for data and metadata in a variety of formats. XML is commonly used for data exchange, especially in the enterprise. Many of W3C's APIs make use of the JavaScript Object Notation (JSON).

W3C aims to counter the fragmentation of the IoT through a semantic interoperability framework that decouples applications from the underlying IoT standards, protocols, data formats and communication patterns, and enables discovery, composition and adaptation to variations across devices from different vendors. The goal is to reduce the costs and risks for developing IoT solutions and create the conditions for unlocking the network effect for sustainable growth in open markets of services on a Web scale, just as we enabled through our standards for Web pages, which saw sustained exponential growth over many years.

The Web of Things is based upon W3C's work on Linked Data and covers the interaction model exposed to applications in terms of the properties, actions and events for things, the semantic models describing the kinds of things and their relationships, and metadata relating to security, trust, privacy, service level agreements and other terms and conditions. The Web of Things, as an abstraction layer for applications, is complementary to IoT standards for lower layers in the abstraction stack, and can be used at the network edge, in the fog, in the cloud or with federated peer to peer architectures. This work is still in progress, and W3C is seeking contributions from organisations with an interest in realising the huge potential of the IoT.

## 4.5 Discussion

At this stage, a view of some of strengths and weaknesses of the IoT standardisation community with respect to the potential requirement of LSPs have been exposed:

- The requirements on interoperability will be spanning a large number of layers from network to business, with an important role of the syntactic and semantic layers. A lot of effort has been done in the recent past on syntactic interoperability, and even more importantly is done currently on semantic interoperability;
- There are a number of "cross-domains" standards that may be applied in several "verticals", provided that they are willing to adopt them as part of their strategy;
- Many gaps remain to be addressed and resolved (not just technical ones) and their resolution will be improved by a common effort across the LSPs when possible.

It is therefore important to better understand the requirements of the "verticals" and the intentions of the LSPs with respect to them. This is the purpose of section 6.

# 5 IoT Pre-normative Activities

## 5.1 Background

This is a burgeoning domain with a lot of actors, e.g., academics, research projects (e.g. Horizon 2020) and a plethora of ideas and directions explored. What will be transformed into actionable solutions (e.g., standards) is very open ended as it is hard to predict what will be adopted by the IoT ecosystem in the future.

## 5.2 Challenges

Current challenges suggest some topics of interest as presented below:

- How to support semantic interoperability in a more scalable way that works well across isolated or weakly coupled communities. If different communities are tackling what are broadly similar use cases, they should address many of the same requirements, but are likely to end up with different approaches. It is unrealistic to expect isolated or weakly coupled communities to agree to a common ontology. Moreover, imposing an ontology may hinder innovation by failing to address the specific needs of each community. One approach is to use bridging ontologies that relate the concepts in the community specific ontologies. One opportunity for research is the potential role of context dependent mapping rules, in which the mapping depends on both the ontologies and the specific data. This would be a step beyond today's context independent mappings, e.g. as used by Inter-IoT and other IoT-European platforms Initiative (IoT-EPI) projects (online at www.ioti-epi.eu).
- Challenges for securing systems of systems. Each IoT standards community tends to approach security slightly different from the others. However, for open markets of services, where one needs to connect services from different vendors and using different underlying standards, there is a huge challenge to establish end-to-end security and build trust across the different systems. One opportunity is to make use of an abstraction layer that decouples applications from the underlying systems. What kinds of standards are needed at the different layers in the abstraction stack and how can they be coordinated?
- Opportunities for federated systems and services. Commercial Internet solutions providers tend to rely on centralised cloud-based services. However, these are at greater risk from cyberattacks compared to distributed peer to peer architectures that can be designed to resist denial of service attacks. If the European Union is to compete effectively with the extremely large US Internet companies, we need to find a way to enable the network effect for federated services on a European scale. One potential example is a ride sharing economy based upon peer to peer IoT solutions as a competitive alternative to Uber.
- Challenges for distributed open ecosystems of services. What would be expected there is a simple means to discover and compose services from different vendors and using different standards and different platforms. Smart applications will need to be able to adapt to variations in the interaction models and capabilities from one vendor to the next. The requirements for contractual relationships between suppliers and consumers of services also need to be addressed. Further work is needed on standards for how to express Service Level Agreements, and terms and conditions, together with mechanisms for payments and automated negotiation. This points to further rationale and opportunities for abstraction layers like the Web of Things.
- Opportunities for combining different scientific disciplines, e.g. AI, Cognitive Science and Computational Linguistics. Traditional approaches to data modelling are based upon symbols and logical inference. By blending ideas from Cognitive Science, there is an opportunity to make recall and reasoning based upon the statistics of experience and bridging the gap to how humans think.

# 6 REQUIREMENTS FROM VERTICALS AND LSPS APPROACHES

## 6.1 Introduction

The capture of the most precise set of requirements is a pre-requisite to the development of a precise standardisation strategy. Two kinds of information have to be gathered to this extent:

- The requirements of the "vertical domains", i.e. the domains in which the LSPs will principally operate (e.g. Smart Aging, etc.). This information may come from the LSP's participants themselves, but also from other actors in the domain;
- The view of the LSP on their approach to standardisation. The definition of a common standardisation strategy will rely on the identification of the commonalities and differences between the various LSPs.

