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 06.05

Initial report on IoT standardisation activities

Revision: 1.00
Due date: 31-07-2018 (m19)
Actual submission date: 30-09-2018
Lead partner: ERCIM

European Commission

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	**D06.05 Initial report on IoT standardisation activities.**				
Status	<Released>	**Due**	m19	**Date**	31-07-2018
Author(s)	D. Raggett (ERCIM), E. Darmois (ETSI), O. Vermesan (SINTEF), M. Serrano (NUIG), M. Menon (MI), P. Annicchino (AS)				
Editor	Dave Raggett (ERCIM)				
DoW	Initial report on IoT standardisation activities. The work has been carried out within task T06.02 (Pre-normative and standardisation activities) and is the second out of three deliverables from this task. The task coordinates the activities with the AIOTI WG on standardisation, SDOs and other various IoT Global Alliances for the validation in usage context of most promising standards and gap analysis identification. It addresses interoperability and integration, through open IoT platforms.				
Comments					

Document history

Rev.	Date	Author	Description
0.00	27-02-2017	SINTEF	Template/Initial version.
0.01	22-12-2017	ETSI	Initial description of work, and structure.
0.02	24-04-2018	ETSI	Improved version
0.03	15-07-2018	ERCIM	Revised structure to match information available
0.04	24-07-2018	ERCIM	Revised structure following ETSI's suggestion
0.05	29-07-2018	ETSI	Quasi completion of sections 2 to 4
0.06	30-07-2018	ETSI	Finalisation of sections 2 to 4 and update of section 5
0.07	31-07-2018	ERCIM, MI	Some editorial changes and updates
0.08	01-08-2018	ETSI, SINTEF	Additional inputs and review
0.09	01-08-2018	ERCIM, SINTEF	Additional input to section 5 and review
0.10	20-08-2018	SINTEF	Section 4 (AUTOPILOT).
0.11	19-09-2018	ETSI	Integration of contributions, review.
0.12	25-09-2018	NUIG, ETSI	Integration of NUIG contributions, review
1.00	30-09-2018	SINTEF	Final version released.

Table of contents

Figures

Tables

1. EXECUTIVE SUMMARY

1.1 Publishable summary

This is the initial report on standardisation for the Create-IoT project and builds input from the IoT European Large-Scale Pilots (LSPs). This report focuses on the use of standards by the LSPs, pre-normative activities and further standardisation opportunities based upon the gaps identified by the LSPs along with emerging new gaps. The content of this report derives from four workshops organised by the Activity Groups AG01 and AG02 set up to support efficient communication between the CREATE-IoT coordination and support action, and the LSPs, as well as a survey of the LSPs conducted in the Summer of 2018 and further information from the CREATE-IoT partners involved in Work Package 06 (WP06).

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 choices and possible strategies of the IoT Large-Scale Pilots (LSPs) regarding standardisation and pre-normative activities. The current status of standardisation in the LSPs – in particular in the LSP Use Cases under development – is examined, both in terms of standards support (which are the main standards used in support of the Use Cases implementation?) and standards gaps (what are the main missing elements that should be provided by standardisation?). Based on this, a detailed analysis is made in order to identify the generic (i.e. non sector-specific) standards that can be used not only by the LSPs, but also by other IoT systems development projects.

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, and in particular regarding the support they can get from the IoT community on pre-normative and standardisation to close the main gaps:

- The identification and description of the Use Cases selected by the LSPs;
- The identification of pre-normative activities of interest for the LSPs
- The selection of the main standards on which the LSP implementation will be based;
- The plans for the resolution of gaps, in particular through contributions to IoT standardisation
- The contributions to standardization generated by LSPs and CREATE-IoT partners.

2.2 Contributions of partners

This deliverable is the second deliverable of CREATE-IoT Task 06.02 ("Pre-normative and standardisation activities"). The list below shows the specific contribution of partners to the current deliverable.

ERCIM: As Task Leader and editor of the deliverable, ERCIM has contributed to the definition of the overall content and scope of the deliverable, to the collection and analysis of the information from the LSPs, to the analysis of standards gaps and promising pre-normative activities based on the Activity Group 02 Workshops, and to the review of the deliverable.
AS has contributed to support the interaction with and integration of multi-protocol frameworks and supports the standardization effort related to personal data protection, with a focus on ITU-T, ISO and IEC, and to the review of the deliverable.
ETSI has contributed to the definition of the overall content and scope of the deliverable, to the definition of the IoT Standards Framework, to the synthesis of the support standards based on the results of Activity Group 01 on Use Cases and on the Activity Group 02 Workshops, and to the review of the deliverable.
MI has provided a contribution to the CREATE-IoT WP06 survey, provided contributions to various sections of the document based on its involvement in one of the LSPs (e.g. SYNCHRONICITY), and to the review of the deliverable. MI continues to contribute to the standardization work of the International Telecommunication Union (ITU), the United Nations agency which also serves as one of the international standards developing organizations (SDOs). MI is involved in Study Group 20 on “IoT and Smart Cities and Communities” and ITU-T Focus Group on Data Processing and Management for Smart Cities and Communities.
NUIG provided contributions to various sections of the document based on its involvement in one of the LSPs (e.g. ACTIVAGE), and to the review of the deliverable.

SINTEF has contributed to the definition of the overall content and scope of the deliverable, provided contributions to various sections of the document based on its involvement in one of the LSPs (e.g. AUTOPILOT), and to the review of the deliverable.
TL contributed to the coordination of the pre-normative interoperability activities in LSPs, with an involvement in Activity Group 02. TL also reflected on its participation to activities in the area of active healthy ageing, smart cities and on security and privacy.

2.3 Relations to other activities in the project

The present document is one of the deliverables of CREATE-IoT Work Package 6 " IoT Interoperability and Standardization". WP06 is structured into two complementary tasks:

- Task 06.01 ("IoT Interoperability, standards approaches, validation and gap analysis") focuses on practical topics regarding the implementation of LSP Use Cases;
- Task 06.02 ("Pre-normative and standardisation activities") focuses on the contributions from the LSPs and CREATE-IoT to the IoT standards ecosystem. The present document is a deliverable of this task.

The present deliverable is a follow-up of Deliverable 06.06 "Strategy and coordination plan for IoT interoperability and pre-normative and standardisation activities" whose primary purpose is to outline the basic requirements for a common interoperability and standardisation strategy to be adopted by the IoT Large-Scale Pilots (LSPs). This deliverable is a basic, initial reference in defining and understanding the main issues regarding IoT interoperability and standards. It sets the scene for additional deliverables in WP06.

The present deliverable is complementary to deliverable D06.02 "Recommendations for commonalities and interoperability profiles of IoT platforms" (produced in Work Package 6 Task 06.01). Whereas the present deliverable focuses on standardisation aspects, D06.02 focuses on other interoperability aspects. Similarly, this deliverable is addressing some of the issues that are in the scope of WP05 ("IoT Policy Framework - Trusted, Safe and Legal Environment for IoT"). The requirements in terms of security as well as in terms of privacy – whose coverage will ensure trust and user acceptance - are key to the success of LSPs.

2.4 Information gathering process

This subsection explains the process used to gather information from the IoT European Large-Scale Pilots (LSPs). A significant part of the information was derived from the three workshops held by the IoT LSPs Activity Group 2 (IoT Standardisation, Architecture and Interoperability) in the first half of 2018 (on January 10th, April 26th and June 6th).

The objectives of these workshops were 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.

The workshops were supplemented by a survey and phone calls with Activity Group 02 representatives for each LSP. The survey questions were designed to gather detailed information about various aspects relating to standardisation.

More details about the LSPs use cases has been gathered by Activity Group 01 and are used in this report in respect to discussion on pre-normative activities and standardisation. In addition, help was sought from the CREATE-IoT project partners, a) to extend the survey data for the LSPs they are involved in, and b) to provide status summaries for relevant work in the standards development organisations and industry alliances the partners are involved in.

3. STANDARDISATION AND INTEROPERABILITY FRAMEWORK

3.1 Interoperability Framework

3.1.1 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 have been outlined in Deliverable D06.07 [i.1]. The main elements recalled below 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.

The scope of the present document is standards and pre-normative activities. Some of the elements below will only be briefly addressed or not addressed at all: more can be found in the associated deliverable D06.02 [2].

3.1.2 Reference Architecture (layers and cross layers)

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 [8] or ISO/IEC [9].

3.1.3 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 such as Scope and breadth, Maturity and ownership, and Standards support.

3.1.4 Standards support and Gaps

Standards are a key element in the IoT Interoperability Framework. A first requirement is to clearly outline the support offered by the current state-of-the-art in standardisation. Beyond this, it is also important to outline the gaps and overlaps (in particular the standards gaps and overlaps): the missing elements of the IoT landscape, mostly due to its complexity, that need to be identified before they may be resolved in the near future

3.1.5 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.

3.2 Standards and Interoperability

3.2.1 The key role of standards

As outlined in Deliverable 06.07 (see [1]):

> *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 is currently 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 and security.

Task 06.02 is focusing on providing recommendations on reference implementations and contributes to pre-normative activities, to standardization, both horizontally and vertically in various domains.

The recommendations on the reference implementation of promising IoT standards serving the interoperability and openness objectives will come from the coordinated consolidation of results obtained through standard implementation and pre- normative activities at the platform and/or pilot levels.

