Symbiosis of smart objects across IoT environments

688156 - symbIoTe - H2020-ICT-2015

Final Report on Standardization Analysis and Recommendations

The symbIoTe Consortium

Intracom SA Telecom Solutions, ICOM, Greece
Sveučiliste u Zagrebu Fakultet elektrotehnike i računarstva, UNIZG-FER, Croatia
AIT Austrian Institute of Technology GmbH, AIT, Austria
Nextworks Srl, NXW, Italy
Consorzio Nazionale Interuniversitario per le Telecomunicazioni, CNIT, Italy
ATOS Spain SA, ATOS, Spain
University of Vienna, Faculty of Computer Science, UNIVIE, Austria
Unidata S.p.A., UNIDATA, Italy
Sensing & Control System S.L., S&C, Spain
Fraunhofer IOSB, IOSB, Germany
Ubiwhere, Lda, UW, Portugal
VIPnet, d.o.o, VIP, Croatia
Instytut Chemii Bioorganicznej Polskiej Akademii Nauk, PSNC, Poland
NA.VI.GO. SCARL, NAVIGO, Italy
Universität Zürich, UZH, Switzerland

For more information on this document or the symbIoTe project, please contact:
Sergios Soursos, INTRACOM TELECOM, souse@intracom-telecom.com

Document Control

Title: Initial Report on Standardization Analysis and Recommendations

Type: Public

Editor(s): Reinhard Herzog

E-mail: Reinhard.herzog@iosb.fraunhofer.de

Author(s): Reinhard Herzog, Hylke van der Schaaf, Michael Jacoby, Giuseppe Bianchi, Giovanni Bartolomeo, Claudio Pisa, Kym Watson, Gino Carrozzo, Matteo Pardi, Gianluca Insolvibile, Ricardo Vitorino, Joao Garcia, Ivana Podnar Žarko, Lara Lopez Muniz

Doc ID: D7.8-Standardization 1.0.doc

Amendment History

Version	Date	Author	Description/Comments
V0.1	31.10.2018	Reinhard Herzog	Base line for final report derived from D7.3 version1.0
V0.2	1.12.2018	Reinhard Herzog	W3C WoT Thing Desctiption (section 4.1) IIC working group on interoperability (section 4.3)
			Summary and Conclusions
	17.12.2018.	Ivana Podnar Žarko	Updates to section 4.6, added new section on ETSI ISG CIM, and section 4.8 ETSI Industry Specification Group
V0.3	18.12.2018	Reinhard Herzog	Review Release
V0.4	19.12.2018	Zvonimir Zelenika, Lara Lopez Muniz	Review and contribution to section 4.16 on AIOTI
V1.0	20.12.2018	Reinhard Herzog	Final Release

Table of Contents

List of Figures

List of Tables

1 Executive Summary

The symbIoTe vision is to deliver a solution for a unified view on IoT platforms with their resources and to support a secure and interoperable collaboration within IoT platform federations. One of the challenges for this vision is to decide when to use existing technologies with established standards and at which point it is required to go beyond the state of the art. A good overview on the current standardisation landscape and the positioning of the symbIoTe consortium within is an essential prerequisite for such decisions. That was the motivation for the first part of Task T7.4 and it was reported in the Deliverable D7.3. The second part of task T7.4 was maintaining the link between the symbIoTe developments and the standard developing groups, in order to stay informed about trends in standardization and to look for opportunities to contribute symbIoTe results into the standardization products.

For the task to monitor standardisation activities related to IoT middleware architectures, we relied on studies performed by market analysts like Machina Research [4] and Standards Developing Organizations (SDO) like ETSI [2], [3]. We also joined a workshop organized by the European Commission in cooperation with ETSI and AIOTI on IoT Platforms & Standardisation (February 8th, 2017 in Brussels, Belgium). During this workshop, many speakers named the security and semantic interoperability as the main gaps where standards are required.

However, the main basis for the analysis was the joined experience of the consortium members, which are using standards and contributing to the many standards developing organizations (like W3C, OGC, oneM2M, IETC, ETSI, IRTF). There are very similar findings among all observers. There is no lack on standards for specific technologies and platforms in the IoT domain, but there is a clear gap in the support of interoperability between platforms from different domains. This gap is also an opportunity for symbIoTe to feed projects results into standards developing organisations, to make them sustainable and widely usable.

A clear recommendation is to use standards whenever possible. This will ease the acceptance of symbIoTe and it will help to develop a robust und mature solution. SymbIoTe is dedicated to working areas where the main gaps for IoT standards are identified, like security and interoperability for IoT platforms. That gave symbIoTe many opportunities to contribute assets to SDOs. These gaps are also the first items on the agendas of the SDOs, so common topics have been found in many groups.

This deliverable gives a summary of the current activities within the SDOs, where symbIoTe had established links. It also gives recommendations on how to contribute or to make use of their results. The standards that have been used within symbIoTe are listen in chapter 5 and the proposed assets to contribute to SDO working groups are described in chapter 6.

2 Introduction

2.1 *Purpose of this document*

This document is the second report on Task T7.4 "Standardization Strategy and Support". In the first working period from M1 to M12, the focus was set to monitoring of standardization activities related to IoT middleware architectures, and to support decisions regarding the selection of standards solutions. The second phase of T7.4 from M13 to project end at M36 was to keep the communication links alive between symbIoTe and the SDOs, and to communicate the symbIoTe results to the SDO working groups.

The IoT community is growing very fast in terms of technologies used and application fields touched. Because of this dynamism, the technology landscape is very broad and very diverse. There is a clear demand for standardization, but Standards Developing Organizations are struggling to keep pace with the market growth. According to [4] open standards in IoT deployments would accelerate growth by 27% and reduce deployment costs by 30%. Their message is that standards are often grown bottom up which leads to overlapping areas and gaps between areas. IoT needs top down approaches like reference architectures to achieve the goal to become an overarching integration technology.

The purpose of this deliverable is to get an "inside" view on the standardization work for the most relevant topics for symbIoTe. The initial analysis was the basis for design decisions during the development of the symbIoTe architecture. This second and final analysis concludes the task and gives an update on the standard developing activities and the recommendations for symbIoTe.

2.2 *Relation to other deliverables*

A major input for this document is Deliverable D7.3 "Initial Report on Standardization Analysis and Recommendations" [5], as it describes the initial analysis on standardization working groups. And overview of relevant IoT reference architectures which have influenced the definition of the symbIoTe architecture is provided in Deliverable D1.4 "Final Report on System Requirements and Architecture."

2.3 *Document structure*

The document is structured as follows: Sections 3 and 4 contain the description of standardization activities, which are most relevant for symbIoTe and where consortium members are already associated. The latter, reflects the main results of the reported working period of Task 7.4. Section 5 is dedicated to the standards that are used by symbIoTe already or are planned to be supported during project time. Section 5 contains an evaluation on the standards used by symbIoTe. Section 6 describes the assets used for standardisation. Section 7 concludes this deliverable by summarizing findings and recommendations.

3 Standardisation Landscape and Gap Analysis

3.1 Standardisation Landscape

Within the IoT EPI cluster meetings, the AIOTI presented its view on the IoT standardization landscape [1]. The central message was that all the verticals within the IoT EPI pilots are well covered with existing or emerging standards. Figure 1 shows these verticals with the many standards developing organizations contributing to these verticals.