In support of the collection of the requirements of both the vertical domains and the LSPs, a survey has been developed with a set of questions as follows:

- Pre-normative activities: those that precede and prepare the ground for standardisation;
- Interoperability: what are the levels of interoperability the LSP wants to address;
- Standards: what are the existing standards and the standards gaps that the LSP will consider;
- Interoperable Platforms: what are the platforms the LSP will be using and how;
- SDO involvement: The various LSP activities related to standardization being carried on within various SDOs by different partners;
- Other: questions regarding topics such as security, privacy, or regulation.

This survey supports the development of the current document as well as the development of Deliverable D06.04 [1] with a set of questions related to "pre-standardisation" issues. It is a living survey that will be kept open and refined (e.g. with a larger set of answers, coming for instance from the users of the LSPs). The survey can be found in section 10.1, Appendix A.

## 6.2 Requirements from vertical domains

This section presents the main results of the survey regarding the 3 dimensions investigated: Interoperability, Standards and Platforms. The scope and the nature of the answers may vary from one "vertical" to another one, in part due to the different levels of understanding of the role of IoT, to the maturity of business models, etc. The information presented represents only a part of what has been collected. It is a snapshot of the current analysis of LSPs and will vary over time: it is a work in progress. At this stage, it is essentially meant to show the diversity of the views and some possible areas of (partial or complete) agreement.

### 6.2.1 Interoperability

The survey has tried to capture the requirements regarding interoperability by first understanding what the levels of interest are for the LSP on four levels: Business Processes, Application, Information and Communication.

*Table 4: LSP level of interest*

| LSP | Levels of interoperability of interest |
|---|---|
| **ACTIVAGE** | Application, Information |
| **AUTOPILOT** | Business Processes, Application, Information, Communication |
| **IoF2020** | Business Processes, Application, Information, Communication |
| **MONICA** | Business Processes, Application, Information, Communication |
| **SYNCHRONICITY** | Business Processes, Application, Information, Communication |

The major source identified by the LSPs for supporting these interoperability requirements is the use of standards.

### 6.2.2 Standards

The Table 5 outlines the major "Horizontal" standards currently identified by the LSPs in a list of 39 standards proposed.

- Note 1: Some of the evaluations are not entirely finalised.
- Note 2: IoF2020 has not finalized the identification of the standards.

*Table 5: Horizontal standards supported by the LSPs*

| Standard or standard family | ACTIVAGE | AUTOPILOT | IoF2020 | MONICA | SYNCHRONICITY |
|---|---|---|---|---|---|
| 3GPP NB-IoT | | X | | X | X |
| AIOTI HLA | X | X | X | X | X |
| BBF TR069 | | | | | X |
| Bluetooth BLE | X | | | X | X |
| DASH 7 | | | | X | |
| ETSI SAREF | | X | | X | |
| IEEE P2413 | | X | | | |
| IETF 6LoWPAN | X | | | | X |
| IETF CoAP | X | | | X | |
| IETF LR-WPAN | | | | X | |
| IETF Oauth | | | | X | |
| IETF Roll | | | | X | |
| IoTivity | X | | | | |
| IPSO Alliance | X | | | | |
| ISO/IEC JTC1 IoT RA | | X | | | |
| LoRa | | | | | X |
| OASIS XACML | | | | X | |
| OASIS MQTT | | | | X | |
| OMA LwM2M | X | | | | |
| OMA NetAPI | | | | | X |
| oneM2M | X | X | | X | X |
| OSGI Core | | | | X | X |
| W3C | X | X | | | |
| WiFi Alliance | | | | X | |
| ZigBee | | | | | X |

The Table 6 outlines the major "Vertical"-specific standards (the question was open).

- *Note 1: Some of the evaluations are not entirely finalised.*
- *Note 2: IoF2020 has not finalized the identification of the standards.*

*Table 6: Vertical standards supported by the LSPs*

| LSP | Supported vertical standards |
|---|---|
| **ACTIVAGE** | ETSI SmartBAN, IEEE 1073 |
| **AUTOPILOT** | 5GAA. ADASIS, CEN TC 278, ETSI TC ITS, ETSI TC ERM, SENSORIS |
| **IoF2020** | Not Yet Available |
| **MONICA** | ETSI EN 300 220-1 V3.1.1, IEEE 802.14a, OGC SensorThings API, UWB (incl. ETSI EN 302 065-2 V1.1.1) |
| **SYNCHRONICITY** | Agri-AEF, ETSI ISG CIM, Industrie 4.0 |

The Table 7 presents a more detailed view on the evaluation of standard gaps and overlaps by the LSPs (than in Table 2). It is interesting to note that may easily range from Low to High on the same line (i.e; across the various LSPs). This is a clear indication that the priorities of LSPs for gaps resolution may be different and that the strategies for resolution may involve different LSPs.

