HORIZONS 2020 PROGRAMME

Research and Innovation Action – FIRE Initiative

Call Identifier:	H2020–ICT–2014–1
Project Number:	643943
Project Acronym:	FIESTA-IoT
Project Title:	Federated Interoperable Semantic IoT/cloud Testbeds and Applications

Design of global market confidence programme on IoT interoperability

Document Id:	FIESTAIoT-D61-160504-Draft
File Name:	FIESTAIoT-D61-160504-Draft.pdf
Document reference:	Deliverable 6.1
Version:	Draft
Editor:	Mengxuan Zhao
Organisation:	Easy Global Market
Date:	04 / 05 / 2016
Document type:	Deliverable
Dissemination level:	PU

DOCUMENT HISTORY

Rev.	Author(s)	Organisation(s)	Date	Comments
V01	Mengxuan Zhao	EGM	2016/02/08	ToC
V02	Amelie Gyrard Mengxuan Zhao	NUIG, EGM	2016/03/07 2016/03/08	Section 5 SPARQL endpoint, validators, user interface,YASQE section, Section 2
	Amelie Gyrard	NUIG	2016/03/29	- Section 5.1 Semantic Web tools analysis - Section reasoning certification - Update reasoning section - Update SPARQL query section
V03	Nikos Kefalakis	AIT	2016/4/6	Update ontologies section
V04	Paul Grace	ITINNOV	2016/4/7	4.5 security; 5.2 interop and compliance testing tools
V05	Mengxuan Zhao	EGM	2016/4/8	Update section “positioning”
	Mengxuan Zhao, Philippe Cousin	EGM	2016/4/18	-Executive summary -Introduction to certification and labelling programme -Certification subject section “the importance of data” -Update on 6.1 6.2
V06	François Carrez, Tarek Elsaleh	UNIS	2016/4/21	-Section “compliance with the IoT architecture -Update for SSN validator and URI checker
V08	Mengxuan Zhao, Philippe Cousin	EGM	2016/5/4	-Integration of contributions -Executive summary update
V09	Amelie Gyrard	NUIG	2016/05/09	Update section 4.4, section 4.5 with an example for correctness, update section 4.6
	Amelie Gyrard	NUIG	2016/05/13	Technical and Quality Review
V07	Martin Serrano	NUIG	2016/05/14	Circulated for Approval
Draft	Martin Serrano	NUIG	2016/05/15	EC Submitted

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TERMS AND ACRONYMS

AIOTI	Alliance for Internet of Things Innovation
API	Application Programming Interface
ARM	Architecture Reference Model
DC/TC	Design & Technology Choices
DM	Domain Model
EaaS	Experimentation-as-a-Service
ETSI	European Telecommunications Standards Institute
EU	European Union
FC	Functional component
FG	Functional Group
FIRE	Future Internet Research and Experimentation
FM	Functional model
FP	Framework Programme
ICT	Information and communication technology
IEEE	Institute of Electrical and Electronics Engineers
IERC	European Research Cluster on the Internet of Things
IoT	Internet of Things
IoT-A	Internet of Things Architecture
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
LOV	Linked Open Vocabularies
LOV4IoT	Linked Open Vocabularies for Internet of Things
M2M	Machine-to-Machine
M3	Machine-to-Machine Measurement
MAS	Management, Abstraction and Semantics
NGSI	Next Generation Service Interface
OWL	Ontology Web Language
RA	Reference architecture
RDF	Resource Description Framework
RFID	Radio Frequency Identification
RM	Reference model

SAREF	Smart Appliances REFerence
SDO	Standards developing organization
SSN	Semantic Sensor Networks
TSL	Transport Layer Security
UML	Unified Modeling Language
URI	Uniform Resource Identifier
VE	Virtual entity
WoT	Web of Things
WP	Work Package
WSN	Wireless sensor Network

EXECUTIVE SUMMARY

This deliverable describes the “Global market confidence programme” of the Fiesta-IoT project. Past FP7 project focusing on IoT interoperability such as PROBE-IT[1] and years of discussion within the IoT Research Community with the IERC Activity Chain 4[2] on interoperability have made evidence that main concern on IoT interoperability relies on Data /Semantic Interoperability.

Recent activities with AIOTI working group on Standardisation have confirmed that one of the most important topic is on the semantic Interoperability. SDOs such as W3C, ETSI, oneM2M are spending a lot of resources to address the semantic Interoperability.

While the topic is now clearly identified, the topic is still quite new and there is a lack of tools and guidance on how ensuring semantic interoperability and even more on tools and processes to ensure conformity to guidelines or specifications

FIESTA project is addressing these issues and therefore aims to provide unique solutions not only for the FIRE communities such as the experimenters but for the whole IoT community.

Therefore, we are willing to follow and also lead this trend by proposing, for the first time within an EU project, a certification programme focusing on data interoperability, more specifically, using semantic technologies. It defines the general approach of a certification process with the key elements. Stakeholders and their role in the programme are identified. Important aspects to assure the semantic interoperability are presented as the essential certification subjects in the programme. Related tools that can be integrated in the certification suite are described. Finally, based on the elements identified previously, a plan for how to positioning the programme.

1 POSITIONING

1.1 FIESTA-IoT Scope

Recent advances in the Internet of Things (IoT) area have progressively moved in different directions (i.e. designing technology, deploying the systems into the cloud, increasing the number of inter-connected entities, improving the collection of information in real-time and not less important the security aspects in IoT). IoT Advances have drawn a common big challenge that focuses on the integration of the IoT generated data. The key challenge is to provide a common sharing model or a set of models organizing the information coming from the connected IoT services, IoT technology and systems and more important able to offer them as experimental services in order to optimise the design of new IoT systems and facilitate the generation of solutions more rapidly.

In FIESTA-IoT we focus on the problem of formulating and managing Internet of Things data from heterogeneous systems and environments and their entity resources (such as smart devices, sensors, actuators, etc.), this vision of integrating

[1] http://www.probe-it.eu/

[2] http://www.internet-of-things-research.eu/activity_chains.htm

IoT platforms, testbeds and their associated silo applications within cloud infrastructures is related with several scientific challenges, such as the need to aggregate and ensure the interoperability of data streams stemming from different IoT platforms or testbeds, as well as the need to provide tools and techniques for building applications that horizontally integrate diverse IoT Solutions. The convergence of IoT with cloud computing is a key enabler for this integration and interoperability, since it allows the aggregation of multiple IoT data streams towards the development and deployment of scalable, elastic and reliable applications that are delivered on-demand according to a pay-as-you-go model.

The activity in FIESTA-IoT is distributed in 7 work packages WP1 is dedicated to the project activities coordination, considering consortium administration, financial management, activity co-ordination, reporting and quality control. In FIESTA-IoT one of the main objectives is to include experimenters and new testbeds to test and feedback the platform and tools generated, thus open calls for those tenders will be issued that are also part of the WP1 activity and is called selection of third-parties.

WP2 focuses on stakeholder's requirements and the analysis on IoT Platforms and Testbeds in order to define strategies for the definition and inclusion of Experiments, Tools and KPIs. The activities in this WP2 are focused on studying the IoT Platforms and Testbeds and the specification of the Experiments, the detail of the needed tools for experimentation and the KPIs for validate the proposed solutions. This WP will conduct the design and development of the Meta-Cloud Architecture (including the relevant directory of IoT resources) and will define the technical specification of the project. WP2 also focuses on analysing the Global Market Confidence and initiate the Certification Programme Specifications, to be established in WP6 by analysing requirements for validation at the testbeds level.

WP3 package focuses on providing technologies, interfaces, methods and solutions to represent the device and network nodes of the test-beds as virtualized resources. The virtualized resources will be represented as services and will be accessible via common service interfaces and APIs (i.e. the FIESTA Testbed interfaces/APIs). The virtualized resources and their capabilities and interfaces will be also described using semantic metadata to enable (semi-) automated discovery, selection and access to the test-bed devices and resources.

WP4 will implement an infrastructure for accessing data and services from multiple distributed diverse testbeds in a secure and testbed agnostic way. To this end, it will rely on the semantic interoperability of the various testbeds (realized in WP3) and implement a single entry point for accessing the FIESTA-IoT data and resources in a seamless way and according to an on-demand EaaS model. The infrastructure to be implemented will be deployed in a cloud environment and will be accessible through a unified portal infrastructure.

WP5 focuses on designing deploy and deliver a set of experiments, so as to assess the feasibility and applicability of the integration and federation techniques, procedures and functions developed during the project lifetime. It would define a complete set of experiments to test the developments coming from other WPs (mainly WP3 and 4), covering all the specifications and requirements of WP2. Developments will be tested over available IoT environments and/or smart cities platforms. WP5 would also provide evaluation of the key performance indicators defined for every experiment/pilot. The final deployed experiments will include a

subset of those coming from WP2, 3 and 4, as well as those provided by FIESTA Open Calls.

WP6 focuses on the establishment and validation of the project's global market confidence on IoT interoperability, which will provide a vehicle for the sustainability and wider use of the project's results. The main activity in this WP focuses on specifying and designing an IoT interoperability programme, including a set of well-defined processes that will facilitate the participation of researchers and enterprises. WP6 works on providing a range of certification and compliance tools, aiming at auditing and ensuring the openness and interoperability of IoT platforms and technologies. WP6 also focuses on Interoperability testing and validation and to provide training, consulting and support services to the FIESTA-IoT participants in order to facilitate platforms and tool usability but also to maximize the value offered to them by using FIESTA-IoT suite and tools.

WP7 work package focuses on ensuring that FIESTA-IoT suite, models and tools engages well with the community outside of the project; from promotion and engagement of new customers, to the front line support of current users, and the long-term exploitation of results and sustainability of the facility itself. This will be carried out in a coordinated manner such that a consistent message and professional service is maintained. Dissemination activities and the KPI to measure the impacts will be studied and used in this WP. An ecosystem plan including the specification of processes, responsibilities and targets will be generated and the evaluation and effectiveness of the operating model will be evaluated within this WP. In this WP the successes of stakeholder engagement and report on their satisfaction with the services offered in FIESTA-IoT will be put in place at the end of the project.

1.2 WP6 Overview

This work package focuses on the establishment and validation of the project's global market confidence programme on IoT interoperability, which provides a vehicle for the sustainability and wider use of the project's results. The main objectives of the work package are:

- To specify and design an IoT interoperability programme, including a set of well-defined processes that will facilitate the participation of researchers and enterprises.
- To provide a range of certification and compliance tools, aiming at auditing and ensuring the openness and interoperability of IoT platforms and technologies.
- To operate the programme on the basis of auditing of real-life IoT platforms and services against their interoperability. These platforms and services will be contributed by the partners of the consortium, as well as by new participants joining the project on the basis of open calls processes.
- To provide training, consulting and support services to the programme participants in order to facilitate their participation, but also to maximize the value offered to them by the programme.

The activities in WP6 will first start with specification and design of the programme to give not only the requirements for tools that are needed in the certification suite, and also the plan for testing and validation and for support. Tools that are developed in WP3 and WP4, together with other available tools from open-source communities or

previous research projects, will be integrated into the certification suite that will be operated on IoT platforms and services against their semantic interoperability. Training, consulting and support services will be provided in parallel with other activities.

The links with different work packages are shown in Figure 1. The work package is divided into several tasks:

- **T6.1 Programme Specification and Design** will focus on the specification and design of the programme, in terms of the establishment of the appropriate processes for participants, as well as for the auditors of openness and interoperability. The programme design will deal with both the technical and business aspects of the interoperability. It will specify the features/capabilities that each platform should provide in order to be considered open and interoperable in the IoT domain. The task will also specify the processes under which enterprises and researchers will participate in the global market confidence programme for IoT interoperability.
- **T6.2 Certification Suite and Tools Implementation and Fine-Tuning**: Based on the technical results of the FIESTA project (notably results on WP3/WP4 towards ensuring the interoperability of IoT data, platforms and resources), this task will provide a certification suite, which will comprise a range of tools for testing the openness and interoperability of a given IoT platform or testbed. The certification suite will score the interoperability of each platform, which at the same time providing guidelines (to the owner) towards improving the interoperability level of its platform. Note that in addition to the initial implementation of the suite, the task will work towards its fine-tuning based on feedback received from the actual participation of platform/testbed owners as part of task T6.3.
- **T6.3 Interoperability Testing and Validation** will focus on the use of the certification suite (and of the accompanying tools) towards testing and validating various IoT platforms against their openness and interoperability. To this end, the task will start from the auditing of the interoperability of the FIESTA testbeds, which will have been adapted to FIESTA principles based on the middleware developments in WP3. Moreover, the interoperability of other platforms contributed by project partners (e.g., UNINNOVA, AIT, UniS, NUIG-DERI) will be audited. Access to additional platforms for testing and validation will be also ensured based on liaisons with the IERC cluster's open platforms initiative, but also through the open calls process, which will attract new partners in the consortium.
- **T6.4 Stakeholders' Training and Continuous Support** will provide a range of indispensable support services to the participants to the global market confidence programme. These will include their general training on IoT interoperability in general and in FIESTA interoperability in particular, targeted consulting services associated with the interoperability of their platforms/testbeds, as well as continuous support in their efforts to use the FIESTA results/tools towards improving the level of interoperability of their systems and applications.

