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 06.10

Workshop on IoT standardisation activities

Revision: 1.00
Due date: 30-04-2019 (m28)
Actual submission date: 20-06-2019
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	**D06.10 Workshop on IoT Standardisation Activities.**				
Status	Final	**Due**	m28	**Date**	30-04-2019
Author(s)	D. Raggett (ERCIM), E. Darmois (ETSI), M. Serrano (NUIG), O. Vermesan (SINTEF), R. Bahr (SINTEF), A. Kung (TI), P. Annicchino (AS)				
Editor	D. Raggett (ERCIM)				
DoW	This deliverable summarizes a part of the work carried out in tasks T06.01 (IoT Interoperability, standards approaches, validation and gap analysis) and T06.02 (Pre-normative and standardisation activities). It includes a short summary of the "IoT Standardisation" workshop carried out on June 18th to 20th, 2019 during IoT Week 2019 in Aarhus. This workshop was composed of a number of sessions dedicated to IoT Standardisation in which the IoT LSPs, the CREATE-IoT CSA and the IoT LSP Activity Group 2 (Standardisation, Architecture and Interoperability) have been contributing and have discussed the most recent progress regarding the IoT Standardisation in general and some specific topics such as Privacy, Semantic Interoperability and the 3D Reference Architecture model.				
Comments					

Document history			
Rev.	**Date**	**Author**	**Description**
0.00	26-01-2019	SINTEF	Template/Initial version.
0.01	28-03-2019	SINTEF	Generic deliverable information.
0.02	21-06-2019	ETSI	Document structure and general information.
0.03	26-06-2019	ERCIM	Integration of Workshop contributions.
0.04	25-09-2019	ETSI, AS, MI	New partners contributions
0.05	28-09-2018	ERCIM	Integration of partners comments
1.00	01-10-2019	SINTEF	Final version released.

Table of contents

1. EXECUTIVE SUMMARY

1.1 Publishable summary

The "IoT Standardisation" workshop has been carried out on June 18th to 20th, 2019 during IoT Week 2019 in Aarhus. This workshop was composed of a number of sessions dedicated to IoT Standardisation in which the IoT LSPs, the CREATE-IoT CSA and the IoT LSP Activity Group 2 (Standardisation, Architecture and Interoperability) have been contributing and have discussed the most recent progress regarding the IoT Standardisation in general and some specific topics such as Privacy, Semantic Interoperability and the LSP 3D Reference Architecture model.

The workshop has been a good opportunity to assess the progress of IoT Standardisation and also to outline what are the current most pressing issues to address. These issues are primarily technical ones, but they also have an impact on the way the IoT standardisation ecosystem is organising in order to deal with them. Both aspects are addressed in the present document.

During the workshop, the need to go beyond the definition of the IoT Standards themselves has been repetitively outlined: all efforts in standardisation have to be systematically disseminated towards the IoT community at large (beyond the IoT standardisation community) in order to inform its participants so that they can make more informed and easier decisions regarding the use of standards in the development of IoT systems.

1.2 Non-publishable information

None, the document is public.

2. INTRODUCTION

2.1 Purpose and target group

This workshop was a very large purpose event where all the IoT community participants concerned by standardisation-related questions have been encouraged to attend. The reasons to do so

- Standards landscape for specific topics (e.g., privacy)
- Relative positioning of standards in an apparently competing situation,
- Support to further decisions related to the usage of standards

The topics discussed are of interest to a large range of the IoT stakeholders, well beyond the technical community (e.g., IoT systems designers and developers, standardisation community participants) but as well non standards-specialists such as IoT systems commissioners, city planners, etc.

2.2 Contributions of partners

ERCIM has contributed to the organization of the event, to the content of the document and several presentations during the event.

ETSI has contributed to the organization of the event, to the overall structure of the present document, to its content and to several presentations during the event.

SINTEF has contributed to the content of the document and to several presentations during the event.

NUIG has contributed to the content of the document and to several presentations during the event.

TL has contributed to the content of the document and to several presentations during the event.

AS has contributed to the content of the document and to several presentations and sessions chairing during the event.

MI has contributed to the organisation standardization related sessions at the IoT Week, and to the dissemination of the standardization activities and tools.

2.3 Relations to other activities in the project

This event has been organized within the framework of activities of CREATE-IoT WP06 (IoT Interoperability and Standardization). It has also benefited from contributions stemming from on-going work in the IoT LSPs and the IoT Activity Group AG02 (IoT standardisation, architecture and interoperability).

3. WORKSHOP SUMMARY

The "IoT Standardisation" workshop has been carried out on June 18th to 20th, 2019 during IoT Week 2019 in Aarhus. This workshop was composed of several sessions dedicated to IoT Standardisation.

The slides of presentations are available in the e-Room of CREATE-IoT and of the IoT European Large-Scale Pilots (LSP) Programme.

3.1 Context of the Workshop

This workshop was held in the larger context of the IoT Week 2019. Given the very broad scope of the conference, a great number of participants (around 1.600 persons registered) have been given the opportunity to discuss topics such as the business opportunities, new applications and services, technology evolutions, future directions, etc.

The topic of IoT standardisation has been addressed in this context with the actual possibility to attract a much larger audience to various sessions, directly or indirectly related to standardisation.

The workshop was attended by a significant number of participants from the Industry, the Academia, the European Commission (EC) but also from cities, taking advantage of the special focus put on Smart Cities. In average the sessions have been followed by 50 participants.

3.2 An overview of the workshop's standards-related sessions

3.2.1 The Standardisation Workshop

The workshop has addressed technical topics (e.g., data models; APIs and architectures; privacy) as well as more general ones addressing the nature and role of the IoT standardisation ecosystem.

The corresponding presentations were, for the most part, structured in several sessions in which a vast range of topics has been discussed.

The technical topics have been addressed in some sessions whose presentations are analysed below in details:

- The Web of Things - and the Future of Business with Smart Data (18/06/2019)
- Data Models and Semantic Interoperability (20/06/2019)
- Interoperability: Towards Common Architectures and APIs (19/06/2019)
- IoT Systems: Architectures, Models, Guidelines (20/06/2019)
- Privacy by Design in Smart Cities (20/06/2019)

In addition, some presentations have been made across various sessions and panels that are viewed as significant for the purpose of the present document.

They are addressed in the "Standardisation Ecosystem" section below and have been extracted from the following sessions:

- Smart City Standardisation – Mapping the Landscape and Capacity (19/06/2019)
- IoT Standards Trends and Convergence (20/06/2019)

3.2.2 The Joint Workshop on IoT for Smart Cities and Communities Convergence - IoT 4 SMART CITIES

In the context of the IoT Week, MI and CREATE-IoT have supported the organizing of a two-days' workshop coordinated by SynchroniCity and titled *"Joint Workshop on IoT for Smart Cities and Communities Convergence - IoT 4 SMART CITIES".* This workshop aimed at discussing and presenting the potential convergence in terms of standardization and interoperability in the smart city domain. The workshop brought together city representatives, LSP partners and SDO representatives.

The programme was structured in nine sessions:
- IoT for Smart Cities & IoT Standardization Convergence Welcome
- LSP INTEROPERABILITY: Towards Common Architectures and APIS
- LSP IMPLEMENTATION: Cities on the forefront of market creation
- Procurement and Market Place
- Wrap up of Day 1
- LSP High-Level Panel on IoT, Smart Cities and Communities for SDGs and Urban Agendas
- LSP Fair and Open Smart Cities: Growing the Local IoT Data Infrastructure Partnerships
- LSP Privacy by Design Smart Cities - Right to Privacy in Smart Cities (joint session w/IoT SEC and Data)
- Wrap up and Closing Remarks

The workshop was followed by a general session on "IoT Standards Trends and Convergence" bringing major SDOs together to discuss and propose ideas to support and accelerate the convergence towards open standards and global interoperability. This session on "IoT Standards Trends and Convergence" is analysed in details in the section 4.8.2 on "IoT Standards Trends and Convergence".

4. TECHNICAL TOPICS

4.1 Introduction

The technical work done within the EU IoT Large Scale Pilots has been dealing with a number of issues that are key for the progress of the IoT at large, in particular:

- How can the definition of data models support the variety of IoT systems domains and situations together with ensuring that interoperability remains possible and practical?
- How to ensure that the progress in Semantic Interoperability goes beyond the definition of academic solutions towards a broader adoption by the industry;
- Which kind of support can be provided to the IoT stakeholders across the IoT system lifecycle in order to understand the implications of the choices made? Which architectures, models, guidelines can help?
- Privacy is considered as a key success factor for IoT systems How can it be handled in the development of IoT systems? How can the adoption and deployment of GDPR be supported and even taken as an opportunity, especially in the context of Smart Cities where the questions of Data Ownership, Data Protection, etc. are of particular importance?

These technical issues have been discussed during the workshop, with a variety of viewpoints presented by the IoT Standardisation community in general, and the IoT LSPs in particular.

4.2 The Web of Things - and the Future of Business with Smart Data

This session was fully dedicated to the Web of Things and included three talks.

4.2.1 Open Markets of Services and the Web of Things

By Dave Raggett, W3C lead for data and champion for the Web of Things.

This talk started by noting the importance of value-added services that combine sensors, actuators and multiple sources of information. There are many application domains for such services. One example is smart irrigation. A basic solution involves a sprinkler controlled by a timer. Adding a soil moisture detector can avoid excess irrigation. Further integrating external information sources, can do even better, by reducing irrigation when rain is predicted. A much more extensive example is for smart manufacturing with rapid reconfiguration of factory resources to cater for predictive maintenance and high levels of customer specific orders. This involves many sensors and actuators as well as integration across many information systems, e.g. in respect to the supply chain and order book.

Unfortunately, the current level of fragmentation is holding this back: the large variety of different IoT technologies, proprietary ecosystems controlled by single vendors, a confusing variety of standards and standards development organisations. This results in silos that are expensive to bridge, and even when you do so, the resulting complexity makes for brittle solutions that are expensive to maintain. The IoT cannot realise its true potential until we solve this!

Suppliers and consumers of services would benefit from open markets based upon open standards, see [1]. Standards are needed to address multiple concerns:

- Standards that enable suppliers and customers to find each other and work together
- Standards for describing services, e.g. different kinds of sensors and actuators, and what they measure or control
- Standards for describing the software interfaces and data formats
- Standards for terms and conditions for service contracts
- Standards for different forms of payments

- Standards for security and enabling trust between suppliers and consumers, including the regulatory framework and legal recourse when there are disputes

Not all of this is in place, and standards development organisations need help with plugging the gaps.

W3C's Web of Things has recently advanced to Candidate Recommendation status and seeks to decouple services from the underlying IoT protocols and protocols. Things are digital twins for sensors, actuators and information services. Each thing is identified by a URI that can be dereferenced to obtain metadata in JSON-LD that describes the kinds of things and how they are exposed to client applications as local software objects with properties, actions and events, independently of the location of the sensors and actuators.

The Web of Things allows applications to supply or consume services and enables such applications to span multiple ecosystems as shown in the following diagram. Thing descriptions can include different classes of metadata, e.g. semantic annotations, the software interface exposed to client applications, and communications metadata covering security, protocols and payloads. The communications metadata is typically automatically generated by the platform that is exposing things for others to consume.

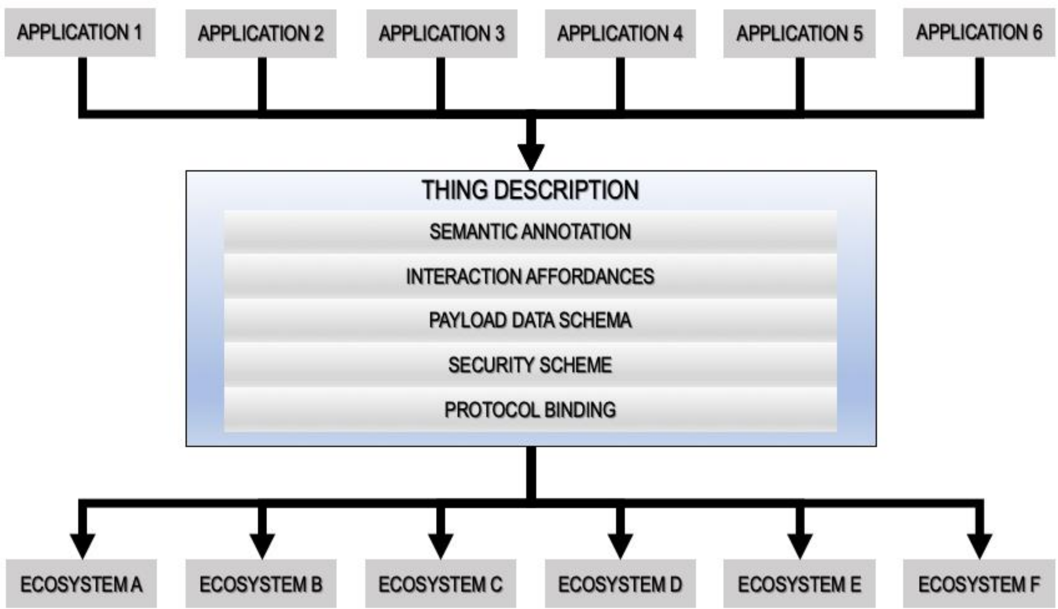


Figure 1: Thing Descriptions as a means to bridge the silos

The talk surveyed the role of the Resource Description Framework (RDF), the Semantic Web and Linked Data, and more generally graphs of nodes and edges as a basis for dealing with data and metadata. This provides a basis for addressing the semantic interoperability (how do I know what you mean), e.g. sensor reading that is a floating-point number that denotes a temperature value in degrees Kelvin. We also need to know what this measurement applies to, e.g. "reactor chamber 7".