*Table 7: Perceived criticality of standard gaps per LSP*

| Nature of the gap | ACTIVAGE | AUTOPILOT | IoF2020 | MONICA | SYNCHRONICITY |
|---|---|---|---|---|---|
| Competing communications and networking technologies | Low | Medium | High | Medium | Medium |
| Easy standard translation mechanisms for data interoperability | Medium | Medium | Medium | Low | Medium |
| Standards to interpret the sensor data in an identical manner across heterogeneous platforms | Medium | High | Medium | High | High |
| APIs to support application portability among devices/terminals | Medium | Low | Medium | Medium | Medium |
| Fragmentation due to competitive platforms | High | Low | Medium | N/A | Medium |
| Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms | Medium | Medium | Low | High | High |
| Easy accessibility and usage to a large non-technical public | Medium | | Low | High | High |

| | | | | | |
|---|---|---|---|---|---|
| Standardized methods to distribute software components to devices across a network | Medium | Low | Medium | Low | Medium |
| Unified model/tools for deployment and management of large-scale distributed networks of devices | Medium | | Medium | Medium | Medium |
| Global reference for unique and secured naming mechanisms | Medium | | Low | Low | Medium |
| Multiplicity of IoT HLAs, platforms and discovery mechanisms | High | Low | Medium | Medium | High |
| Certification mechanisms defining "classes of devices" | High | | Low | N/A | Medium |
| Data rights management (ownership, storage, sharing, selling, etc.) | High | Medium | High | Medium | Medium |
| Risk Management Framework and Methodology | Medium | Medium | Medium | Medium | High |

Another important aspect of the role of standards must be outlined: standards should also enable LSPs to meet the requirements for the right to data portability enshrined by Article 20 of Regulation 679/2016 (General Data Protection Regulation, "GDPR").

### 6.2.3 Platforms

The survey has proposed a list of 10 potential platforms, amongst which the LSPs show some interest in the following ones:

*Table 8: Platforms of interest for the LSPs*

| LSP | Supported platforms |
|---|---|
| **ACTIVAGE** | FIWARE, SOFIA, IPSO Framework |
| **AUTOPILOT** | FIWARE, oneM2M |
| **IoF2020** | FIWARE, CRYSTAL, SOFIA |
| **MONICA** | FIWARE, oneM2M, Open source LinkSmart middleware components, open source SCRAL component |
| **SYNCHRONICITY** | FIWARE, oneM2M, Eclipse OM2M, OpenDaylight IoTDM |

It should be noted that, during the first meeting of the Activity Group 2, the LSPs have outlined that there are many other platforms or elements of platforms under analysis and – in some case - likely to be used by the LSPs.

## 6.3 Current strategies within the LSPs

### 6.3.1 Introduction

The five LSPs, a few months of their official launch, have started to consider their intentions with respect to standards, and how standards can help them address the "vertical domains" requirements outlined in section 6.2 above. However, the status of the LSP work on standards differs depending on the project. Some are close to having a proper "standardisation strategy" whereas others are more in the evaluation phase. This section intends to capture the current status within the LSPs

that will be used for the definition – in section 7.2 - of an initial set of recommendations for filling the gap between an "approach" and a "strategy".

### 6.3.2 An overview of the IoT Large-Scale Pilots

The European Commission'- in particular within the Internet of Things Focus Area (IoT-FA) – has selected and launched the IoT Large-Scale Pilots with the intention that the LSPs will foster the take up of IoT in Europe and enable the emergence of IoT ecosystems supported by open technologies and platforms. The IoT LSPs are intended to make use of the rich portfolio of technologies, standards and tools - currently developed and demonstrated within environments limited in size and scope - within real-life use case scenarios, in order to validate IoT's expected socio-economic potential though advanced IoT solutions across complete value chains involving real-life users.

The five LSPs analysed below are addressing the needs and requirements of the "verticals" analysed in section 6.2 above. A succinct description of these projects can be found in 10.2 (Appendix B). These projects are addressing:

- ACTIVAGE: Smart living environments for ageing well
- AUTOPILOT: Autonomous vehicles in a connected environment
- IoF2020: Smart Farming and Food Security
- MONICA: Wearables for smart ecosystems
- SYNCHRONICITY: IoT Large-Scale Pilot for Smart Cities

### 6.3.3 ACTIVAGE

The following extract from the project definition outlines the intention of ACTIVAGE with respect to all the elements discussed above:

*The project delivers the ACTIVAGE IoT Ecosystem Suite (AIOTES), a set of Techniques, Tools and Methodologies for interoperability at different layers between heterogeneous IoT Platforms and an Open Framework for providing Semantic Interoperability of IoT Platforms for AHA, addressing trustworthiness, privacy, data protection and security.*

The activities of ACTIVAGE related to standardisation have the objective to:

- Develop innovative business plans;
- Support standardization and concentration activities through and based on the interoperability of structured components;
- Monitor and align with working groups focused on standards in AHA & IoT.
- Define the framework to assure the privacy protection, security and safety of the users.
- Co-design standardisation with the IoT industry.

### 6.3.4 AUTOPILOT

The following extract from the project definition put the focus on the service aspect:

*AUTOPILOT develops new services on top of IoT to involve autonomous driving vehicles, like autonomous car sharing, automated parking, or enhanced digital dynamic maps to allow fully autonomous driving.*

The intentions of the LSP regarding standardisation are still in definition.

### 6.3.5 IoF2020

The following extract from the project definition puts the focus on architecture, reuse of components and open standards:

*A lean multi-actor approach focusing on user acceptability, stakeholder engagement and sustainable business models boost technology and market readiness levels and bring end user adoption to the next stage. This development is enhanced by an open IoT architecture and*

*infrastructure of reusable components based on existing standards and a security and privacy framework.*

The agriculture and food industries have heavily worked an invested in activities in support of interoperability (e.g., AGROVOC, agroXML, EPCIS, GODAN, ISOBUS, UN/CEFACT). Moreover, diverse IoF2020 partners are involved in related standardisation activities already for a long time. Therefore, the LSP support actions could facilitate the horizontal aspects, in particular for an IoT related semantic interoperability.