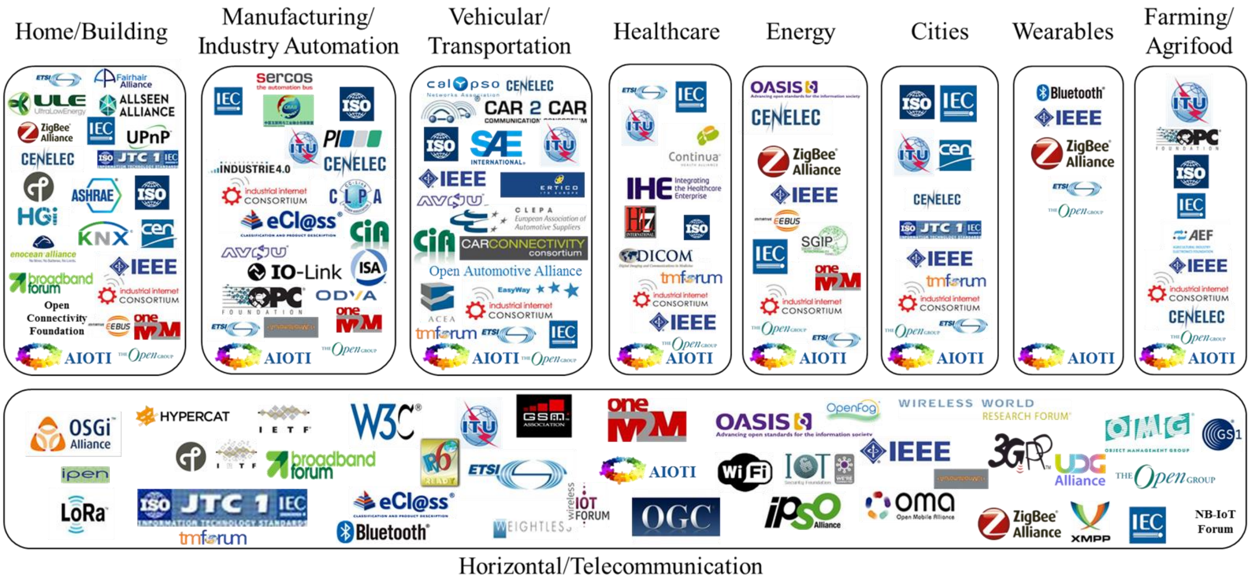

Figure 1: IoT Standards Landscape (ref [1])

Also for the standards across vertical domains, there is a large number of ICT standards that can be applied to several IoT verticals, like the domain agnostic standards from OMG, oneM2M, OSGi and many more. Thus, there is a significant potential for a common ground to develop interworking IoT solutions, such as IoT reference architectures, IoT resource description, interworking interfaces, etc. However, this potential will only materialize if these standards are being applied within the emerging IoT solutions. But the amount of standards within the same domains also shows that there a huge competition between SDOs and no clear leading standard. SDO and their standards are associated with communities often driven by commercial interest. A company that uses a standard, gains access to potential customer, but it also shares the market with competitors and it becomes exchangeable. That make decision for a certain standard not just a technical issue, but even more a strategical business decision.

The fragmentation of the standardization landscape is already visible and with the dynamic within the IoT domain (ref to conclusion in [2]), it must be assumed that this fragmentation will increase. While this makes the selection of the right standard even more difficult, the fact remains true, that using an existing standard should always be favored compared to a proprietary solution.

3.2 Standardization Gap Analysis

The ETSI performed a gap analysis of requirements in certain IoT areas and their available standards [3] in November 2016. This study explicitly focused on the “symbIoTe-area” of “Cross IoT platform interoperability and harmonization”. The list below shows the topics identified as the main gaps in this specific area (individual gaps are numbered for later reference).

GAP 1. Duplication of IoT architectures and models.

GAP 2. A large number of communication protocols address heterogeneous types of communication requirements.

GAP 3. Data models are developed on a proprietary basis and mostly specific to the vertical domains to which they apply.

GAP 4. Processing rules and decision-making processes under the reception of sensor data lack harmonization.

GAP 5. Security and privacy are addressed on an isolated basis for part of the applications.

GAP 6. Ease of use and of maintenance after purchase would require a more global approach.

These gaps can be mapped to the objectives declares by the symbIoTe project. The following Table 1 shows the symbIoTe objectives with the specific mappings to task and deliverables and the mapping to the gaps identified by the ETSI report [3].

Table 1: Mapping of standization gaps to symbIoTe tasks

OBJ/#	Specific	Measurable[1]	Achievable	Timely[2]	Gap Relevance
OBJ/01: Interoperability of IoT platforms for rapid crossplatform application development	Semantics for IoT and Cloud resources	T1.3 (D1.2, D1.4), T2.1 (D2.1, D2.2)	Formal semantic description	M10 to M18	GAP 1
	Virtual symbIoTe environments	T1.3&T1.4 (D1.2, D1.4), T2.2 (D2.3, D2.4)	Architecture specification, Implementation	M10 to M18	GAP 2
	symbIoTe dom specific enablers	T1.1 (D1.1, D1. T1.3&T1.4 (D1.2, D1.4); T2.3 (D2.5, D2.6)	Use case specification, design and implementation of enablers	M6 to M21	GAP 1

[1] The success of each objective item can be measured whenever the listed deliverables have been reported to the European Commission, while the means of success verification is listed in “Achievable”.

[2] “Timely” refers to the *first* and *final* month of reporting or demonstration of results. Detailed intermediary reporting information is captured in the WP descriptions in Section 3.1.3.

	IoT Federation	T1.3&T1.4 (D1.2, D1.4), T3.3 (D3.2, D3.3)	Architecture specification, Implementation	M10 to M30	GAP 1, 2, 3
OBJ/02: Hierarchical, adaptive and dynamic IoT environments	Local Registration, Discovery and Interoperability of Smart Objects	T1.3&T1.4 (D1.2, D1.4), T4.1 (D5.1)	Architecture and protocol specification, Middleware implementation	M10 to M30	GAP 3
	Wireless network virtualisation and management	T1.3&T1.4 (D1.2, D1.4), T4.2 (D4.2, D4,3)	Dynamic access schemes for coordinating different radio technologies	M10 to M30	GAP 2
	symbIoTe smart space middleware and client	T1.3&T1.4 (D1.2, D1.4), T4.3 (D4.2, D4.3)	Architecture specification, Middleware implementation	M10 to M30	GAP 2
OBJ/03: Security, access scopes and identity management	Monitoring and anomaly detection	T1.3&T1.4 (D1.2, D1.4), T3.2 (D3.1)	Architecture specification, Implementation	M10 to M30	GAP 5
	Access scopes & Identity Management	T1.3&T1.4 (D1.2, D1.4), T3.2 (D3.1)	Architecture specification, Implementation	M10 to M30	GAP 5
	Heterogeneous communication techniques	T1.3&T1.4 (D1.2, D1.4), T4.2 (D4.2, D4,3)	Secure sharing of the wireless medium	M4 to M36	GAP 2, 5
OBJ/04: Realistic crossplatform deployments	Integrated symbIoTe release	T1.3&T1.4 (D1.2, D1.4), T2.1 (D2.1, D2.2), T2.2 (D2.3, D2.4), T2.3 (D2.5, D2.6), T3.3 (D3.2, D3.3), T4.3 (D4.2, D4.3)	Implementation, API, Documentation	M18 to 30	GAP 4, 6
	Application development and use case deployments	T1.1 (D1.1, D1.2), T5.2 (D5.2), T5.4 (D5.4)	Implemented & demonstrable use-cases (see list of use cases)	M6 to M34	GAP 6
	Use case end-user validation	T1.1 (D1.1, D1.2 T5.3 (D5.3)	Implemented & demonstrable & validated use-cases	M6 to M29	GAP 6
OBJ/05: Open source and commer-cialisation	Distribution & dissemination of symbIoTe system through open source communities	T7.2 (D7.5)	Implementation, Apache 2.0 Licensing, Dissemination	M13 to M33	GAP 6
	Potential for Commercialisation & Diffusion	T1.2 (D1.3, D1.5), T5.3 (D5.4), T7.3 (D7.3, D7.6)	Economic Evaluation & Recommendations	M12 to M36	GAP 6

As it can be seen, this analysis shows a large overlap with the symbIoTe objectives and the respective tasks. All work packages were involved in those activities, which clearly indicates that symbIoTe is tackling the most pressing standardisation gaps in the IoT domain.