3.2.2 Importance of the Narrow Waist for IoT Standards

The huge potential for the IoT is being held back by fragmentation into incompatible platforms, standards and technologies.

The key to rectifying this is to identify where convergence on a small set of standards is necessary and where large diverse set of standards are beneficial. Figure 1 is taken from the bIoTope project's landscape of IoT standards (see [4]):

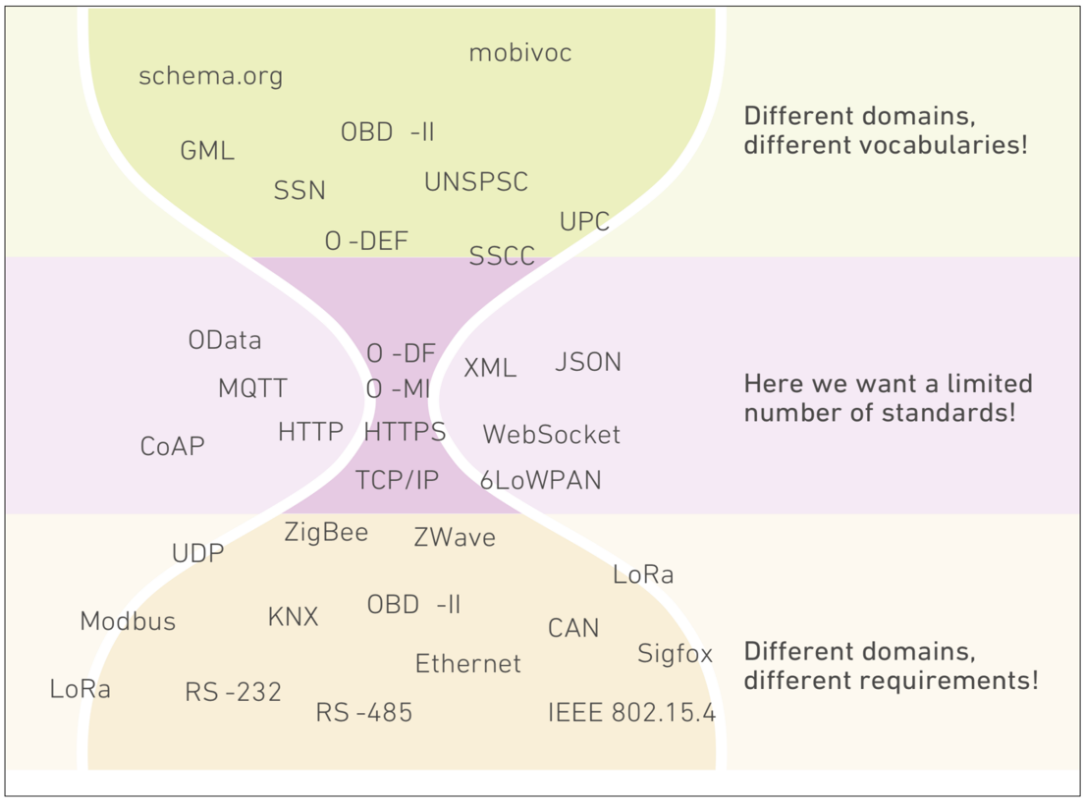

Figure 1: Narrow Waist for IoT Standards

This illustrates the concept of a narrow waist for the communication protocols that work across IP networks. It is important to note that interoperability relies on more than (for instance) just using HTTP or CoAP.

The Levels of Conceptual Interoperability Model (LCIM) is a conceptual framework for interoperability created in the context simulation and modeling to be used in determining potential for interoperability between systems.

LCIM defines six levels of interoperability: technical, syntactic, semantic, pragmatic, dynamic and conceptual interoperability [5][4].

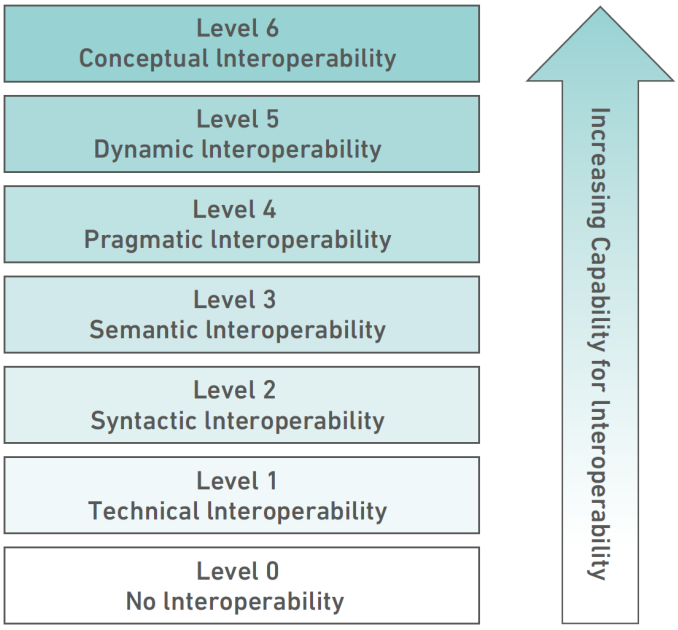

Figure 2: The Levels of Conceptual Interoperability Model [5]

A more IoT-specific classification is provided by ETSI and AIOTI [3] that propose to model this in terms of four layers:

- **Technical Interoperability**: usually associated with communication protocols and the infrastructure needed for those protocols to operate.
- **Syntactic Interoperability**: usually associated with data formats and encodings, e.g., XML, JSON and CSV along with techniques for compressing them.
- **Semantic Interoperability**: associated with shared understanding of the meaning of the exchanged content (information).
- **Organisational Interoperability**: associated with the ability of organisations to effectively communicate and transfer information even across different information systems, infrastructures or geographic regions and cultures.

3.3 Interoperability Layers

The next section reviews the requirements for these different layers in terms of what minimal set of standards are needed and how these will enable a healthy ecosystem of services. Further details will be given in section 5.3 "Emerging New Gaps".

3.3.1 Technical Interoperability

This layer is concerned with the communication technologies. At the network edge, IoT devices vary considerably in technical requirements, e.g. wired or wireless, short or long range, ambient, battery or mains powered, low or high data rates. As a result, a wide range of technologies are needed, and it is reasonable to expect a diversity of corresponding standards. A further consideration is how long the devices will be expected to operate and whether this is likely to introduce heterogeneity into the standards that will need be used. It may be likely that a given service will need to work with a mix of devices from different vendors and using different standards.

Away from the network edge, communications will be over IP networks and subject to weaker constraints on power and speed. Here we should expect to see just a few protocols being able to fulfil the requirements for the vast majority of use cases. Some protocols in common use include: CoAP, HTTP, WebSockets, MQTT and AMQP. A strong case can be made to encourage convergence on just HTTP and WebSockets over TLS (transport layer security).

CoAP is a datagram-based analogue of HTTP, but away from the network edge, there is little benefit to using a protocol intended for low power devices. MQTT is a pub-sub protocol layered on top of TCP/IP, with messages routed through brokers according to their message topic, and has been widely used for sensor data.

HTTP provides an effective alternative to MQTT. An HTTP client can push data to an HTTP server, e.g. in the cloud. There are then two approaches for efficiently pushing the data to applications that require it. One is for the application itself to expose an HTTP server as the target for HTTP POST requests that convey the data. This is covered by a W3C standard named *WebSub* [20]. The other approach is for applications to use a long polling mechanism for HTTP in which the server response is a stream of messages using the chunked transfer encoding (aka *Server Sent Events* [21]).

The Advanced Message Queuing Protocol (AMQP) offers reliable asynchronous delivery of messages routed by brokers according to the message topic, utilising message queues. HTTP can be used in place of AMQP with the appropriate messaging software that maintains the message queues and delivery guarantees. One example is Server-Sent Events, where clients can indicate which point in the message queue to resume from when restarting a stream after a loss of connection.

WebSockets is related to HTTP, and offers asynchronous two-way messaging, and is increasingly popular on the Web. WebSockets makes it easy for applications to define simple messaging protocols, avoiding the overhead of establishing an HTTP connection for each message. Interoperability would benefit from standardising a WebSocket subprotocol that provides a generic means to support digital shadows for sensors and actuators.

In summary, at the network edge the diversity of requirements justifies the range of IoT communications protocols, but away from the edge, we should be encouraging convergence on a much smaller set of protocols to minimise barriers to technical interoperability. HTTP is sufficient for the majority of use cases, but a case can be made for using WebSockets and AMQP when appropriate. Some recommendations for HTTP and WebSockets will be discussed in a later section.

3.3.2 Syntactic Interoperability

This layer is concerned with the data formats and encodings used for messages. Some popular text-based data formats include JSON and XML. This can be used with binary encodings for greater efficiency. CBOR [22] is a common binary encoding for JSON, and EXI [23] is a common binary encoding for XML. Binary encodings reduce message sizes and may be advantageous in high throughput situations such as when a cloud serve needs to handle a very large numbers of messages. Another common text-based data transfer format is comma separated values (CSV). There are other equivalent data formats and encodings, but there are clear benefits to converging on a small number that are widely supported.