### 6.3.6 MONICA

Extract from the project definition:

*MONICA demonstrates a large-scale IoT ecosystem that uses innovative wearable and portable IoT sensors and actuators with closed-loop back-end services integrated into an interoperable, cloud-based platform capable of offering a multitude of simultaneous, targeted applications.*

MONICA bases its solutions on general IoT relevant standards as well as on other standards and technologies (such as 3G and 4G (LTE) public commercial networks), supporting the three main project applications:

- Management of public security and safety during events, where very large amounts of people are gathered in open air settings such as concerts, carnivals, sports events and general city manifestations;
- Acoustic monitoring and active noise controlling applications, monitoring and reducing the emission of unwanted “noise” to the neighbouring communities together with engaging the citizens in better adaptation of open air events to city living (e.g., active involvement of citizens using their smartphones with special apps to measure and report concert/noise Sound Pressure Levels both indoor and outdoor and submit assessment of perceived disturbing sound levels).
- Integration with additional ecosystems, such as Smart City IoT platforms, Open Data portals, Social Media blogs and generic FIWARE cloud federation enablers.

The strict adherence to de-jure standards (e.g., ETSI Standards) will ensure future competition in the devices market and help reducing the overall cost of MONICA elements.

### 6.3.7 SYNCHRONICITY

The perceived intentions of the LSP regarding standardisation. Extract from the project definition:

*SYNCHRONICITY is working to establish a reference architecture for the envisioned IoT-enabled city market place with identified interoperability points and interfaces and data models for different verticals. This includes tools for co-creation & integration of legacy platforms and IoT devices for urban services and enablers for data discovery, access and licensing lowering the barriers for participation on the market.*

A lot of links and contribution to the Standards community are foreseen and will have to be confirmed: EC Rolling Plan for ICT Standards; ETSI Industry Specification Group for Context Information Management (ISG CIM); ITU-T; AIOTI: WG3 (standards), WG8 (smart cities) SF-SSCC (SSCC-CG) etc.; EIP-SCC: 2 CSAs: CITYKeys & ESPRESSO.

SYNCHRONICITY will also propose its methodology for a Privacy Impact Assessment in Smart Cities to the attention of the ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities.

# 7 IoT Strategy and coordination plan

The present strategy and coordination plan (SCP) in support of IoT Focus Area objectives and key activities intends to address the following objectives and key activities:

- Improving industry's and IoT LSPs stakeholders' understanding of the European regulatory framework;
- Engaging effectively with European and international institutions to influence the development of European-wide and international standards.

## 7.1 Introduction

The work program of IoT standardisation is, by nature, not fully predictable. However, some considerations may be outlined in order to ensure that new standards developments will foster collaboration and reduce fragmentation:

- Solutions should be transversal, with "horizontal layer" standards rather than "vertical domain" specific;
- Interoperability will be essential for the deployment of the IoT systems, to ensure seamless communication and seamless flow of data across sectors and value chains;
- New interoperability solutions should seek for integration into "horizontal" frameworks (e.g., oneM2M) rather than provide point solutions;
- Effective security and privacy solutions are key to user acceptance and should be based on global holistic approaches (e.g., security by design, privacy by design) that involve all the actors (and not just the specialists);
- Solutions are often not just technical solutions and existing standards may have to address non-technical issues.

## 7.2 Strategy toward IoT interoperability and standardization

A certain number of possible activities can be started in order to support the considerations in the previous section. The list of such actions provided below is not exhaustive and will be refined during the course of the development of the LSPs and will be a significant part of Deliverable 06.02 ("Recommendations for commonalities and interoperability profiles of IoT platforms").

### 7.2.1 Vocabularies, definitions

A frequent roadblock to collaboration between technical teams is the variety of meanings and the lack of common understanding on the terms and definitions that are routinely used in each team and may have to be shared. The definition of a common vocabulary and an agreed set of definitions may be an enabler to technical discussions. Some examples of such definitions are provided (as a non-committing illustration) in section 10.3 (Appendix C).

### 7.2.2 Commonality of standards

One key challenge for the LSPs is to allow cross-domain interoperability, to ensure that the systems developed are not developed in silos. To achieve this, it is recommended to make the choice for common solutions, in particular regarding the architecture, to use as much as possible standards that are listed in the standards identified in section 4.2.1 as "Common Standards across vertical domains", extending up to the application layer.

### 7.2.3 Promotion of SDO/SSO cooperation

One key action that LSPs – through a coordinated standardisation strategy – may foster towards the IoT community is to encourage large SDOs/SSOs to strengthened collaboration and cooperation: the potential of standards identified as common standards 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.

### 7.2.4 Coordinated contributions to standards

When several LSPs have identified the same potential activities on a certain topic and selected a possible target in the IoT standardisation community, a form of coordinated participation may be envisaged: it will be in particular the role of the Activity Group to foster and support this collaboration.

Cross-LSP collaborations are already outlined in the intentions expressed by the LSPs regarding their own strategies, e.g., potential participation of two LSPs to the ETSI Industry Specification Group (ISG) CIM.

### 7.2.5 Plugtests

The interoperability requirements of the LSPs are varied and complex. There are different interoperability layers involved, several existing or emerging standards with possible usage, systems architectures with different building blocks and APIs.

In order to improve and validate interoperability, and possibly foster a larger adoption of common solutions (e.g., standards, APIs), plugtests may be a good vehicle. Their existence may be the result of discussions involving the LSPs, the standards organisations, the users, etc.