This gives symbIoTe an excellent opportunity to create an impact with its results and to approach those SDO, which are dedicating their agenda to these gaps.

4 Standards Developing Organisations in the Focus of symbIoTe

This section extends the more general considerations on the standardization landscape in Section 3, with a detailed analysis of the current agendas of those SDOs, which we considered relevant for the symbIoTe working areas. Fortunately, some of the symbIoTe consortium members are quite active in several SDO working groups, so this deliverable can rely on an inside view for most of these groups. Table 2 shows the current affiliations of consortium partners with such working groups.

Table 2: symbIoTe Consortium Standardisation Activities

Standardisation Organization	Working group / Standard	Involved Partner
World Wide Web Consortium (W3C)	Web of Things	IOSB
	RDF Stream Processing Group	IOSB
Industrial Internet Consortium	Industrial Internet Reference Architecture (IIRA)	IOSB
Open Geospatial Consortium (OGC)	Sensor Things API	IOSB
OPC Foundation	OPC-UA	IOSB
Internet Engineering Task Force (IETF)	6tisch	CNIT
	Constrained RESTful Environments (CORE WG)	NXW
European Telecommunications Standards Institute (ETSI)	TC-CYBER	CNIT
	Next Generation Protocols ISG	NXW
	oneM2M	UNIZG
Internet Research Task Force (IRTF)	Thing-to-Thing Research Group (T2TRG)	NXW
AIOTI	WG08 Smart Cities (including IoT Research, Innovation Ecosystems, IoT Standardisation and IoT Policy)	ATOS

The analysis in the following subsections will describe for each SDO the general objectives and the current working areas, as well as the relevance for symbIoTe. In some cases proposal are formulated, about potential contributions between symbIoTe and an SDO.

4.1 W3C Web of Things Interest Group

In the charter of the Web of Things Interest Group (WoT IG), the **mission** is stated as[3]: *"…to counter the fragmentation of the Internet of Things by introducing a Web-based abstraction layer capable of interconnecting existing Internet of Things platforms and complementing available standards*".

The group's motivation was the lack of interoperability across platforms with the resulting data silos, the high costs for integration and limitations for market potentials. The core idea of the group is the Web Thing Model, as shown in Figure 2. Based on the established HTTP protocol the group defines best practices on how to define resources and data models and how to include semantic enriched information in order to define a common framework to deal with "Things".

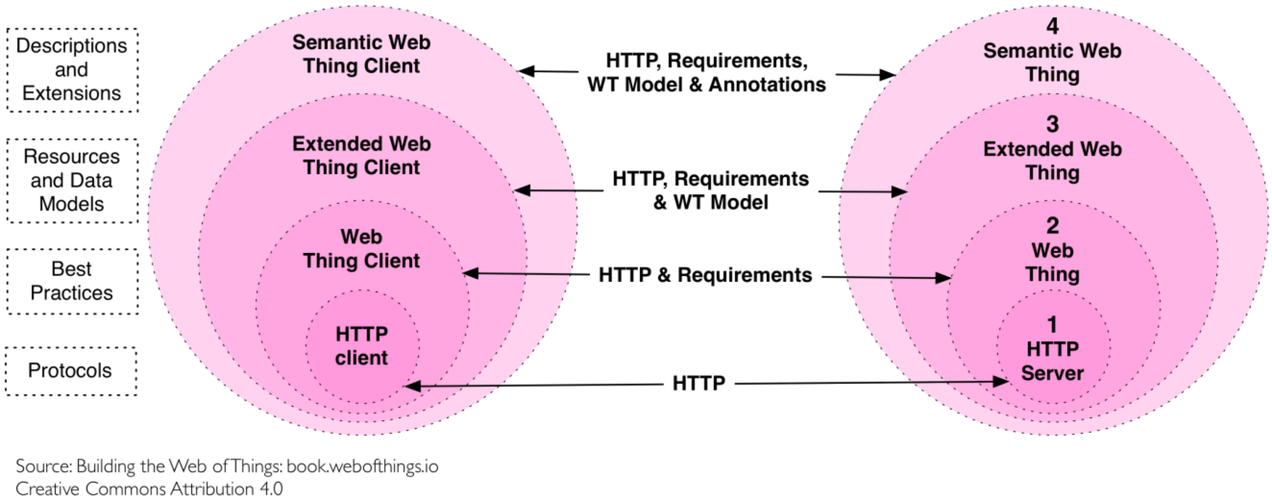

Figure 2: Web Thing Model

The current working areas of the interest group have been the evaluation of use cases and the collection of requirements, as well as the definition of the technology landscape and the proposed architecture for the Web of Things. The next steps are the collection of current practices with the adoption of the proposed concepts. These "current" practices will be further developed into "best" practices. The main vehicle will be the organization of so-called PlugFests to evaluate the current working assumptions in regards to Web of Things technologies. A PlugFest is essentially meeting between developers to share ideas on implementations and to try and evaluate solutions within small experiments.

The interest group is open to other SDO's or any kind of interested party or community. Their intention is to get in touch with people as many people as possible in order to collect feedback. The collaboration concept of the interest group is depicted in Figure 3. In that picture, symbIoTe would appear in the box "Interested Parties, Vendors & Communities". Outreach and collaboration activities are used to support this relationship.

[3] https://www.w3.org/WoT/IG/

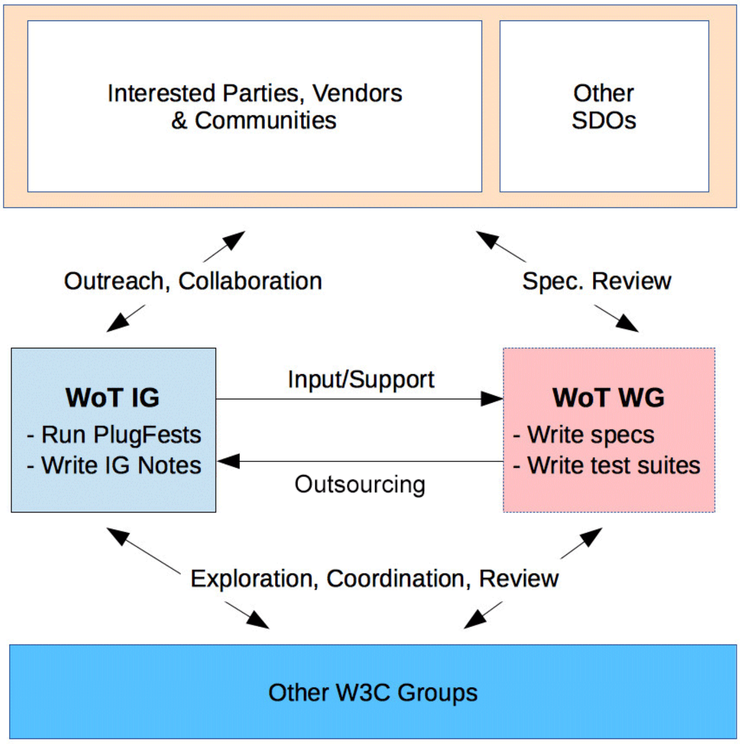

Figure 3: Web of Thing Interest Groups Relationships

The WoT IG covers several topics related to the work of symbIoTe, listed in Table 3.