Some use cases justify different formats, e.g. streaming audio and video. These are not considered further here apart from the desirability for using widely supported standards. One final thought is the potential for using encryption at high levels than transport layer security. This may be necessary when routing messages via brokers where you want to ensure that the broker doesn't have access to the data in the clear. A message may include several components that are individually encrypted for their different target clients.

3.3.3 Semantic Interoperability

This deals with agreement on the meaning of data amongst the parties involved, for example, that this numerical value is a temperature measurement in Celsius, and moreover is the temperature of a particular room in a building. Traditionally, the semantics of data has been implicit in the application code and associated documentation, including device standards. However, there are

considerable benefits from providing machine interpretable descriptions for the semantics. These include the ability to search for services based upon the kind of data they provide, the ability to validate data for increased robustness, and to create smart applications that can adapt to variations in data models and semantics.

Machine interpretable descriptions are applicable to different aspects of semantic interoperability, for example:

- Data models and data types
- Models that describe how to interact with things
- Frameworks for describing different versions of devices and software
- Semantic descriptions of things, e.g. a light, an air conditioner and so forth
- Semantic descriptions of the context, e.g. rooms in a building
- Privacy policies covering use of personal data
- Security policies, e.g. access control and security updates
- Smart contracts and terms & conditions

To minimise barriers for digital services that span different platforms, there is a strong need to encourage convergence on modelling frameworks and languages. Some relevant work includes:

- W3C's Web of Things which uses JSON-LD to describe things as object with properties, actions and events, using JSON Schema for describing the data types
- W3C's Resource Description Framework (RDF) using graphs with directed labelled arcs
- W3C's Web ontology language (OWL) and RDF Schema
- Chen's Entity Relationship Diagrams
- OMG's Unified Modelling Language (UML)
- Object-Role Modelling (ORM)

RDF and the Semantic Web were popularised by a seminal article by Tim Berners-Lee, Jim Hendler and Ora Lassila in the Scientific American in May 2001 [6]. RDF uses URIs for identifiers for nodes and arc labels. Recommended practice[1] is to use HTTP based URIs (i.e. URLs) and for these to be dereferenceable to further descriptions of the concept denoted by the identifier. In other words, you should be able use the HTTP GET method on the URL to access a description the concept. HTTP content negotiation can be used to request a human readable description (e.g. in HTML) or a machine interpretable serialisation of an RDF graph, e.g. Turtle or JSON-LD. A hybrid approach uses RDFa to embed RDF in HTML documents.

The current version of RDF is awkward when you want to annotate a particular arc. Use cases for doing so include the means to indicate the provenance, the data quality, a time interval the arc is valid for (start time, stop time), and so forth. Future work is planned on extending the RDF core semantics to make this simpler, and as such, to provide a framework for embracing Property Graphs[2] and making it easier to exchange models between different graph database platforms. Related work is looking at graph query languages and building bridges with work on SQL and relational databases. Another meme has been working on constraint languages for RDF graphs such as SHACL and ShEx. The Semantic Web focuses on deductive reasoning using description logics and the open world hypothesis. There is now growing interest in other forms of reasoning that are better suited to incomplete, uncertain and inconsistent knowledge, and instead of sound reasoning using formal deduction, are based upon what has been found to work in past experience. Examples include inductive reasoning from a set of examples, abductive reasoning that seeks consistent explanations for observations, analogical reasoning based on structural similarities with

[1] This essentially depends on the DNS registry of domain names whose stability reflect those of the organizations that own them. URN based schemes may offer greater longevity, depending on the stability of the means for resolving them. See also Digital Object Identifiers [24].

[2] One such proposal is called RDF* with implementations including Blazegraph and Amazon Neptune.

other situations, spatial and temporal reasoning, causal reasoning relating to plans, and social and emotional reasoning[3].

Many of these require a synthesis of symbolic and sub-symbolic or statistical techniques. People are starting to consider hybrid techniques combining artificial networks with symbolic approaches and allowing for continuous learning from relatively small sets of examples as compared to current deep learning algorithms. Inspiration may also come from work in Cognitive Science that combines graph representations, production rules and sub-symbolic approaches that mimic the operation of human cognition.

Projects should be encouraged to collaborate on re-use of shared vocabularies/ontologies[4] where practical, for example, vocabularies for expressing units of measure. To support this, we need frameworks for discovering existing vocabularies, for understanding the assumptions that underlay their design, and for access to best practices. In general, weakly coupled or independent communities can be expected to develop their own vocabularies with some overlap in semantics, but also some differences due to starting from differing requirements. Web-scale open markets of services will inevitably have to deal with such complications. This calls for work on standards for context sensitive rule languages for mapping data between such vocabularies. Some ontologies of interest to the LSPs include W3C's Semantic Sensor Network (SSN) ontology, and ETSI's SAREF family of ontologies. FIWARE's Context Information Manager (CIM), combines a RESTful interface, based upon HTTP and JSON, with vocabularies for describing things and their relationships. To seek greater harmonisation, we should encourage the AIOTI to play a stronger role in establishing a shared vision on vocabulary development across standards development organisations such as ETSI, W3C, oneM2M and OCF, as well as the Open Data Institute which focuses on community standards for open data with a particular emphasis on data sources provided by governments and cities.

3.3.4 Organisational Interoperability

Much of the current solutions for IoT focus on situations involving relatively few partners, and a dominant role for a particular platform and technology suite. This has resulted in ongoing fragmentation due to incompatibility across platforms from different vendors. To realise the huge transformative potential of the IoT, we will need convergence on standards that assist with the ability of organisations to effectively communicate and transfer information even across different information systems, infrastructures or geographic regions and cultures.

Standards are needed in respect to privacy and the management of personal information across organisational boundaries. The introduction of the General Data Protection Regulation (GDPR) is forcing organisations to rethink how they manage information across multiple systems within an enterprise, so that they can more easily track, update and delete information relating to a given person. Complications may arise when people change their online identity, or when organisations change their internal structure and information systems, or are subject to changes due to companies splitting, mergers and acquisitions, or being shut down and their assets sold off. Standards are likewise needed in respect to security and enabling end-to-end security across heterogeneous systems and organisational boundaries. There is an opportunity for new standards on security metadata that will permit reasoning about the security properties of compositions of services, as well as standards for security policies, vulnerability disclosures, security event notifications and so forth. To realise the full potential of the Internet of Things, we will need standards that enable open markets of services that bring together suppliers and consumers of services. This is discussed in more detail in section 5.3 "Emerging new gaps", along with opportunities for federated storage and compute services, and the role of distributed ledgers in respect to privacy, safety and smart contracts.

[3] Human reasoning is often influenced more by feelings and emotions than by facts.
[4] Vocabulary is an equivalent term to ontology and is often seen as more accessible.

4. STANDARDS IN LSP USE CASES

4.1 LSP Use Cases

All the LSPs have defined a number of Use Cases that are under development in a number of pilot sites. For the sake of information sharing, all these Use Cases have been gathered into a single source of information that present in a common template (as illustrated in Figure 3) the main elements of a given Use Case.

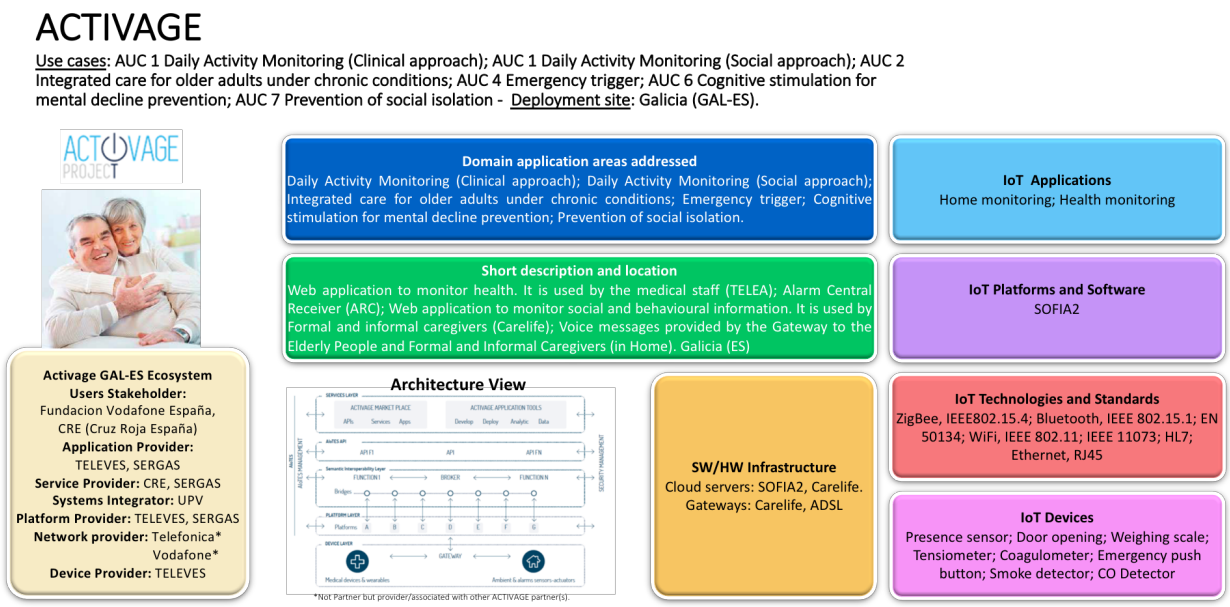

Figure 3: An example of LSP Use Case template

The above template gathers information related to the main elements of the IoT Interoperability Framework: Reference Architecture, Platforms, Devices and Standards. This section gathers the information related to the support of standards in each of the LSP.