## 7.3 Coordination plan toward IoT interoperability and standardization

The current document – as already outlined – intends to present a set of concepts, information, analysis in order to form the basis of a common understanding of what a standardisation strategy for the IoT Large-Scale Pilots (LSPs) may be. This strategy will be developed by actors, within an agreed planning and communicated to all the stakeholders involved.

### 7.3.1 Stakeholders

The mains stakeholders in the definition and implementation of the standardisation strategy are:

- The LSPs and, more precisely, the participants involved in the technical work of defining the LSP use cases, specifying the requirements, selecting the reference architecture and the main functional building blocks, implementing the pilots, etc. In particular, the LSP participants involved in standardisation and in charge of the potential relations with the IoT standardisation community will be involved;
- The Activity Group (AG) 2 ("IoT standardisation, architecture and interoperability") includes already identified members of the LSPs and the CREATE-IoT participants involved in Work Package 6. The AG will meet physically twice a year and on-line on a monthly basis. The AG2 will address in particular issues related standards and the standardisations strategy will be part of them;
- The CREATE-IoT participants in order to ensure that the links and dependencies identified in section 2.3 are properly handled.
- The SDOs and organisations with which liaisons may be established during the implementation of the actions related to the strategy;
- The European Commission that will provide guidance to all the stakeholders.

### 7.3.2 Workshops

The coordination of the activities related to the definition of the IoT Interoperability and Standardisation strategy is handled by the Activity Group 02 (Standardisation, Architecture and Interoperability).

The progress the work will be ensured by the organisation of a series of workshops. At this stage, four workshops are planned in 2018 and four in 2019. The objectives of these workshops are:

- To establish a common basis across the different IoT Large-Scale Pilots (LSPs) regarding their results related to topics such as: mapping pilot architecture approaches based on possible reference architecture models; interoperability framework and reference implementations based on use cases; analysis of components and standards, existing IoT platforms that may be reused/tested across multiple use cases and enable interoperability across those.
- To contribute to the Digitising European Industry (DEI) WG2 on standardisation.

The results of these workshop will be fed into subsequent deliverables of CREATE-IoT.

# 8 EARLY FINDINGS AND FUTURE WORK

## 8.1 Contribution to overall picture

The present document reflects the different views and requirements of the LSPs on aspects related to interoperability and standardisation. This is a first contribution to the overall work of the technical definition of the pilots.

## 8.2 Relation to the state-of-the-art and progress beyond it

The present document offers a snapshot of the IoT standardisation and how its current standards portfolio can serve the immediate needs of the LSPs. Moreover, it also addresses the issues related to missing elements (i.e. gaps) that have to be resolved by the IoT technical community.

## 8.3 Other conclusions and lessons learned

The present document is coming from the merge of two documents produced 6 months after the launch of the LSPs and somehow reflects the various levels of progress across the LSPs relative to interoperability and standards. However, despite different LSP situations, all LSPs have provided significant contributions (e.g., for the survey) that will allow the present document to serve a reference for the next steps of the work.

At this stage, most of the elements required for a good start of the strategy and coordination plan (SCP) are in place. Setting-up the proper team to deal with it has been longer than expected – probably due to an excess of optimism. The task undertaken within the SCP is complex and requires people from very different backgrounds (work domains, technical expertise, etc.) to come together and share a common understanding. Now that the team in place and the definition phase for the LSPs is finished, the possibility of a constant and permanent progress has become a reasonable expectation.

# 9 REFERENCES


[1] CREATE-IoT, Deliverable D06.04, " IoT pre-normative activities"

[2] European Commission communication on "ICT Standardisation Priorities for the Digital Single Market", COM(2016) 176 final, Brussels, 19.4.2016

[3] Interoperability; http://www.businessdictionary.com/definition/interoperability.html

[4] GridWise Interoperability Context-Setting Framework (March 2008), GridWise Architecture Council, www.gridwiseac.org/pdfs/

[5] AIOTI WG03 Report: " IoT LSP Standard Framework Concepts Release 2.7" February 2017; https://docbox.etsi.org/SmartM2M/Open/AIOTI/

[6] AIOTI WG03 Report: "High Level Architecture (HLA) Release 3" June 2017; https://docbox.etsi.org/SmartM2M/Open/AIOTI/

[7] STF 505 TR 103 375 "SmartM2M IoT Standards landscape and future evolution", 10/2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

[8] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs: GROW - Rolling Plan for ICT Standardisation 2016, http://ec.europa.eu/DocsRoom/documents/14681/attachments/1/translations/en/renditions/native

[9] STF 505 TR 103 376 "SmartM2M; IoT LSP use cases and standards gaps", 10/2016. https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505

[10] ACTIVAGE (ACTivating InnoVative IoT smart living environments for AGEing well); https://european-iot-pilots.eu/project/activage/

[11] AUTOPILOT (AUTOmated driving Progressed by Internet Of Things); https://european-iot-pilots.eu/project/autopilot/

[12] IoF2020 (Internet of Food and Farm 2020); https://european-iot-pilots.eu/project/iof2020/

[13] MONICA (Management Of Networked IoT Wearables); https://european-iot-pilots.eu/project/monica/

[14] SYNCHRONICITY (Delivering an IoT enabled Digital Single Market for Europe and Beyond); https://european-iot-pilots.eu/project/synchronicity/

# 10 APPENDICES

Further information is described in related background documents.