Table 3: Web of Things Working Group Topics

SDO Topic	Relevance for symbIoTe
Generic Meta Data Models to describe a "Thing"	To be aligned with the Core Information Model (CIM) developed in WP2.
Extension of Thing Descriptions with other semantic models	To be aligned with the concept of platform specific models developed in WP2.
API to access Thing Properties and services	To be aligned with Resource Access Proxy definition developed in WP2.

During a W3C Technical Plenary / Advisory Committee meeting week in Lyon (22-26 October 2018) we presented the solutions for the semantic description of Things as they are being used within SensorThingsAPI, which is the baseline definition for the symbIoTe registry. The discussion during the meeting have shown that these are very similar approaches. It was decided to use one of the upcoming "plug-fest" meetings to work on an interoperability solution to use the Thing.property service to implement a W3C WoT ThingDirectory. Such an implementation could be easily adopted to the symbIoTe core, in order to provide a W3C compliant interface symbIoTe Core Registry.

4.2 W3C RDF Stream Processing Community Group[4]

In times of Big Data and Responsive Design, Stream Processing gains more and more importance to analyse massive amounts of data in near real-time. As, at the same time, Linked Data and the Semantic Web gained attention in the communities, stream processing of semantic data becomes of interest. Currently there are multiple research prototype implementations of such Semantic Streaming Engines, each using their own query language and a different set of operations. For this reason, *“the mission of the RDF Stream Processing Community Group (RSP)* [5] *is to define a common model for producing, transmitting and continuously querying RDF Streams.” [5]*

The RSP group is currently working on two documents:

- Collection of requirements for a unified query language for RDF stream processing, which is currently available online [6], but still waiting to be agreed upon by the members
- The definition of such a query language itself.

A draft version of the first document is available online [6] but still waiting to be agreed upon by the members. Unfortunately, the group has been very inactive since fall 2016 (which is mainly due to a change of affiliation of the group’s chair).

The work of this group is not directly relevant to symbIoTe in terms of the current implementation, but rather in terms of the overall vision of an IoT interoperability framework. Bringing together the data of multiple platforms is only the first step in fully exploiting the potential of IoT. Adding support for sophisticated continuous queries and near real-time analysis of the combined data will be the next big one. Therefore, the symbIoTe consortium observes the work of this group and may eventually contribute by providing some requirements in the second half of the project.

4.3 Industrial Internet Consortium

The Industrial Internet Consortium[6] describes itself as follows:

“The Industrial Internet Consortium (IIC) is a global, member-supported, organization that promotes the accelerated growth of the Industrial Internet of Things by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure. The Industrial Internet Consortium is managed by the Object Management Group (OMG).”

Detailed information is available under www.iiconsortium.org.

IIC is itself not a standards organization. However, it has developed the IIC IIRA (Industrial Internet of Things Reference Architecture)[7]. It evaluates standards against this architecture, identifies requirements for standards and proposes these requirements to

[4] https://www.w3.org/community/rsp/
[5] https://www.w3.org/community/rsp/
[6] http://www.iiconsortium.org
[7] http://www.iiconsortium.org/IIRA.htm

standards organizations. IIC advocates open standard technologies and aims to influences standards development.

Further, IIC aims to advance innovation and establish interoperability in the Industrial Internet of Things (IIoT)[8]. Therefore, IIC works in five application domains called verticals: Transportation, Public Sector, Manufacturing, Healthcare, and Energy. IIC has started its initiative Industrial Internet Interoperability Coalition (I^3C) to identify hotspots requiring interoperability standards and to bring SDOs, open source organizations and technology providers together in a coalition to address clusters of interoperability hotspots. IIC distinguishes between domain-specific and generic interoperability clusters. The I^3C overview document[9] describes the current IIoT interoperability heat-map of hotspots in terms of verticals, use cases, architectures and patterns. The IIC IIRA is the reference here for positioning the interoperability hotspots. For example, the hotspot cluster "Smart Facility Operations in Manufacturing" addresses three interoperability hotspots:

1. Industrie 4.0 Administration Shell, OPC-UA and OMG DDS
2. Wireless shopfloor data exchange
3. Energy data exchange.

IIC intends to establish a coalition of liaisons for each hotspot cluster. The activities follow an Interoperability Cluster Maturity Model with four steps:

1. Identification of clusters
2. Architecture definition and official confirmation of coalition of liaisons
3. Confirmation of technical feasibility in testbeds
4. Establishment of a certification process

Step 3 uses the IIC testbed mechanism to validate the technical feasibility of proposed solutions. IIC testbeds[10] follow a rigorous approval process and serve to advance and validate the IIRA and the IIC Security Framework[11].

Moreover, IIC has a Vocabulary Working Group that has produced an Industrial Internet Vocabulary Technical Report[12]. Results from this working group may be used as a best practice for defining important and common terminology in IIoT.

symbIoTe assets could be mapped on concepts within the IIRA and Security Framework to demonstrate our solutions and potentially propose improvements or extension to the IIC IIRA. This work would be relevant for industrial IoT verticals, such as healthcare and smart cities.

As an input from symbIoTe to the IIC, and specifically to the "Distributed Data Interoperability and Management Task Group", was the symbIoTe approach to semantic interoperability. This group is co-chaired by our college Dr. Kym Watson (Fraunhofer IOSB), and their current task is to review candidate information models to enable interoperability to IIoT applications. As we in symbIoTe worked within task T2.1 on exactly

---

[8] http://www.iiconsortium.org/accelerating-innovation.htm
[9] http://www.iiconsortium.org/pdf/IIC_I3C_Overview_Aug_2016.pdf
[10] http://www.iiconsortium.org/test-beds.htm
[11] http://www.iiconsortium.org/IISF.htm
[12] http://www.iiconsortium.org/pdf/Industrial-Internet-Vocabulary.pdf

the same topic, our results are very relevant to the IIC. Our deliverable D2.4 is currently analysed by the for mentioned IIC task group on interoperability.

4.4 OGC Sensor Things API

The SensorThings API [7] is a standard defined by the Open Geospatial Consortium (OGC), specifically by the Sensor Web Enablement for IoT (SWE-IoT) working group. The goal of this group is to define standards based on the existing SWE standards (like Sensor Observation Service or SOS, Sensor Planing Service SPS) that are specifically suitable for IoT use. The "*OGC SensorThings API Part 1: Sensing"* is the first standard resulting from this process. It defines how to exchange Observations between server and client, like the SOS standard, but using a modern HTTP/REST based interface.