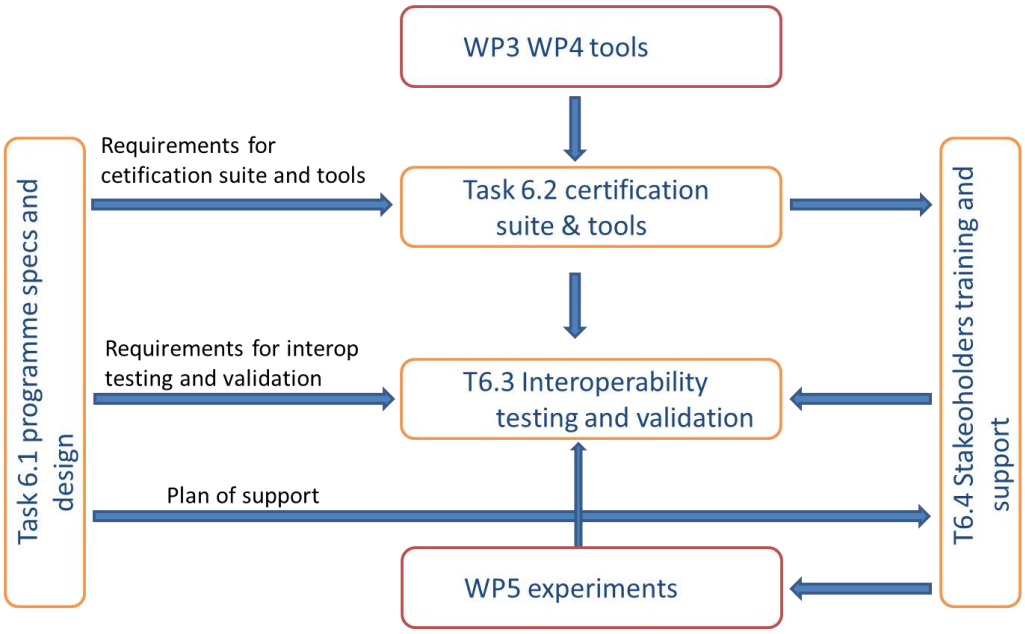


Figure 1: WP6 relation with other work packages

The WP6 will also result in five deliverables listed in Table 1.

Table 1 WP6 Deliverables

No.	Deliverable	Responsible partner	Contributors
D6.1	Design of Global Market Confidence Programme on IoT interoperability	EGM	AIT, UNIS, NUIG, ITINNOV
D6.2	Certification Suite V1	EGM	All
D6.3	Certification Suite V2	EGM	All
D6.4	Training, Consulting, Testing and Validation V1	UNPARALLEL	ITINNOV, EGM, SODERCAN
D6.5	Training, Consulting, Testing and Validation V2	UNPARALLEL	ITINNOV, EGM, SODERCAN

1.3 Terminology and definitions

This sub-section is intended to clarify the terminology used during this project. This initial step is intended to clarify all the important terms used, in order to minimise misunderstandings when referring to specific parts involved in the generation of data and the FIESTA-IoT concepts. The following definitions were set regarding the domain area of FIESTA-IoT, and so are aligned with terminologies used in FIRE community and in reference IoT-related projects (such as IoT-A).

Table 2 Terminology and Definitions table

Term	Definition
Requirement	A quantitative statement of business-need that must be met by a particular architecture or work package. [1]

Test	A test is to evaluate the characteristics of a particular entity, generally by considering a specific frame of reference in relation to which conformity is to be verified. The test is carried out either by the entity in question or by an independent testing laboratory, which then issues a 'test report'.
Validation	A validation is to verify that an entity conforms to a frame of reference; this is generally achieved by using the results of tests, though it may also involve other aspects, such as on-site inspections.
Certification	A certification is the conformation of the conformity of an entity with respect to the chosen frame of reference. Certification may relate to a product, the quality assurance system of an establishment or enterprise, the skills of an individual, or to a service. It always results in a written document (certificate) issued by the certifying body by which the latter provides an assurance that the entity in question conforms to the specified requirements.
Resource	Computational element that gives access to information about or actuation capabilities on a Physical Entity [2]
Stakeholder	An individual, group, or organization, who may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project [3]
Testbed	A testbed is an environment that allows experimentation and testing for research and development products. A testbed provides a rigorous, transparent and replicable environment for experimentation and testing [4]
Federated testbeds	A testbed federation or federated testbeds is the interconnection of two or more independent testbeds for the creation of a richer environment for experimentation and testing, and for the increased multilateral benefit of the users of the individual independent testbeds [4]
Interoperability	The ability of two or more systems or components to exchange information and use the information that has been exchanged [5]
Experimentation facility	An experimentation facility can be understood as an environment with an associated collection of tools and infrastructure that sits on top of one or several testbeds and can be used to conduct experiments to assess and evaluate new paradigms, architectural concepts and applications [6]
Experiment	Experiment is a test under controlled conditions that is made to demonstrate a known truth, examine the validity of a hypothesis, or determine the efficacy of something previously untried [7]
Semantic Interoperability	Semantic interoperability is the ability of computer systems to exchange data with unambiguous, shared meaning. Semantic interoperability is a requirement to enable machine computable logic, inference, knowledge discovery, and data federation between information systems
Service	Services (Technology) are services designed to facilitate the use of technology by end users. This services provide specialized technology-oriented solutions by combining the processes/functions of software, hardware, networks, telecommunications and electronics

1.4 Audience

This Deliverable address the following audiences:

- **Researchers and engineers within the FIESTA-IoT consortium** will take into account various requirements in order to research, design and implement the APIs needed to support Testbed associated to FIESTA-IoT Platform.
- **Testbed owners who wish to join FIESTA-IoT, including open call participants,** will be able to use the tools defined to annotate the data their testbed in producing. By doing so, the testbed can either become Class I or Class II or Class III testbed (see deliverable D2.4 “FIESTA-IoT Meta-Cloud Architecture” [8] for the definitions of various classes of testbeds).
- **Researchers on Future Internet Research and Experimentation (FIRE) focusing on semantically storing data produced by their experiments** will find guidelines to store data produced by their experiments in a semantic manner either in their own repository or utilise FIESTA-IoT platform. The researchers will be able use the ontology and the tools as the reference. Further, if they wish to extend/modify the ontology and tools for their own research, they would be able to do so.
- **Members of other Internet of Things (IoT) communities and projects (such as projects of the IERC cluster)** can take this document as an initial reference or inspiration to design and implement their own testbed that either stores data that is semantic annotated interoperable experiments.
- **Standardization bodies:** this deliverable will be a public document. The ontology developed can be standardized following the involvement and wider adoption.

2 DEFINITION OF GLOBAL MARKET CONFIDENCE PROGRAMS

The main goal of the Fiesta-IoT project is to enable EaaS (Experiment-as-a-service) over multiple testbeds through the semantic interoperability, thereby to serve as a basis for alleviating the fragmentation of the IoT market, through boosting openness and building market confidence. Therefore, Fiesta-IoT will establish, implement and support a global market confidence programme by providing a range of certification and compliance tools, which will encourage and facilitate stakeholders beyond the project consortium as third parties to comply with the Fiesta-IoT interoperability guidelines and accordingly to deploy large scale innovative interoperable IoT applications in order to demonstrate the added value of Fiesta-IoT. Another important successful element of the programme is to increase robustness and validate Fiesta-IoT design and implementation which may be a reference and inspiration for future research and application on IoT platform/application/methodology.

2.1 Approach from D2.5

In D2.5 [9], we have set up a certification framework for testbeds that wish to join the FIESTA-IoT federation. Compared to the current global market confidence program, the framework defined in D2.5 limits its scope to the testbeds within and beyond the FIESTA-IoT project, which means it is “testbed-oriented”.

The general methodology to establish the certification framework is however similar in the two cases: for the testbeds and for the general IoT market. In D2.5, we first identified the stakeholders of the framework, then we defined the structure of the framework which are: 1) interoperability aspects and requirements that related to the general requirements for the FIESTA-IoT federation; 2) interoperability scores that consist of scoring the testbeds in terms of the underlined interoperability features and aspects; 3) classification and overall assessment that consists of categorizing the testbeds according to the interoperability score it gets from the previous step. Finally we designed an interoperability self-assessment scorecard including the previously identified features and aspects that the testbed can fill it in before taking the decision to join the FIESTA-IoT federation. This scorecards gives not only a score that is the basis of interoperability classification, and also some suggestions and an estimation about how much investigation needed to join the federation. This scorecard can be adapted to the current global market confidence program.

We should note that the work done in D2.5 is a subset and is a start point of the current confidence program.

2.2 Introduction to certification or labelling

Certifications (or equivalent process) are organized all over the world in quite all-industrial domains either for regulators or for organization in voluntary approach. A set of worldwide standards and guidance are successfully used worldwide (e.g. ISO Guides, ISO 9000 and ISO 17000 series) in a broad range of different sectors and for many years.

It is assumed that the overall approach developed in these reference standards can be usefully and harmoniously used for a particular community although some specific guidelines might be developed as in other sectors.

2.2.1 General presentation of certification

Conformity is understood to denote that ‘the fact that a product, system, body or even a person… meets specified requirements’ (definition from ISO/IEC Guide 2 [10])

The keyword with regards to certification of conformity is ‘confidence’. The reason for this is that conformity certification procedures have been established with the main aim of creating or strengthening the confidence which business interests may have both with regard to each other and with regard to products, goods and services placed on the market.

From the original concept of certification, the existence of potential methods for evaluating and certifying conformity derives from a demand from customers (in the broad sense of the term) to be assured of the characteristics of a product, service or body. It also derives from a demand from producers themselves, either to increase the level of quality of their production or to give their customers confidence. All conformity certification procedures are therefore based on the combined interest of the various concerned parties.

As time has gone by, various procedures have been established on the basis of this demand, irrespective of whether the latter has been explicitly expressed. These procedures, which will be examined below, all tend to have a dual objective: to

evaluate and control the safety or quality of the product supplied or the service provided, and to promote confidence.

In the case of IoT related community, we will focus on the Quality of the product supplied (including all aspects such as interoperability) or the service and all over promoting confidence in IoT solutions indeed

The coexistence of three elements thus appears to be of fundamental importance, namely: the **existence of demand**, the existence of a **frame of reference** which can be used to assess the entity in question and, lastly the existence of **organized procedures and structures** for carrying out this assessment.

2.2.2 What frames of reference are used to carry out the assessment?

This question has two aspects to it: the **nature of the frame of reference** and to **what it relates**. As seen above, this is because the frame of reference may be a regulation, a standard, a public contract specification, a code of professional specifications, a company standard or any type of private specifications (e.g. FIESTA specifications) such as safety requirements imposed by the final buyer.

However, the frame of reference may also relate to different subjects: one naturally thinks of requirements which apply to a product, but in fact requirements increasingly cover characteristics relating to the **production tool itself**, as with the ISO 9000 series of quality assurance standards), ISO 17025 on testing, which may even be applied within the company, or even requirements governing the qualifications of personnel (e.g. (Data) IoT qualified engineers).

The above considerations clearly show that the development of frames of reference used in conformity certification procedures is closed linked with the needs of the economy, as is the case with standards.

2.2.3 Who carries out the assessment and how?

1. The declaration of conformity:

The first option - and the simplest one - is the supplier's "declaration of conformity", which is sometimes incorrectly referred to as "self-certification", this being a contradiction in terms. This is a procedure whereby the supplier provides a written assurance that a product, service, etc. conforms to one or more specified requirements. This declaration of conformity may be provided either directly or following various contributions by a laboratory.

In order to assist suppliers with drawing up their declarations of conformity, the standards bodies have formulated an international standard, namely ISO 17050; compliance with this standard should, in addition, enable greater weight to be given to declarations of conformity vis-a-vis different customers.

It should be stressed that the declaration of conformity is the most widespread type of certification of conformity in free-market economies, in keeping with the way in which such economies are organised.

2. Tests and checks:

The purpose of a test is to evaluate the characteristics of a particular entity, generally by considering a specific frame of reference in relation to which conformity is to be verified, though not necessarily so: a test which is designed to determine the safety of a product may be carried out on the basis of the 'recognised state of the art', i.e. in actual fact on the basis of current scientific and technical knowledge in general; a broad measure of consideration is in this case given to the judgement of the expert carrying out the test.

In addition, a test may be performed on a particular example, without necessarily having to take into consideration series production or the repetition of actions or services (otherwise, the test becomes an integral part of a certification process). The test is carried out either by the entity in question or by an independent testing laboratory, which then issues a "test report".

The prime function of a check, on the other hand, is to verify that an entity conforms to a frame of reference; this is generally achieved by using the results of tests, though it may also involve other aspects, such as on-site inspections. The term "audits" is used when a company's quality assurance system is checked.

2.2.4 Certification/labelling procedures:

The aim of these procedures is to ascertain the conformity of an entity with respect to the chosen frame of reference. Although "certification", in the widely accepted sense of the term, encompasses any procedure carried out by a party from outside the company and could thus cover certification by a 'second party', i.e. by the customers, it is preferable to restrict use of the term to procedures carried out by an independent body which comes from outside the entity in question and which is specifically designed to carry out such activities (third-party certification).

Certification may relate to a product (certification of products), the quality assurance system of an establishment or enterprise (quality-control system certification), the skills of an individual (personnel certification), or to a service (service certification). This is a procedure, which generally involves long-term monitoring of the certified entity to ensure that the conditions under which certification was awarded still apply.

Certification always results in a written document (certificate) issued by the certifying body by which the latter provides an assurance that the entity in question conforms to the specified requirements. Generally speaking, third party certification of a products or services also results in the certified entity being entitled to use a mark granted to it or being authorized to use a distinctive sign.

2.2.5 Documentation for Certification/labelling scheme

In order for a certification scheme to be workable and open to other parties it must be clearly documented from an organizational viewpoint and from an operational viewpoint. Figure 2 provides a general overview of the type of documentation necessary for a certification schemes and shows the documents necessary for each of the players in the scheme.