This information is provided in tables with the following columns:

- Standard: short name of the identified standard;
- SDO: name of the Standards Development (SDO) or Standards Setting Organisation (SSO), sometimes also "Open Source" for generic components;
- #UC: number of Use Cases where the standard is used;
- G/S: is the standards Generic (i.e. cross-sector) or Specific (to the LSP sector).

4.2 Standard Support in the LSPs Use Cases

4.2.1 ACTIVAGE

4.2.1.1 Use Cases and Standards Support

ACTIVAGE has developed (and documented) 9 Use Cases. The standards in support of these Use Cases are listed in the table below in a form of summary table. ACTIVAGE has monitored and as possible participated on the different activities of standards working groups in the area of AHA and on the basis of IoT technologies (e.g. FIWARE, oneM2M) and the different Standardization bodies such as ETSI, IEEE, OMA, etc.

This section summarizes the initial results from ACTIVAGE in reference to the analysis of the standards ecosystem around AHA and IoT, at the same time that also making an inventory of the existing standards impacting the solutions developed within ACTIVAGE as show in Table 1.

Table 1: Standards Support in ACTIVAGE Use Cases

Standard	SDO/SSO	#UC	G/S
3GPP EDGE	3GPP	1	G
3GPP 3G	3GPP	2	G
3GPP 4G UMTS/HSPA, LTE	3GPP	3	G
3GPP2	3GPP2	1	G
ITU-T G.992 (ADSL)	ITU-T	1	G
Bluetooth 3.0 / 4.0 / 4.2	Bluetooth SIG, IEEE	6	G
CEN TC278 WG16 (Intelligent Transport Systems)	CEN	1	G
EN 300 220-1 (Electromagnetic compatibility)	ETSI	1	G
EN 50 134 (Social Alarms)	CENELEC	1	G/S
GPS	-	2	G
HL7 (Health Level Seven International)	HL7 International	1	S
IEEE 802.15.4 (Low Rate Wireless PAN)	IEEE	1	G
ISO/IEEE 11073 (Personal Health Data)	ISO/IEEE	1	S
ISO/IEC/IEEE 8802-3 (Ethernet)	ISO/IEC/IEEE	4	G
ISO/IEC 14443 (Identification Cards)	ISO/IEC	1	G
ISO 11898 (CAN Bus)	ISO	1	G
ISO TC204 WG 18 (Intelligent Transport Systems)	ISO	1	G
MQTT	Open Source	1	G
NFC / NDEF	NFC Forum, ISO/IEC	2	G
PLC/Modbus	-	1	G
SIP	IETF	1	G
USB 2.1	-	1	G
VDE 0834/ESPA-X (Call functions)	VDE	1	S
Wi-Fi (IEEE 802.11)	IEEE	4	G
Z-wave (Home Automation)	-	3	G
ZigBee	ZigBee Alliance	1	G

4.2.1.2 Comments

This section describes the specific actions that have been carried out during the eighteen months of the project, but also the initial set of compromises into a set of assets such as whitepapers for IEEE and Specific Group Documents for ETSI. The main areas that ACTIVAGE will focus for standardization are:

- Data Privacy and data management strategy and guidelines.
- Interoperability / Platforms Federation as part of the AIOTES valorisation.
- Large Scale deployment guidelines using IoT and Internet technologies.
- Integration of wearables and personal devices (SmartBAN)
- Guidelines and best practices based on the ACTIVAGE pilot experiences.

These different areas will be addressed through different standardization bodies and alliances such as ETSI, IEEE, AIOTI etc. The following subsections present in details the opportunities in each one of these bodies and the level of engagement from ACTIVAGE consortium. For this purpose, first a survey to all the partners has been carried out in order to understand the standards ecosystem

that they are part of, they are interested in and they will be able to engage / contribute. This initial survey has been used to identify what the initial assumptions are about the areas with lack of standards and/or inadequacy of current available standards that we could approach from ACTIVAGE activities.

The standardisation activities of ACTIVAGE are mainly focused on three areas:

- Protection of privacy, security, health and safety of users, since the healthcare orientation of the AIoTES dictates the strictest requirements. The European Directives and data protection standards (Opinion 2/2013 of the ArtXe 29 Working Party of 27 February 2013 on apps on smart devices, etc.) as well as the U.S. HIPAA will be the main references in this direction.
- Interoperability and data management into the IoT platforms, where a strong cooperation of AIoTES with FIWARE, oneM2M, IoT-EPI, AIOTI and other platforms will be carried out, in addition to benefiting from a variety of platforms already being used by the deployment site, such as SOFIA2 and universAAL.
- Deployment and maintenance of LSPs, managing sensitive data, with a special focus on device management in bodies, such as OMA and ETSI IP6.

ACTIVAGE is very much involved on analysing the opportunities to establish new ETSI Industrial Specification Groups (ISGs), contribute to existing ETSI ISGs related to IoT and LSPs, propose new standards and/or contribute to the existing ones; identify the key priority areas for ACTIVAGE. It is remarkable that ACTIVAGE has presented an ecosystem with a high engagement in this initial stage with 34 inputs about the different activities in the top relevant bodies around the world.

4.2.2 AUTOPILOT

4.2.2.1 Use Cases and Standards Support

AUTOPILOT has developed (and documented) 14 Use Cases. The standards in support of these Use Cases are listed in the table below.

Table 2: Standards Support in AUTOPILOT Use Cases

Standard	SDO/SSO	#UC	G/S
3GPP 3G	3GPP	8	G
3GPP 4G	3GPP	9	G
3GPP 4G LTE-V2X	3GPP	4	G
3GPP 4G NB-IoT	3GPP	1	G
6LowPAN	IETF	5	G
Bluetooth	Bluetooth SIG, IEEE	4	G
CAM (Cooperative Awareness Message)	Open Source, ETSI	6	S
CAN Bus (ISO 11898)	ISO	4	S
CoAP (Constrained Application Protocol)	IETF	3	G
DATEX (Exchange of traffic related data)	CEDR	1	S
DDS (Data Distribution Service)	OMG	2	G
DENM (Decentralized Environm. Notificat. Message)	Open Source, ETSI	6	S
GPS	-	6	G
HTTP/S	W3C	5	G
IEEE 802.15.4 (Low Rate Wireless PAN)	IEEE	2	G
ITS-G5 (ad-hoc V2V communications at 5,9 GHz)	ETSI	9	S
LDM (Local Dynamic Maps, ISO/TS 18750:2015)	ISO	2	G/S
MQTT	Open Source	3	G

oneM2M	oneM2M	13	G
SPAT / MAP (Signal Phase and Time)	ETSI	4	G
USB 2.0	-	2	G
Wi-Fi (IEEE 802.11)	IEEE	4	G

4.2.2.2 Comments

The standardisation activity is an essential part of the AUTOPILOT project strategy. Automated driving solutions require future proof decisions and addressing many issues such as interoperability between systems, security aspects, the IoT ecosystem and applications. The project finalized a Standardisation plan in May 2017 [17].

This derivable document includes the initial standardization plan approach/methodology, the main applicable standards in the IoT and ITS domain that shall be considered in the project architectural framework/design choices, a preliminary standard gaps analysis and a first selection of standards under development of interest for the AUTOPILOT standardisation activity.

The analysis has been performed based on the competence and the experience the partners developed in the different knowledge areas and through the Standard Development Organization (SDO) participations concerning the AUTOPILOT areas of interest [17].

In addition, two standards organizations overview documents were used in the analysis phase; "IoT LSP Standard Framework Concepts" by AIOTI [18] and "SmartM2M; IoT Standards landscape and future evolutions" by ETSI [19].

4.2.3 IoF2020

4.2.3.1 Use Cases and Standards Support

IoF2020 has developed (and documented) 19 Use Cases. The standards in support of these Use Cases are listed in the table below.