The current activities of the OGC Sensor Things working group are:

- Refining the SensorThings API based on experiences made by several groups creating implementations.
- Defining and building a conformance suit to test both client and server implementations.
- Defining Part 2 of the SensorThings API that deals with actuators.
- Defining a JSON version of the "*SWE Common Data Model Encoding Standard*" for use with the SWE-IoT standards.

symbIoTe has taken inspiration from the SensorThings API, both for the Resource Access Proxy and data model. Since the group is currently working on standardising the interface for controlling actuators, experiences from symbIoTe on this topic are warmly welcomed.

Another topic on which symbIoTe results can contribute to the SWE-IoT standards is how to deal with semantics in the Internet of Things. One way for doing this would be a best-practices paper to be proposed to the OGC, describing the symbIoTe approach to attach semantic information about things. Recent developments within the W3C web of things working group created the idea of using the W3C Things Directory as an approach to handle semantic annotations with the SensorThingsAPI. This is closely related to the symbIoTe semantic registry and offers a convenient way to use the JSON-based properties extensions for semantic annotations based on JSON-LD.

Since September 2018, Dr. Hylke von der Schaaf (Fraunhofer IOSB) is Co-Chair of the Sensor Things API working group. As also being a member of the symbIoTe project group, there is a close link established between both groups.

4.5 OPC Foundation

"*The mission of the OPC Foundation is to manage a global organization in which users, vendors and consortia collaborate to create data transfer standards for multi-vendor, multi-platform, secure and reliable interoperability in industrial automation. To support this mission, the OPC Foundation:*

- *Creates and maintains specifications*
- *Ensures compliance with OPC specifications via certification testing*

- *Collaborates with industry-leading standards organizations”* [13]

The core technology maintained by the OPC Foundation is ‘OPC’. Initially, the OPC standard was restricted to the Microsoft Windows operation system. The acronym OPC is derived from OLE (object linking and embedding) for Process Control. With the introduction of service-oriented architectures, the OPC Foundation developed the ‘OPC UA’ specification. Nowadays the original specification is often referred to as OPC Classic.

The Foundation established several working groups, which are open for members only. These groups are[14]:

- Compliance Working Group (CWG) – Responsible for the OPC Foundation Compliance program. This group analyzes OPC specifications to determine how products are to be tested for compliance. The group meets weekly to discuss test procedures, Compliance Lab standard operating procedures, and to continually update and enhance the Compliance Test Tools.
- ISA-95 Working Group – Responsible for the definition and maintenance of the ISA-95 OPC UA information model. The first release (in early 2013) of the ISA-95 OPC UA companion specification includes support for the following ISA-95 models: Physical Assets, Equipment, Personnel and Material Handling. This mapping of the abstract ISA-95 model provides a high-speed, secure information flow from the lowest levels of the automation hierarchy to Manufacturing Execution Systems (MES) and Enterprise Resource Planning (ERP) systems. ISA-95 was developed for transferring information in Level 3 and 4 of the enterprise; the OPC UA mapping allows this information to be securely transferred between levels 3 and 4 and to be extended down to Level 2 of the enterprise.
- PLCopen Working Group – A joint effort between PLCopen and the OPC Foundation to develop an OPC UA information model companion specification for IEC 61131-3. While many vendors already provide controllers that conform to IEC 61131-3, there is no standard that describes how a controller should communicate with applications external to the controller. The first release of the companion specification provides native OPC UA function blocks that support the OPC UA information model inside any IEC 61131 compliant device.
- Technical Advisory Council (TAC) – This group is comprised of leaders and visionaries from major automation suppliers and core OPC Foundation members. They advise Foundation management on current and future technical matters and provide guidance on overall technical direction. Specific tasks include commissioning new work and final release approval of deliverables from all technical working groups.
- Unified Architecture Working Group – Responsible for defining and maintaining the OPC UA specifications, including enhancements for transactional support, global discovery and increased reliability. Additionally, base architecture enhancements are evaluated for extensibility into other companion specifications (e.g. information modeling; adding native OPC UA data types).

[13] https://opcfoundation.org/about/opc-foundation/mission-statement/
[14] https://opcfoundation.org/about/working-groups/

The project partner Fraunhofer IOSB is a foundation member and, thus, access to these groups would be possible for the symbIoTe consortium. As the IoT-topic has become very relevant for industrial solutions, the Technical Advisory Council is generally interested in any kind of IoT-innovations.

4.6 oneM2M

oneM2M is global standardization body for M2M and the IoT[15]. It was established as an alliance of SDOs similar to 3GPP. SDOs that participate in oneM2M are ARIB, ATIS, CCSA, ETSI, TIA, TSDSI, TTA and TTC. To become a member of oneM2M, an organization must already be a member of one of those standardization bodies. UNIZG-FER, as a member of ETSI, is also a oneM2M member and is monitoring developments within the relevant working groups.

oneM2M is defining a set of specifications that will enable users to build platforms independently of industry solutions. Currently there are three published releases of the oneM2M specification. Release 3 is the latest release published in September 2018 which focuses on interworking of oneM2M's service layer with 3GPP's underlying network – in particular cellular IoT (NB-IoT and LTE-M) – and new capabilities to unlock value in industrial and smart home applications.

Work in oneM2M is organized in the following working groups[16]:

- REQ – use cases and requirements identifies and documents use cases and service and system requirements;
- ARC – develops and specifies an architecture for an M2M system;
- PRO – develops and specifies APIs, protocols and message formats used across oneM2M interfaces, including mapping to commonly used M2M protocols;
- SEC – has the overall responsibility for all technical aspects related to security and privacy within oneM2M;
- MAS – Management, Abstraction and Semantics deals with the technical aspects related to management of M2M entities and/or functions. It also deals with support for application specific abstraction and semantics;
- TST – identifies and defines test requirements for the oneM2M system and the services related to it. It also develops and maintains a set of specifications for conformance and interoperability testing.

We have identified the following features proposed and prototyped within the scope of the symbIoTe project as features of interest for oneM2M:

- interworking protocol between IoT platforms and service providers;
- bartering and trading between platforms;
- access control between platforms.

---

[15] http://www.onem2m.org
[16] http://www.onem2m.org/about-onem2m/organisation-and-structure

oneM2M already identifies an interaction between two platforms and names this interface Mcc’ reference point, but further details and specification of the interworking protocol using Mcc' (between 2 service providers) are currently not yet available. During the ETSI IoT Week 2018, the symbIoTe team has demonstrated the interworking of a oneM2M-compliant platform provided by Sensinov (winner of the symbIoTe OC2 call) with a proprietary IoT platform Symphony developed by NXW. The symbIoTe middleware components were used to enable transparent access to sensors and actuators controlled by the two platforms and provide both semantic and syntactic interoperability with secure interactions. Our demonstration has shown a single mobile application working seamlessly on top of two different platforms using devices with different technologies (e.g, Zigbee, EnOcean, Z-Wave and KNX) and attracted a lot of attention as example of good practice which can influence further standardisation of the Mcc’ reference point.

4.7 FIWARE

FIWARE[17] is a middleware platform that provides a set of APIs to ease the development of Smart Applications in multiple vertical sectors (such as environment, transportation or industry). The API specification is open and royalty-free, making the involvement of users and developers essential for the platform to become a standard.