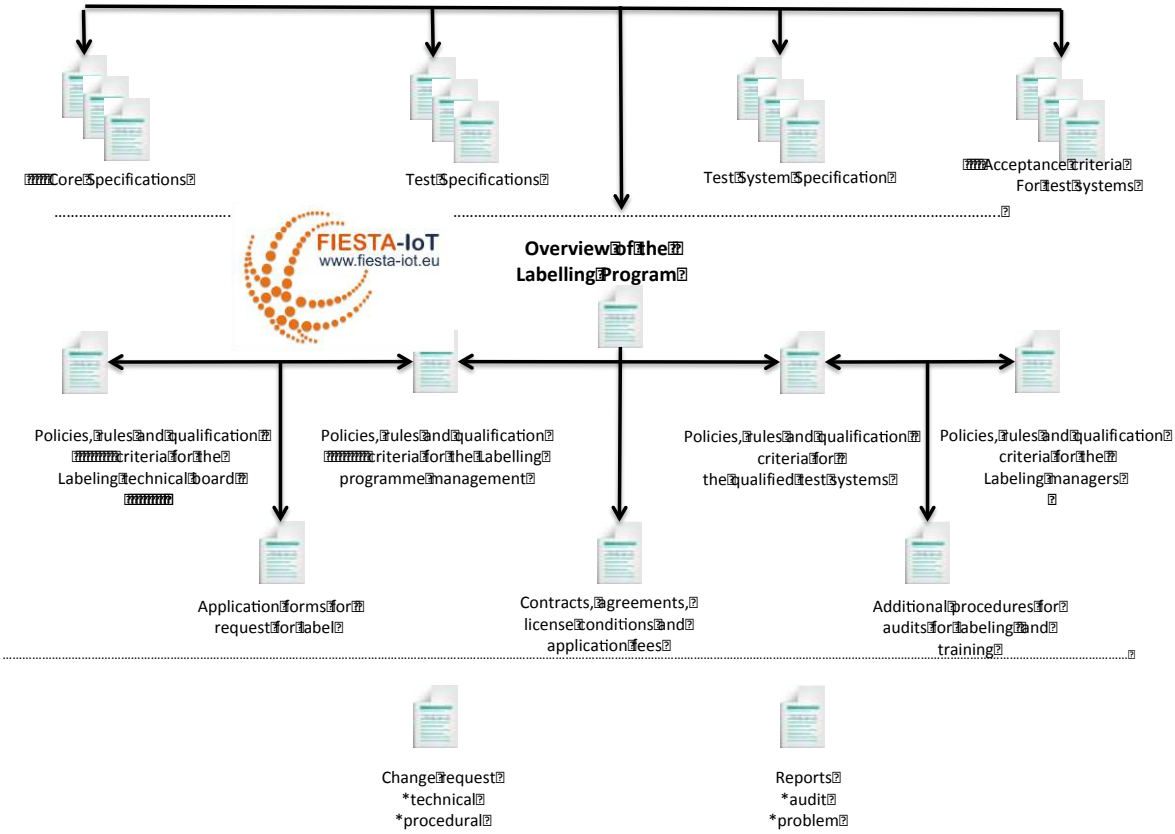


Figure 2: Certification/Labelling Programme Overview

To sum up we can quickly identify the following documents:

- General OVERVIEW documents
  - Overview of the overall certification scheme
  - Rights, obligations and contractual requirements between concerned parties
  - Guidelines to audits and auditors
  - Document on the financing of the certification scheme
  - Timescale for the certification scheme implementation
  - Rules and requirements to terminate, abandon, withdraw or annul a certificate
  - Database of certified products, test tools etc.
- Approval authority
  - List of criteria to be an approval authority in the domain
  - Rules and requirements of approval authority
  - Standards/specifications covered by the labelling/certification scheme
  - Test specifications
  - Test system specifications
  - Validation criteria for test system
  - Rules and requirements - basis of policies and operation of the labelling/certification bodies
  - Appeals procedure
  - Quality procedures
- Certification body or labelling manager(s)

  - Documentation to be approved as certification body by approval authority, e.g. ISO 17020 or other criteria decided by approval authority
  - Appeals procedure
  - Rules and requirements for labs and their personnel
  - Certification criteria for personnel etc.
  - Guidelines for modification of equipment
  - Laboratory inter-comparison
- Declaration of conformity, etc.
  - Documentation to be approved as lab by certification body, e.g. ISO 17025 or other criteria as decided by certification body
  - Test methods
  - Metrology documentation if applicable
  - Test system validation
  - Test support documentation, test report, etc
  - Fees
  - Training records
  - Administrative forms
  - Confidentiality agreements

2.3 General approach of a Fiesta related certification programme

A traditional approach toward confidence building is the set-up of certification programs that recognises the existence of certain characteristics to products, software, services, people, etc. based on increasing levels of acceptance criteria. Overall designing a confidence program requires defining a number of topics:

1. What is to be certified? In the case of Fiesta-IoT, we can immediately think of the critical aspects when a testbed wants to join the EaaS infrastructure, or when an experiment needs to be deployed on the infrastructure, such as the ontologies accepted by the EaaS, the SPARQL queries used to interact with resources.
2. What are the objectives of the certification? For example, to increase visibility of member testbeds, to facilitate the success of an experiment.
3. What are the important dimensions to be evaluated? For example, compliance to the reference, openness, quality of service.
4. Who are the stakeholders? Stakeholders are people or organizations that are interested in or benefit from the confidence program.

In the following parts of this document, the above aspects will be addressed.

In Fiesta-IoT, we take the second approach explained in 2.2.3 to issue a certificate, which means by approved tests and checks. The following diagram Figure 3 shows a simplified and general workflow of a certification program, and the roles of each component in this workflow, they are:

1. Authority that regulates or monitors the domain, and delivers the certificate “stamp”. It can have two sub-bodies that are more specialized respectively in technical aspects and management aspects. In the case of the project, it is the Fiesta-IoT Consortium. It may also be i.e. oneM2M if oneM2M wants to use the same approach and the available tools from the programme, the authority will be oneM2M who accredits the Fiesta-IoT consortium to be the

certification body and testhouse, and finally, it is oneM2M who decides the delivery of a certificate based on the results from Fiesta.

2. Certification body or equivalent that receives the requests from applicants and reports to the authority of the result of certification (conformity or other aspects) tested against the agreed KPIs or process from the authority. In some case, the authority delegates the role of certification delivery to certification body. In the case of the Fiesta-IoT project, it is the Fiesta consortium which is the same as the authority.
3. Test execution body or Test House which performs the tests against the requirements. It is accredited by the certification body to offer testing of Fiesta technologies and the issuing of a Test Report, which will be suitable for forming basis for filing for product certification.
4. Applicant who submits their product as candidate for certification.

Note: do not confuse the roles in a certification program with the roles of stakeholders in the project.

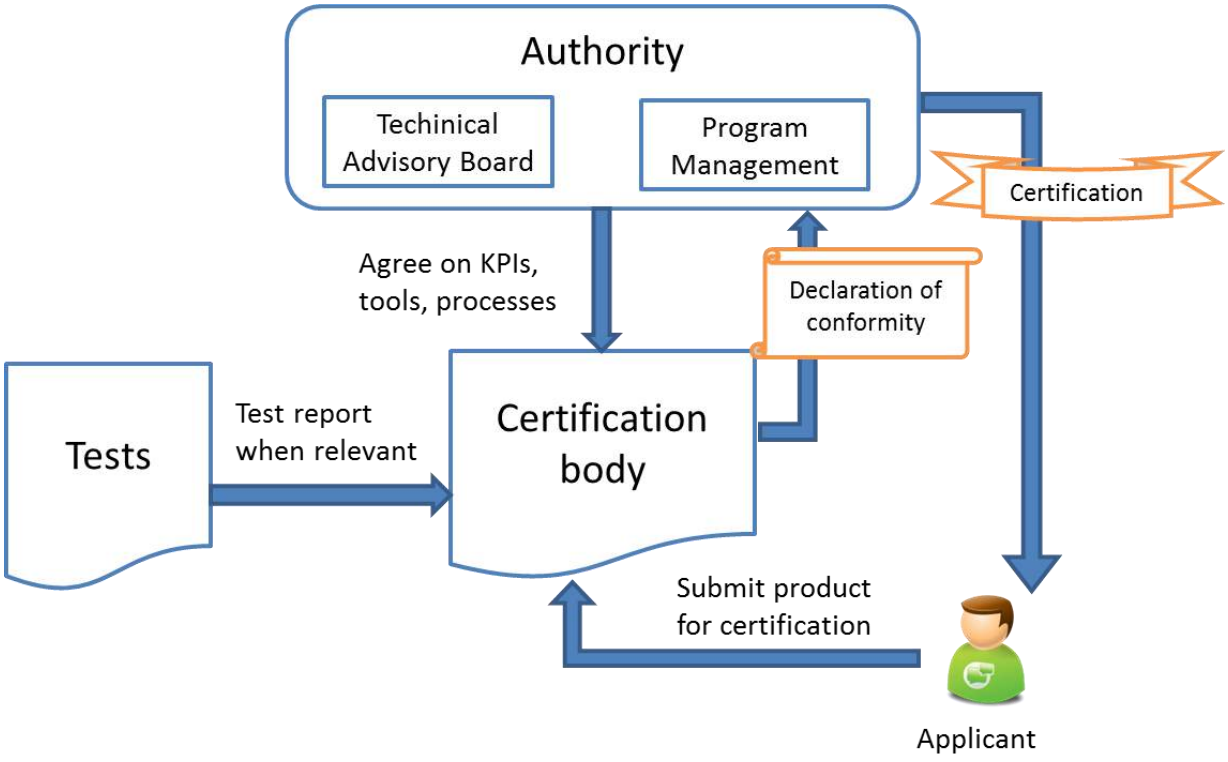


Figure 3: General certification workflow

The typical workflow is:

1. The authority releases the requirements for certification, including KPIs, tools, process. This step is to be done at the design phase of the certification program and only re-performed if there are any updates of the requirements.
2. The applicant submits his product to the certification body.
3. The test execution body takes the submitted product and performs tests against requirements. It generates a test report at the end of the tests to certification body. The test execution body or Test House takes the submitted

product and performs tests against requirements. It generates a test report at the end of the tests to provide to the certification body.

4. The certification body compares the test result and the reference to decide if to declare a certification or refuse the request.
5. If the candidate meets all the requirements, a positive declaration for certification is transmitted to the authority that delivers a certification for the candidate.

3 STAKEHOLDERS AND ROLES

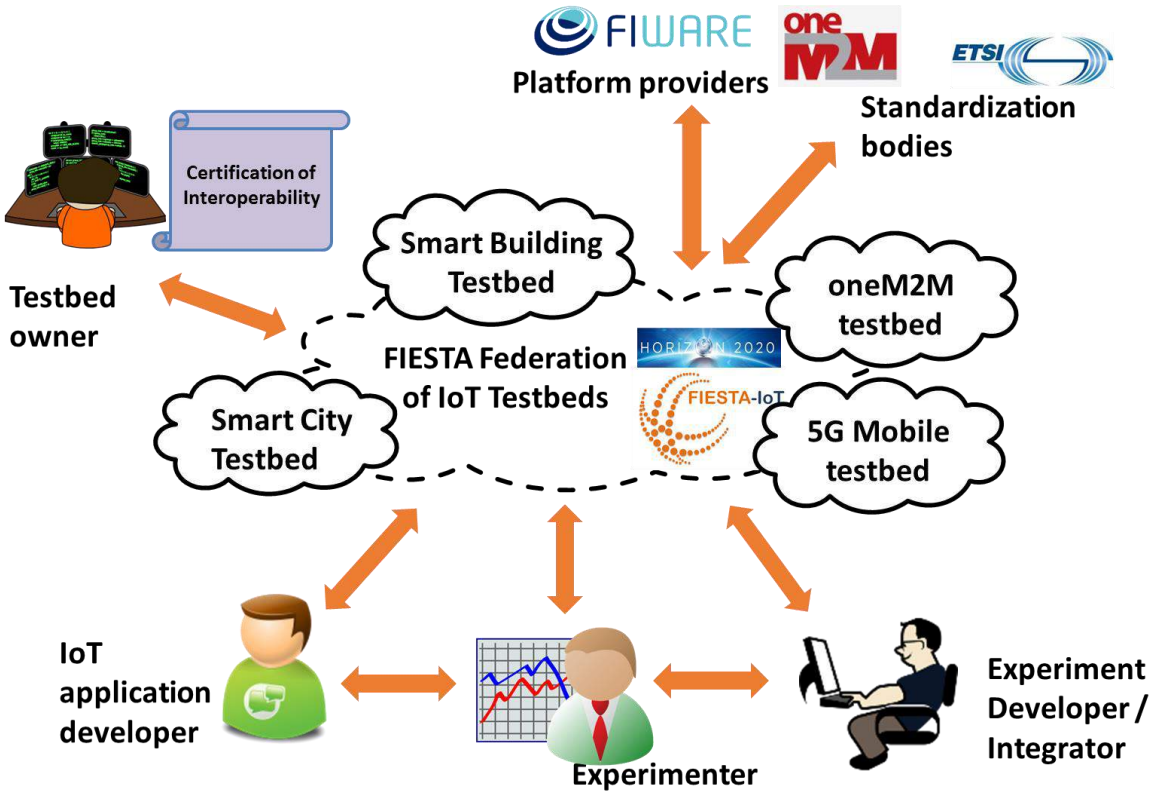


Figure 4: Stakeholders

The Fiesta-IoT project aims to attract the IoT market in general, not limited to experiment/testbed federation. Therefore, the stakeholders that we specified in D2.5 stay in the scope of the current confidence program, together with other important stakeholders in the IoT market such as IoT application developer and standardization bodies.