## 10.1 Appendix A: Full text of the survey

The full text of the on-line survey can be found below. The different clauses are printed without page breaks. In the on-line survey, they are separated by a line with "Previous" and "Next" buttons.

CREATE-IoT LSP Requirements for Interoperability, Standards and Platforms

Setting the scene

This survey is designed by the team of CREATE-IoT Work Package 6 on "IoT Interoperability and Standardisation".

It is meant to help the LSPs easily express their requirements regarding:
- Pre-normative activities: those that precede and prepare the ground for standardisation;
- Interoperability: what are the levels of interoperability the LSP wants to address;
- Standards: what are the existing standards and the standards gaps that the LSP will consider;
- Platforms: what are the platforms the LSP will be using and how;
- Other: a few questions regarding topics such as security, privacy, or regulation.

For the LSPs, this works is part of their participation to the Activity Group 2 on Standards.

It is expected that the LSPs will answer this survey at the best of their current knowledge.
In some cases, the information related to some of the questions may not be yet available.
However, every snippet of information will be useful to the CREATE-IoT team.

These requirements will be compiled in the first drafts of CREATE-IOT WP6 deliverables.
This drafts will discussed in the Activity Group meeting in June and further published at he end of June 2017.

We will first ask a few question in order to identify who responds and the domain in which the LSP operates.
The information collected will be kept within WP6 and only used in the WP6 Deliverables.
Many thanks in advance.

* 1. Please provide your name,

* 2. your email,

* 3. and the LSP domain concerned

- ◯ Smart Aging
- ◯ Smart Cities
- ◯ Smart Food and Farming
- ◯ Smart Transportation
- ◯ Smart Wearables

Most of the following questions are open and can be skipped if no answer is possible.
Whenever it is making sense, multiple choices are possible (with a square-shaped checkbox).

1

CREATE-IoT LSP Requirements for Interoperability, Standards and Platforms

Requirements on pre-normative activities

The pre-normative activities are those that precede and prepare the ground for standardisation, e.g.

- Gathering and analysing use cases to identify requirements;
- Surveying existing standards to identify gaps in respect to the requirements;
- Exploration of new ideas and techniques to gain a better understanding;
- Incubation of ideas through implementations and interoperability experiments;
- Outreach and discussion as a basis for building a shared mindset.

The following questions are open and should be answered at the best of your current knowledge.

We first need to understand what is the basic framework that your LSP will use.
The first question will capture the main generic aspects of your approach to those issues.
More questions will address the horizontal domains for pre-normative standardisation.

- are there applicable reference architectures?
- what are the protocols to be considered (e.g. CoAP)?
- what are the IoT standards for using this protocols (e.g. oneM2M)?
- what are the requirements on security, privacy, semantic interoperability, etc.?
- what is the approach related to testing?

## 4. What is the basic framework used by your LSP?

## 5. Is there a reference architecture for your LSP?

2

6. What are your LSP requirements on security?

7. What are your LSP requirements on privacy?

8. What are your LSP requirements on semantic interoperability?

9. What are your LSP requirements on discovery, scaling, ... ?

3

## 10. What is your LSP approach for testing?

## 11. Would you like to add something on this topic?

CREATE-IoT LSP Requirements for Interoperability, Standards and Platforms

Requirements on interoperability

Interoperability comes at many levels for systems (see the TOGAF model for instance).
We are trying to understand what are the levels concerned and how they will be addressed.

4

## 12. What are the levels of interoperability your LSP wants to address?

- [ ] Business Processes
- [ ] Application
- [ ] Information
- [ ] Communication

Please characterize in details if appropriate

## 13. What are the Business Process level interoperability requirements for your LSP?

## 14. What are the Application level interoperability requirements for your LSP?

## 15. What are the Information level interoperability requirements for your LSP?

- [ ] Common Information Models
- [ ] Ontologies
- [ ] Semantic Interoperability

Please characterize in details if appropriate

## 16. What are the Communication level interoperability requirements for your LSP?

5

## 17. Which kind of interoperability support will your LSP investigate?

- [ ] Standards
- [ ] Development of (Open Source) Components
- [ ] Plugtests

Please characterize in details if appropriate

## 18. Would you like to add something on this topic?

## CREATE-IoT LSP Requirements for Interoperability, Standards and Platforms

### Requirements on Standards

A number of standards are available to develop IoT systems:
- Horizontal standards, that are in essence cross-domain
- Vertical standards, that are specific to a given domain

We are trying to understand what are the most critical ones your LSP.

On the other hand, a number of standards gaps have been identified (the the ETSI STF 505).
We are trying to understand which ones are of concern and will be addressed by your LSP.

Multiple answers to questions are possible, including none.

6

## 19. What are the IoT "horizontal standards" your LSP intends to adhere to?

- [ ] 3GPP NB-IoT
- [ ] AIOTI HLA
- [ ] AllSeen
- [ ] BBF TR069
- [ ] Bluetooth BLE
- [ ] DASH7
- [ ] EnOcean EEP
- [ ] EnOcean WSP
- [ ] ETSI DECT
- [ ] ETSI LTN
- [ ] ETSI SAREF
- [ ] Hypercat
- [ ] IEEE 1901.2 PLC
- [ ] IEEE LR-WPAN
- [ ] IEEE P2413
- [ ] IETF 6LoWPAN
- [ ] IETF CoAP
- [ ] IETF Oauth
- [ ] IETF ROLL
- [ ] IETF XMPP
- [ ] IIC IIRA
- [ ] IoTivity
- [ ] IPSO Alliance
- [ ] ISO/IEC 29182
- [ ] ISO/IEC JTC1 IoT RA
- [ ] ITU-T G.9959 Z-Wave
- [ ] ITU-T Y.2060
- [ ] LoRa
- [ ] M2.COM
- [ ] OASIS XACML
- [ ] OASIS MQTT
- [ ] OMA NetAPI
- [ ] oneM2M
- [ ] OSGI Core
- [ ] SensorML
- [ ] UpNp
- [ ] W3C
- [ ] WiFi Alliance
- [ ] ZigBee