Table 3: Standards Support in IoF2020 Use Cases

Standard	SDO/SSO	#UC	G/S
365 FarmNet	-	1	S
3GPP GSM	3GPP	1	G
3GPP 3G	3GPP	2	G
3GPP 4G	3GPP	1	G
6LowPAN	IETF	2	G
ADAPT (AG Data Application Programming Toolkit)	Open Source	1	S
ADLS 2 (ITU-T G.992.3)	ITU-T	1	G
Bluetooth LE	Bluetooth SIG, IEEE	3	G
CoRE (Constrained RESTful Environments)	IETF	1	G
EFDI (Extended Farm Managmt. Information Syst.)	AEF	1	S
FMIS (Farm management Information System)	AEF	1	S
GPS	-	2	G
HTTP/S	W3C	8	G
I2C (Inter-Integrated Circuit)	-	1	G
ISO/IEC/IEEE 8802-3 (Ethernet)	ISO/IEC/IEEE	3	G
ISOBUS (ISO 11 783)	ISO/AEF	1	G
JSON (JavaScript Object Notation)	IETF	2	G
LLRP (Low Level Reader Protocol)	GS1	1	G

LoRa	LoRa Alliance	4	G
LWM2M (OMA Lightweight M2M)	OMA	1	G
MODBUS	MODBUS Organisa.	1	G
MQTT	Open Source	5	G
NFC (Near-Field Communication)	NFC Forum	1	G
NGSI (Next Generation Service Interface)	OMA, FIWARE	4	G
NTAG213	NFC Forum	1	G
OAuth v2	IETF	1	G
QR Code (ISO/IEC 18004)	ISO/IEC	1	G
REST (Representational State Transfer)	W3C	1	G
RFID (Radio Frequency IDentification)	ISO	1	G
RS-232	EIA	1	G
RS-485	EIA	1	G
SDI-12 (Serial Digital Interface at 1200 baud)	SDI-12 Supp. Group	2	G
SigFox	-	3	-
SOAP (Simple Object Access Protocol)	W3C	1	G
SPI (Serial Peripheral Interface)	-	1	G
SQL (Structured Query Language)	ISO	2	G
Sub-1Ghz (IEEE 802.15.4 Low Rate Wireless PAN)	IEEE	1	G
TLS (Transport Layer Security)	IETF	1	G
USB	-	1	G
Wi-Fi (IEEE 802.11)	IEEE	5	G
XML (Extensible Markup Language)	ISO	1	G
XMPP (Extensible Messaging & Presence Protocol)	XMPP-IoT	2	G
ZigBee	ZigBee Alliance	1	G

4.2.3.2 Comments

The adoption of standards in IoF2020 is of major importance. All Use Cases were requested to identify standards being used in several aspects of the Use Case.

The majority of Use Cases identified the connectivity standards that are being used by each one.

Being an IoT project, the choices about connectivity were maybe the most relevant technology choices made within the use cases from a project perspective.

It was studied which connectivity standards and protocols are used in the different use cases.

The connectivity protocols that we have observed throughout the IoF2020 project roughly fall into 3 categories:

- General purpose connectivity protocols - Although the internet of things has spawned a number of innovations in the area of networking, existing general-purpose networking standards are still widely used too. Examples are Wi-Fi, conventional cellular communications, ethernet, and, often in the context of machines and equipment, serial interfaces.
- IoT-specific connectivity protocol - In the context of the internet of things, a number of standards have been developed that combine long range with low power consumption. They are most frequently referred to as Low Power Wide Area Networks (LPWAN). Best known examples are LoRa and Sigfox, but also some specialized parts of the 4G and 5G cellular standards have similar properties. The low power consumption combined with long range is typically part of a trade-off: these standards support (very) low bandwidths. For example: LoRa gateways are claimed to have a range of tens of kilometres in the open field and can support

thousands of nodes per gateway. But a typical LoRa node is only allowed to send the equivalent of 100-200 text messages per day.

- Short range, low energy standards - Another class of standards supports short range connectivity in the tens to sometimes hundreds of meters. Examples of such standards are Bluetooth Low Energy (BLE) and a number of variants of the Low Rate Wireless Personal Area Network (LR-WPAN) protocol, such as Zigbee. The best-known examples of BLE are the beacon standards of Google and Apple respectively. The LR-WPAN family often support mesh-type networking across the different nodes to extend the range in which nodes can collaborate and communicate.

4.2.4 MONICA

4.2.4.1 Use Cases and Standards Support

MONICA has developed (and documented) the following 4 Use Case Groups, namely:
#1 - Sound Monitoring and Control
#2 - Crowd and Capacity Monitoring and Management
#3 - Missing Persons/Locate Staff Members
#4 - Health/Security Incidents

The standards in support of these Use Cases groups are listed in the table below.

Table 4: Standards Support in MONICA Use Cases

Standard	SDO/SSO	#UC	G/S
ETSI EN 300 220-2 V3.1.1 (2017-02) for the Crowd Wristbands operating in the frequency range 865 – 868 MHz	ETSI	2-4	S
ETSI EN 302 065-2 V2.1.1 (2016-11) for the Staff Wristbands using Ultra Wide Band technology (UWB) in the band 3.4 – 3.8 GHz	ETSI	2-4	S
Bluetooth LE	Bluetooth SIG, IEEE	3, 4	G
Wi-Fi (IEEE 802.11)	IEEE	1-4	G
NFC (Near-Field Communication)	NFC Forum	2, 3	G
RFID (Radio Frequency Identification)	ISO	2-4	G
LoRa	LoRa Alliance	3	G
OGC SensorThings API	OGC	1-4	G
MQTT	Open Source	1-4	G
oneM2M	oneM2M	1-4	G
IEEE 802.15.4 Low Rate Wireless PAN	IEEE	1	G
IETF 6LoWPAN	IETF	1, 2	G
IETF ROLL	IETF	1, 2	G
IETF CoAP	IETF	1, 2	G
ETSI SAREF	ETSI	1-4	G
REST (Representational State Transfer)	W3C	1-4	G

4.2.4.2 Comments

OGC Sensor Things API and oneM2M are the two most widely adopted standards in MONICA.

The defined “MONICA data model”, based on the OGC standard, together with a very well documented set of APIs allowed MONICA to provide an open and unified way to interconnect devices over the Web as well as interfaces to analyse the collection of observations.

The OCG standard is also supported by specific server implementations, so that also services such as resource/service catalogues and historical data storage are provided.

Currently, MONICA is using a Go implementation of OGC called GOST.

The OGC standard is split into two parts:

- Part1: "Sensing" was released in 2016 and allowed management and reception of observations or measurements made by IoT sensors.
- Part2: "Tasking Core" provides a mechanism to tell the sensor/actuator what to do.

Since Part2 was officially released in early months of 2018, initially MONICA identified this gap regarding the support of actuation messages, where device actions are triggered by commands sent through the platform. Now this gap was filled with Part2 of the standard issued in 2018.

Moreover, MONICA integrates the oneM2M interfaces (Mca and Mcc/Mcc') allowing the platform to expose the IoT data according to the oneM2M standard.

The oneM2M module is also used to integrate data coming external IoT platform like the Hamburg Smart City one.

Concerning the wearables, the following two ETSI standards have been taking into account for the two types of wristbands:

- ETSI EN 300 220-2 V3.1.1 (2017-02) for the **Crowd Wristbands**, Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; (865 – 868 MHz)
- ETSI EN 302 065-2 V2.1.1 (2016-11) for the **Staff Wristbands**, Short Range Devices (SRD) using Ultra Wide Band technology (UWB) in the band 3.4 – 3.8 GHz

MONICA identified a need for a new spectrum optimized IoT radio standard that may be a "Streaming Optimized" RF link with flow control etc.

There could be off-load connections to sensors of all kinds delivering time sensitive streaming information. This aspect will be further studied by MONICA in liaison with ETSI.

It is also important to report that if non-compliant devices are demonstrated then Art. 9.2 of the RED 2014/53/EU safeguards the regulator that such devices are not brought outside the pilot area.

4.2.5 SYNCHRONICITY

4.2.5.1 Use Cases and Standards Support

SYNCHRONICITY has developed (and documented) 6 Use Cases. The standards in support of these Use Cases are listed in the table below.

Table 5: Standards Support in SYNCHRONICITY Use Cases

Standard	SDO/SSO	#UC	G/S
FIESTA (FIESTA-IoT Semantics Library)	EU FIESTA	1	G
GTFS (General Transit Feed Information)	-	1	S
Hypercat (hypermedia catalogue format)	Hypercat	1	G
MQTT	Open Source	3	G
NGSI	ETSI	5	G
OASC (Principles and data model)	OASC	5	S
OAuth v2	IETF	5	G
ODF (Open Document Format)	ISO	1	G
OpenTripPlanner (Multimodal Trip Planning)	Open Source	1	S

Other standards being developed in relation to the work conducted for SYNCRONICITY.

Table 6: Other related standards

Standard	SDO/SSO	Partner involved
Draft Recommendation on Open Data Application Programming Interface for IoT Data in Smart Cities and Communities	ITU-T SG20	MI
Draft Technical Report Unlocking Internet of Things with Artificial Intelligence: Where we are and where we could be	ITU-T SG20	MI
Draft Technical Report "Data Processing and Management Framework for Data-driven IoT and Smart Cities and Communities"	ITU-T (FG-DPM)	MI, AS, TL
Draft Technical Report "Data Processing and Management Functional Architecture"	ITU-T (FG-DPM)	MI, AS

4.2.5.2 Comments

MI and AS are extensively involved in the pre-standardization activities of the ITU, which is attended by representatives from 193-member states along with private sector members in the ICT domain. including the Focus Group on Data Processing and Management. Within this Focus Group, MI and AS are spearheading the development of over 4 deliverables relating to IoT and Data Management. These deliverables will be subsequently submitted to the standardization group for smart cities known as the Study Group 20 on IoT and Smart Cities and Communities, for their approval as international standards on the topic.

More recently, MI has also made in-roads into the work of ITU-T Study Group 13 on "Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures" on behalf of CREATE-IoT. The current draft standards, MI and AS are collaborating on at ITU are expected to be finalized by December 2018. MI and AS further intend to contribute to the new Focus Group on "Machine Learning for Future Networks including 5G".