IoT testbed owner/infrastructure provider, experimenter/resercher and experiment developer/integrator have already been depicted in D2.5 [9], here we only present a brief description as a reminder:

- **IoT Infrastructure Providers and Testbed Owners** provide the test environment and are most interested in using the certification tools to improve their interoperability according to a reference to attract more experimenters to conduct their testing on the testbed.
- **Experiments Developer and Integrators** develop and perform experimentations, and are most interested in features such as the ease of use of

the testbeds, the performance of services and tools provided by the testbeds for development and deployment, and the effectiveness of collecting experimentation results.

- **Experimenters/Researchers** use the experiments running on the test federation to obtain the results they want and are most interested in the variety and availability of resources provided by the federation to design the experiment they need.

In the current certification program that expands the scope defined in D2.5, more stakeholders are addressed:

- **IoT application developer**. All successful ICT ecosystems have demonstrated the importance of activeness of application development based on a common platform. We believe that it is also true that various and numerous IoT applications will release the full potential of Fiesta-IoT technical results in the general IoT market during the project's exploitation phase. Application developers are interested in tools and services provided by the federation to develop and deploy their applications easily and efficiently. Also, they care about provided mechanism that helps their applications to get more visibility.
- **Standardization bodies.** Their main activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise producing technical standards that are intended to address the needs of some relatively wide base of affected adopters. They are most interested in earning better visibility of the standards and a wider adoption of their standards in the products on the markets. They are also interested in taking adaptable certification tools, technologies and processes for their own certification program of standard technologies.

4 CERTIFICATION SUBJECTS

4.1 The importance of the Data

Internet of Things (IoT) is an emerging area that not only requires development of infrastructure but also deployment of new services capable of supporting multiple, scalable (cloud-based) and interoperable (multi-domain) applications. The concept of IoT has found its origin in the area of Radio Frequency Identification (RFID) domain where RFID tags are extensively used for data collection. Since then, the evolution has continued with more and more IoT technologies developed, not only for connecting physical things, but also for every"thing" including devices, services, platforms, users, etc.

In the view of interoperability dimensions presented in [11], it is clear that technical and syntactical interoperability has been the focus of research and development for last years, and also the focus of most standards organizations, alliances and consortia, that they have been made generally available. Whereas IoT researches and products benefits already the interoperability through specifically defined services, data models and other architectural elements, the IoT context is much more dynamic that the current technology-driven and static services are far from satisfactory for users to take the full benefit of IoT. According with the last report from Gartner on emerging technologies and particularly on IoT [12], we are heading towards a world of billions of things and trillions of pieces of data. In a dynamic

environment like the Internet of Things, where technology evolves rapidly and thus data sources change formats at all the time, there is an strong requirement to integrate multiple information sets. This describes the necessity to be interoperable at the data/event level so that it becomes easier to combine/aggregate data/event coming from heterogeneous data sources. This raises also the challenge of being able to look up/discover data source and relevant data. The work that has been done on these challenges in relation to semantic-web looks promising to achieve the next-level interoperability: the semantic one.

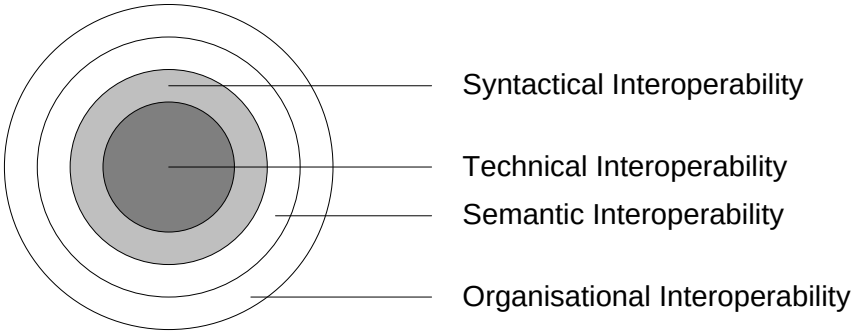


Figure 5: The Dimensions of Interoperability

Several IoT projects [13] have started work on the semantic interoperability of diverse IoT platforms, services and data streams. To this end, they leverage IoT semantic models (such as the W3C Semantic Sensor Networks (SSN) ontology [14], [15]) as a means of achieving interoperable modelling and semantics of the various IoT platforms. Fiesta-IoT, based on the feedback and experience from those projects, aims to establish a unique EaaS Platform by connecting various testbeds using semantic technologies, i.e. semantic annotation on testbed data.

The present certification and labelling programme is also unique in the sense of providing for the first time a set of tools and process addressing the semantic challenge issues. The programme is also hoped to be a first experience for similar programme set-up in IoT in the future.

4.2 Validation & certification process for Semantic interoperability

In order to set up the programme, we identify firstly the related aspects to be validated, such as i.e. data collection, aggregation, discovery as mentioned in 4.1. They are as follows (more details will be given in next sections):

- Ontology
- Data Annotation
- Reasoning
- SPARQL query
- Security

A complete validation and certification of semantic interoperability consists of a standard validation process of all the above subjects and plus a practical interoperability tests putting the systems under test together. Figure 6 shows the data workflow from data collecting by testbeds to agnostic data access by SPARQL queries in Fiesta (source T4.3). Here is a synthesized description of each layer in the workflow, more details should be given in T4.3:

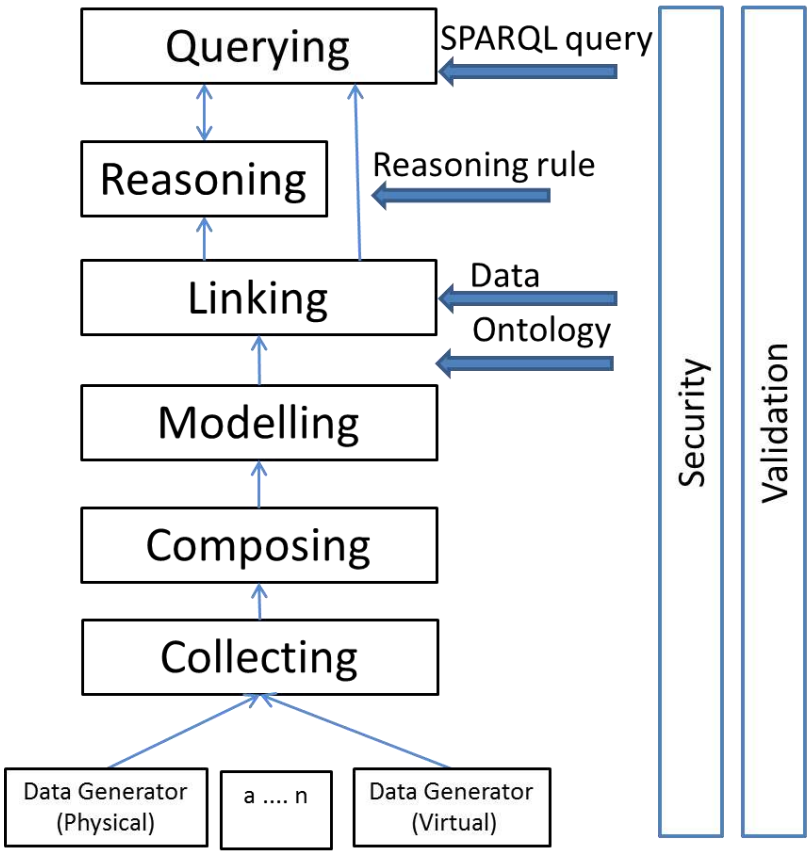


Figure 6: Fiesta validation and certification process for semantic interoperability

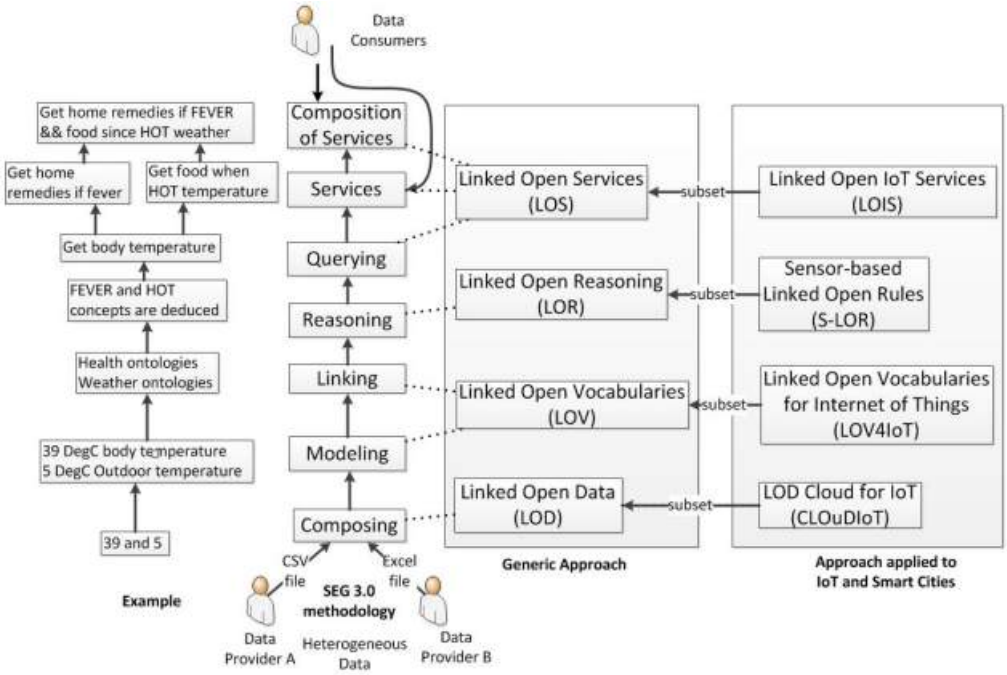


Figure 4: The SEG 3.0 methodology ensuring Semantic Interoperability from data providers to data consumers

- **Collecting** layer where raw data are generated from testbeds

- **Composing** layer where raw data are formatted in common used format such as xml, json, csv.
- **Modelling** layer where formatted data adopt a data model such as NGSI, or more precisely in Fiesta-IoT, using RDF triples.
- **Linking** layer where modelled data are enriched with information enabling the linking with other dataset
- **Reasoning** layer where new knowledge can be deduced from linked datasets.
- **Querying** layer where desired datasets can be selected using SPARQL queries.

  NOTE: The querying layer can access directly to the result of the linking layer, which means the original linked datasets without deduced knowledge from the reasoning. Reasoning layer can also use subset of the linked datasets resulted from the querying to deduce knowledge. Thus the arrow between the two layers is bidirectional.
- **Security** is a transversal module that should be considered for every layer

From the description, we can see that the upper layer depends on the function or the results of the lower layer. For example, if the reasoning layer should achieve a useful and satisfying result, the linking layer should make effort to link the most datasets that it is capable. Therefore, the points of validation of a specific subject that we marked in the data workflow should be validated from lower to upper layer to the final semantic interoperability test of more than one specific system implementations:

- **Ontology** used by one dataset, usually one dataset represents the data from one testbed, is often an extension of the general one to meet some specific needs of the given dataset. In the case of Fiesta, it consists of extensions of the Fiesta ontologies. This ontology extension should be validated before being used to annotate the dataset.
- **Data** are annotated with the ontology by a piece of software or a service called annotator. The annotated data should be validated before being reasoned in the next step.
- **Reasoning rules** should be validated to eliminate conflicts between rules or logical error before being used by the reasoner to generate new knowledge that enrich the dataset possible to be selected by users.
- **SPARQL queries** should be validated before pushed to the RDF server.

Security mechanism is checked in every validation point.

4.3 Ontologies

The most important aspect for a system to achieve compliance with the FIESTA-IoT platform and IoT interoperability is the capability of it to support the FIESTA-IoT ontology. FIESTA-IoT ontology uses a combination of existing widely used ontologies in order to be able to support in one hand as many system types as possible but also to be able to provide simple interoperable solutions. **Error! Reference source not found.** shows an overview of the Fiesta-IoT ontology. More information regarding the FIESTA ontology can be found in deliverable [16].