This involves the need for agreed vocabularies of terms (*aka* ontologies) and the challenge for mapping data between ontologies developed and used by different communities. This can be likened, loosely speaking, to translating between human languages.

Whilst there is a lot of work on ontologies, is RDF and logical deduction going to scale up to millions of facts and rules, different communities with different viewpoints, and the awkward nature of all too prevalent edge cases? In practice, we can't afford to ignore uncertainty, incompleteness, inconsistency and the presence of errors. Unfortunately, traditional approaches

based upon logical deduction are unsuited to this, necessitating work arounds using rules of thumb to clean up data before passing it for further processing.

We need a new paradigm that combines symbolic and statistical approaches, inspired by decades of work in Cognitive Psychology. This paradigm focuses upon rational belief that is justified by what we were taught (prior knowledge) and what we've learned for ourselves (past experience).

This will enable many forms of reasoning: deductive, inductive, abductive, causal, counterfactual, spatial, temporal, social, emotional, humour, empathy, compassion, and reasoning about reasoning. This will make computers more like us and easier to collaborate with, rather than requiring us to act like machines. The Sentient Web is a new term for ecosystems of service, based upon the combination of digital twins, graph data and rules, graph algorithms and AI/ML.

The talk can be summarised by the following bullet points:

- Huge opportunities for open markets of services that combine sensors, actuators and multiple sources of information
- Fragmentation + over emphasis on IoT edge technologies is holding this back
- W3C's Web of Things as the solution, but further work needed on standards for open marketplaces
- The role of graph data and the need for agreement on meaning
- The emergence of the Sentient Web = awareness + reasoning = Digital Twins + graphs + AI/ML
- The need to combine symbolic and statistical approaches
- W3C as the global forum for Web technology standards
- Please get involved as standards are critical for commercial exploitation

4.2.2 AMICA – Activity Monitoring and Coaching Application

By Soumya Kanti Datta, Digiotouch

This talk looked at the role of IoT in respect to digital health as defined by enhancing the efficiency of healthcare delivery and making treatment more personalised and precise. This is being fuelled by low cost connectivity, inexpensive cloud computation, the high penetration of personal devices, a greater acceptance of digital technology and low entry barriers.

The Web of Things is promising in respect to digital healthcare, but further work is needed in respect to privacy and security. For instance, thing descriptions should only be made available to clients that have already agreed to safeguard the user's privacy. For another, personal data should be handled and processed in ways that reflect the trust of the user. Europe's GDPR is just a starting point. Digital healthcare requires multidisciplinary solutions which can create challenges for standardisation.

The talk looked at opportunities for monitoring health for active and healthy aging, with automatic and early detection of health conditions, resulting in improved outcomes and a better quality of life. By collecting data in the cloud, machine learning can be applied to diagnosis and treatment. The talk focused on AMICA (Activity Monitoring and Coaching Application) which has been developed as part of the ACTIVAGE IoT Large Scale Pilot.

Example data presented during the talk showed an instance of a sensor error, reinforcing the need to address errors, as discussed in the preceding talk. Common sense is needed for dealing with IoT data, and this is a tough challenge for automated systems.

In conclusion:

- More digitalisation will come to the healthcare sector.
- Software engineering will be a central aspect of Digital Health.
- Security, privacy, and trust are key aspects when designing winning user experience (UX).

4.2.3 Future Business with Smart Data

By Kim Nikolajsen, CGI Denmark

Most companies are on a digital transformation journey. Data created by users of smart products and by IoT devices themselves is key to gaining insight in customer behaviour and use patterns, thus enabling the development of new products and services. But, while algorithms and AI begin making increasingly important decisions in central and distributed systems, user data is not only an opportunity. It can also pose a threat. Distribution of ownership is becoming critical. This talk discussed how society as a whole, and individual users, will distribute ownership of user generated data. The talk considered how companies looking for growth opportunities can leverage data to build more consumer centric products and services.

The Web has seen the growth of huge companies that have been able to collect and monetise user data. This is exploited to offer personalised services and targeted advertising. Europe's GDPR gives users back limited control, but in practice is mostly a click-through intervention. Data ownership is a growing concern in respect to IoT devices. An example is a privately-owned car. Digitalisation will mean that the manufacturer will be able to access operating data throughout the car's lifetime. Who does this data belong to?

From the manufacturer's perspective the operation of the car's engine involves trade secrets, and it would harm their business to release this information to their competitors. From the car owner's perspective, they appreciate the idea of timelier, and more cost effective servicing, including automated software updates to the car's systems. This points to a more nuanced approach to data ownership where low-level data is the responsibility of the manufacturer, and higher level, more personal data is handled sensitively according to the preferences of the owner. In addition, data should be associated with terms and conditions that restrict its use, and which allows the "owner" appropriate control, e.g. to delete the data if so needed.

4.3 Data Models and Semantic Interoperability

This session included talks by five speakers.

4.3.1 Overall Introduction

By Dave Raggett, W3C

This talk started by reprising the importance for the IoT of open markets of value-added services that combine data from multiple sensors and information services and spanning multiple ecosystems. This is made more challenging by fragmentation. The Web of Things is a solution that decouples client applications from the underlying IoT technologies and protocols, making it easy to integrate data across different ecosystems. More details are given in the section above on "The Web of Things - and the Future of Business with Smart Data".

Interoperability across suppliers and consumers of services requires agreement at multiple levels, including protocols, data formats, data models and the meaning of data. As an example, consider a sensor reading that is a floating-point number, that denotes a temperature value in degrees Kelvin. We also need to know what this measurement applies to, e.g. "reactor chamber 7".

This requires a means to associate data with metadata that describes it. This in turn requires the use of agreed vocabularies of terms. Ontologies are vocabularies that describe different aspects of the World in terms of concepts and relationships. Different ontologies may be a widely varying levels of maturity and designed for different needs. There is a need to

make it easier for people to discover existing ontologies and to share experiences. Reuse is to be encouraged, but in practice there is a need to map data across vocabularies used by different communities, and loosely speaking this is analogous to translating between human languages, and in principle, this suggests that we may want to look at statistical approaches for data mapping, given the success of statistical approaches by Google translate and similar services.

Graphs with nodes and edges are a flexible way to represent data and metadata, can be reasoned over with rules, and operated on by efficient graph algorithms. Knowledge graphs are graphs that describe concepts and relationships, and are often in the form of taxonomies (hierarchies of terms). They were popularised by Google for smart search and are increasingly relevant to businesses for enterprise wide data management.

Traditionally, data has come in several forms, e.g. tabular databases (SQL/RDBMS), PDF documents, Comma Separate Values (CSV) and spreadsheets. We are now in the midst of a transition to graph data with rapid adoption as can be seen in the following figure.

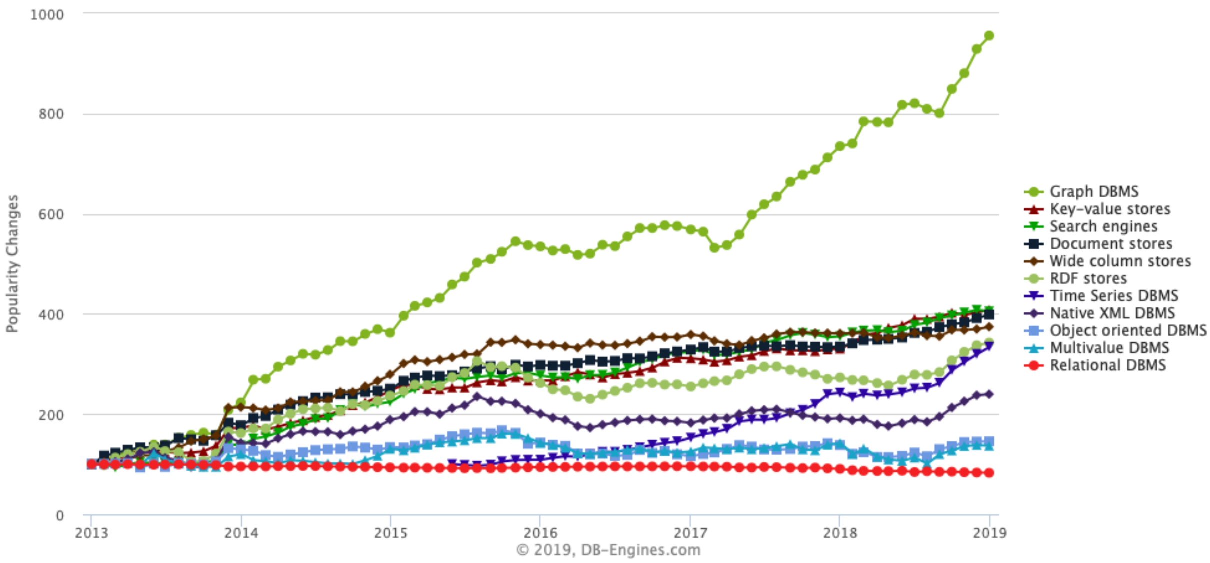


Figure 2:Courtesy of dbengines.com

Graphs are:

- Faster than using SQL and associated JOIN operations
- Better suited to integrating data from heterogeneous sources
- Better suited to situations where the data model is evolving

W3C has a mature suite of standards for graphs: RDF, Semantic Web and Linked Data, and has gained considerable traction for work on ontologies. Property Graphs are a form of graphs in which both nodes and edges may have associated sets of named property values. The ability to annotate graph edges is useful, e.g. to express the time interval a given edge is valid for, to declare the location of a sensor for a given reading, for provenance and for quality, e.g. error bars on readings, and many other purposes.

While several companies have recently brought graph databases to market, there is a lack of interoperability across them. W3C organised a workshop in Berlin in March 2019 [2] to bring together people from different communities: SQL/RDBMS, Property Graph, RDF/Semantic Web/Linked Data. A W3C Business Group is now planned to gather use cases and requirements, to coordinate future technical standards work and liaisons with other standards development organisations and industry alliances.

The value of RDF for graph data has been well established over the 20+ years since it was first introduced. RDF is perceived as difficult to use, limiting its adoption. W3C is therefore seeking to

make it easier for a much wider audience. The EasierRDF initiative [3] has the following guiding principles:

- Goal to make RDF, or some RDF-based successor, easy enough for *average developers*, who are new to RDF, to be consistently successful
- Solutions may involve anything in the RDF ecosystem: standards, tools, guidance, etc. All options are on the table
- Backward compatibility is highly desirable, but *less* important than ease of use

This is expected to lead to proposals for a higher level framework designed around property graphs. This would be layered on top of RDF and designed for visual rendering as a graph, along with if-then rules for easy operation over graphs.

One of the challenges for scaling up the use of graphs for semantic interoperability is to make it easier to discover and learn about existing vocabularies. We need to make it easier to support work on vocabularies at any stage of maturity for 2 or 3 companies getting together, to international de jure standards. What is the sustainability model for developing vocabularies?

Different communities will have different needs and different ways of talking about things. This means that the IoT needs to support integration across such differences. We will thus need scalable solutions for mapping data and services across communities and vocabularies.

- Peer to peer mappings vs mappings based on a shared upper ontology
- Context sensitive mappings
- A potential role for statistical models
- Glue code for spanning gaps

This will need to address different approaches to identifiers: URLs, URNs, local names, paths from known names, etc.

The talk introduced the Sentient Web as the means to address real-world concerns with handling incomplete, uncertain and inconsistent data that is also likely to include errors. This has already been explained in the earlier section in this report, titled: "The Web of Things - and the Future of Business with Smart Data".

4.3.2 AIOTI WG3 work on Semantic Interoperability

By Martin Bauer, NEC Labs Europe

This talk started with the premise that explicit agreement on semantics is vital to the success of IoT, i.e. we need semantic interoperability. The value of the IoT grows with the information available. Today we have heterogeneity, silos and tight coupling. For true IoT we need: sharing of information, federation across silos and dynamic use of sources.

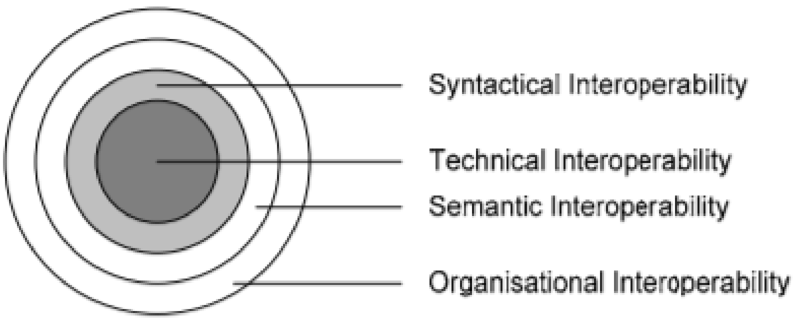


Figure 3: Interoperability requires agreement across multiple layers

What are the barriers for semantic interoperability? There are some tools, but these are currently limited to a relatively small community. There is a misguided perception that semantic interoperability is academic, difficult and for experts only. To counter this, we need to describe best practices, and to reach out and make it easier to use for all stakeholders.