Other (please specify)

## 20. What are the IoT "vertical standards" your LSP intends to adhere to?

7

## 21. How critical are the following standards gaps for your LSP?

| | N/A | Low | Med | High |
|---|---|---|---|---|
| Competing communications and networking technologies | ◯ | ◯ | ◯ | ◯ |
| Easy standard translation mechanisms for data interoperability | ◯ | ◯ | ◯ | ◯ |
| Standards to interpret the sensor data in an identical manner across heterogeneous platforms | ◯ | ◯ | ◯ | ◯ |
| APIs to support application portability among devices/terminals | ◯ | ◯ | ◯ | ◯ |
| Fragmentation due to competitive platforms | ◯ | ◯ | ◯ | ◯ |
| Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms | ◯ | ◯ | ◯ | ◯ |
| Easy accessibility and usage to a large non-technical public | ◯ | ◯ | ◯ | ◯ |
| Standardized methods to distribute software components to devices across a network | ◯ | ◯ | ◯ | ◯ |
| Unified model/tools for deployment and management of large scale distributed networks of devices | ◯ | ◯ | ◯ | ◯ |
| Global reference for unique and secured naming mechanisms | ◯ | ◯ | ◯ | ◯ |
| Multiplicity of IoT HLAs, platforms and discovery mechanisms | ◯ | ◯ | ◯ | ◯ |
| Certification mechanisms defining “classes of devices” | ◯ | ◯ | ◯ | ◯ |
| Data rights management (ownership, storage, sharing, selling, etc.) | ◯ | ◯ | ◯ | ◯ |
| Risk Management Framework and Methodology | ◯ | ◯ | ◯ | ◯ |

Other (please specify)

8

## 22. What are the standards gaps your LSP intends to address?

- [ ] Competing communications and networking technologies
- [ ] Easy standard translation mechanisms for data interoperability
- [ ] Standards to interpret the sensor data in an identical manner across heterogeneous platforms
- [ ] APIs to support application portability among devices/terminals
- [ ] Fragmentation due to competitive platforms and standards
- [ ] Tools to enable ease of installation, configuration, maintenance, operation of devices, technologies, and platforms
- [ ] Easy accessibility and usage to a large non-technical public
- [ ] Standardized methods to distribute software components to devices across a network
- [ ] Unified model/tools for deployment and management of large scale distributed networks of devices
- [ ] Global reference for unique and secured naming mechanisms
- [ ] Multiplicity of IoT HLAs, platforms and discovery mechanisms
- [ ] Certification mechanisms defining “classes of devices”
- [ ] Data rights management (ownership, storage, sharing, selling, etc.)
- [ ] Risk Management Framework and Methodology

Other (please specify)

## 23. Would you like to add something on this topic?

CREATE-IoT LSP Requirements for Interoperability, Standards and Platforms

9

## Requirements on Platforms

A number of platforms are available to develop IoT systems:
- Some have emerged from European projects (e.g. FIWARE)
- Some have been developed by standardisation (e.g. oneM2M)
- Some have been provided by the Open Source communities
We are trying to understand what are the ones that your LSP will use and intemperate with.

Multiple answers to questions are possible, including none.

### 24. What are the following IoT Platforms your LSP intends to use?

- [ ] FIWARE
- [ ] CRYSTAL
- [ ] SOFIA
- [ ] oneM2M
- [ ] AllJoin
- [ ] IoTvity
- [ ] IPSO Framework
- [ ] Thread
- [ ] Eclipse OM2M
- [ ] OpenDaylight IoTDM

Other (please specify)

### 25. What are the non IoT platforms your LSP will have to interoperate with?

10

## 26. What are the interoperability requirements between these platforms?

- [ ] Interoperability between more than one IoT platforms
- [ ] Interoperability between one IoT platform and several non-IoT platforms
- [ ] Interoperability between several IoT platforms and several non-IoT platforms
- [ ] Interoperability between several non-IoT platforms

Please characterize in details if appropriate

## 27. Which kind of platform interoperability support will your LSP investigate?

- [ ] Development of (Open Source) Components
- [ ] Plugtests
- [ ] Standards

Please characterize in details if appropriate

## 28. Would you like to add something on this topic?

11

## 10.2 Appendix B: Short description of the IoT LSPs

### B-1 ACTIVAGE

The main objectives of the project are described in [10]:

ACTIVAGE (ACTivating InnoVative IoT smart living environments for AGEing well) brings together 48 partners from 9 European countries with the objectives to build the first European IoT ecosystem across 9 Deployment Sites (DS) in seven European countries, reusing and scaling up underlying open and proprietary IoT platforms, technologies and standards, and integrating new interfaces needed to provide interoperability across these heterogeneous platforms, that will enable the deployment and operation at large-scale of Active & Healthy Ageing IoT based solutions and services, supporting and extending the independent living of older adults in their living environments, and responding to real needs of caregivers, service providers and public authorities. The project delivers the ACTIVAGE IoT Ecosystem Suite (AIOTES), a set of Techniques, Tools and Methodologies for interoperability at different layers between heterogeneous IoT Platforms and an Open Framework for providing Semantic Interoperability of IoT Platforms for AHA, addressing trustworthiness, privacy, data protection and security. User-demand driven interoperable IoT-enabled Active & Healthy Ageing solutions are deployed on top of the AIOTES in every DS, enhancing and scaling up existing services, for the promotion of independent living, the mitigation of frailty, and preservation of quality of life and autonomy.