5. GENERIC STANDARDS ACROSS THE LSPS

This report focuses on the role of standards which are applicable across multiple use cases and application domains. There will of course be a requirement for use case specific standards, but even these will often fit into a generic framework. An example is use case specific data models for smart city services. Having a standard for these data models avoids the need to develop different applications for different cities, lowering costs and encouraging innovation. The data models can be expressed in a generic framework and the corresponding data accessed using generic protocols.

The following sections review the usage of standards by the LSPs at different layers in the IoT architecture along with the gaps that each LSP has identified. The traditional IoT architecture layers are good for some purposes but not for others. Section 5.3 therefore considers different architectural viewpoints with a look at challenges and opportunities for new standards that are key to realising the potential for open markets of services.

Whilst CREATE-IoT focuses on coordination and support for the IoT European Large-Scale Pilots, it would be remiss to ignore work in related areas that have a large potential bearing on the transformative effects of IoT for European prosperity. This report therefore includes a look at the activities of related public private partnerships in the areas of big data, cybersecurity, robotics cloud computing and AI.

5.1 Standards Support across LSPs

The standards in support of the LSPs Use Cases listed in section 4 could be specific (to the sector in which the LSP operates) or generic, i.e. potentially usable in all LSP sectors. The current section focuses on the generic standards, those that could be used in support of the design and development of future IoT systems.

Table 7: Standards Supported across at least 3 LSPs

Standard	SDO/SSO	ACTIVAGE	AUTOPILOT	IoF2020	MONICA	SYNCHRONICITY
3GPP 3G	3GPP	X	X	X		
3GPP 4G UMTS/HSPA, LTE	3GPP	X	X	X		
Bluetooth	Bluetooth SIG, IEEE	X	X	X	X	
GPS	-	X	X	X		
HTTP/S	W3C		X	X		
IEEE 802.15.4 (Low Rate Wireless PAN)	IEEE	X	X	X		
MQTT	Open Source	X	X	X	X	X
NFC (Near-Field Communication)	NFC Forum	X		X	X	
RFID (Radio Frequency IDentification)	ISO					
USB	-	X	X	X		
Wi-Fi (IEEE 802.11)	IEEE	X	X		X	

The following observations can be made on the generic standards identified in section 4:

- The vast majority of identified standards is supporting only one LSP and, in most cases, a relatively low number of the Use Cases of a given LSP. This is probably reflecting the importance of the legacy systems in which the LSP Use Cases are deployed;
- A large part of the identified standards falls into two categories:
  - Standards for communications and,
  - Standards for (the definition of) data models;
- Very few standards relate to security, with only one being used by two LSP (i.e. OAuth v2), and some LSPs mentioning no such standards at all;
- No standards related to security have been identified, not even from a methodology standpoint. The "privacy gap" previously identified is still wide-open.

Table 7 is listing the generic standards that have been identified in section 4 by at least 3 LSPs. This can be seen as a measure of the wide applicability of such standards to a variety of IoT systems.

A few observations can be made:

- There is a relatively small number of such standards (or family of standards);
- They address various layers of the IoT stack and, for the large part, are focusing on communications;
- Some are not proper standards but rather "de facto" standards (e.g., GPS);
- Some are actually Open Source Software (OSS) solutions (e.g., MQTT) indicating the emerging role of OSS (and probably of microservices-based architectures);
- No standards related to privacy or security.

Table 8 is listing the generic standards that have been identified in section 4 by 2 LSPs.

Table 8: Standards Supported across two LSPs

Standard	SDO/SSO	ACTIVAGE	AUTOPILOT	IoF2020	MONICA	SYNCHRONICITY
6LowPAN	IETF		X	X		
CAN Bus (ISO 11898)	ISO	X	X			
HTTP/S	W3C		X	X		
ISO/IEC/IEEE 8802-3 (Ethernet)	ISO/IEC/IEEE	X		X		
NGSI (Next Generation Service Interface)	OMA, ETSI			X		X
OAuth v2	IETF			X		X
RFID (Radio Frequency IDentification)	ISO			X	X	
ZigBee	ZigBee Alliance	X		X		

Just as in the case of standards in Table 7, there is a small number of standards supporting two LSPs and they are, for the large part, focusing on communications.

5.2 Cross LSPs – Standards Gaps and Issues

5.2.1 Security

There are widely acknowledged concerns around standards for IoT security, e.g. Olaf Kolkman, chief internet officer at the Internet Society, attributes the lack of a global IoT security standard to

differing security requirements across industries [25]. He notes "The plethora of security standards and technologies being used to secure the internet of things (IoT) today could make it difficult for a global IoT standard to emerge." In the news article, Kolkman says "the Internet Society has reached out to policy makers to provide recommendations about what they can do, such as setting minimum standards of IoT security and accountability. We advise them to work with stakeholders, such as the Consumer Technology Association, to come up with solutions and certifications that have buy-in from government and industry," adding that liability laws will also ensure all players in the IoT market have skin in the game. In the USA, NIST has published a recent study: "Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)", February 2018 [26]. This report considers security standards across five application areas:

- Connected vehicles IoT enables vehicles, roads, and other infrastructure to communicate and share vital transportation information
- Consumer IoT in the home, including wearables and mobile devices
- Health IoT including electronic health records and patient generated health data
- Smart building IoT, including energy usage, physical access and lighting
- Smart manufacturing IoT, e.g. enterprise-wide integration of data, technology, advanced manufacturing capabilities, and cloud and other services.

The Report's conclusions focus upon the issue of standards gaps and the effective use of existing standards. The gaps include: the application of cryptographic techniques (e.g. blockchains), cyber incident management, hardware assurance, information security management systems, network security, software assurance, security automation and continuous monitoring, supply chain risk management and system security engineering.

5.2.2 Progress on Identified Gaps

5.2.2.1 Security

This subsection introduces organisations that are addressing IoT security challenges but should not be considered as a comprehensive list.

The Embedded Microprocessor Benchmark Consortium (EEMBC) [27] have developed a benchmark suite named IoT-Secure that is aimed at testing and analysing various security profiles that should be implemented in IoT devices.

The GSMA has published a suite of guidelines for IoT Security [28]:
- GSMA IoT Security Guidelines
- IoT Security Self-Assessment
- IoT Security Guidelines for Network Operators
- IoT Security Guidelines for Endpoint Ecosystem
- IoT Security Guidelines for Service Ecosystem

The International Electrotechnical Commission (IEC) has published related white papers:

- White Paper IoT 2020: Smart and secure IoT platform [29]
- White Paper Internet of Things: Wireless Sensor Networks [30]

The IoT Security Foundation has several active groups as of July 2018 [31]:
- IoT Certification
- Best Practice Guides
- Compliance Validation and Test
- Vulnerability Disclosure Guidance
- IoT Security Landscape
- Smart Buildings

- IoT Security Trust Mark

The EU Agency for Network and Information Security (ENISA) have published a study on "Baseline Security Recommendations for the Internet of Things in the context of critical information infrastructures" [32].

The European Cyber Security Organisation (ECSO) represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership. It covers the following areas of interest:

- ICT Infrastructure (including cloud, mobile, networks, etc.)
- Smart Grids (Energy)
- Transportation (including Automotive / Electrical Vehicles)
- Smart Buildings and Smart Cities
- Industrial Control Systems (Industry 4.0)
- Public Administration and Open Government
- Healthcare
- Finance and Insurance

ESCO Working Group 1 covers standardisation, certification, labelling and supply chain management.

The Internet Engineering Task Force (IETF) is responsible for the core standards for the Internet. Some IoT Security relevant groups include:

- The DTLS In Constrained Environments (DICE) WG produced a TLS/DTLS profile that is suitable for constrained IoT devices.
- The Authentication and Authorization for Constrained Environments (ACE) WG is working on authenticated authorization mechanisms for accessing resources hosted on servers in constrained environments.
- This work is supported by the chartered COSE WG that is building simplified CBOR analogues for the JSON object signing and encryption methods that were developed in the JOSE WG.
- The Web Authorization Protocol (OAuth) WG. This protocol allows a user to grant a third-party web site or application access to the user's protected resources, without necessarily revealing their long-term credentials, or even their identity.

The Open Connectivity Foundation (OCF) Security Working Group is working on identity and confidentiality of IoT devices as well as making devices more laborious to compromise. This includes work on a public key infrastructure (PKI) that allows centralized management of devices and grants interoperability for certificates that are issued by individual manufacturers.

ETSI is working on various aspects of IoT Security, such as electronic signatures, lawful interception, security algorithms and smart cards as well as cyber security.

oneM2M is working on security as part of a suite of standards for machine to machine communication. This covers authentication, encryption, integrity verification, including support for secure device management.

The World Wide Web Consortium (W3C) is working on security guidelines and standardised security metadata for the Web of Things, an object-oriented abstraction layer for the IoT based upon W3C's framework for Linked Data.

5.3 Emerging New Gaps

5.3.1 Big Data standardisation activities

The deployment of the IoT is expected to lead to staggering amounts of data. For example, IDC has predicted a growth from 1.5 Zeta Bytes of data in 2013 to 18 ZB in 2018. This is being driven

by market growth in connected objects. Gartner, for instance, in 2015 predicted a market growth of connected objects from 6.4 billion in 2016 to 20.8 billion in 2020. There is thus a clear case for coordination between work on IoT and work on Big Data, and an effective path for this through the corresponding EU public-private partnership organisations: The Alliance for Internet of Things Innovation (AIOTI) and the Big Data Value Association (BDVA).