The European Commission launched in 2014 the FIWARE Acceleration Programme[18] funding SMEs and start-ups with the goal of developing innovative solutions using FIWARE technology. Based on the submissions and success stories of this initiative, data models[19] have been elaborated and harmonized to enable data portability for different applications with common scenarios or use cases. This allows interoperability not only through a standard but also through the data structure. The models are intended to be used with the version 2 of FIWARE Next Generation Service Interface (NGSI) (Section 4.12), currently available in the following:

- **Alarms** related to events that require action taking
- **Civic Issue Tracking** models for civic issue tracking interoperable with Open311[20]
- **Device** with details regarding IoT devices characteristics and status
- **Environment** to monitor air quality and other environmental conditions
- **Indicator,** key performance indicators to measure success of a company or activity
- **Parking** on street and off street parking data, interoperable with DATEX II[21]
- **Parks & Gardens** to facilitate the management of green areas
- **Point of Interest** particular location of useful/interesting things (e.g., touristic landmarks, restaurants)
- **Street Lightning** to model street lights and their controlling equipment
- **Transportation** for smart mobility and efficient management of municipal services

[17] https://www.fiware.org/about-us/
[18] https://www.fiware.org/fiware-accelerator-programme/
[19] https://www.fiware.org/data-models/
[20] http://www.open311.org
[21] http://www.datex2.eu

- **Waste Management** models for effective Waste Management
- **Weather** models for weather related data (e.g. extreme weather conditions)

It is also possible for symbIoTe to contribute to FIWARE's data models by following a set of guidelines[22].

4.8 ETSI Context Information Management (ISG CIM)

The ETSI Industry Specification Group on cross-sector Context Information Management (ISG CIM) has been established in January 2017 with a goal to define standard APIs for Context Information Management in particular for smart cities applications. The general idea of symbIoTe L1 solution and ETSI CIM are quite similar since both address the problem of accessing sensor data over different IoT platforms by defining a Restful API and extendable information models. The Distributed Architecture defined by ISG CIM can easily be mapped to symbIoTe's L1 architecture: RAP is comparable to ContextSource, Core Registry is comparable to Context Registry and symbIoTe Enabler to Distribution Broker. However, the REST-based interface of the ContextSource and RAP are bound to the corresponding information models and are thus quite different.

In terms of information models, symbIoTe's CIM is comparable to the Cross-Domain Ontology defined by ISG CIM, while symbIoTe's BIM/PIM can be seen as Domain-Specific Models defined by ISG CIM. However, as much as the approaches are comparable as both rely on a core information model that can be extended, the actual information models are quite different. ISG CIM's core model is framed around context, while symbIoTe specifies devices (sensors and actuators) and services as core concepts of its information model.

Nevertheless, software components developed by the symbIoTe team represent examples of good practice and can influence further evolution of standards developed by ISG CIM since two consortium partners, namely UW and ICOM, are participating in the working group.

4.9 ETSI, TC-CYBER

ETSI TC CYBER's specific objectives include to act as the ETSI centre of expertise in the area of Cyber Security[23], advise and assist all ETSI Groups with the development of Cyber Security requirements, developing and maintaining standards, specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI. TC CYBER is also intended to identify gaps where existing standards do not fulfil the requirements and provide specifications and standards to fill these gaps. This includes coordination with the work in other ETSI committees and partnership projects to avoid duplicated standards.

The activities of ETSI TC CYBER include the following broad areas:

- Cyber Security,
- Security of infrastructures, devices, services, and protocols,

[22] http://fiware-datamodels.readthedocs.io/en/latest/guidelines/index.html
[23] http://www.etsi.org/technologies-clusters/technologies/cyber-security

- Security tools and techniques,
- Provision of security mechanisms to protect privacy, and
- Advice (guidance and operational security requirements to users, manufacturers and network and infrastructure operators).

The ongoing work item DTS/CYBER-0020 on “Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services” is specifying an application of ABE to implement “attribute based access control” (ABAC) for specific environments where access to data has to be given to multiple parties and under different conditions. This work item will describe the ABE encryption and decryption mechanisms, the boundary conditions relating to the underlying cryptography, the key distribution protocols and any related architectural aspect. Three main use cases will be addressed: Cloud, Mobile, and IoT.

In particular, for the IoT use case, is addressing edge scenarios where data access mechanisms are actioned either in the network or on the device. The objective is to retain flexibility w.r.t. re-use of the work by other standardisation bodies, such as oneM2M.

At the time of this report, no results of this SDO are being used in symbIoTe, but an eye will be kept on the activity for future purpose.

4.10 ETSI – Next Generation Protocols ISG (ETSI NGP)

The TCP/IP protocol suite is at the core of most of the modern digital communications systems providing network connectivity and transmission of applications and services for end users. The “ETSI’s Industry Specification Group on Next Generation Protocols” (ETSI NGP) was established in 2015 to review the landscape of Internet Protocols, to identify and to document requirements and to trigger co-ordinated follow up activities beyond TCP/IP, in order to support a number of Internet Protocols capable of fulfilling the new emerging requirements among others of IoT, Industry 4.0, connected and mobile objects, and 5G. For these various market segments, the ETSI NGP group is working on identifying requirements and initial scenarios where the next generation of protocols should significantly simplify the architecture and solutions. ETSI NGP is also developing other case studies in LTE-mobile networks, Industry 4.0, and multiple Packet Data Network gateways in 4G. ETSI NGP also focuses on innovative protocol solutions for addressing, security, identity, location, AAA and mobility, capable of enhancing the end-to-end control and performance of communications.

With focus on IoT, the nature of communications, scale and mobility of connected objects in IoT poses critical challenges to the traditional TCP/IP based Internet architecture, which is not fully capable of supporting large number of interconnected objects, complex event-driven IoT systems with frequent change of location, or add or drop connections. The Ultra-Reliable, Low Latency (URLLC), Internet-Of-Things (IoT) is an important use case scenario that ETSI NGP is using to highlight requirements that are difficult to satisfy with existing internet connectivity paths. Other IoT related use cases include those identified within the Massive IoT of the 3GPP SMARTER use cases (e.g., IoT Device Initialization, subscription security credentials update, domestic Home Monitoring, etc.), the 5GPPP use cases for Active Assisted Living (AAL) and cooperation between factories and remote applications.

In terms of technologies, the ETSI NGP group is analysing the various architecture and requirements alternatives defined by the different industrial alliances, such as IP Smart Objects (IPSO), Industrial Internet Consortium (IIC), and the most widely accepted protocols are based on IETF 6LoWPAN over IEEE 802.15.4 and 3GPP IoT cellular network (NarrowBand IoT, NB-IoT). Overall, ETSI NGP ISG is currently working on scenarios, future protocol stack requirements and evolved architectures for mobility using identity-oriented networks as core documents of its standard development roadmap.

ETSI NGP work on scenarios is of potential interest for symbIoTe, as well as the work on protocol stacks for future IoT. In addition, the implementation of the symbIoTe Smart Spaces can be a valuable result to present and discuss in ETSI NGP.

4.11 IETF – Constrained RESTful Environments

The IETF "Constrained RESTful Environments Working Group" (CoRE WG) was established in IETF in late 2010 to work on defining a framework for resource-oriented applications intended to run on constrained IP networks. Most IoT devices are typical CoRE systems, having communications based on limited packet sizes, being grouped in large sets of devices that may be powered off at any point in time but periodically "wake up" for brief periods. Low-Power Wireless Personal Area Networks (LoWPANs) are an example of this type of network. Constrained networks can occur as part of home and building automation, energy management, and the Internet of Things.