### B-2 AUTOPILOT

The main objectives of the project are described in [11]:

AUTOPILOT (AUTOmated driving Progressed by Internet Of Things) brings together 43 partners from 14 European countries and 1 from South Korea with the objectives to increase safety, provide more comfort and create many new business opportunities for mobility services. The market size is expected to grow gradually reaching 50% of the market in 2035. AUTOPILOT develops new services on top of IoT to involve autonomous driving vehicles, like autonomous car sharing, automated parking, or enhanced digital dynamic maps to allow fully autonomous driving. AUTOPILOT IoT enabled autonomous driving cars are tested, in real conditions, at four permanent large-scale pilot sites in Finland, France, Netherlands and Italy, whose test results will allow multi-criteria evaluations (Technical, user, business, legal) of the IoT impact on pushing the level of autonomous driving.

### B-3 IoF2020

The main objectives of the project are described in [12]:

IoF2020 (Internet of Food and Farm 2020) brings together 70 partners from 16 European countries with the objectives to accelerate adoption of IoT for securing sufficient, safe and healthy food and to strengthen competitiveness of farming and food chains in Europe. It will consolidate Europe's leading position in the global IoT industry by fostering a symbiotic ecosystem of farmers, food industry, technology providers and research institutes. The heart of the project is formed by 19 use cases grouped in 5 trials with end users from the Arable, Dairy, Fruits, Vegetables and Meat verticals and IoT integrators that demonstrate the business case of innovative IoT solutions for a large number of application areas. A lean multi-actor approach focusing on user acceptability, stakeholder engagement and sustainable business models boost technology and market readiness levels and bring end user adoption to the next stage. This development is enhanced by an open IoT architecture and infrastructure of reusable components based on existing standards and a security and privacy framework.

## B-4 MONICA

The main objectives of the project are described in [13]:

> MONICA (Management Of Networked IoT Wearables – Very Large-Scale Demonstration of Cultural Societal) brings together 28 partners from 9 European countries with the objectives to provide a very large-scale demonstration of multiple existing and new Internet of Things technologies for Smarter Living. The solution will be deployed in six major cities in Europe. MONICA demonstrates a large-scale IoT ecosystem that uses innovative wearable and portable IoT sensors and actuators with closed-loop back-end services integrated into an interoperable, cloud-based platform capable of offering a multitude of simultaneous, targeted applications. All ecosystems are demonstrated in the scope of large-scale city events, but have general applicability for dynamically deploying Smart City applications in many fixed locations such as airports, main traffic arterials, and construction sites. Moreover, it is inherent in the MONICA approach to identify the official standardisation potential areas in all stages of the project.

## B-5 SYNCHRONICITY

The main objectives of the project are described in [14]:

> SYNCHRONICITY (Delivering an IoT enabled Digital Single Market for Europe and Beyond) brings together 33 partners from 9 European countries and 1 from South Korea with the objectives to deliver a Single Digital City Market for Europe by piloting its foundations at scale in 11 reference zones – 8 European cities and 3 more worldwide cities. SYNCHRONICITY is working to establish a reference architecture for the envisioned IoT-enabled city market place with identified interoperability points and interfaces and data models for different verticals. This includes tools for co-creation & integration of legacy platforms & IoT devices for urban services and enablers for data discovery, access and licensing lowering the barriers for participation on the market. SYNCHRONICITY pilots these foundations in the reference zones together with a set of citizen-centred services in three high-impact areas, showing the value to cities, businesses and citizens involved, linked directly to the global market.

## 10.3 Appendix C: Some definitions

One of the potential action to implement the standardisation strategy plan listed in section 7.2.1 regards common vocabularies. The following is a provisional list of terms that will have to be clarified, discussed, and agreed upon during the development of the full strategy plan in Deliverable D06.02 (due end of June 2018).

More terms will have to be agreed upon like frameworks, platforms, etc.

Gaps

The coverage of the IoT landscape – and the possibility to develop large-scale interoperable solutions – is not fully guaranteed when some elements in this landscape may be missing. These missing elements are referred to as "gaps".

Three categories of gaps can 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, investment.

See [9] for more information and developments.

Interoperability

The ability of a computer system to run application programs from different vendors, and to interact with other computers across local or wide-area networks regardless of their physical architecture and operating systems. Interoperability is feasible through hardware and software components that conform to open standards such as those used for internet. See [3].

Specification

The output from an SSO that may become a standard when ratified by an SDO.

Standard

The output from an SDO.

Standards Development Organization (SDO)

An organization that develops standards that has a formal recognition by international treaties, regulation, etc.

Standards Development Organization (SSO)

Any entity whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining specifications and standards that address the interests of a wide base of users outside the standards development organization.

*NOTE 1: Examples of SDOs are: ETSI, IEC, ISO, ITU, ITU-T.*
*NOTE 2: The SDOs are a subset of the SSOs.*