The BDVA Strategic Research and Innovation Agenda (v4) states in relation to standardisation:

> *Standardisation is a fundamental pillar in the construction of a Digital Single Market and Data Economy. It is only through the use of standards that the requirements of interconnectivity and interoperability can be assured in an ICT-centric economy.*

It further notes the need to leverage common standards as the basis for an open and successful Big Data market, along with supporting Standards Development Organisations (SDOs), such as ETSI, CEN- CENELEC, ISO, IEC, W3C, ITU-T and IEEE, by making experts available for all aspects of Big Data in the standardisation process. Standardisation is needed for both the technology and the data. For CREATE-IoT, the standardisation strategy should consider how to encourage a shared vision for IoT and Big Data, and an exchange of information on standardisation gaps between AIOTI and BDVA.

5.3.2 Artificial Intelligence (AI)

AI includes some powerful techniques to identifying patterns across very large amounts of data that would be impractical to analyse in other ways. Processing data for IoT is a very good fit for AI based algorithms such as deep learning that rely on large data sets, provided that the characteristics of the data remain similar to the data used for training purposes. The open question is what kinds of standards are needed to support AI and IoT.

5.3.3 Security and Trust

With the emergence of open markets of services and an increased focus on cybersecurity, we can expect to see increased interest in standards that support security, e.g. standard ontologies for security metadata, standards for signalling security events and disclosing vulnerabilities, standards for logs as a basis for re-use of automated analysis tools, standards for security policies and standards around authentication, and authorisation.

Trust is an important topic, e.g. mechanisms for bootstrapping trust when installing a device or service, and after a change of context. Examples include a transfer of ownership when a personal device is sold or given to another person, a change in the company that provides security support for a device (i.e. security updates), or a change to the company that hosts a cloud-based service using the device. Similar examples apply to commercial applications, e.g. when an office building is sold from one company to another, where the building is fitted out with a variety of IoT systems. A related example is where office or factory machinery is paid for on a per use basis rather than with a flat fee. The security and trust setup needs to be re-run for each new client and likewise decommissioned when a given client is done with the machinery.

Trust is also important for open markets of digital services where suppliers and consumers need a way to establish trust. One approach is via attestations by a mutually trusted third party that has a solid reputation for the quality of its vetting processes. Such third parties act as identity brokers, associating given identifiers with particular attestations or claims.

This relates to requirements for smart contracts including, legal jurisdiction, applicable regulatory frameworks, e.g. GDPR for privacy, and obligations in respect to liability. Some relevant work includes: W3C's Verifiable Claims Working Group aims to make expressing and exchanging credentials that have been verified by a third party easier and more secure on the Web.

Of potential relevance is work on trust service principles and criteria by American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) [33].

Table 9: Definition of Terms

Term	Definition
Security	The system is protected against unauthorized access (both physical and logical).
Availability	The system is available for operation and use as committed or agreed.
Processing Integrity	System processing is complete, accurate, timely, and authorized.
Online Privacy	Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
Confidentiality	Information designated as confidential is protected as committed or agreed.

5.3.4 Open Market of Services

Today, IoT services tend to involve a prearranged contract between known partners. To realise the full potential of the IoT we need to open this up to a free market for suppliers and consumers of services. An example is for smart cities, where the city provides a variety of datasets and makes them available to anyone who wants to use the data to create a service for others to use. An open market requires a means for suppliers to offer services, and for would be consumers to discover available services and enter into agreements with suppliers on terms and conditions covering data licensing and other details.

A distinction can be made between centralised and distributed marketplaces. A centralised marketplace involves a marketplace operator that hosts a directory of services. A distributed marketplace involves the means for service providers to advertise their services on websites, blogs, and social media. Search engines index websites to allow people to discover sites relating to their search terms. Richer search results are possible through using standards for annotating web sites, e.g. as defined by schema.org. End users of services may be able to install applications on their smart phones, tablets, and desktop/laptop computers. A further opportunity is to install services on a home hub/gateway or a cloud-based service platform.

Open standards for centralised and distributed marketplaces would help to boost growth of ecosystems of IoT services by reducing barriers to entry. Further work is needed to identify specific opportunities where there is a good chance for stakeholders to reach agreements on new standards. This needs to work alongside regulatory requirements which vary from one domain to another, for example GDPR in respect to the handling of personal data.

5.3.5 Shared Ledgers

Ledgers are books used to keep records of business activities and monies received or paid. Computers gave rise to digital ledgers, which are now central to everyday business. Until recently every business unit needed to maintain its own ledger with costly synchronisation mechanisms for cross unit transactions. The advent of blockchain networks has now made it possible for organisations to use shared ledgers with greatly reduced transaction times and costs as well as tighter security. If a blockchain network is permissioned, it is limited to a set of members with proof that the members are who they say they are, and that transactions are exactly as represented.

Shared ledgers based upon blockchain networks offer the following key characteristics [34]:

- **Consensus**: for a transaction to be valid, all participants must agree on its validity
- **Provenance**: participants know where the asset came from and how its ownership has changed over time
- **Immutability**: no participant can tamper with a transaction after it's been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible
- **Finality**: a single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction

There are variety of opportunities for shared ledgers, including:

- **Privacy**: operations on personal data can be recorded as transactions in a shared ledger. This includes the deletion of personal data in conformance with exercising the right to be forgotten. The record of the transactions is immutable – of course this means that the personal data itself needs to be held elsewhere, e.g. in a trusted federated storage solution (see next section). A permissioned shared ledger and federated storage solution can be used across partners in an ecosystem of services.
- **Digital object memories**: i.e. an immutable record of operations on physical objects that are shadowed by a digital twin. Examples include service histories for machinery, records of their use, e.g. the distance a vehicle has been driven, logs of sensor readings, and so forth. This is applicable to payments, regulatory requirements, liability, and safety, e.g. food safety across supply chains and safety critical components such as jet engines.
- **Smart Contracts**: digital records of contracts and associated payments between suppliers and consumers in open markets of services

Further is needed to identify opportunities for specific standards relating to the use of shared ledgers for the IoT.

5.3.6 Federated Storage, Analytics and Edge Computing

The very large numbers of IoT devices anticipated within a few years will provide a vast amount of information that risks overwhelming centralised approaches to storage, analytics and device management. Open standards are needed to provide a common approach across vendors for interoperable federated solutions.

The volume and rate of streaming data can be reduced through implementing analytics at or near the network edge. This may necessitate spatiotemporal sensor-data analysis and summarisation across sensors and over time. A related technique seeks to identify events from sensor data and context information, and this may feed into a hierarchy of progressively higher-level analysis. This in turn creates requirements for managing the data, algorithms and devices across a system of systems.

Federated approaches to storage are likewise important for scalability and robustness. Devices at the network edge may be constrained in how much data they can hold. At the same time data buffering and batched transmission may be important for network efficiency, as well as for prolonged battery life for battery operated devices. One approach is for each entity to host its own data, but it may be more cost effective to delegate storage to a federated storage solution that manages data on behalf of multiple entities. In principle federated storage could be operated by multiple companies for a solution that scales to extremely large amounts of data. Such an infrastructure needs to be secure and resilient in respect to faults, cyber-attacks and rapidly changing loads.

A further consideration is to support efficient processing against very large datasets. For instance, Apache Hadoop [35], which is an open source collection of tools for using a network of computers to solve problems, involving massive amounts of data and computation, based upon the MapReduce algorithm together with a distributed file system.

Another example is provided by the International Data Spaces Association [36], previously referred to as the Industrial Data Space. This can be used to create a virtual data space that supports the secure exchange and simple linking of data in business ecosystems on the basis of standards and by using collaborative governance models.

Other work goes under the term “federated database systems” which involves a meta-database management system which transparently maps multiple autonomous databases into a single federated database [37]. This is related to the emergence of enterprise knowledge graphs for enterprise-wide metadata describing data and resources throughout an enterprise, and a key component for enterprise-wide approach to data management and governance.

6. CONCLUSIONS AND FUTURE WORK

6.1 Early lessons learned

Although the application domains and associated standards vary considerable across the LSPs, there are some points in common where cross-domain standards are clearly important. These include security, protocols, data formats and encodings, and frameworks for semantic interoperability. Interoperability is easier at the higher levels that abstract away from the diversity of IoT technologies. Open markets of services will be facilitated by a convergence on a small set of Internet protocols away from the network edge, along with standard formats and shared vocabularies for metadata, including terms and conditions for data licensing. Other commonalities related to the need for a federated approach to analytics and storage in order to cope with every increasing volumes of data. Shared ledgers based upon blockchain networks look promising in relation to open frameworks for privacy, digital object memories and smart contracts.

6.2 Future Workshops on Standards

The present report is reflecting the progress of standards and pre-normative activities at the end of the first half of the LSPs. The work is going to continue

- Within the LSPs, in particular for the resolution of the major standards gaps, and
- Within the LPS Activity Group 02 ("Standardisation, Architecture and Interoperability") which will organise several Workshops (1 in 2018 and 3 in 2019) with a series of associated CREATE-IoT deliverables.

A final deliverable (D06.06 " Final report on IoT standardisation activities") will summarize the global findings at the end of (most of) the LSPs at the end of 2019.