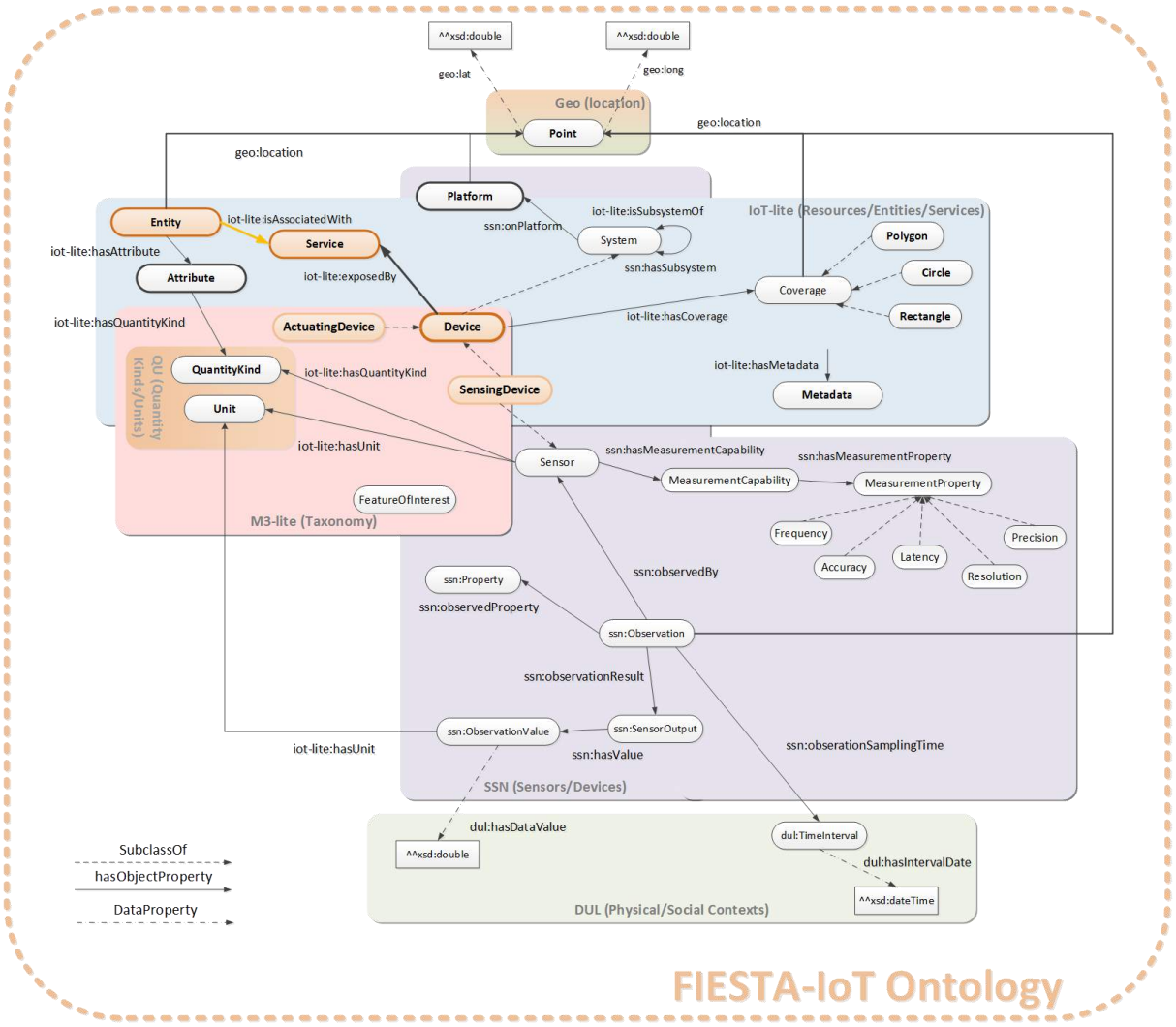


Figure 7: FIESTA-IoT Ontology

In the next paragraphs we summarize the ontologies that are utilized from the Fiesta-IoT ontology which are:

- **The SSN ontology**

The SSN ontology is based around concepts of systems, processes and observations. It supports the description of the physical and processing structure of sensors. Sensors are not constrained to physical sensing devices: rather a sensor is anything that can estimate or calculate the value of a phenomenon. Thus, either a device or computational process or a combination of them could play the role of a sensor. The representation of a sensor in the ontology links together what it measures (the domain phenomena), the physical sensor (the device) and its functions and processing (the models). Figure 8: Overview to SSN ontology classes and properties contains an overview of the main classes and properties inside the SSN ontology modules

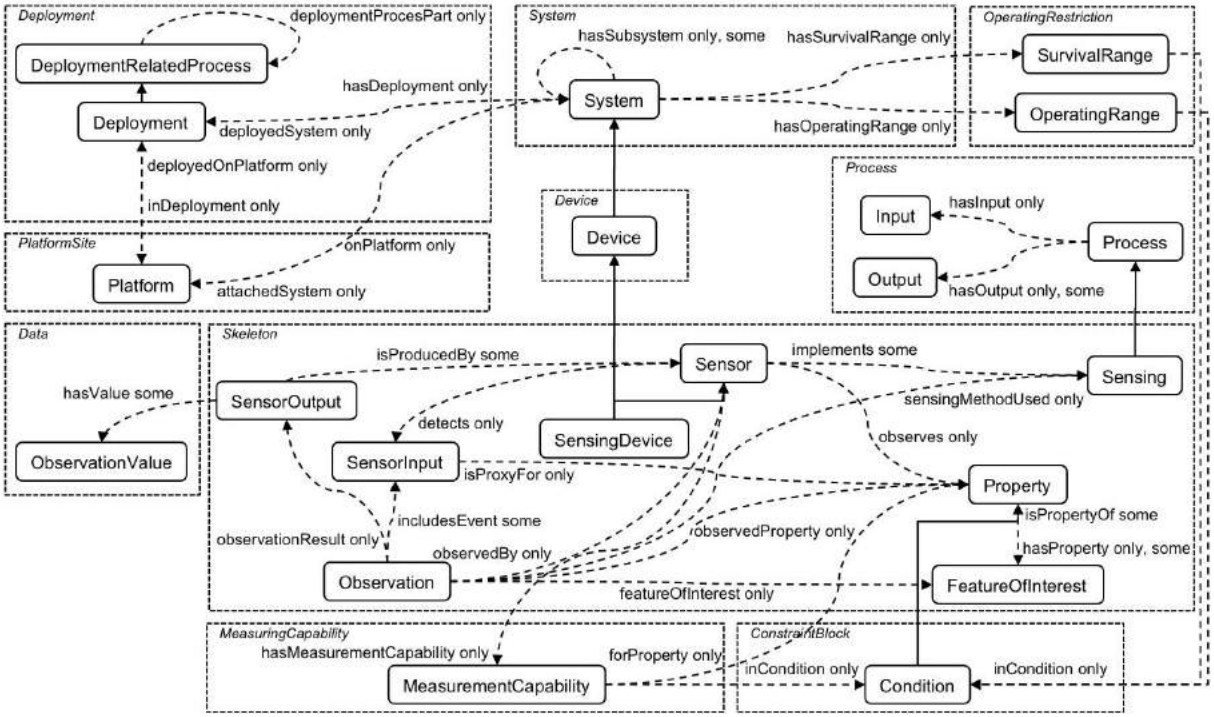


Figure 8: Overview to SSN ontology classes and properties

The SSN ontology can be used for a focus on different perspectives – or a combination of different perspectives:

- a sensor perspective, with a focus on what senses, how it senses, and what is sensed,
- a data or observation perspective, with a focus on observations and related metadata,
- a system perspective, with a focus on systems of sensors, or
- a feature and property perspective, with a focus on features, properties of them, and what can sense those properties.

- **The IoT-Lite ontology**

The IoT-lite[3] (see Figure 9: IoT-lite Ontology is intended to be a "lite" ontology for describing devices, sensors, services and object (Virtual Entities). It is simpler than the IoT-A ontology but keeps its "spirit". It also references a fragment of SSN (dealing with Sensor and Device descriptions). Figure 9: IoT-lite Ontology shows the main concepts in the ontology and how they relate to each other.

[3] http://iot.ee.surrey.ac.uk/fiware/ontologies/iot-lite

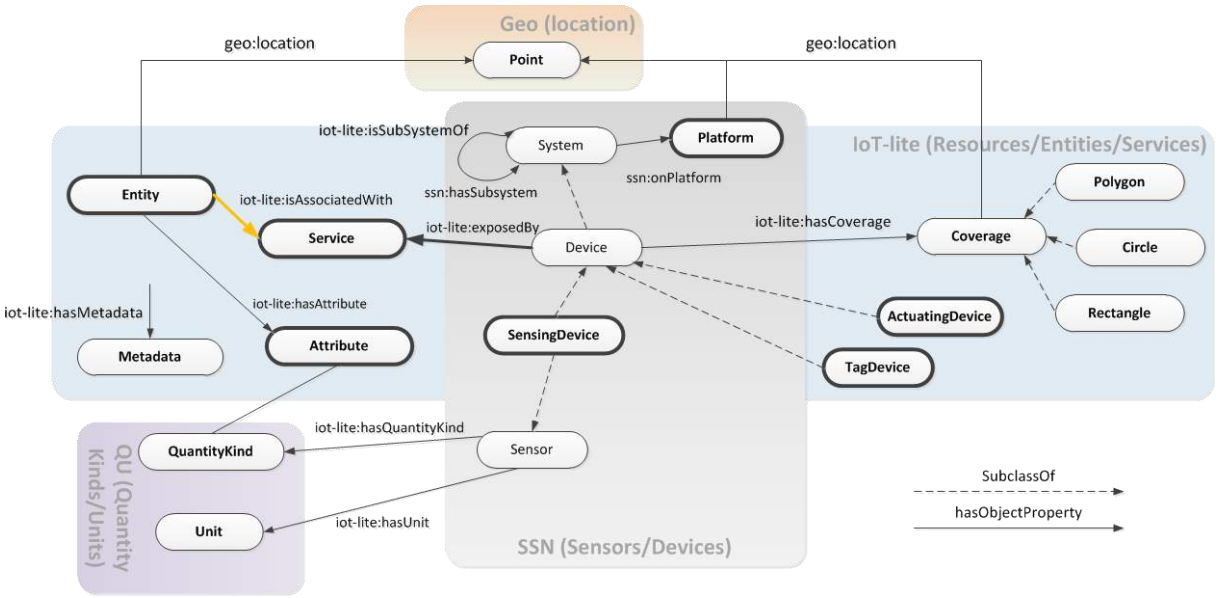


Figure 9: IoT-lite Ontology

- **The SAO ontology**

The Stream Annotation Ontology[4] (SAO [17]) (see Figure 10: SAO Ontology

- **The M3 Ontology**

) is an extension of the SSN ontology and the PROVO ontology[5] to allow the representation of real-time data streams, analyzed data streams and stream events. It links to additional ontologies like the Quality Of Information ontology (QoI[6]) and the Timeline[7] ontology. The core concept of StreamData extends the `ssn:Observation` class, and can hold data with respect to a "point" in time or an array of data over a "segment" in time.

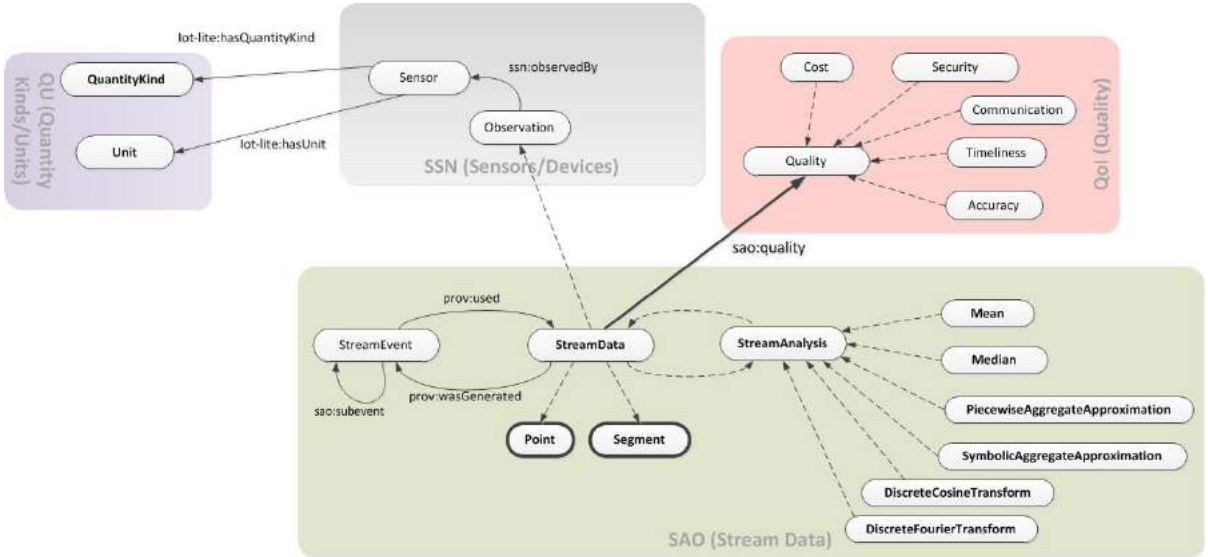


Figure 10: SAO Ontology

[4] http://iot.ee.surrey.ac.uk/citypulse/ontologies/sao/sao
[5] https://www.w3.org/TR/prov-o/
[6] http://purl.oclc.org/NET/UASO/qoi
[7] http://motools.sf.net/timeline/timeline.html

- **The M3 Ontology**

Machine-to-Machine Measurement (M3) Ontology [18] is designed to make the data interoperable and explicitly add the context when required to delete any ambiguities. The M3 ontology synthesizes and unifies all terms to describe sensors, measurements, actuators and domains found in existing IoT projects.

4.4 Annotators

The **Resource Annotator** validation should follow the FIESTA-IoT ontologies designed in WP3 Task 3.1. It will take inspiration from the W3C SSN validation process explained below, mainly used to validate data semantically annotated with the W3C SSN ontology. In the same way, the FIESTA-IoT validation service could be an extension of the W3C SSN validation process and could be designed to validate data semantically annotated with the FIESTA-IoT ontology explained above.

The **Data Annotator** validation should follow the M3-lite taxonomy. It means that all the terms used to describe sensor measurements, should come from the M3-lite taxonomy to avoid any issues to deal with synonyms (e,g,, precipitation and rainfall). The main benefit of checking that the terms used to describe data produced by devices follow the M3 taxonomy would ensure the data workflow without issues (e.g., no results).

4.5 Reasoning

Reasoning consists of being able to deduce new information from semantic data. For instance, to deduce high level information for each quantity kind referenced in the M3-taxonomy or supported by existing FIESTA-IoT testbeds (Com4Innov, KETI, UNIS, Santander).

For instance with a precipitation quantity kind, the mm/h unit and value 0, an abstraction is expected such as “No Precipitation”.

For each quantity kind, we expect one “$IF\ THEN\ ELSE$” rule to be able to provide reasoning.