AIOTI WG03 is working on two joint white papers. One is focused on developers and the other on semantic experts, standardisation engineers and standards development organisations. The following diagram illustrates the sequence for developing semantic solutions:

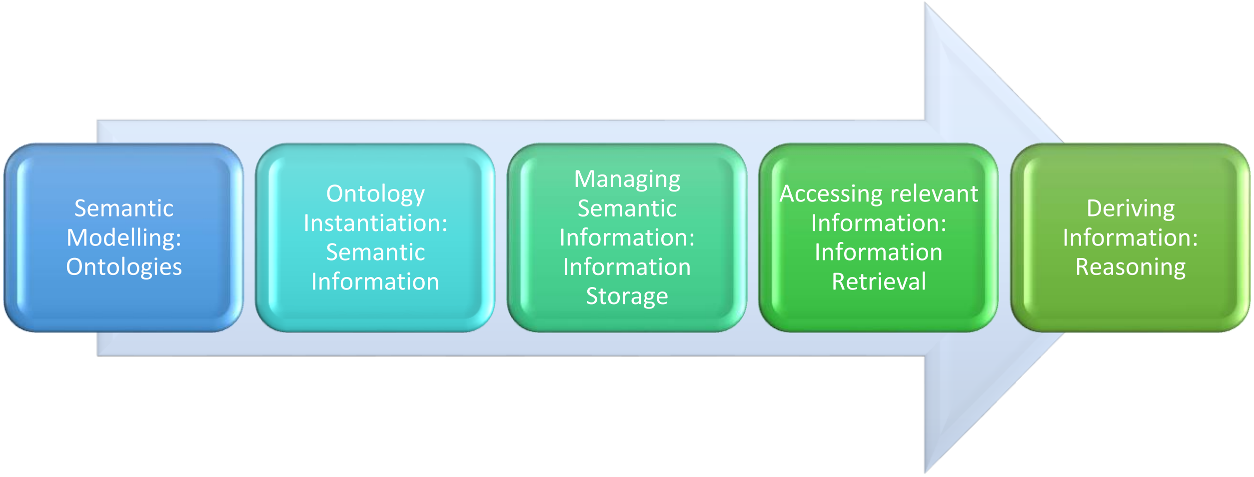


Figure 4: Lifecycle for developing semantic solutions

Best practices are defined in terms of co-creation by parties with different expertise and viewpoints, along with a modular approach to a separation of concerns. In respect to deployment, the may be a need for profiles and discovery along with support for version management. The following example was presented for coupled ontologies:

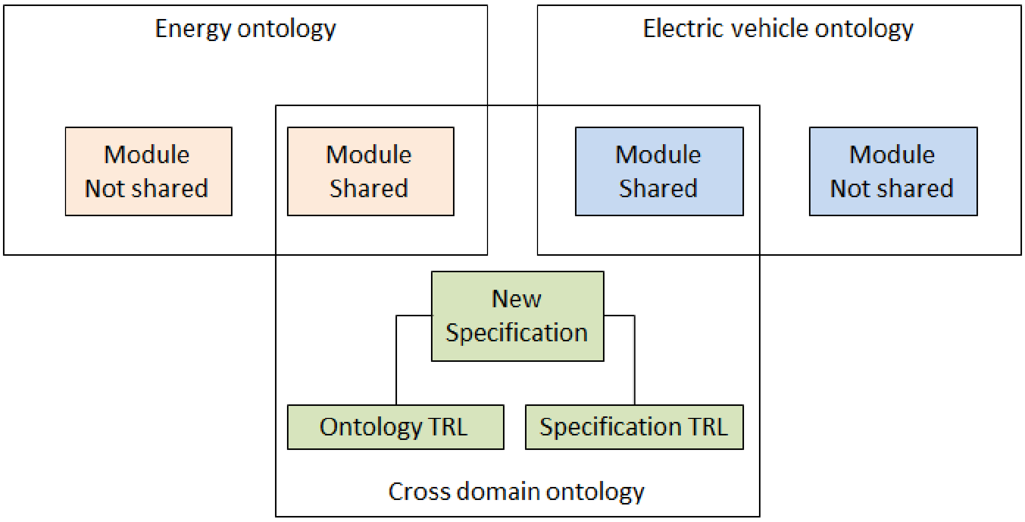


Figure 5: Maximising re-use of domain ontologies

4.3.3 Guidelines for using semantic interoperability in industry, ETSI STF 547

By Mahdi Ben Alaya, Sensinov

This talk presented the work by the ETSI Specialist Task Force 547. This describes a framework for IoT standardisation focusing on interoperability, privacy and security. The aim is to identify guidelines and best practices, and to provide comprehensive materials for information, teaching/learning and demonstration, taking a practical perspective. There are seven technical reports.

- Privacy: standards landscape and best practices TR 103 591
- Security: standards landscape and best practices TR 103 533
- Guidelines for using semantic interoperability in industry TR 103 535
- Plug tests preparation on semantic interoperability TR 103 537
- Guidance on existing standardised IoT platforms TR 103 536

- Teaching material: IoT Security TR 103 534-1
- Teaching material: IoT Privacy TR 103 534-2

In addition, SR 003 680 is a special report providing an introduction aimed at all stakeholders.

The following glossary was presented:

- **Glossary** is a terminological dictionary which contains a list of designations from a subject field with equivalents in one or more languages.
- **Dictionary** is an alphabetical list of terms in a particular domain of knowledge with the definitions for those terms.
- **Taxonomy** is a simple hierarchical arrangement of entities where you have a parent-child kind of relationship.
- **Thesaurus** is a reference work that lists words grouped together according to similarity of meaning containing synonyms and sometimes antonyms. Unlike a dictionary, a thesaurus entry does not give the definition of words.
- **Topic map** A standard for the representation and interchange of knowledge, with an emphasis on the findability of information.
- **Meta data repository** is a database created to store metadata. Metadata is information about the structures that contain the actual data. Metadata may describe the structure of any data, of any subject, stored in any format.
- **Microformat** is a web approach to semantic markup which uses tags supported for other purposes to convey additional metadata and other attributes in different contexts.
- **Ontology** is the specification of conceptualizations used to help programs and humans share knowledge. Definitions of how concepts are inter-related which collectively impose a structure on the domain and constrain the possible interpretations of terms.

STF 547 has surveyed existing solutions from academia, standards and industry:

- **H2020 IoT European Platform Initiative (IoT-EPI)**: SymbIoTe, Agile IoT, Inter IoT, Vicinity and BIG-IoT
- **H2020 Large Scale Pilots**: Autopilot, Monica
- **Industry Solutions**: IBM Watson
- **Standards and specifications**: oneM2M, NGSI-LD, OPC-UA, ETSI SAREF, W3C SSN
- **Open source**: Mainflux
- **Other projects**: Pilot test for interfacing oneM2M platform with Smart Agriculture (STF 542)

Today, developers face complex integration challenges and vendor lock-in. Centralized management of IoT solution often forces the owners to go through costly replacements to adopt mono-vendor solutions. Installation of new equipment requires costly system integration because devices are often designed to communicate with specific applications only. There is no uniform manner to access and filter the huge amounts of datasets that are generated. Huge amounts of data are generated but never get analysed and used. IoT systems remain isolated from their surroundings and environment, resulting in poor or non-existing synergies

The need for semantic interoperability in industry can be described as follows:

- **Continuous solution integration/operation**: The main idea is to quickly plug and play new equipment, networks and services in a cost-efficient manner and without disturbing the ongoing IoT system management operations.
- **Efficient data exposure:** IoT devices generate huge amounts of data. The exposure of these data sets through modern APIs allows proliferation of new services such as situational awareness, energy efficiency, preventive maintenance and smart data.
- **Centralized management of heterogenous IoT infrastructure** allows increased efficiency by setting global policies, quicker reactions and optimized decisions across all buildings. It also brings-down operational costs thanks to a single software set.

- **Wider integration** allows the IoT system to give rise to fully integrated solution supporting mass scale deployment in multiple domains. The IoT system stops existing on its own and starts to interwork with other verticals.

The simplest method of integrating data from one application to another is to manually export the data to a file and import it to the target system. A refinement is to use a process that automatically extracts, transforms and loads data, keeping data synchronised with minimum human effort.

Point to point integration involves ad hoc connections between applications for near real-time processes such as monitoring, alerting and triggering. This may become unmanageable as the number of connections increases.

The enterprise service bus is a design pattern using a hub and spoke approach instead of many point to point connections. It features a central broker capable of forwarding messages in near real-time.

The integration platform as a service design pattern features a user-friendly dashboard for designing and maintaining connections, monitoring results and resolving errors. It comes with a broad array of application and technology connectors.

The semantic interoperability platform design pattern enables heterogeneous devices and applications to understand exchanged data in a similar way, implying a precise and unambiguous meaning for the information exchanged.

In respect to market drivers: as part of improving existing services, vendors need to be proactive in the introduction of semantics to their customers. Semantics can also help with new services resulting from new user requirements, such as context awareness, collaboration, data sharing and automation.

Many companies have indicated the public sponsorship for projects and proactive roles of standardisation bodies are leading to an increased focus on semantic and its adoption, and as a driving force for innovation. Wider integration will allow IoT to give rise to fully integrated solutions, supporting mass scale deployment in multiple domains. The IoT system stops existing on its own and starts to interwork with other verticals.

Contrarywise for market inhibitors: today there is a lack of familiarity with semantic technologies due to immature supplier technology, weak development capabilities, insufficiency of experts and culture issues in industry.

There is a lack of “killer” applications and successful deployments. Many developers feel that semantic technologies are complex to understand and have a low opinion of the maturity of semantic tools as a result of the perceived gap between academic and industrial perspectives.

There are concerns about performance when processing data at a large scale, and a lack of standards and tools supporting project development, along with difficulty in projecting costs and evaluating quality performance. Semantic interoperability can be a lengthy process making it harder to justify its value to businesses focused on the short term.

The talk briefly covered ontology types and concepts, distinguishing between upper and domain ontologies. An upper ontology is a model of the common relations and objects that are generally applicable across a wide range of domain ontologies. It usually employs a core glossary that contains the terms and associated object descriptions as they are used in various relevant domain ontologies.

A domain ontology represents concepts which belong to a part of the world, such as building, energy or environment. Each domain ontology typically models domain specific definitions of terms. Since domain ontologies are written by different people, they represent concepts in very specific and unique ways, and are often incompatible within the same project.

Ontology concepts include classes, relations, instances and axioms. Classes represent a set or class of entities or things within a domain including both primitive and defined concepts. Relations describe the interactions between concepts or a concept's properties including taxonomies and associative relationships. Both concepts and relations could be organized into taxonomy. Instances are the things represented by a concept. Axioms are used to constrain values for classes or instances.

Some of the challenges with using ontologies are as follows: there is no generally accepted upper ontology in use today. Upper Ontologies are difficult to design compared to domain ontologies because they describe our consensus reality and concepts, they define are more abstract. In addition, the skillset needed to design upper ontologies are quite different from those needed for domain ontologies.

There are many knowledge niches containing tens of thousands of class definitions that still relatively limited in their conceptual breadth, depth and resolution. Today, most vertical domains have yet to be modelled ontologically. Domain ontologies need to be made publicly and connected together so that they can be normalized and mapped to one another.

Integrating ontologies can be very challenging. It easy for developers to develop new ontologies from scratch but quite hard to make them compatible with other existing ontologies.

In theory, we should be able to integrate all ontologies together, however the task of actual doing such integration is difficult in practice. Hard to express the similarity and difference in meaning between concepts, relationships, attributes and their constraints. The complexity of ontology integration increases exponentially to the number of concepts being integrated.

Some strategic guidelines for adopting semantic interoperability include a proactive attitude in analysing trends or technological features and a determined will for a successful introduction is required. Experts must persuade internally their department heads and resolved any conflict with managers who have a negative opinion of the semantic.

You should invest in communication and training: Provide educational programs for developers who do not have enough understanding or knowledge of semantic and persuaded them to participate in the programs. Communicate with sales and train them is essential to overcome their knowledge gap and can align the capability of the semantic with the needs of customers.

Providing an outline expectation upfront helps. There is a gap between the user perspective expecting substantial performance and that of supplier recognizing some limitations due to the early stage nature of semantic. The gap resulted from the frequent promotion that the reasoning engine can enable fantastic services that are not possible with existing technologies such as database and data mining.

It is valuable to promote success and expand diffusion throughout your organisation. Even though semantic is adopted, further efforts will be necessary to make it easier for the system to get diffused in an organization. A stage model of technology diffusion consists of initiation, adoption and acceptance, adaptation, routinization, and infusion.

The talk ended with some technical guidelines. You are recommended to use an upper ontology. Provide a common ontological foundation for semantic interoperability across domains (e.g. oneM2M base ontology). High-level compatibility and plausibility check for domain ontologies and their semantic integration. Fundamental concepts defined by upper ontologies covers space and time, categories and individuals, time, space, processes, etc.