7. REFERENCES

[1] CREATE-IoT, Deliverable D06.07, "Strategy and coordination plan for IoT interoperability and pre-normative and standard activities", 2018.

[2] CREATE-IoT, Deliverable D06.02, "Recommendations for commonalities and interoperability profiles of IoT platforms", 2018.

[3] H. van der Veer and A. Wiles, Achieving Technical Interoperability – the ETSI Approach, ETSI White Paper No.3, 3rd edition, April 2008

[4] Advancing IoT Platforms Interoperability, River Publishers, Gistrup, 2018, 978-87-7022-005-7 (ebook), IoT European Platforms Initiative (IoT-EPI) White Paper, online at: https://iot-epi.eu/wp-content/uploads/2018/07/Advancing-IoT-Platform-Interoperability-2018-IoT-EPI.pdf

[5] A. Tolk and J. A. Muguira, "The levels of conceptual interoperability model" in Proceedings of the 2003 Fall Simulation Interoperability Workshop, Citeseer, 2003, pp. 1-11.

[6] T. Berners-Lee, J. Hendler and O. Lassila, The Semantic Web - A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities, online at: https://bit.ly/2bCLEC7

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

[8] AIOTI WG03 Report: "High Level Architecture (HLA) Release 4" June 2018; https://docbox.etsi.org/SmartM2M/Open/AIOTI/

[9] "Internet of Things Reference Architecture (IoT RA)", ISO/IEC CD 30141, Online at: https://www.iso.org/standard/65695.html.

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

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

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

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

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

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

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

[17] G. Larini, et. al. *Standardisation plan*. AUTOPILOT Deliverable D5.7, May 2017.

[18] AIOTI. *IoT LSP Standard Framework Concepts*, (rel.2.7). AIOTI WG03 - IoT Standardisation, 2016. Online at: https://docbox.etsi.org/SmartM2M/Open/AIOTI/!!20170102Deliverables/AIOTI%20WG3_sdos_alliances_landscape_-_iot_lsp_standard_framework_concepts_-_release_2_v7.pdf

[19] ETSI. *SmartM2M; IoT Standards landscape and future evolutions*. ETSI TR 103 375 v1.1.1, October 2016. Online at:

https://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf

[20] W3C Recommendation 23 January 2018. Online at: https://www.w3.org/TR/2018/REC-websub-20180123/

[21] W3C Recommendation 3 February 2015. Online at: https://www.w3.org/TR/2015/REC-eventsource-20150203/

[22] Concise Binary Object Notation (CBOR). Online at: https://tools.ietf.org/html/rfc7049

[23] W3C Recommendation 11 February 2015.Online at: https://www.w3.org/TR/exi/

[24] Digital Object Identifiers. Online at: https://www.doi.org

[25] Aron Tan. *Global IoT security standard remains elusive.* Tech Target, Computer Weekly, June 2018. Online at: https://www.computerweekly.com/news/252443777/Global-IoT-security-standard-remains-elusive

[26] NIST - National Institute of Standards and Technology. *Interagency report on Status of International Cybersecurity Standardization for the Internet of Thing (IoT);* Prepared by the Interagency International Cybersecurity Standardization Working Group. Draft NISTIR 8200, February 2018. Online at: https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf

[27] EMBC - Embedded Microprocessor Benchmark Consortium. Online at: http://www.eembc.org/index.php

[28] GSMA. *GSMA IoT Security Guidelines and Assessment*. Online at: https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

[29] IEC - International Electrotechnical Commision. *IoT 2020: Smart and secure IoT platform*. White paper 2016. Online at: http://www.iec.ch/whitepaper/pdf/iecWP-loT2020-LR.pdf

[30] IEC - International Electrotechnical Commision. *Internet of Things: Wireless Sensor Networks*. White paper 2014. Online at: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

[31] IpT Security Foundation. *IoT is vast and has many security related issues – how do we go about addressing them?* Online at: https://www.iotsecurityfoundation.org/working-groups/

[32] Enisa - European Union Agency for Network and Information Security. *Baseline Security Recommendations for IoT - in context of Critical Information Infrastructures*. Enisa November 2017. Online at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/

[33] SAS70 - Statement on Auditing Standards No. 70. *Trust services assurance*. Online at: http://sas70.com/sas70_trustservices.html

[34] IBM. *Blockchain for Dummies*. Online at: https://www.ibm.com/blockchain/what-is-blockchain

[35] The Apache Hadoop - project develops open-source software for reliable, scalable, distributed computing. Online at: http://hadoop.apache.org/

[36] International Data Spaces Association. Online at: https://www.internationaldataspaces.org/en/

[37] Wikipedia. Federated database system. Online at: https://en.wikipedia.org/wiki/Federated_database_system

8. APPENDICES

8.1 Information Sources for this Report

The workshops, survey questions, other Activity Groups, AIOTI, and other stakeholders.

8.1.1 2018 Standardisation Survey Questions

The time available during the Activity Group 2 workshops is limited, so the idea is to supplement the workshops with one on one discussion with the Activity Group 2 representatives for each Large-Scale Pilot, and to use the information gathered as the basis for analysis and recommendations for action by the Large-Scale Pilots.

Please provide answers relevant to your LSP in respect to the following questions:

- **In respect to the use cases, we would like to better understand which standards you have found useful and where you have identified gaps, and how you have addressed them in the implementation work.**
    - *This is interesting in respect to whether existing standards are a good fit, an imperfect fit, or don't apply at all. This will help us provide advice for IoT projects on which standards to use and where new standards are needed. We are interested in your use of standards at all layers, not just the IoT communication layers.*
- **We're interested in any use cases you have looked at that involve integration of information across different platforms, or where you have had to deal with differences in devices from different vendors.**
    - *This question is motivated by the desired to avoid being locked into a particular platform or device, something essential to reducing friction and enabling open markets of services. In principle, Europe would benefit from open standards that decouple services from being tied to the details of platforms, protocols and devices. Regarding devices, each manufacturer typically aims to differentiate their products from those from other manufacturers. This points to the need for high level (semantic) descriptions of devices as a basis for services to adapt to variations in capabilities and interfaces across devices.*
- **In the implementations of your use cases, can you describe which parts are use case specific and which parts are more general and could be re-used in other contexts? How does this relate to your chosen architecture?**
    - *Understanding the architectural context will enable us to consider commonalities and mappings across variations in architecture and application domains.*
- **How you have addressed scaling challenges, e.g. in respect to the volume of data or latency requirements.**
    - *Such scaling challenges can point to the role of distributed compute and storage as a means to reduce the load on cloud servers, by providing higher level interpretations of data and events. Scaling can also be involved in respect to the need for event-based processing of large data streams versus the need for persistent storage for long term access. A further consideration is the challenge for synchronisation across sets of sensors and activators in distributed systems.*
- **Descriptions of interoperability challenges you are facing at different layers in the architecture - for example, where the same protocol is being used in incompatible**

ways, differences in units of measure for sensor readings, where you've needed semantic models of devices in terms of their capabilities, models of the context, and so forth.

- *Whilst there are many standards for the IoT, there are still plenty of risks for a lack of interoperability at different layers. If convergence is impractical, then work arounds may be possible using brokers. The availability of machine interpretable descriptions can enable cheaper declarative solutions as opposed to more expensive procedural (code-based) solutions.*

- **What experience you have had with information modelling, e.g. which ontologies you have used or had to develop for yourselves? What tooling and formalisms have you used for modelling?**
  - *This will help us to provide useful recommendations to IoT projects.*
- **How you have handled requirements relating to open markets of services, and adaptation, as well as data licenses, terms & conditions, privacy policies, analytics and so forth? What standards you have used in relation to security, e.g. identity, authentication, authorisation, trust, monitoring and reporting, and where you have identified gaps that you have had to work around?**
  - *IoT standards tend to focus on communication technologies, but there is a large set of requirements in respect to enabling open markets of services. Gathering input across the LSPs will help us to provide useful guidance to future work on standards and to other IoT projects.*
  - *We're also interested in how you are handling smart contracts, and your view of the potential role for shared ledgers (based on blockchains) for smart contracts, and satisfying regulatory requirements for privacy and for safety, e.g. for food supply chains and for safety critical engineering components.*
- **Which standard development organisations your project partners have connections with and in what respect? What information do you have on relevant standardisation activities at those standard development organisations?**
  - *The European Commission would like to better understand and encourage engagement in standards development organisations. This makes it valuable to track current standardisation activities as a basis for recommendations for which standards development organisations would be a good target for work on filling gaps, and for encouraging harmonisation across different standards development organisations.*
- **What kinds of relevant pre-normative standardisation activities any of your partners are engaged in - this includes contributions of use cases, requirements, analysis of challenges, technical proposals etc.**
  - *This will help us to provide valuable advice to LSPs on pre-normative activities based upon best practices across the LSPs.*
- **Your experience with "community standards" involving collaboration across a small number of parties, as contrasted with standards from traditional international standards development organisations?**
  - *This refers to the need for agile development of technology agreements across stakeholders, e.g. in respect to data models, choice of data formats, licensing models and so forth. Community standardisation is lightweight compared to what's needed for international standards. However, Community standards benefit from being able to borrow from existing work and practices by others.*

One challenge is how to fund sustainable infrastructure to support best practices for community standards.