Another important aspect is checking correctness and completeness:

- **Correctness** means that are no incompatibility with other rules. A dataset of interoperable rules has been built, when new rules are integrated within the dataset, correctness is checked. Taking inspiration from the M3 nomenclature[8], each quantity kind is provided with associated "$IF\ THEN\ ELSE$" rules when available. Sometimes, it happens that different projects are redefining rules. If the rules are compliant with each other, correctness is ensured; if not the project defining more specific rules is preferred. For instance, 2 rules to interpret body temperature quantity kind have been defined in [32, whereas 3 complementary rules have been defined in [33]. In this example, the correctness is ensured by two different projects defining complementary rules.

[8] http://sensormeasurement.appspot.com/documentation/NomenclatureSensorData.pdf

- $\boldsymbol{IF}\ BodyTemperature > 38\ and\ \ BodyTemperature < 39\ \boldsymbol{THEN}\ HighFever\ (unit: DegreeCelcius)$
  This rule has been defined in [32]
- $\boldsymbol{ELSEIF}\ BodyTemperature > 36\ and\ \ BodyTemperature < 38\ \boldsymbol{THEN}\ Normal\ BodyTemperature\ \ (unit: DegreeCelcius)$
  This rule has been defined in [32]
- $\boldsymbol{ELSEIF}\ BodyTemperature < 28\ \boldsymbol{THEN}\ SevereHypothermia\ (unit: DegreeCelcius)$
  This rule has been defined in [33]
- $\boldsymbol{ELSEIF}\ BodyTemperature < 28\ and\ BodyTemperature > 32\ \boldsymbol{THEN}\ ModerateHypothermia\ \ (unit: DegreeCelcius)$
  This rule has been defined in [33]
- $\boldsymbol{ELSEIF}\ BodyTemperature > 32\ and\ BodyTemperature < 35\ \boldsymbol{THEN}\ MildHypothermia\ \ (unit: DegreeCelcius)$
  This rule has been defined in [33]

- **Completeness** means that all sensor values are covered by a high level information. For instance, five rules have been defined to deduce high level knowledge from solar radiation measurements in [19]:
  - $\boldsymbol{IF}\ SolarRadiation = 0\ \boldsymbol{THEN}\ NoRadiation$
  - $\boldsymbol{ELSEIF}\ SolarRadiation > 0\ and\ SolarRadiation < 250\ \boldsymbol{THEN}\ LowRadiation\ (unit: WattPerMeterSquare)$
  - $\boldsymbol{ELSEIF}\ SolarRadiation \geq 250\ and\ SolarRadiation < 500\ \boldsymbol{THEN}\ MediumRadiation\ (unit: WattPerMeterSquare)$
  - $\boldsymbol{ELSEIF}\ SolarRadiation \geq 500\ and\ SolarRadiation < 750\ \boldsymbol{THEN}\ HighRadiation\ (unit: WattPerMeterSquare)$
  - $\boldsymbol{ELSEIF}\ SolarRadiation \geq 750\ \boldsymbol{THEN}\ VeryHighRadiation\ (unit: WattPerMeterSquare$

This example shows whatever the positive number generated by the device, high level knowledge (e.g., LowRadiation) can be deduced by the rule based reasoning engine.

- **Logical consistency** means that no contradiction has been detected among ontologies or rules. For instance a woman cannot be a man when “Woman” and “Man” have been designed as `owl:DisjointClass`).

More information regarding interoperability of rules applied to Internet of Things are explained in [20] [21].

4.6 SPARQL query

The SPARQL query engine should not generate any errors. The syntax of SPARQL queries needs to be checked. For instance, a same SPARQL query cannot be loaded by all semantic web frameworks. For instance, ARQ[9] is a SPARQL processor for the Jena framework which has a slight different syntax to execute SPARQL queries. It requires to add “.” at the end of each line, which is not the case with the Corese[10]

[9] https://jena.apache.org/documentation/query/

[10] http://wimmics.inria.fr/corese

SPARQL engine. Such implementation issues hinder the interoperability of the reuse and execution of SPARQL queries.

Another aspect could be considered such as security flaws provided by query languages (e.g., SQL injection).

4.7 Security

Certifying that a particular platform is secure is beyond the scope of FIESTA and the certification programme, whose focus is on standards compliance and interoperability. Instead the FIESTA certification programme for security will focus on the interoperability angle of security: does a platform comply with particular security mechanisms and protocols? If these are in place then it is likely that IoT systems can interoperate with one another with both functional and non-functional end-to-end properties.

The following platforms and standards will be investigated in terms of certifying whether systems and applications comply (and/or interoperate with).

1) FIESTA testbed security:

Each testbed that joins and participates in the FIESTA federation must comply with the security technologies, protocols and practices in order that it can be used. Hence, a testbed must be certified to conform to the security practices. These have been previously fully described in Deliverable D2.5 [9]; however, they are listed again here for illustrative purposes:

- **Secure encrypted communication channel**. The testbed must deploy and expose HTTPS interfaces i.e. HTTP over TLS (the secure transport layer protocol). The testbeds must exchange keys with FIESTA using DH-RSA.
- **Authentication***.* The testbed must trust FIESTA to identify and authenticate experimenters on its behalf. A request received by a FIESTA is deemed to be authentic (n.b. FIESTA is authenticated in the previous step).
- **Identity Management (optional)***.* A testbed testbed should comply with the OpenID-Connect and OAUTH protocol, such that it can invoke FIESTA's identity management API (for the required information).
- **Authorization***.* The testbed must provide FIESTA a set of access policies for its resources. These policies are described in the UMA[11] specification.
- **Testbed-based Access Control (optional).** A testbed endpoint must be able to read HTTP messages and extract the authorization token from the message and then utilise the OpenID Connect APIs to inform the authorisation policy.

2) FIWARE security specifications:

The FIWARE initiative created a number of security specifications based upon common standard specification e.g. OAuth and XACML. These are illustrated in the Authentication and Authorisation diagrams in Figure 11: FIWARE Security Specifications. These offer potential IoT security specifications that can be utilized by application developers; and hence tested for compliance by the market confidence

[11] https://docs.kantarainitiative.org/uma/rec-uma-core.html

programme. Such testing can be modelled and carried out using the tool described in Section 5.2.1.

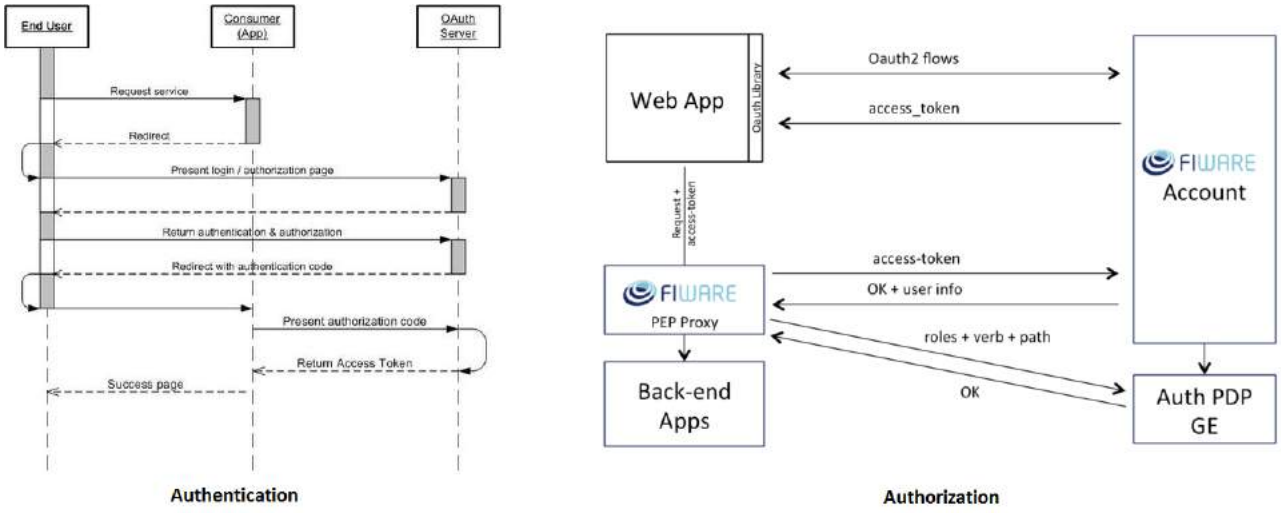


Figure 11: FIWARE Security Specifications.

3) Other security specifications

IoT application and systems developers may consider other IoT standards and hence these could also be covered by the testing programme. Security specifications are in review for the following important technologies:

- OIC – http://openconnectivity.org/resources/specifications
- OneM2M - http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V1_0_1.pdf

4.8 Compliance with the IoT Architectural Reference Model

The IoT Architectural Reference Model (IoT ARM) is a framework that aims at helping system architects to design a concrete architecture for their targeted IoT System. Following the IoT ARM methodology (which is also derived from the work by Rozanski & Woods [22]), a concrete IoT architecture consists of a set of Views and Perspectives. While Views traditionally pertain to functional requirements, Perspectives are more focusing on non-functional requirements relating to global system properties of the targeted IoT system (like for instance Security, Interoperability and Performance to name just a few) and consists of Activities/Tactics declined into Design & Technology Choices (DC/TC).

More precisely the IoT ARM consists of three parts:

- The IoT Reference Model (RM): as the name may suggest, the RM consists of a set of Models (mainly Domain, Information and Functional) that are not expected to be changed along the architecting process;
- The IoT Reference Architecture (RA): this part consists of Views and Perspectives. While views focus on specific aspects of the system, like functional, information, deployment aspects, perspectives tackle global properties spanning across the views. Indeed e.g. Security concerns can be seen at the functional, information and deployment levels, and ensuring

security at those levels results in very different actions; the two IoT Context and Physical-Entity Views are complementing the Functional, Information and Deployment Views. While the three later ones are thoroughly described within the RA, The IoT Context and P-E Views are not, because they are far too much specific to the targeted IoT System; However the Guidance chapter of the IoT ARM gives some clues about how to derive them;

- The Guidance: is a comprehensive process that describes thoroughly all phases and steps which need to be undertaken when designing a concrete architecture for an IoT sytem.

In the following section we consider the different constituents of the IoT ARM and discuss ways to ensure compliance.

4.8.1 Compliance with the IoT RM

4.8.1.1Compliance with the IoT Domain Model

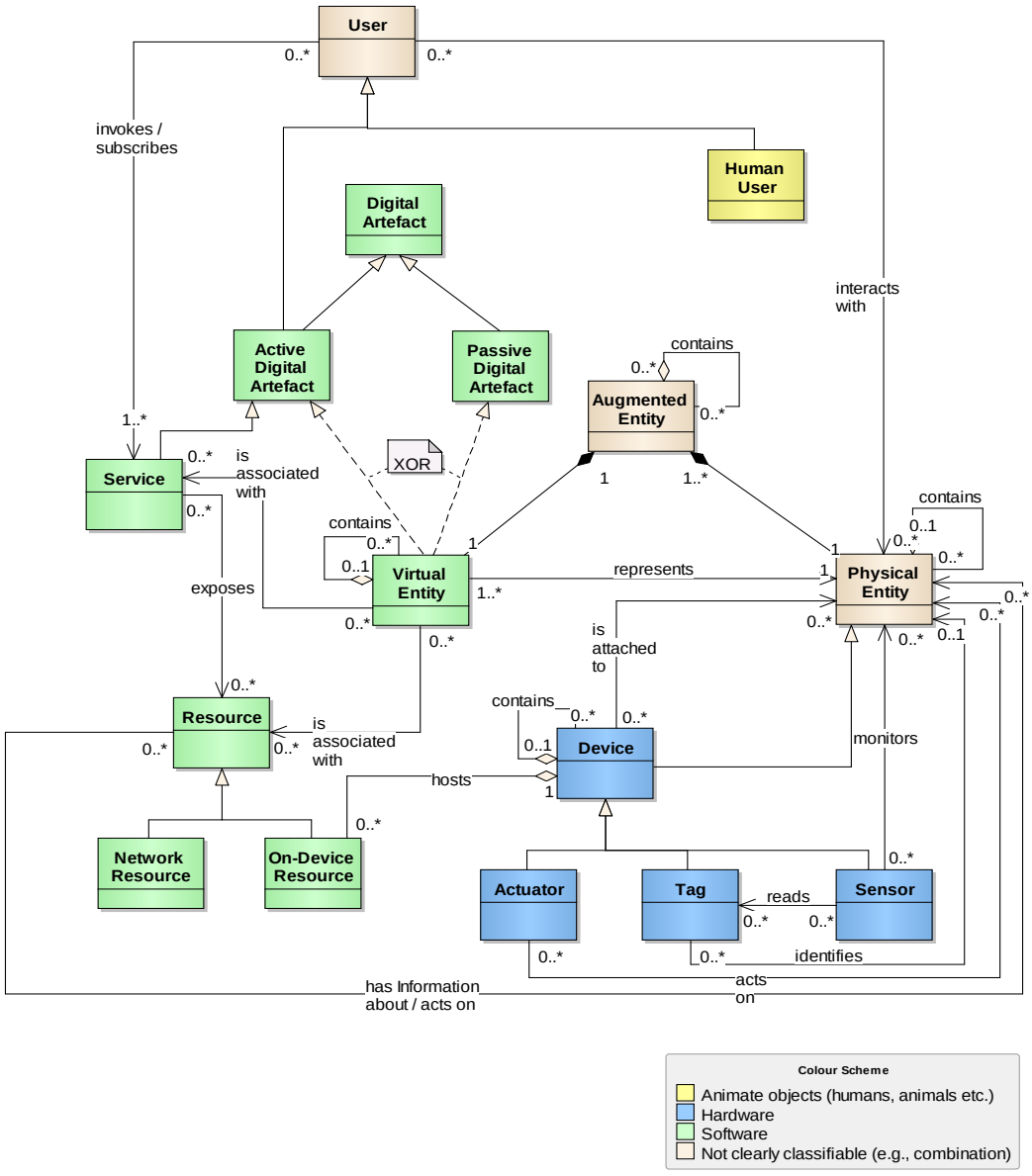


Figure 12: IoT Domain Model

There are different ways of using the IoT Domain Model (see Figure 12) when designing an architecture and it all depends which phase of the design is considered.