Where practical, you are recommended to reuse existing domain ontologies. The ability to effectively and efficiently perform ontology reuse represents a potential solution to the problem of standardization. It is more cost effective to build an ontology reusing existing ontologies than from scratch. Reusing an ontology is far from an automated process, and instead requires significant effort from developers and experts.

You are advised to insert ontologies into the development process. During the proof of concept phase, the need for semantic interoperability is not necessarily visible. If not initially adopted, semantic interoperability becomes extremely costly and almost impossible to integrate properly in the future.

Semantic interoperability in general and ontologies in particular should be inserted at an early stage in the development process to ease the mass scale deployments of IoT systems and avoid vendor-lock in.

For more details, see ETSI Specialist Task Force 547 [4].

4.3.4 The IoT and schema.org,

By Darko Anicic, Siemens

Schema.org is a website with a set of vocabularies for smart Web search. This talk focused on schema.org extensions for IoT. The talk started by citing W3C's Candidate Recommendation for Thing Descriptions for the Web of Things, and noting that a few other IoT ecosystems have similarly provided means to express the data and interaction models for things: Amazon Web Services (AWS) IoT Things Graphs Data Model (TDM), the Alibaba Cloud Thing Specification Language (TSL) and Mozilla's Web Thing Description.

Iotschema.org is an open, publicly available, repository of semantic definitions for connected things. It is an extension of schema.org to enable descriptions of things in the physical world and their data. There is a common set of tools and patterns, and a community process for contribution and publication of standardised definitions. Domain experts can easily create semantic definitions relevant to their application domain.

Iotschema.org provides a layer to bridge device ecosystems and Semantic Web technology. It includes property and relation types to enable reuse of existing ontologies and definitions, e.g. SSN, SOSA, SAREF and QUDT.

Property types can be defined, e.g. Feature of Interest. It provides an annotation vocabulary for use in Thing Descriptions for the Web of Things, with common definitions for application specific events, actions and properties.

Iotschema.org is aimed at IoT platform providers, device vendors and SDOs, domain experts and application providers.

IoT platform providers can utilise IoTschema to make it easy for third party applications to use the platform. Device vendors and SDOs will use IoTschema to publish protocol neutral definitions of the devices with a view to web-scale adoption.

Domain experts will use IoTschema to create domain specific languages for connected things and their applications. Application providers will use IoTschema to make applications portable across platforms.

Semantic definitions consist of three categories or classes that describe a measurement or actuation of some physical property or item: A *capability* describes the smallest practical composable unit of functionality (measurement and/or actuation), e.g. the temperature of something or the brightness of a lightbulb. Capabilities have related interactions.

An *interaction* (event, action or property) describes the affordance exposed to applications for the capability, which may be to read or write a value or to perform a complex action.

Data item descriptions contain data types, units, minimum and maximum values, and other information about the data model, for example a shape or schema.

The following diagram provides an example involving an air conditioning unit:

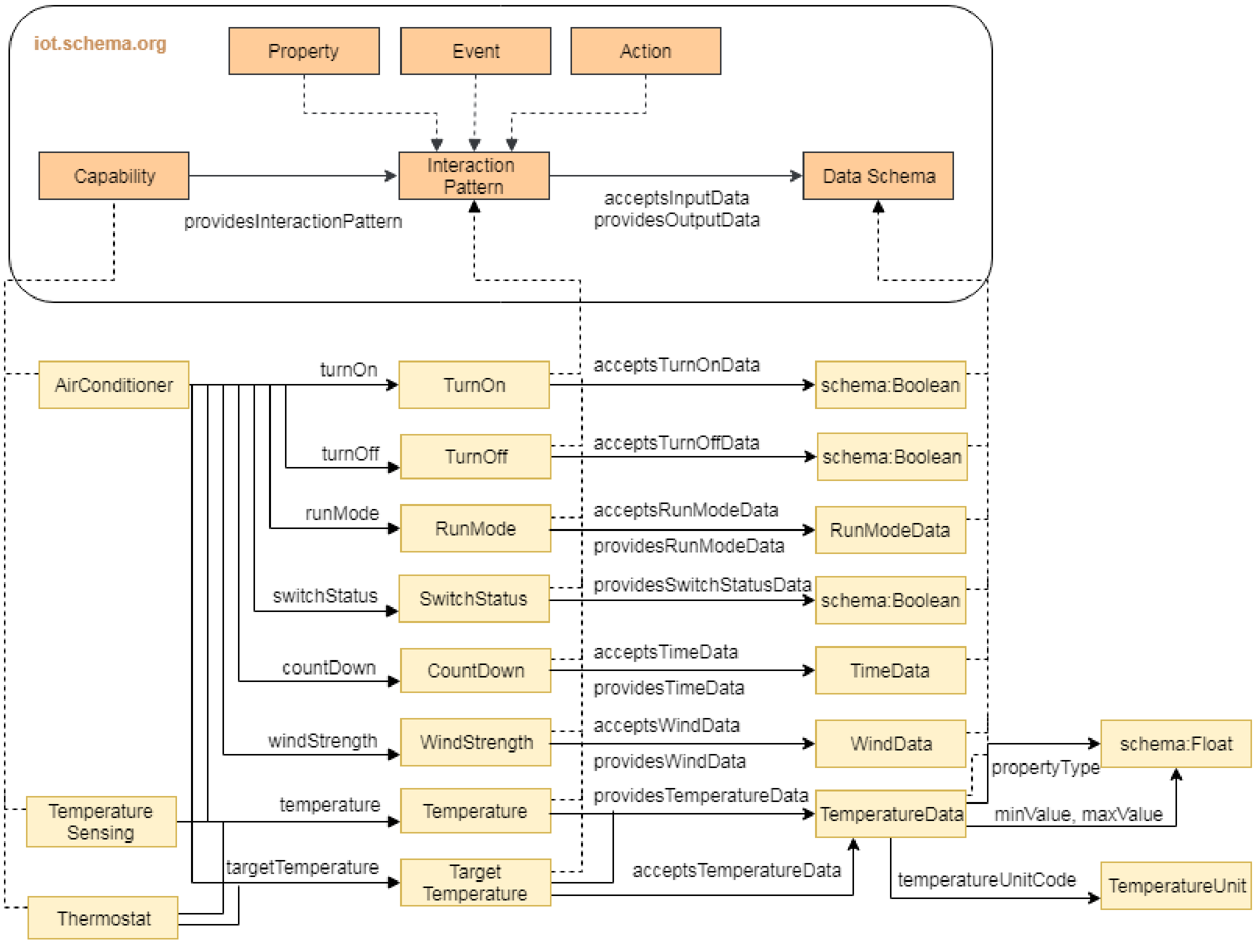


Figure 6: Modelling an air conditioning unit

The next diagram introduces features of interest.

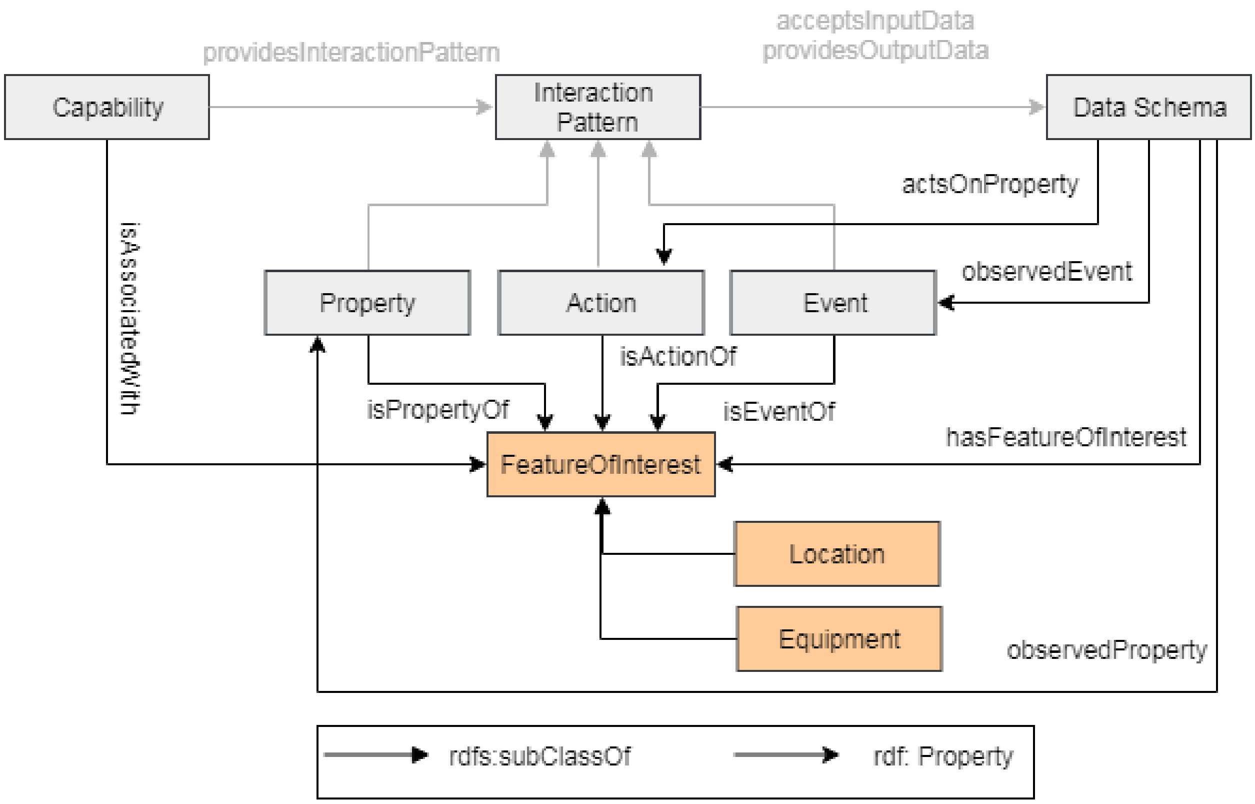


Figure 7: Extending models with features of interest

Features of interest concepts and property types can be used to describe location, equipment and other classifiers. Example include the BrickSchema definitions from Haystack. Quantity and Unit constraints can use QUDT concepts and identifiers. SSN, SOSA and SAREF can be used to extend definitions. You can contribute to IoTschema via GitHub. We have had monthly teleconferences since mid-2017. The approach has been tested at the W3C Web of Things Plugfests and WISI/IETF Hackathons, and the next step is to build out the tools and processes. This is being managed as a W3C Community Group. Current members include Fujitsu, Siemens, Google, Samsung SmartThings, Berkeley Lab, Schneider Electric, UPM, INRIA and Ericsson.

4.3.4.1 NGSI and IoT Context Information Management

By José Manuel Cantera Fonseca, FIWARE

The talk started with the following figure for the Semantic IoP @ Information management layer.

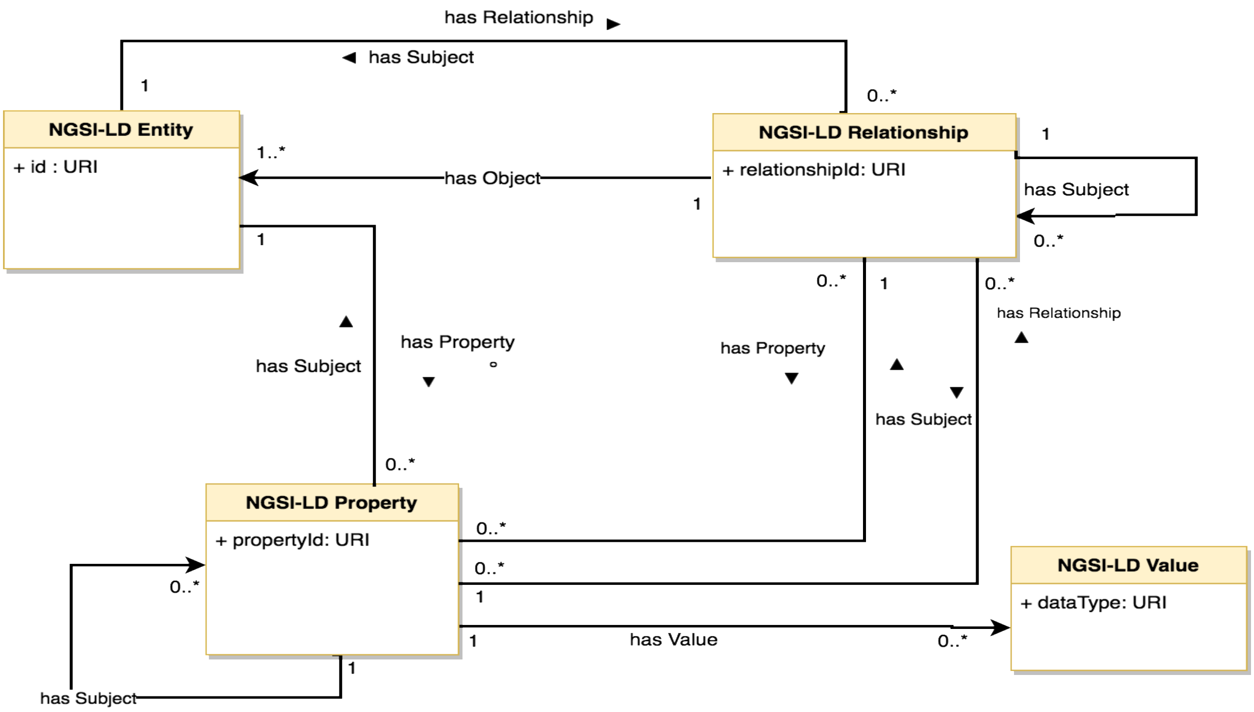


Figure 8: UML description of the NGSI-LD data model

In other words, the NGSI model defines a Property Graph where nodes (entities) and relationships can both have sets of property values. Entities are physical or virtual objects, identified by a URI, and have an entity type. Each property has a value which can be either a single value (number, string or Boolean) or a complex value (array or structured value). Relationships have a subject and an object, which may be a collection.