As of today, the CoRE WG has defined the general architecture for constrained networks in RFC6690and has defined a Constrained Application Protocol (CoAP) for the manipulation of Resources on a Device in RFC7252, RFC7390, RFC7641, and RFC7959.

The WG is currently working on the following topics:

- Resource discovery
- Operational and manageability aspects of the CoAP protocol
- RESTCONF-style management functions and their alternative in Open Mobility Alliance (OMA) Lightweight M2M (LwM2M) management functions
- Security in CoAP via Datagram Transport Layer Security (DTLS)
- Models and design patterns for CoRE devices

The full CoAP protocol specification is of interest for the symbIoTe Smart Devices communications. Current specifications (RFC or WG drafts) could be adopted in some symbIoTe devices, and thus, a close look at the WG activities is fundamental for the project consortium.

Specific aspects related to the device information modelling in symbIoTe can possibly be matured within the CoRE WG in the form of Internet drafts.

4.12 OMA / FIWARE - Next Generation Services Interface

The Next Generation Services Interface NGSI-9/NGSI-10[24] is a RESTful API based on OMA-defined specifications[25] with the purpose of exchanging availability and context information of entities (a virtual representation of all kinds of physical objects in the real world). It has been specified by OMA, further developed in the FIWARE initiative and is currently supported by ETSI. NGSI provides three main interactions:

- One-time queries for context information,
- Subscriptions for context information updates (and consequent notifications), and
- Unsolicited updates invoked by context providers.

Orion Context Broker[26] is a C++ implementation of the NGSI API, enabling the management of the lifecycle of context information. Subscriptions to resources' context work through REST-callbacks. NGSI is a viable specification for the interoperability proposed at the Level-1 compliance (application level) in symbIoTe. By using Orion as the Resource Access Proxy, IoT platforms symbIoTe-compliant would be able to push their context information in the NGSI standard.

4.13 IRTF – Things-to-Things Research Group

The Thing-to-Thing Research Group (T2TRG) has been established within the Internet Research Task Force (IRTF) at the end of 2015 to investigate open research issues in building an Internet made of low-resource nodes ("things", "constrained nodes"). T2TRG focuses on aspects related to adaptation layer connecting devices to IP, architectures and APIs for communicating, management and security functions. A number of areas of interest have been identified in T2TRG that include:

- Deployment considerations, scaling and cost of ownership
- Management and operation of "things"
- Lifecycle aspects
- Data models, formats, and semantics
- Operating "things" that have multiple masters/stakeholders (including understanding role definitions of devices, owners, operators, etc.)
- Aspects of distribution (cf. "fog computing"); reliability and scalability considerations
- Containerization and other forms of mobile code

The main goal of the T2TRG is to explore possible solutions and approaches in these fields to support the innovation cycle of established IETF WGs, like the CoRE WG. Within the general areas of interest, the group currently concentrates its work on the following topics:

[24] https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/NGSI-9/NGSI-10_information_model
[25] http://www.openmobilealliance.org/wp/
[26] https://fiware-orion.readthedocs.io/en/master/

- Management and Operation of networks involving constrained nodes
- Security and Lifecycle aspects in constrained nodes
- REST and pub/sub architectures
- Guidance for designing REST-based IoT Applications ("cookbook")

The symbIoTe architecture and the security approach for Smart Devices could be one of the project results that can be proposed for discussion in T2TRG in one of the periodic meetings it organises. The objective is to mature this presentation into a draft about guidelines to build secure and federated Smart Environments including a variety of different nodes.

4.14 AIOTI – Alliance for Internet of Things Innovation

According to AIOTI[27] self-description "*The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in 2015, with the aim to strengthen the dialogue and interaction among Internet of Things (IoT) players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT*".

One of the main objectives of AIOTI is to support the interoperability of IoT standards, bridging the gap to avoid market obstacles. Based on this, WG08 "*refers to IoT solutions used by a city in order to enhance performance, safety and wellbeing, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens*".

symbIoTe is addressing interoperability issues among existent platforms and this directly tackles the objective of this working group for solving interoperability issues. Main activity performed within this group is the collaboration in the development of a set of guidelines for creating the interoperable smart cities of the future. symbIoTe participate in the identification of gaps and was included as an interoperable platform of reference to address the issues that may arise when trying to interconnect all the existent platforms within a smart city.

[27] https://aioti.eu/

5 Standards used within symbIoTe

Currently symbIoTe already uses well established standards from the groups mentioned in Section 4. The usage of standards is an essential element for the acceptance of an architecture and, therefore, this section concentrates on the once already in use in symbIoTe or are envisioned to be used.

5.1 Semantic Technologies

- Web Ontology Language (OWL)
- Resource Description Framework (RDF)
- SPARQL Protocol And RDF Query Language (SPARQL)

5.2 Vocabularies for the Core Information Model (CIM)

- SSN (as input for the definition of the CIM, potentially as PIM with alignment to CIM)
- SensorThings API (as blueprint for the CIM)
- OGC O&M (indirect usage via SSN)
- OWL Time[28]
- Geo Vocabulary[29]

5.3 Best Practice Information Model (BIM)

- Units of measurements & Observed Properties[30] (based on Quantities, Units, Dimensions and Values (QUDV) from OMG SysML)

5.4 Protocols

- Open Data Protocol (OData) from OASIS
- OAuth (open standard for authorization)

[28] https://www.w3.org/TR/2016/WD-owl-time-20160712/
[29] https://www.w3.org/2003/01/geo/
[30] https://www.w3.org/2005/Incubator/ssn/ssnx/qu/qu, https://www.w3.org/2005/Incubator/ssn/ssnx/qu/qu-rec20.html

6 symbIoTe Assets for Standardisation

The "IoT Standards landscape and future evolutions" report [2] states: *"There are many connectivity and interoperability standards and specifications that are not IoT-specific. What is missing is the choice across verticals for one solution that allows for interoperability."* This is a strong support of the symbIoTe objectives and a clear indication for many opportunities to apply project results within standardisation activities. From the sustainability point of view, a good way to ensure that symbIoTe assets are well connected to solid user community is the integration into a standard.

From the current status of the architecture development and the performed landscape analysis in the last moths, the symbIoTe consortium sees the most potential in applying symbIoTe assets for standardisation in the following areas:

- symbIoTe Core Information Model (CIM): As the CIM is dedicated to IoT platform metadata and common resource description patterns, it may be a candidate for the Web of Things Interest Groups.
    - D2.4 Revised Semantics for IoT and Cloud resources
- Definition of compliance levels: That could be proposal for a common conceptualization of compliance levels.
    - D1.4 Final Report on System Requirements and Architecture
- Interworking API: The definition of a platform interworking API would be contribution to the oneM2M consortium and the definition of an actuator interface could be proposed to the OGC SensorThings API group.
    - D1.4 Final Report on System Requirements and Architecture
    - D3.3 Complete Federation Environment
- Bartering and trading: There is no standards definition work known for that topic and we assume there is a standardization gap. The definition of common design pattern, services, concept definitions, and probably ontology designs, could be contribution of a new standardisation working group.
    - D1.4 Final Report on System Requirements and Architecture
    - D3.1 Basic Resource Trading Mechanisms and Access Scope
    - D3.2 Resource Trading, Security and Federation Mechanisms
    - D3.3 Complete Federation Environment
- Resource Discovery Interface: A platform independent discovery concept for IoT resources is still unresolved issued. This is opportunity for the symbIoTe search and discovery concepts, to be considered by SDOs.
    - D1.4 Final Report on System Requirements and Architecture
- IoT Security: While there are many security related standards and products are available, there is not yet a dedicated and platform independent IoT-profile available. The appliance of the ABAC (attribute-based access control) concept to IoT could potentially be such a profile.