- Early phase / early discussions: This is the most informal use of the DM. As the DM introduces a list of concepts pertaining to the IoT Domain in general and explains the relation taking place between those concepts, the least that can be done on the compliance chapter is to ensure that all members of the teams involved, do adhere to the concepts and their definitions and to their relationships. For example, when referring to the projection of a Physical-Entity (P-E) into the cyber-world it has to be clear to everyone that one is talking about Virtual Entities (VE). It has also to be admitted that Resources maybe accessed only through the IoT Service exposing them, etc… Compliance at this level is hard to verify formally and is therefore rather informal. However ensuring compliance at early stage of the architecture design has proven to me paramount, and resulting in lot of energy / time savings;
- IoT Context View with Instantiated Domain Model: deriving an instantiated DM consists of taking as a starting point the native IoT DM and then instantiating all generic concepts like VE, P-E, IoT Service, Resources, Devices etc… according to the targeted system. For instance when dealing with a SmartPublicTransportation system (see the example Figure 13 below) for buses, we may consider BusP-E, BusVE, busStopsP-E, busStopVE, BusLine VE, OccupancySensors, BusPositionSensors etc etc with in addition all IoT Services exposing the resources hosted by the devices… all concepts instances are then shown in one whole figure (with inter-concepts relations). Compliance of the instantiated DM with the native DM schema can be easily checked. One smart way to ensure compliance is also to provide tools like UML editor that by-design can only edit complying UML schema, forcing concepts type and related relationships and checking on cardinality of those relations etc.

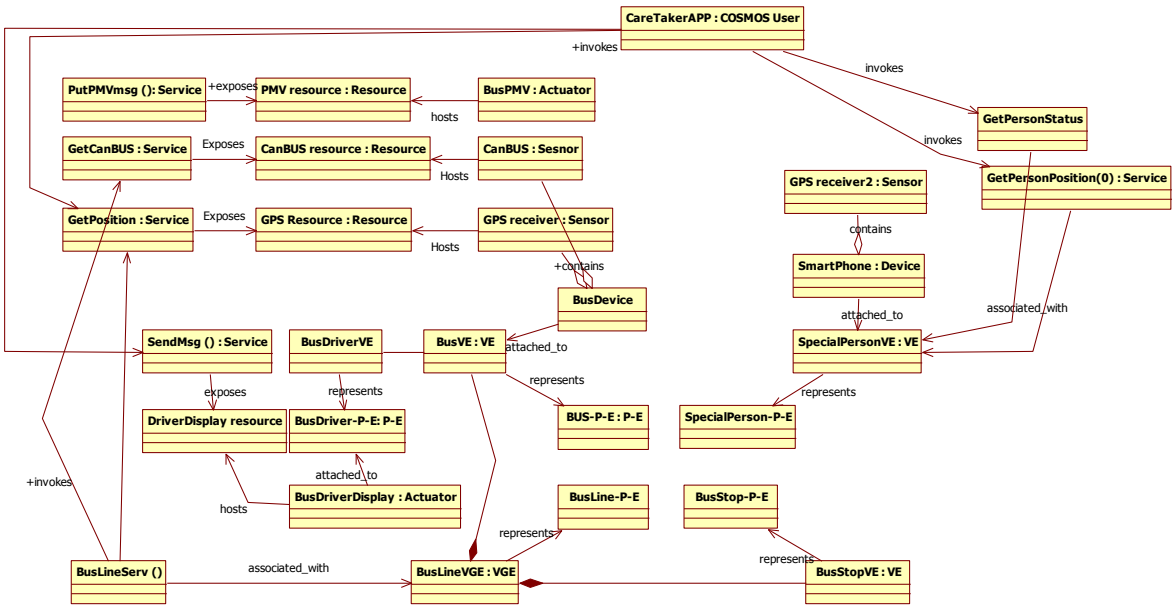


Figure 13: Example of an Instantiated Domain Model for Public Transportation

4.8.1.2 Compliance with the IoT Information Model

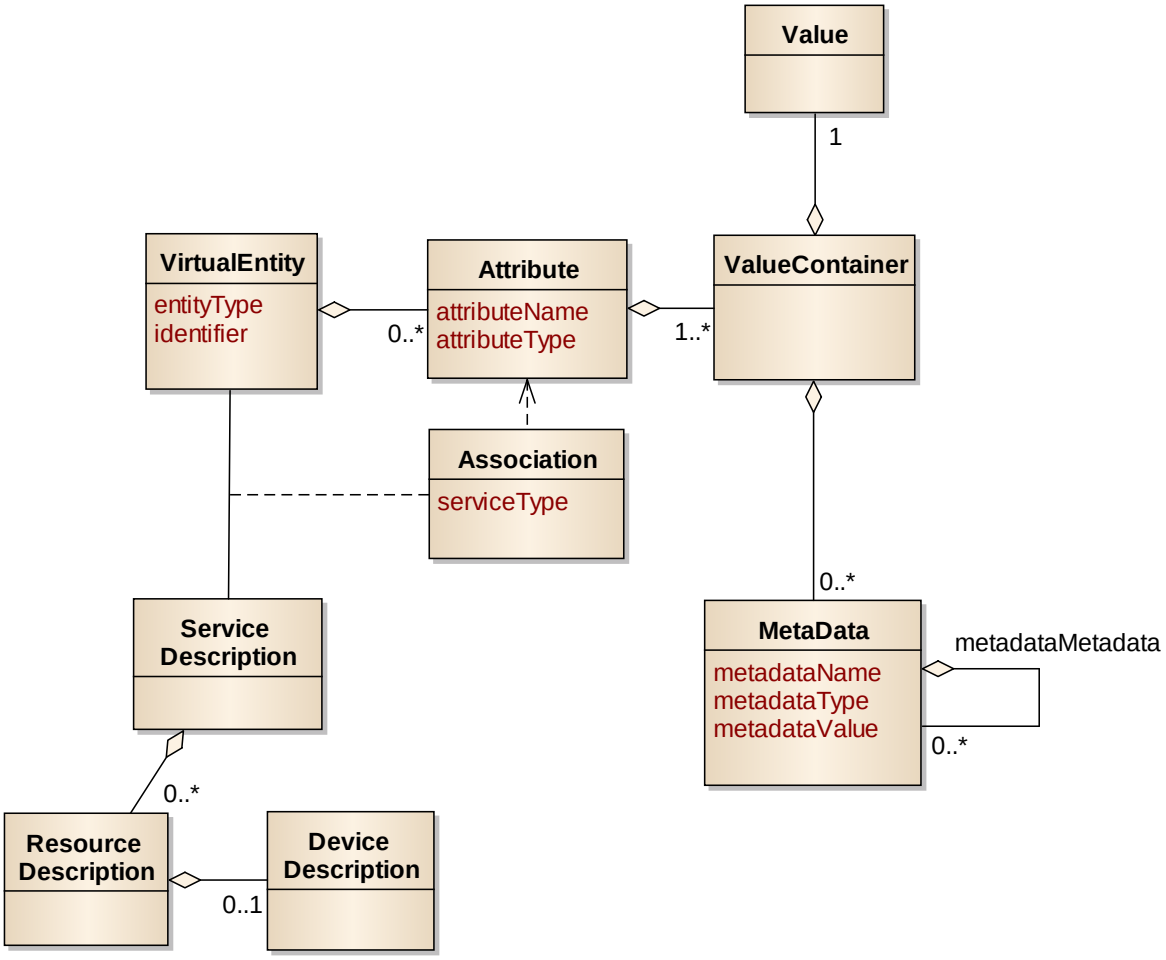


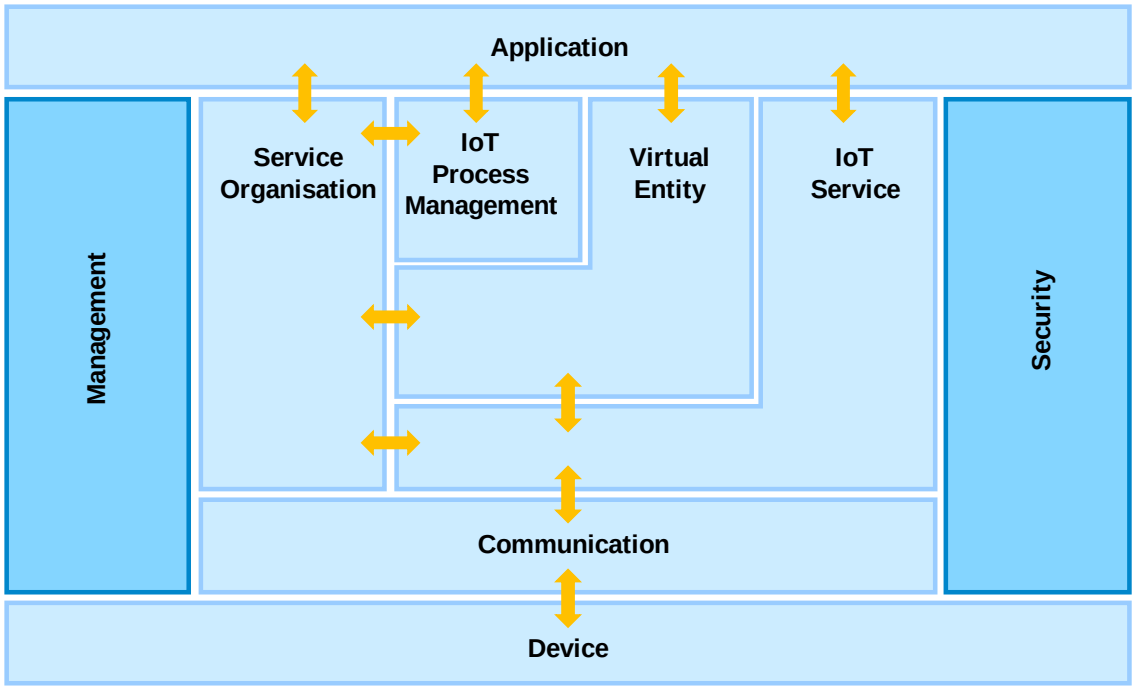
Figure 14: IoT Information Model

The IoT Information Model (IM) – see Figure 14 above- defines how some concepts of the IoT Domain Model are to be modeled information-wise. The IM e.g. explains the structure of VEs in term of properties, shows that Services, Resources and supporting Devices can be described (of course later on some Functional Components will directly refer to those descriptions for look-up or discovery purpose for instance). It also introduces the important concept of Association that links VE properties to IoT Services making therefore a link between the high abstraction VE layer (Virtual-entities representing objects) and lower abstraction level made of supporting Resource/IoT Service layer. The IM is very technology independent (like all models of the RM); for instance it does not give much detail about the structure of various Service, Resource and Device descriptions and does not preclude or even recommend any use of semantic technologies.

Recommending a particular technology choice like the use of Semantic for describing services and Resources, or even more precisely, recommending the use of OWL/RDF ontologies, is the purpose of Design and Technology Choices. In this particular case it could be a DC relating to a particular tactic (e.g. “ensuring semantic interoperability at data level”) part of the more general Interoperability Perspective.

Like the DM, the IM can also to be instantiated, even if this step is not mandatory. The instantiated Information Model can be therefore used to guide the elaboration of the Information View. Instantiating the IM follows the same principles used for instantiating the IoT Domain Model. Checking compliance of the Instantiated IM against the native and generic IM (above) can be achieved also the same way: either manually or by using an IM-constrained UML Editor.

4.8.1.3Compliance with the IoT Functional Model



IoT Functional Model

The main aim of the IoT Functional Model (FM) is to provide an insight of the main Functionalities Groups (FG) and their purposes, organized as a layered model, highlighting as well the way they interact with each other. The process of functional decomposition, which ultimately leads to the Functional View, leverages on Functional requirements in order to come up with FG-assigned Functional Components (FC).

Understanding well the purpose of each FG is paramount as the identification of the needed FCs is heavily relying upon this understanding. Once again, maintaining a common understanding between members of the architecture team is of the utmost important for ensuring a sound overall architecting process.

In order to be compliant with the FM, the concrete architecture must provide a functional decomposition that assigns FCs to the FGs as described by the FM and in accordance with their purposes. The verification of compliance to the FM is informal, however we will see later on, that compliance with the IoT Functional View can be achieved in a more formal way (via compliance to logical interfaces in particular).

4.8.2 Compliance with the RA

The IoT RA defines a set of viewpoints that can be used to describe the architecture views of the concrete targeted IoT system, and more generally defines what the

proposed views (Context, Physical-Entity, Functional, Information and Deployment views) should contain and focus on.