Here are two examples:

```
{
  "id": "urn:ngsi-ld:WasteContainer:A3456 ",
  "type": ”WasteContainer",
  "fillingLevel": {
     "type”: "Property",
     "value" : 0.85,
     "observedAt" :  “2019-22-05T12:34:55Z”,
  },
   "color" : {
     "type”: "Property",
     "value”: "green"
   },
```

```
  "@context": [
        "https://schema.lab.fiware.org/ld/context",
        "https://uri.etsi.org/ngsi-ld/v1"
  ]
}
```

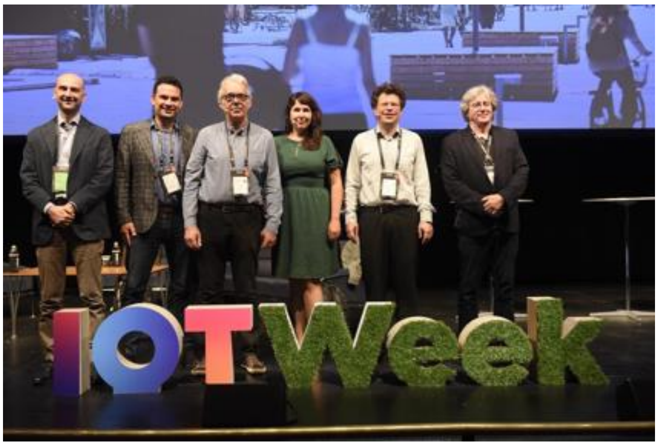

and


```
{
    "id": "urn:ngsi-ld:AirQualityObserved:Madrid:BG345",
    "type": "AirQualityObserved",
    "airQualityLevel": {
        "type": "Property",
        "value": "moderate"
    },
    "CO": {
        "type": "Property",
        "value": 500,
        "unitCode": "GP"
    },
    "temperature": {
        "type": "Property",
        "value": 12.2
    },
    "@context": [
        "https://schema.lab.fiware.org/ld/context",
        "https://uri.etsi.org/ngsi-ld/v1"
    ]
}
```


FIWARE is an open source project for an IoT platform, and has developed multiple data models, mainly for smart cities. These are described using markdown and JSON Schema. There are guidelines for creating new data models. These will be submitted to TM Forum for standardisation. An example was shown describing the relationship to W3C's Web of Things.

Some further reading:
- NGSI-LD Specification, (January 2019) [5].
- FIWARE Data Models [6].
- W3C WoT TD Specification, (CR May 2019) [7].
- ETSI SAREF Ontology [8].
- W3C SSN Ontology [9].

4.4 Interoperability: Towards Common Architectures and APIs

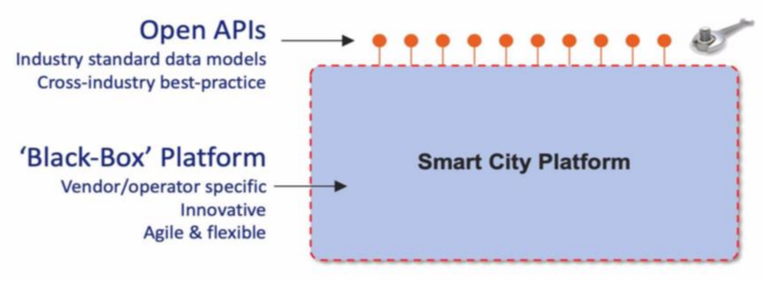


Interoperability is, since quite some time, no longer only about IoT protocols and requires more complex agreements between elements of a system that may be of very different nature, such as models, definitions or well-defined set of vocabularies, APIs or high-level architectures. These are elements of a common interoperability framework that the LSPs as well as other actors in the IoT community are trying to define.

The discussion in this session addressed this question in a pragmatic manner under a variety of angles. The session has included five talks.

4.4.1 Towards Common Architectures and APIs

By Pierre Gauthier, TM Forum



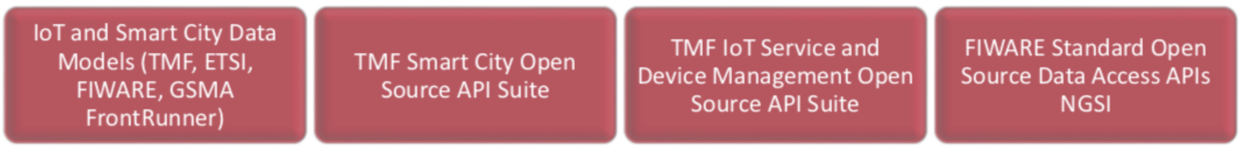
The talk has presented the TM Forum approach to the provision of Open APIs in a manner that can be compatible with the existence of a number of (often proprietary) platforms and the co-existence of standardised data models.

The TM Forum Open APIs range from IoT Device Management to complex B2B value fabrics which allow to manage arrangement between partners across business boundaries. Examples of such APIs are Product Inventory API, Billing API or SLA Management API.

Those APIs are provided in a hierarchical manner in growing proximity to the resources and devices:

- Product and Customer Management Platform: a set of APIS supporting the E2E management of Customer, Product Offerings, Orders, Charging and Billing;
- Service Management Platform: a set of APIs supporting the E2E management of Services;
- Resource Management Platform: a set of APIs supporting the E2E management of Resources and Devices.

Regarding Smart Cities, the support of data models is illustrated below:



The TMF API Component Suite for IoT Device Management is available at www.tmforum.org.

4.4.2 Interoperability in practice: results from SynchroniCity project

By Martino Maggio, Engineering Ingegneria Informatica SpA

SynchroniCity addresses how to incentivise and build trust for companies and citizens to actively participate, in finding common co-created IoT solutions for cities that meet citizen needs and to create an environment of evidence- based solutions that can easily be replicated in other regions.

Its Framework relies of a number of principles:

- Open Architecture and Open API – no vendor lock-in no city lock-in
- Interoperability, replicability and reusability across the cities and across sectors.
- Reuse of existing and standard approaches
- Compliance with existing technologies of the cities
- OASC principles and the definitions of Minimal Interoperability Mechanisms (MIMs)
  - Interoperability Points represent the main interfaces that allow a city (or any Reference Zone, RZ) and applications to interact with SynchroniCity platform. They are independent from the specific software components that realize them and can be implemented by cities in different steps to reach different levels of compliance;
  - The architecture has been designed following the OASC principles and the definitions of Minimal Interoperability Mechanisms (MIMs). MIMs, are the actual specifications of the interfaces at the Interoperability Points

The main results of SynchroniCity are regarding:

- Data interoperability: Around 30 Common data models (already adopted by Cities and applications) coming from existing initiatives and developed by SynchroniCity partners; and around 200K entities published by cities, compliant with SynchroniCity specifications;
- Software components: 11 Atomic services (generic components based on SynchroniCity specifications useful to build applications and services) and Open Sources components (to simplify the deployment of a ready-to-use SynchroniCity framework);
- Ecosystem transaction Management: to deliver a Digital Single Market for IoT-enabled smart cities in Europe and beyond; and to open innovation ecosystem around the proposed digital single smart city marketplace:
  - IoT Data Market: an open data trading platform;
  - IoT Product Market Places: a multi-service e-commerce platform.

4.4.3 Increased interoperability by simplified sharing of IoT data

By Alex Gluhak, Digital Catapult

The presentation is addressing the SynchroniCity approach to sharing data. Considering that one city is not a market, two principles are highlighted:

- Technology is only useful, if it can be effectively scaled;
- Data is only useful if it can be effectively shared.

Regarding the sharing of IoT data sources, the choice between to deploy or to buy is linked to the availability of IoT data sources.

The IoT Data Marketplaces can make data offerings in different areas (with the examples of Air Quality, Railways, Lamp posts, Traffic Lights, Scooter sharing or Parking Places).

4.4.4 Enabling IoT for Smart Cities: Open APIs and Common Data Models

By Martin Bauer, NEC Laboratories Europe

The presentation has addressed the approach of SynchroniCity regarding the reuse of information and, in particular, the Common Information (Meta) Model offered by NGSI-LD.

The challenge is to address the current reality of information silos and heterogeneous information accessible through a plethora of APIs in large scale deployments with dynamically changing sources. The information should be available on a suitable abstraction level accessible through a single API, thus allowing applications to find relevant information and be independent from specific sources.

NGSI-LD offers an information-centric API with:

- Knowledge graphs. Entities have properties and relationships;
- Annotated properties and relationships;
- Synchronous query and asynchronous subscription and notification;
- Filtering and paging;

- Geographic scoping;
- Temporal queries;
- Support for centralised, distributed and federated architectures.

4.4.5 Helsinki's standardization timeline: lessons learnt

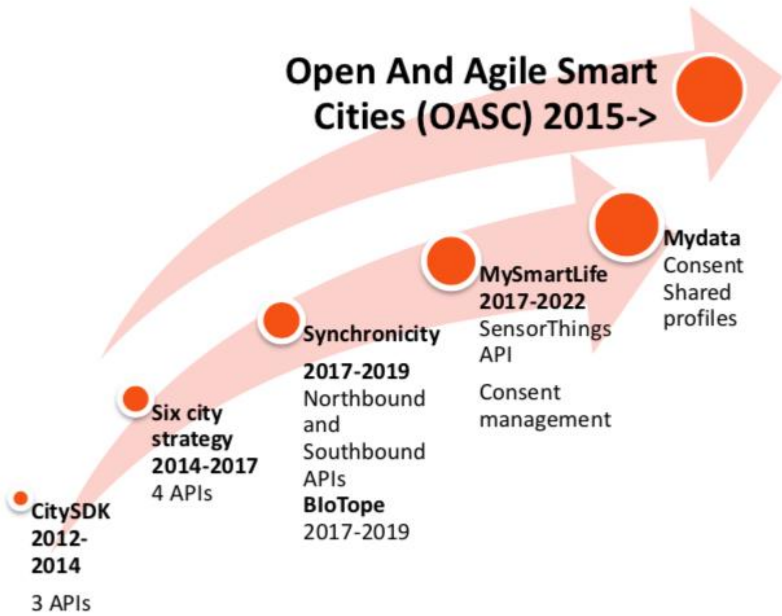
By Hanna Niemi-Hugaerts, Forum Virium Helsinki

The Helsinki approach for an open and modular IoT infrastructure and ecosystem taking out friction from utilizing data and IoT technologies is to develop new means for collecting meaningful data; to support piloting through physical and digital platforms and technologies; to provide funding and resources, training and workshops and to build a digital single market.

Three approaches are used from BIoTope (contributing to Open Group's O-MI/O-DF ecosystem), MySMARTLife (contributing to OCG SensorThings data model) and SynchroniCity (driving DSM for IoT-enabled Smart City solutions.

This results in an API harmonisation timeline.

- Validated through pilots;
- Using precommercial procurement as a tool for shaping the landscape;
- Fostering harmonisation through co-created platforms;
- Guidelines and principles (GDPR interpretations and implementations, installation policies, city engagement models)
- Documentation and dissemination (Harmonised Smart City APIs; Open API recommendation for cities)
- Collaboration at all possible levels.



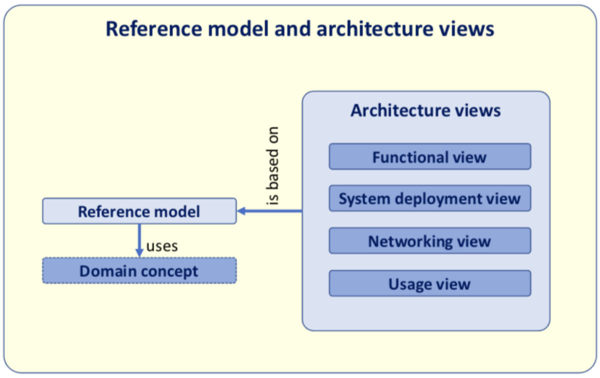
4.5 IoT Systems: Architectures, Models, Guidelines

One issue, sometimes overlooked, in the provision of effective IoT systems is the involvement of all stakeholders across the entire lifecycle of the system. This implies providing support to the IoT stakeholders in order to understand the implications of the choices they have to make. The objective of the session is to address architectures, models and also guidelines.

The session has included three talks.

4.5.1 Preparing the ISO/IEC 30141 IoT reference architecture edition 2 through a mindshare

By Osten Franberg, 1Akonsult (presented by Antonio King, Trialog)



The ISO/IEC 30141:2018 IoT Reference architecture has been developed between October 2014 and August 2018 in five stages. The Reference Architecture is used for building Context Specific Architecture (CSA) that are used to build IoT-Systems in specific domain(s).

ISO/IEC 30141 offers reference models and architecture views.