- D3.2 Resource Trading, Security and Federation Mechanisms
- D4.3 Final symbIoTe Middleware Implementation

The challenge is now to make use of these assets within the ongoing involvements between the SDO working groups and individual consortium members.

7 Conclusion

This Deliverable D7.8 reports on the task T7.4, which is the monitoring of standardization activities related to IoT middleware architectures and continues on the Deliverable D7.3. Primary sources of information for the task was the report from ETSI on the standardization landscape [2] and the AIOTI report on standards framework concepts [1]. Both reports are showing a very populated but also very fragmented landscape. Many standards are overlapping and competing, and there are many gaps when focusing on IoT specific topics.

Fortunately, the members of the symbIoTe consortium are very well connected to many SDOs and active in working groups dedicated to IoT related topics. We used that opportunity to collect inside evaluation on the standardization working groups we considered as most relevant. As a result of this evaluation, we identified many areas where standards can be and should be used by symbIoTe, and also many areas where no standards are available and where results from symbIoTe would have the potential to be recommend for standardization.

Figure 4 shows the principal relations symbIoTe has with the standards developing organisations. In the cases where symbIoTe applies a standard, there will always be some kind of adaption and evaluation work to be done. We recommend using this evaluation experiences to provide feedback to the SDO responsible for the standards. With that kind of feedback we will help to improve the standards, and we will gain visibility in the community attached to the standards.

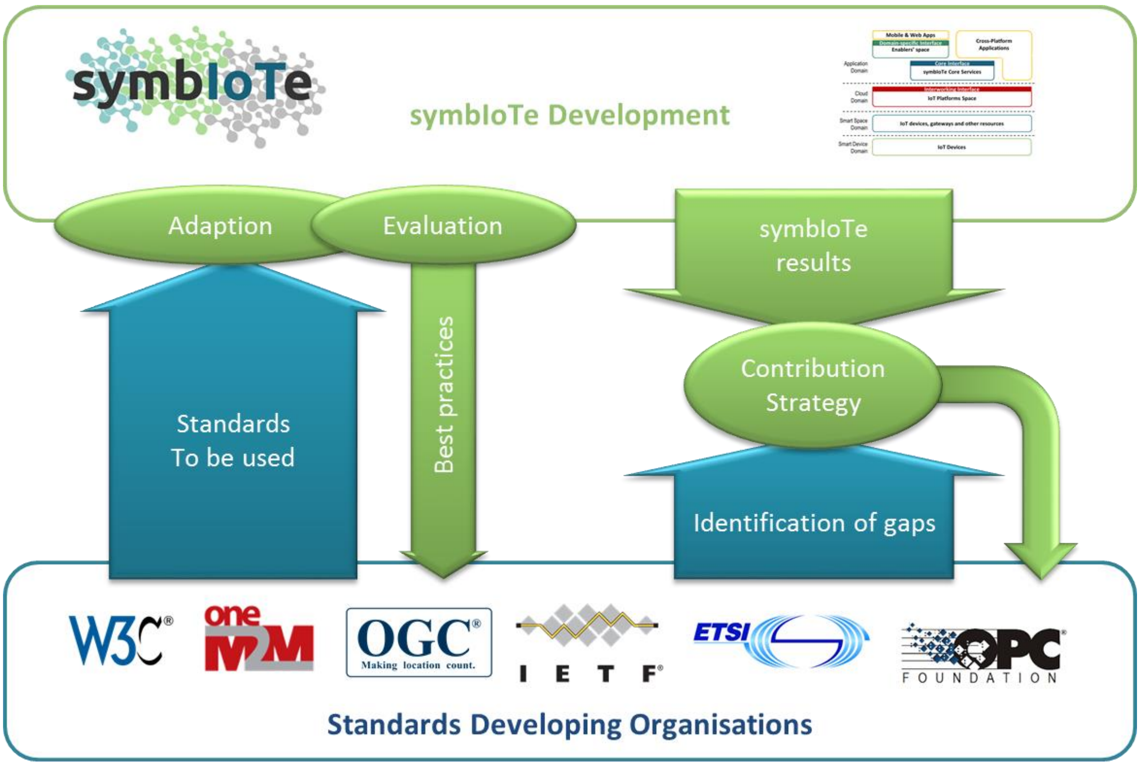

Figure 4: symbIoTe interworking with SDO's

In cases where symbIoTe solutions are not covered by standards, we found good opportunities to get in contact with SDO working groups that are active on these topics. Having symbIoTe results as a standard candidate would be one of the best sustainability models we could achieve.

From our experience, there are two general conclusions to be drawn:

1. Use standards whenever possible. Standards are the defining elements in future IoT landscapes. This is especially important for a middleware framework like symbIoTe, which is dedicated to bridge IoT platforms to enable multi domain application.
2. Find opportunities to fill standardization gaps with symbIoTe assets. In cases where symbIoTe is ahead of the SDO working group agendas, we have a unique opportunity to propose symbIoTe results as solutions for future standards. This can create a long-term impact and set symbIoTe offerings into the “pole position”.

While the task T7.4 ends, the SDO working groups will continue their work on creating the defining elements for future IoT solutions. Many symbIoTe consortium members are maintain a long-term engagement in those standards developing working groups. We are positive that many symbIoTe results will find their way into future applications and possibly into future standards as well.

8 References

[1] AIOTI WG03: "IoT LSP Standard Framework Concepts", Release 2.0, October 2015".

[2] ETSI TR 103 375 V1.1.1 (2016-10), SmartM2M; IoT Standards landscape and future evolutions

[3] ETSI TR 103 376 V1.1.1 (2016-10), SmartM2M; IoT LSP use cases and standards gaps

[4] Machina Research, White Paper on Open standards in IoT deployments, May 2016

[5] symbIoTe project Deliverable D1.2 – Initial Report on System Requirements and Architecture; 29/09/2016.

[6] Deliverable D7.3, Initial Report on Standardization Analysis and Recommendations, Version 1.0

[7] OGC SensorThings API Part 1: Sensing, Open Geospatial Consortium, 2016, Version 1.0

9 Abbreviations

AAA	Authentication, Authorization and Accounting
AAL	Ambient Assisted Living
AIOTI	The European Alliance of IoT Innovation
BIM	Best Practice Information Model
CIM	Core Information Model
CoAP	Constrained Application Protocol
CoRE	Contstrained RESTful Environments
ETSI	European Telecommunications Standards Institute
GA	Grant Agreement
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoE	Internet of Everything
IoT	Internet of Things
IRTF	Internet Research Task Force
NGSI	Next Generation Services Interface
OGC	Open Geospatial Consortium
OPC	OLE (object linking and embedding) for Process Control
OPC UA	OLE (object linking and embedding) for Process Control Unified Architecture
OWL	Web Ontology Language
POPD	Protection of Personal Data
QoE	Quality of Experience
RDF	Resource Description Framework
RDF	Resource Description Framework
REST	Representational State Transfer
RESTful	A service following the REST principles
SDO	Standards Developing Organizations
SPARQL	SPARQL Protocol And RDF Query Language
T2TRG	Things-to-Things Research Group
W3C	World Wide Web Consortium
WoT	Web of Things