The functional view is using two main dimensions:

- The Domain functions that identify basic building blocks (e.g., BSS, Access Control) into a layered model (from Physical Entity Domain up to User Domain).;
- The Cross-Domain Capabilities like Connectivity, Security, PII protection.

The development of Edition 2 has started in August 2018, based on the experience of creating Edition 1, with a publication target in 2021/22 and main objectives of:

- Improved quality;
- Sharing a similar vision on IoT reference architecture (Mindshare);
- More guidance on integration;
- Addressing new technology (AI, Big data, Interoperability, Cloud, Blockchain etc.).

A great focus is put on Mind Share: cooperation with standards organisations for share of minds on key technology in IoT. This is done through liaisons or participating in mirror groups at national bodies level.

Amongst the topics addressed are:

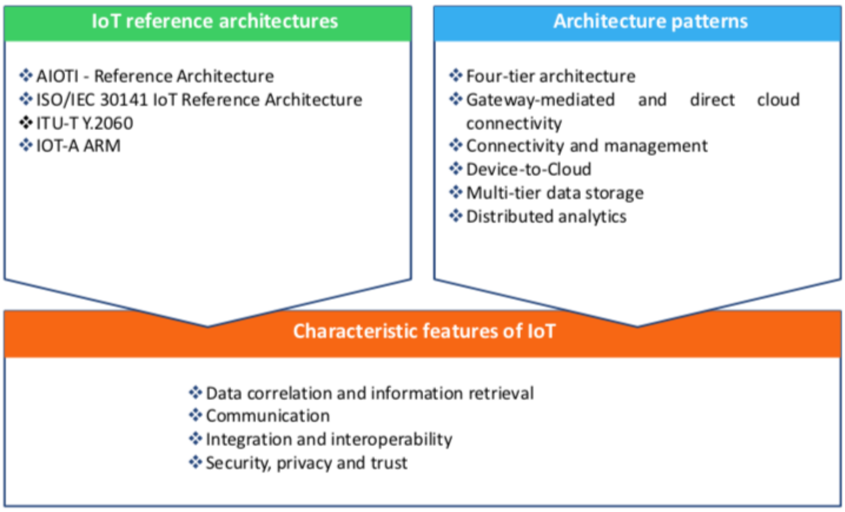
- the collaboration with the ISO/IEC JTC1 study group on “Meta Reference Architecture and Reference Architecture for Systems Integration”. A workshop will take place in Montreal in August with the participation of a representative of the IoT Large Scale Pilots Activity Group 02 (Interoperability and Standardisation);
- the collaboration with open groups such as AIOTI, in particular regarding White Papers on Semantic Interoperability.

4.5.2 3D IoT Architecture

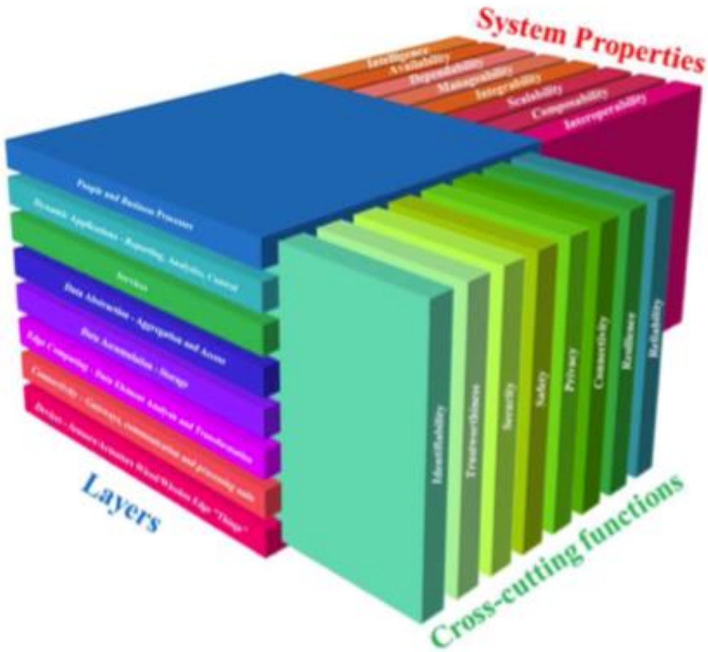
By Ovidiu Vermesan, SINTEF

The presentation has focused on the Architecture approach of the AUTOPILOT IoT Large Scale Pilot (LSP).

The approach taken is to relate to IoT Reference Architectures (with the aim to propose a 3D Reference architecture), generic architecture patterns (considering current developments such as cloud or edge computing; data analytics; etc.) and specific characteristics of IoT.



The resulting LSP model (developed in the IoT Large Scale Pilots Activity Group 02 “Interoperability and Standardisation”) offers an extension of current architectures and is aiming at ensuring a common view of the different layers of the IoT systems from Physical up to Business; and providing additional viewpoints to the different stakeholders (not just to the developers);



Those additional viewpoints are introducing two additional dimensions to that of the layered functional view, regarding cross systems functions such as security, privacy or safety and properties (e.g., integrability) that support shared analysis of some between different stakeholders.

The additional dimension of properties is a new way to discuss the properties of the IoT system between different involved parties (e.g., users, contractors, designers) and identify the elements in support (e.g., functional building blocks, APIs) and those missing

The resulting Reference Architecture is a 3D Reference Model that has been used to analyse an AUTOPILOT pilot site (in Versailles, France) on Urban driving.

This architecture consists of a 3D representation presenting the key components for IoT/IIoT applications under the 8 layers, the cross-functions and system properties views. The applications may require different components presented in the architecture depending on the requirements and specifications.

The 3D architecture is generic and offers a representation that can include the different IoT/IIOT applications across different sector domains (e.g. automated/autonomous vehicles, smart farming, wearables, smart cities, energy, manufacturing, health, etc.). The architecture includes the function by design concept with end-to-end functions addressed across the 8 layers. This allows to address the heterogeneous applications including different IoT platforms and processing at the edge, fog and cloud.

The architecture allows to address the device management, capabilities, including command/control of devices and the inclusion of various gateways for implementation of the different functions across the 8 layers. The services that ingests events from IoT devices and the message broker functions implementations between devices and backend services can be highlighted using this new 3D architectural views.

The 3D architecture provides an optimised view of the stream processing across the 8 layers allowing to evaluate the rules and functions for analysing the information streams.

By including the system properties view elements as intelligence, dependability, manageability, integrability, composability, interoperability can be specified and implemented across the 8 layers.

The intelligence system property allows defining for example machine learning components across the 8 layers for predictive algorithms to be executed over historical IoT data, enabling scenarios such as predictive maintenance.

Information transformation across the 8 layers and the aggregation of IoT data stream can be specified for different applications including protocol transformation and interoperability interfaces.

This 3D Reference Architecture is meant to be fed to the discussion initiated by ISO/IEC JTC1 outlined in the previous presentation.

4.5.3 IoT Standards: A Global Approach The ETSI Specialist Task Force 547

By Emmanuel Darmois, ETSI STF 547

The intrinsic complexity of IoT have a profound impact on IoT Standardisation and how standards are actually used. It is therefore difficult to make decisions in a fragmented standards landscape. Standards are only a party of the picture. Addressing IoT systems complexity requires not only to deal with IoT characteristics (e.g., stakeholders' involvement, technical strategy) and more technical aspects (privacy, security, interoperability), but also to integrate some important aspects such as stakeholders and roles; Reference Architecture; support to the non-specialist involved.

This is the approach taken by the ETSI Specialist Task Force (STF) 547 with the purpose to provide the elements of a framework for IoT standardisation addressing interoperability across IoT domains, focusing on major aspects (such as Semantic Interoperability; an end-user focused approach to Privacy; methods and techniques for Secure IoT) whose essential objectives are to

- Identify guidelines and best practices
- Build a bridge for potential designers / implementers of IoT systems
- Provide comprehensive material for information, teaching/learning and demonstration with a very practical usage and implementation perspective

The STF has developed a set of 7 coordinated Technical Reports, including one providing teaching material for Privacy and for Security. These reports are introduced by a Special Report to be seen as an umbrella document for the non-specialist, associated with the analysis of relevant use cases.

Some take-aways are provided, regarding in particular:

Privacy:

- See section 4.6 below.

Semantic Interoperability:

- Market inhibitors
  - Lack of familiarity with semantic
  - Lack of killer applications and successful use cases
  - Complexity and immaturity
  - Uncertainty regarding scalability and performance
  - Difficulty to perceive immediate value
- The ontology problem
  - No generally accepted upper ontology in use
  - Many fragmented knowledge niches
  - The ontology integration nightmare
- Guidelines proposed
  - Strategic: decision, investment, promotion, …
  - Technical: use upper ontology, reuse domain ontology, adapt the development process, …

Standardised Platforms:

- Lessons learned
  - Still fragmented & immature landscape
  - Proprietary platforms are not a panacea
  - Open platform adoption in the Enterprise is (even more) complex

    - The key role of integration
    - A growing role for standardised solutions
    - Semantic Interoperability is a key issue and enabler to open platform adoption
    - Many issues related to platform adoption are cultural
- Conclusion:
    - Standardised platforms can be considered
    - Strategy choices (proprietary vs standardised, development organisation, training, …) are as important as technical ones

4.6 Privacy by Design Smart Cities - Right to Privacy in Smart Cities

Mandat International in conjunction with the SynchroniCity Project has organized and participated into the session on *Privacy by Design Smart city*. The session has included four talks.

4.6.1 Human Centric Approach in IoT

By Olajumoke Ogunbekun, ETSI STF 547

The ETSI Specialist Task Force (STF) 547 has produced two Technical Reports regarding Privacy: one on the "Standards Landscape and Best practices" and the other one as "Teaching Material" on Privacy.

The challenge of Privacy in IoT identified as a basis for the report are mostly:

- IoT forms a clear example of hyper connectivity and distributed control;
- Appropriate safeguards are needed to ensure that individuals' right to privacy is effectively protected;
- The following are some of the challenges in identifying:
    - the stakeholders that are impacted by Privacy
    - the personal data and who is responsible for the data
    - privacy in various domains in IoT
    - how stakeholders need to think of Privacy as part of design not an afterthought the implication of non-compliance with Regulation not just standards.

In addressing the privacy gaps, the STF547 work showed that there does not appear to be any new standards or regulations needed with respect to privacy. The effective use of existing standards and regulation in a circular manner would seem to be sufficient to maximize the possible resulting benefits. What is suggested is the need for new codes of conduct and certification, as they are clearly embraced as accountability tools under the GDPR and they are, of course, highly relevant, also, for the IoT environment.

Key Takeaways:

- GDPR is mandatory
    - An effective protection of privacy and (personal) data protection requires technical and organizational measures
    - Organizations need to deliver documented and continuous proof of appropriate levels of protection
    - Compliance with GDPR should not be a mere a ''box-ticking exercise'' but should aim at the effective protection of personal information in reality
- A holistic approach of IoT would presume the engagement of all IoT stakeholders and would, therefore, possibly, increase the likelihood of their wide adoption and actual implementation;
- No new standards or regulation needed on privacy but:
    - Any new IoT standard should be adapted to GDPR
    - Need for new codes of conduct and certification

4.6.2 What is privacy and how should we design it?

By Robert Lewis-Lettington, UN Habitat

The common base elements of data privacy as described in ISO 29100:
- consent and choice,
- purpose,
- collection limitation,
- data minimization,
- use limitation,
- accuracy and quality,
- openness/transparency/notice/,
- individual participation and access,
- accountability,
- security

The presentation has addressed the following questions:
- What do we understand by privacy?
- Is loss of privacy always a risk?
- Can privacy and service be balanced?
- Is privacy a distraction?
- What are we designing: A socio-legal framework or technological solutions?

4.6.3 Privacy by Design - Smart City

By Sebastien Ziegler, Mandate International

Through the different Smart City pilots carried by the SynchroniCity project in different cities the following remarks came out.

There is a Dilemma between Open Data & Interoperability (Open API & Pre-Standardization) and Privacy & Personal Data Protection implying close monitoring and innovative approaches.

Considering the main privacy and data protection risks for smart cities which are – first of all User/Market acceptance, secondly non-negligible legal risks, financial and political and reputational risks – the main objective is to ensure data protection.

With the European General Data Protection Regulation (GDPR), putting pressure on this market and all markets, it is essential to identify and mitigate any privacy related risks, to organize Data Protection Officer functions, to develop specific tools and resources for smart cities and to educate and promote data protection.

A promising strategy is to put in place a detailed Data Management Plan with guidelines for Data Protection, Open Data Access and Data Processing and retention policy.

Besides the centralization of Data Protection Coordination, a Project DPO (MI) to which the local DPOs report is recommended. These functions endorse different responsibilities. The DPO needs ensure GDPR compliance and monitoring as well as running a Data Protection Impact Assessment (DPIA). The local DPOs need to coordinate and enforce Data Protection

policies, manage issues and report to the main DPO.

According to article 25 of the GDPR, the implementation of appropriate technical and organisational measures such as pseudonymisation and data minimisation is essential to ensure data protection by design.

For this reason, the Data Protection Impact Assessment (D01.04) was created within the project SynchroniCity to map the stakeholders, data flows and processes and to analyse compliance and risks for Smart Cities.

The DPIA encompasses EU (GDPR), national and international obligations, is compliant with ISO standards and is applicable to various emerging technologies (Smart Cities, Big data, Internet of Things, etc.)

As for the transparency of the approach, the duty to inform is required per Article 12 of the GDPR. "*The data controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form*…[and]… the controller shall facilitate the exercise of data subject rights".

Thus, SynchroniCity has come out with a user-friendly solution that allows citizens and the smart cities' inhabitants to know all the data collecting devices and other IoT devices that are around their area and to report new ones.

Engaging the users in this process fosters awareness raising and facilitates the DPOs working functions while enabling total transparency.

In a nutshell, legal financial and political risks of managing data are not to be underestimated and the GDPR provides large potential for innovation.

By anticipating the needs of the users and their perception, raising awareness and implementing data protection policies and continuous improvement measures in accordance, privacy by design can be respected in any smart city.

4.6.4 Privacy by Design - Right to Privacy in Smart Cities

By Berit Skjernaa, Alexandra Institute

The presentation in one sentence: Privacy requires human centricity

- Our mission is to empower individuals by improving their right to self-determination regarding their personal data

The principles of MyData:

- Human centric control and privacy
- Usable data
- Open business environment

How it works:

- A concept: API ecosystem + Platform Model + MyData Model
- MyData Operators: Personal Data Spaces (PDS), Personal Information Management Services (PIMS), Information Banks, Information Fiduciaries, Data Facilitators …
- An approach to the newcomers: Think about
    - How are you and your organisation addressing the challenges, and moreover the opportunities on how personal data is used today?
    - How can we make the digital world a fairer and safer place for all citizens, locally and globally?

More on MyData 2019 conference [10].

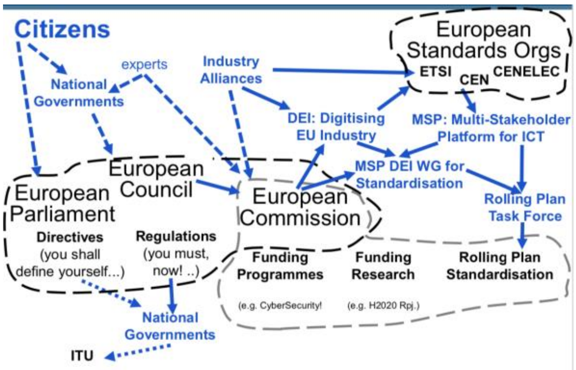
The IoT Standardisation Ecosystem.

4.7 IoT Standards Trends and Convergence

Two presentations of this session are analysed below.

4.7.1 How IoT platforms for smart cities DO converge towards an ecosystem of interoperable resources

By Lindsay Frost, NEC Laboratories Europe



What the problem is: “Cities need solutions; SDOs offer modules”. Atomisation is the culprit.

Smart Cities using IoT need solutions which are integrated, flexible, replicable, scalable, standards based.

Standards development is achieving Minimum Interop Methods (but in many, many ways and organisations!)

Who is working on it?

- Global Standards Bodies
- De Jure SDOs and De facto SDOs (fora)
- ETSI and ETSI technical groups and ISGs (Industry Specification Groups)
- Policy Makers, politicos, experts

That is not the chaos, that is an ecosystem and we have to grow with it.

The presentation shows a possible tool to gather a mind map of the 600+ organizations and groups that work in the Smart City standardisation space with URLs, abstract:

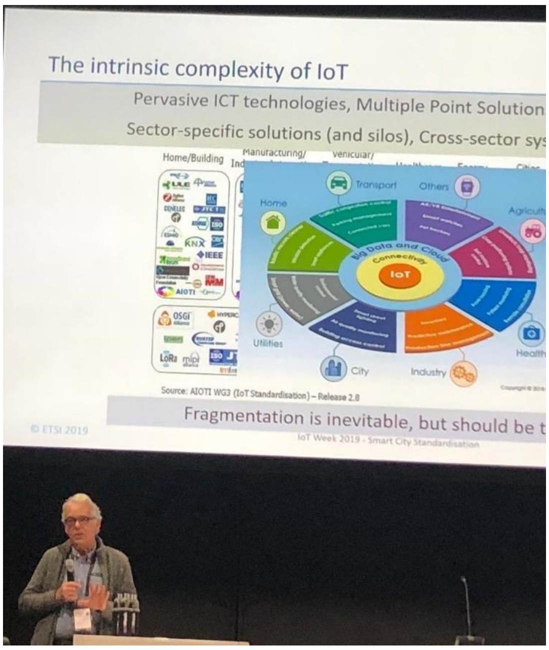
- Simple tools exist to compile, share, crowd-source filter the specs
- Volunteers needed to adapt/improve/share list of specs (... and one size does NOT fit all!)

4.7.2 De-fragmenting IoT

By Emmanuel Darmois, CommLedge

The intrinsic complexity of IoT:

- Pervasive ICT technologies, Multiple Point Solutions (e.g., protocols)
- Sector-specific solutions (and silos), Cross-sector system deployment
- Fragmentation is inevitable but should be tamed.



Some possible remedies are outlined:

- SDO collaboration with the example of oneM2M;
- Meta standards with the example of the LSP 3D Reference Architecture (see 4.5.2);
- Stakeholders guidelines with the example of ETSI STF 547 (see 4.5.3);
- Citizens involvement with the example of ETSI STF 561 that addresses the problem of the involvement of citizens in the development of standards related to Smart Cities. The objectives of the project are to:
    - Take a first overview of what the needs of citizens in smart communities are

- o Relate those needs to standardisation activities, ongoing or foreseen, and assess if they are being met; If not, make recommendations as to how to rectify this;
- o Lay down some basic principles as to how citizen needs should be addressed Make recommendations to standardisation (not standards)

Though the approach may not be silver bullet (the complex IoT and Smart City ecosystem is here to stay), some progress can happen for instance in the consolidation of the (currently cluttered) communication layer, in more coordination between the plethora of standards organizations involved or in converged vocabularies for users to improve currently difficult stakeholder's communication.

4.8 Smart City Standardisation – Mapping the Landscape and Capacity

The session has included five talks.

4.8.1 Interworking between Information Silos with NGSI-LD API

By Lindsay Frost, NEC Laboratories Europe (ETSI Board Member, ETSI ISG CIM Chairman)

The NGSI-LD Information Model prescribes the structure of context information that shall be supported by an NGSI-LD system. It specifies the data representation mechanisms that shall be used by the NGSI-LD API itself. The NGSI-LD Information Model is defined at two levels: the foundation classes which correspond to the Core Meta-model and the Cross-Domain Ontology.

Smart Cities need Information Management "between silos".

Information Management is being considered by all major SDOs.

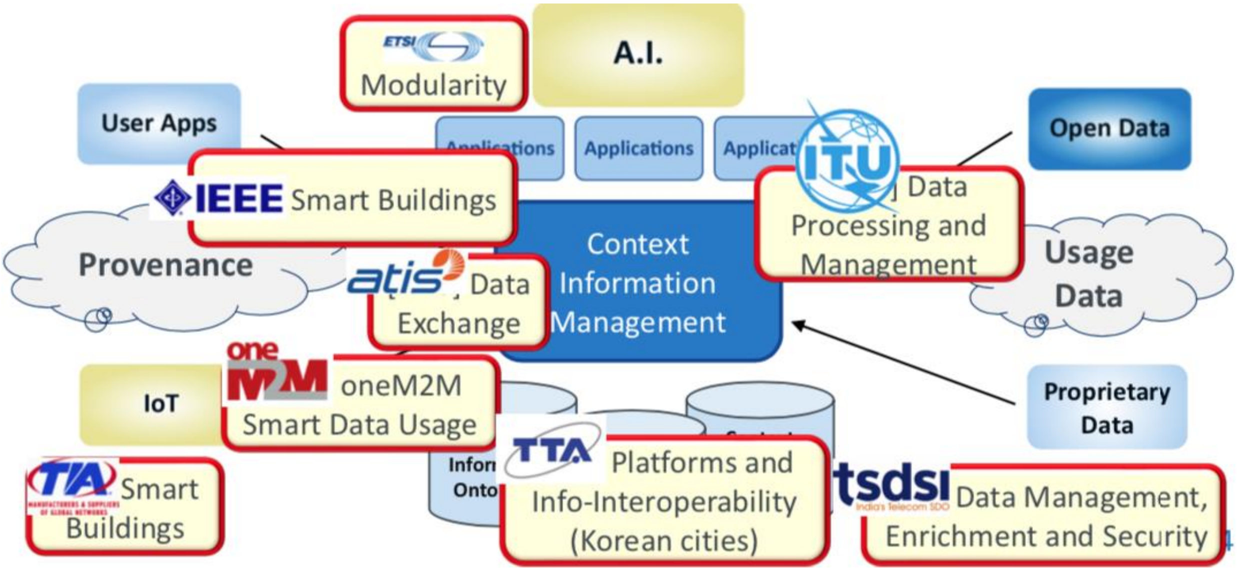


Figure 9: Information management

NGSI-LD can help in cross domain apps, e.g.:

- Show the air-pollution geomap near you, whatever your city
- Show the combined traffic/crime/rental "heat map" to help locate a new apartment to help city planners
- Combine public-transport usage data with "special deals" on tickets data, to help determine optimum usage?
- Compare hospital admissions data, with weather and pollution data, to help plan emergency services (i.e. reduce spare capacity, but make sure surges can be covered)

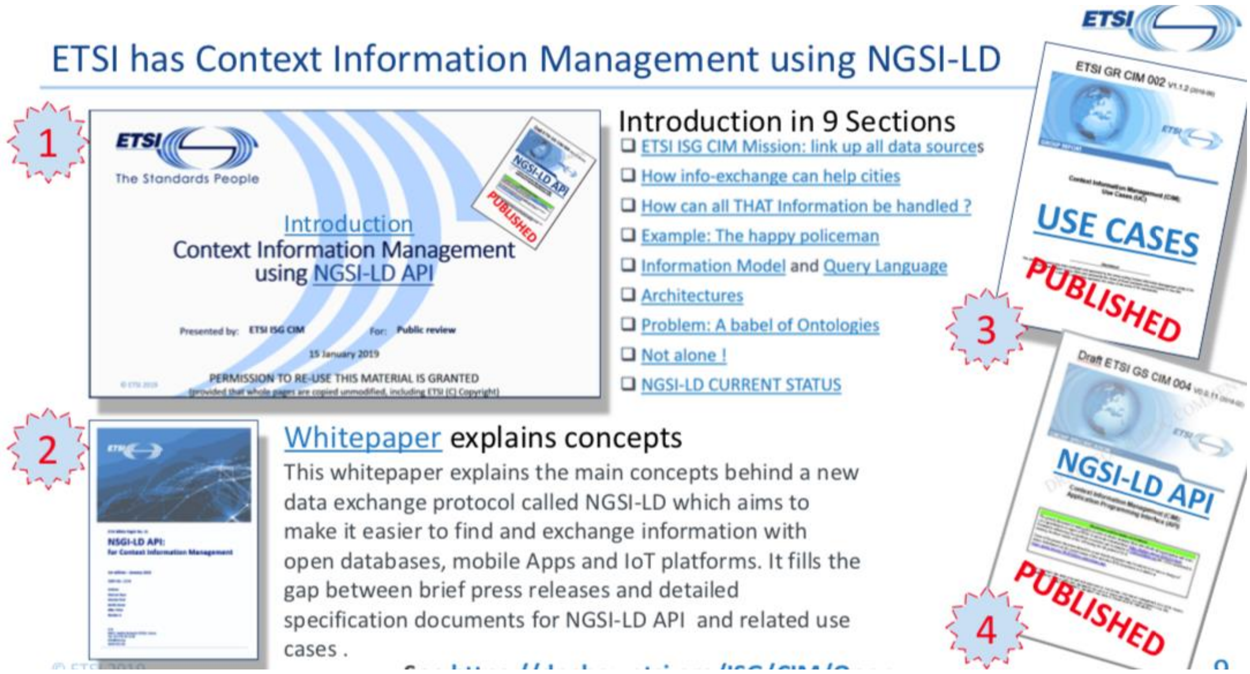


Figure 10: Introduction to Context information management using NGSI-LD API

4.8.2 IoT Standards Trends and Convergence

Pierre Gauthier, TM Forum

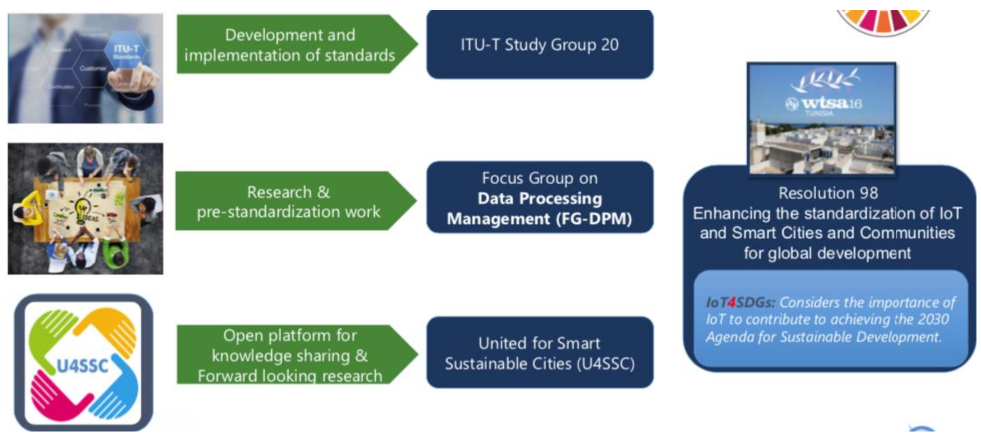
A large part of the presentation can be found in 4.4.1 which presents the TM Forum approach to the provision of Open APIs in a manner that can be compatible with the existence of a number of (often proprietary) platforms and the co-existence of standardised data models.

More details are provided regarding:

- The TMF Business Framework APIs Version 2.0;
- The TMF Data Model entities;

4.8.3 ITU-T: IoT and Smart & Sustainable Cities and Communities

By Ramy Fathy, NTRA



The presentation addresses the ITU-T activities on IoT & Smart Sustainable Cities.

The Study Group 20 is responsible for studies relating to IoT and its applications, and to smart cities and communities.

It includes studies relating to Big Data aspects of IoT and SC&C, e-services and smart services for smart cities and communities (SC&C).

The most recently approved ITU-T recommendations for IoT and Smart Cities include:

- Recommendation ITU-T Y.4114 "Specific requirements and capabilities of the IoT for Big Data". This Recommendation complements the developments on common requirements of the IoT [ITU-T Y.2066] and functional framework of the IoT [ITU-T Y.2068] in terms of the

specific requirements and capabilities that the IoT is expected to support in order to address the challenges related to Big Data;

- Recommendation ITU-T Y.4115 "Reference architecture for IoT device capability exposure". This Recommendation specifies reference architecture of IoT device capability exposure (IoT DCE) which supports IoT applications in DCE devices (e.g., smart phones, tablets and home gateways) to access device capabilities exposed by IoT devices connected to the DCE device.
- Recommendation ITU-T Y.4805 "Identifier service requirements for the interoperability of Smart City applications". This Recommendation explores the set of requirements for identifier services used in Smart City. An identifier service for Smart City must be scalable and secure, and not only promote interoperability among different Smart City applications, but also compatible with any existing practices in the application domain.

A major problem to address is the lack of Frameworks for Interoperability/Interworking in specific industry domains: In complex systems of systems (smart cities), adopting an interoperable architecture and selecting optimal integration points to satisfy stakeholders' requirements is challenging!

If platforms (technologies) are not endorsed or used by relevant stakeholders, they will be useless! The wider the stakeholders group involved. the higher the impact. The "United for Smart Sustainable Cities" (U4SCC) UN initiative is a global platform for smart city stakeholders which advocates for public policy to encourage the use of ICTs to facilitate the transition to smart sustainable cities.

oneM2M focused on developing a common services horizontal framework for the application layer. They are now ITU-T Standards.

A Framework for Service Discovery Interworking is being developed to solve the problem of the use of different service discovery protocols by different IoT service platforms. Cross-platform service discovery is hence needed.

The ITU-T SG20 draft Recommendation ITU-T Y.IoT-sd-arch is being developed to define the functional architecture of service discovery for interworking between heterogeneous IoT platforms.

4.8.4 IoT Standards in the Convergence Turmoil

By Emmanuel Darmois, ETSI STF 457

Most of the presentation is also described in sections 4.5.3 and 4.7.2. The presentation in the context of this session has insisted on:

- The growing role of Open Source, in particular for Open APIs and Data Models;
- The emergence of new promises and issues:
  - Big Data (aka IA) and Semantic Interoperability;
  - Effective privacy; Secure IoT;
  - Growing role of (possibly proprietary) ecosystems;
  - Standards and OSS: collaboration or replacement.

4.8.5 Internet of Things: From R&D to Standardisation The challenge of convergence

By Olavi Luotonen and Franck Boissière, European Commission – DG CONNECT

IoT Adoption is maturing. This is raising the question of standards: which ones, what for? Some European Commission initiatives have been launched in support of this.

The EU Multi-Stakeholder Platform on ICT Standardisation (MSP) has the role to advice and foster Standards Collaboration and Coordination with the support of the "Rolling Plan on ICT Standardisation" which has evolved with its various iterations from 2016 to 2019.

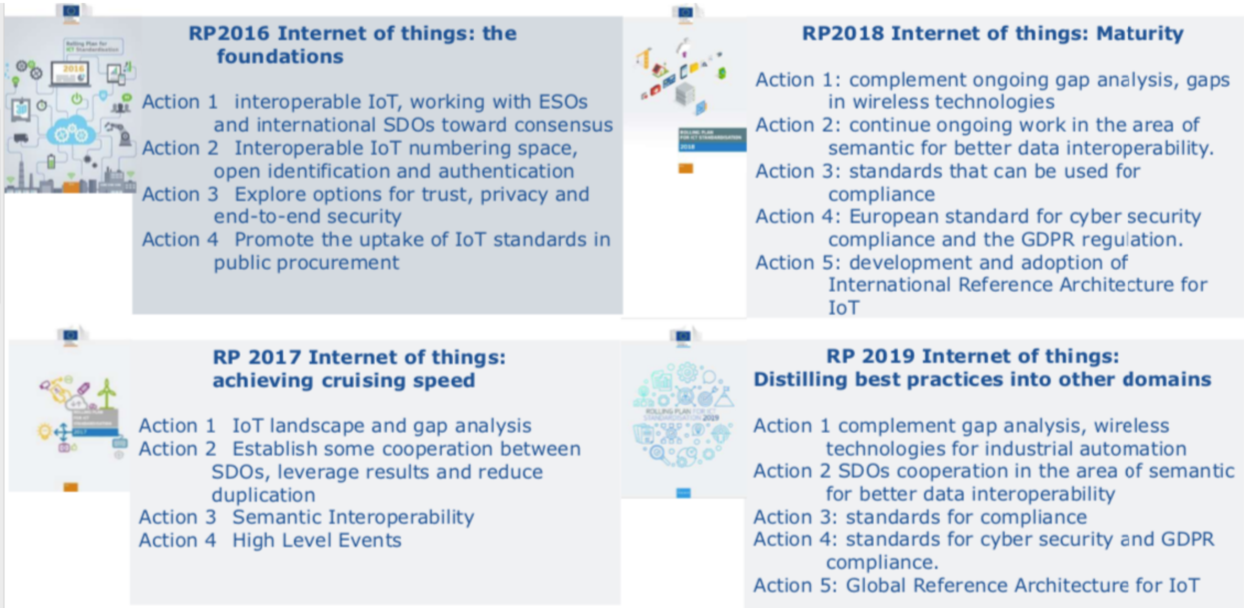


Figure 11: Rolling plan for IoT

The Standardisation challenges:

- Interoperability – essential for a Digital Single Market (DSM);
- Supply- and demand-side are both struggling to define standards at appropriate level;
- Open innovation systems move fast, and the standards processes struggle to keep up;
- Solutions should be more than technical solutions and take into account organisational aspects and cross-domain issues;
- Security and privacy are still a limiting factor;
- Communities are sceptical, often for good reasons, this complicating adoption.

A systemic approach has been taken for IoT Standards:

- Large Scale Pilots;
- Focus Areas and Project Clusters;
- Stakeholder and Industrial engagement in PPP: AIOTI, BDVA, ECSO, ARTEMIS, 5GPPP;
- Open meetings and workshops; light steering.

What's next in 2019 and beyond:

- New technical standards (cross domain)
- The next frontier is where ICT standards meet Operational Technology standards
- PPPs cooperation and joint activities (data spaces, converged reference architectures, semantic interoperability main streaming)
- Dissemination best practices across domains (e.g. DEI MSP WG)

4.9 IoT Standardisation and the Question of Data Ownership

Competition in open markets is a major driver for adoption of standards and likewise motivates companies to invest in developing standards. Successful standardisation for the IoT will thus be boosted by the establishment of open markets of data and data services. However, data is unlike regular products, and understanding the differences is critical to understanding what is needed for the success of such markets.

- After passing data from one entity to another entity, both entities hold a copy of the data. This is unlike physical goods where the entity transferring the goods loses access to the goods as a consequence of the transfer.
- Because data is easy to copy, it is also hard to delete, due to the difficulty of finding and deleting all the copies across all of the entities holding a copy of that data.

- As data is repeatedly copied, it is likewise hard to control how it used by different entities.
- The value of data grows with the amount of data, encouraging entities to hoard their data rather than share it.

To stimulate a market for data with lots of suppliers and consumers, we need to find a way to reward sharing, and to give suppliers control over the data they provide.

A purely technical solution is impractical, so we need to look at other mechanisms, in particular, contract law where both supplier and consumer agree to some set of commitments by entering into a legally binding joint contract. To be effective, this needs a means to record a non-modifiable audit trail as a basis for tracking adherence to the contract. Distributed ledgers based upon block chains look like a promising potential solution for smart contracts.

Contracts will often involve an exchange of value. This could take multiple forms: a one-off payment that provides for indefinite access, a subscription-based payment providing access for a given time period, or a per-use payment. There are many potential payment mechanisms.

A further consideration is the potential to support automatic negotiation between suppliers and consumers. For example, some consumers may be willing to pay more for fresher data or for broader rights in respect to how data can be exploited.

The value of a market to suppliers and consumers scales with the size of the market. A larger market includes more potential consumers for a given supplier, and vice versa, offering consumers a wide range of suppliers. In addition, larger markets will enable specialisation as suppliers identify and target niche market opportunities.

The final report on standardisation will look at the experience gained on work on open marketplaces as part of the LSPs, and what implications there are in respect to future projects and the prospects for the development adoption of IoT standards.

The European Commission is already working on a single digital market across EU Member states and the policy recommendations discussed during the workshop can be used as means to encourage rapid growth of a shared single market for ecosystems of digital services for the IoT Based on the best practiced developed by various IoT large-scale pilot projects.

5. CONCLUSIONS

5.1 Contribution to overall picture

The Workshop has addressed the current questions under analysis within the IoT standardisation community. Some of these questions are already dealt with by Standards Organisations and the development of standards is on-going. From this standpoint, progress can be seen compared to the previous snapshot made during IoT Week 2018 in Bilbao. In particular, the contribution of the LSP has been consolidated and the following points can be provided as examples of significant contributions of the LSPs to the IoT standards landscape:

- The collaborative development by LSPs of a 3D Reference Architecture model expanding the reach of architecture specification and aimed at contributing to standardisation;
- The development by the MONICA of requirements for a new standard for time-critical data links for IoT sensors (partner Ring Advocacy has made a submission for a new wireless interface);
- The contribution of AUTOPILOT to OneM2M standardisation documents and to the description of IoT and 5G use cases for automated/autonomous vehicles applications.
- The contribution of AUTOPILOT to the IoT Policy Framework for automated/autonomous vehicles applications including AI issues and the mapping of use cases to the 3D Reference IoT Architecture model.
- The LSPs contributions to SAREF (Smart Appliances REFerence ontology), a modular network of standardised semantic models led by ETSI, which is being extended to IoT application environments such as Smart Cities and Smart AgriFood, contributing to the development of a strong EU standards ecosystem;
- The contributions of SynchroniCity to the ITU Study Group 20 on IoT and Smart Cities, where 2 standards promoted by the project are under work since 2017: Draft recommendation on Open API for IoT in Smart Cities and the Technical Report on Artificial Intelligence in the IoT and Smart City ecosystem. SynchroniCity is also contributing to the Focus Group (FG) on Data Processing and Management.

5.2 Next steps

The overall discussion during the Workshop has confirmed the relevance, for the on-going and future IoT standardisation of several topics. Some are discussed in the above sections; some will require further elaboration. A short list of these topics is the following:

- The emergence of the Sentient Web (ecosystems for IoT + Graphs + AI/ML)
- Open markets of services – at the network edge and in the cloud
- Bridging the silos and connecting the ecosystems
- Opportunities for convergence across different axes
- Privacy and security for resilient services
- Addressing the challenges for semantic interoperability
- Recommendations for collaborations across PPPs, SDOs and other alliances

These topics will be further analysed in the CREATE-IoT Deliverable D06.06 (Final report on IoT standardisation activities) due at the end of 2019.

6. REFERENCES

[1] OpenStand's principles for open standards. Online at: https://open-stand.org/about-us/principles/
[2] W3C Workshop on Web Standardization for Graph Data, Creating Bridges: RDF, Property Graph and SQL. Online at: https://www.w3.org/Data/events/data-ws-2019/
[3] GitHub. Online at: https://github.com/w3c/EasierRDF
[4] ETSI Specialist Task Force 547. Online at: https://portal.etsi.org/STF/STFs/STFHomePages/STF547
[5] NGSI-LD Specification (January 2019). Online at: https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.01.01_60/gs_CIM009v010101p.pdf
[6] FIWARE Data Models. Online at: https://github.com/FIWARE/dataModels
[7] W3C WoT TD Specification, (CR May 2019). Online at: https://www.w3.org/TR/wot-thing-description/
[8] ETSI SAREF Ontology. Online at: http://ontology.tno.nl/saref/
[9] W3C SSN Ontology. Online at: https://www.w3.org/TR/2017/REC-vocab-ssn-20171019/
[10] MyData 2019 conference. Online at: https://mydata2019.org/