4.8.2.1Functional aspects

The IoT FV consists of a *typical functional decomposition* into FCs as shown in the following Figure 15:

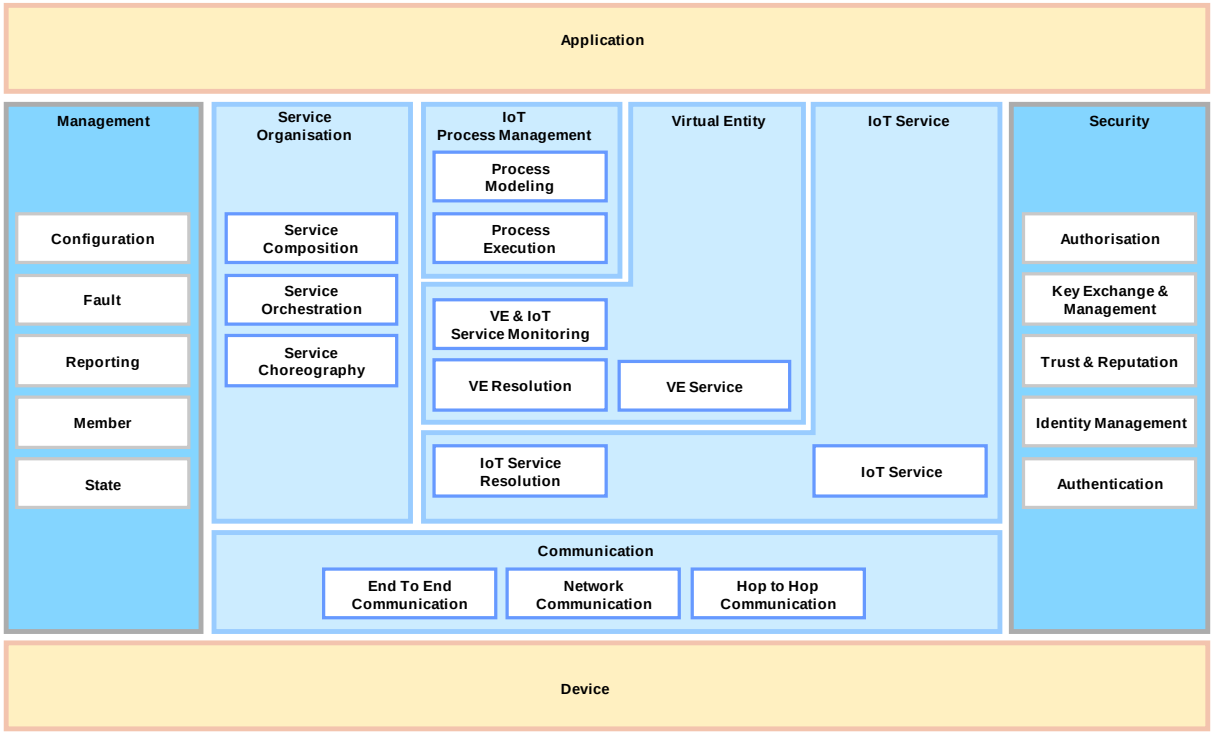


Figure 15: IoT Functional View ("native")

In Figure 15 above, FCs are mapped to FG as described by the FM.

Each FC is thoroughly described within the IoT ARM document and annex C provides detail about the Functionalities provided by each FC and their high-level interface (remember that the Functional Decomposition is a logical decomposition).

By “typical functional decomposition” we meant: a set of functional components that are expected to be part of most of IoT systems. There is therefore no fancy/highly specialized FC in this decomposition but rather just the bare minimum.

It is quite clear then, that when deriving a concrete architecture, and especially when dealing with concrete functional requirements, the architects will probably:

1. come up with some functional components that are already part of the “native” IoT Functional View(as shown above)
2. ignore some of those components that may be not needed, and finally
3. come up with new FCs corresponding to some functional requirements (which were not part of the list of Unified Requirements originally used for creating the “native” FV).

Compliance with the RA is mainly relating to the item 1/ from the previous list: components that are reused from the original IoT RM list must comply in term of offered functionalities and related interfaces. However it is accepted that those lists of functionalities (for given FCs) would be extended. If this is the case, the logical

interfaces must reuse the objects and concepts introduced by the various models if available. This constraint also applies to the case 3/ where fully new FCs are introduced; maximum reuse of existing concept is highly advised before thinking of creating new ones.

4.8.2.2Information aspects

When deriving the Information View the architect must provide information about how the information relating to the concepts considered in the IM is structured and represented. This structure can be described in a very abstract way following insights from the instantiated Information View. The IV also provides a more detailed definition and structure of the information after design choices pertaining to the perspectives have been chosen (see perspective chapter and how perspectives are applied to the views).

In addition to the information structure, the IV also deals with describing the information life-cycle and flows. The “native” IoT Information View provides therefore detail about how information flows between FCs should be reused/complied with when the related components are considered as part of the concrete architecture.

As far as information is concerned, compliance with the IoT ARM is mainly about complying with the IoT Information Model; typically a concrete architecture which does not implement the concept of Association would not be considered as fully ARM compliant.

4.8.2.3Perspectives

A perspective consists of a list of activities and related tactics that can be applied for reaching a particular system quality. Each identified quality comes with possibly more than one tactic. When applying a perspective to the views, each activity and tactics derives into design choices per view, as e.g. applying a tactic to one view (e.g. functional view) is different from applying the same tactic to a different view (e.g. deployment view).

The IoT ARM comes with 4 perspectives and a large number of activities and related tactics per perspective. It is very important to consider that applying perspective to views is the process where explicit technology and design choices are made, and like for any choice, wrong decision may be taken. This is the reason why using the IoT ARM does not guaranty any particular system quality. Reaching or not reaching a certain system quality will always be the result of design choices which have been chosen or not.

As a reminder, those perspectives consist of:

1. Evolution and Interoperability
2. Availability and Resilience
3. Trust, Security and Privacy and
4. Performance and Scalability

Complying with perspectives is not foreseen to be meaningful. Perspectives and design choices are at the disposal of the architect; they may be used or not.

However the concept of “Profile” is introduced in order to restrict the degree of architects’ freedom and of course, compliance with a profile become much more meaningful.

4.8.3 Compliance with Profiles

4.8.3.1ARM Profile

This section tentatively defines what an ARM profile may consist of. However it is work noting that this is an initial definition that may change or being fine-tuned following forthcoming results from other Work Packages in the course of the second half of project work period 2.

As it was emphasised in the previous subsection that the IoT ARM and especially the methodology supporting it, leaves a large degree of freedom to the architects. This is especially the case when dealing with Perspectives, and hence with non-functional requirements and targeted system properties spanning all aspects (i.e. Views) of the architecture.

The way an architect applies the perspectives onto his views determines the way perspectives activities and tactics are handled and ultimately how technology and design choices are selected; it also determines consequently how the desired system qualities are reached and at which level.

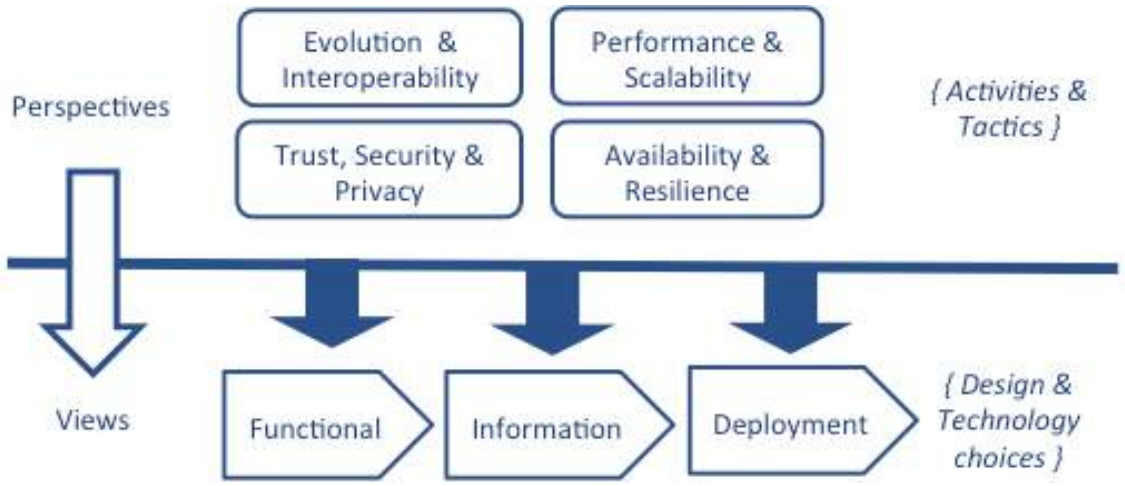


Figure 16: Applying Perspectives to Views

An easy example for illustrating this, is to consider the Trust, Security and Privacy (TSP) perspective. It is easy to understand that many different levels of TSP can be targeted, depending on the risk analysis conducted for the targeted system, added to given business goals and pricing constraints. So in general the IoT ARM should offer a variety of TSP profiles featuring increasing level of Trust, Security and Privacy, and it would be up to the architect to select the one fitting best all constraints and objectives.

In this particular TSP case, each elaborated profile (associated hence to a mechanism strength) comes with some Technology and Design constraints (as the choice is no more an option) which are aimed at “ensuring” that the desired TSP properties are met.

The aim of a profile is hence all about restricting the level of architect’s freedom with the adding’s of constraints of various natures as described in the list below.

More precisely we see a profile definition as a list of constraints to be complied with, as follows:

1. Functional-related constraints
    - Mandatory logical FC and related interfaces (to be reflected in the Functional View)
    - Mandatory system use-cases and Message Sequence Charts: the logic of interactions between those mandatory components must comply with very precise MSCs, which means that not only interfaces must be complied with but also dynamic behaviors;

2. Information-related constraints:
    - Information flows between components
    - Data format and serialization
    - Ontologies (if any)
    - Technologies for storing information (high impact on performance, resilience and scalability e.g.)

3. Communication-related constraints
    - Communication protocols
    - Higher-level protocols

4. Deployment-related constraints:
    - Mandatory concrete interfaces to be used in the actual implementation
    - Possibly concrete components and products (or at least class of products)

5. Perspective constraints: have direct impacts upon the Views (as Perspective are ultimately applied to the architectural views)
    - Mandatory Design Choices: which – when applied- results in the use of specific components and specific interaction schemas (System use-cases and Message Sequence Charts). Going for PKI is an example of strategy for providing overall high security based on the use of x509 certificates as main credential. It implies the use of TTP for instance and specific key generation components and interaction schemas (incl. specific use-cases);
    - Mandatory Technology Choices: which –when applied- results in the use of specific languages, data formats (incl. Serialization), information structure and consequently database type choice. For semantic interoperability profile, an example of technology choice could be the adoption of Jena and RDF and use of triple stores for storage. Applying scalability tactics on top could result in the use of other specific database technologies (still to be compliant with RDF/Jena for instance) that would support many more triples with faster retrieval time.

5 RELATED TOOLS

5.1 Semantic Web tools

A state of the art analysis has been done regarding the semantic web tools encouraging best practices within the Internet of Things community, the Web of Things (WoT) community [23] and Machine-to-Machine (M2M) community [24]. The set of tools and APIs are frequently updated on this web page[12] as well referencing the URLs and research articles when available.

Tools have been classified as follows:

5.1.1 Syntax validators

W3C RDF Validator[13] is a web-based tools that checks the given RDF/XML document, either by a direct text paste in a textfield, or from an URL, against the RDF RDF syntax[14] and the RDF Test Cases[15] Recommendations. It retrieves all the triples triples in the input RDF if there is no syntax error, or it indicates the error and where it where it occurs in the document (

- Figure 17). This tool does not provide APIs, however, its servlet which does the validation job is open source and is developed from the jena ARP[16] which is the RDF/XML parser for jena for handling the syntax.

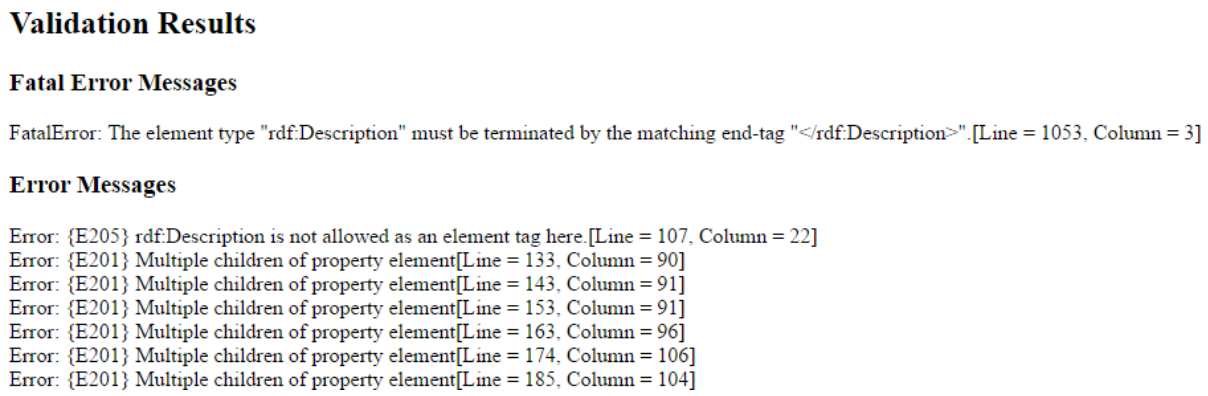


Figure 17: Error message in RDF validator

- **SPARQL query validator**[17]. This online tool checks the syntax of the SPARQL query entered by pasting on the web page, and formats it in several SPARQL based language (i.e. SPARQL algebra). It does not provide any documentation neither the source code. Still, it can be a preliminary tool for checking SPARQL query syntax. Figure 18 shows an example of SPARQL query validation using the tool. The “Input” section shows the original SPARQL query provided by the user.

[12] http://sensormeasurement.appspot.com/?p=bestPractice

[13] https://www.w3.org/RDF/Validator/

[14] http://www.w3.org/TR/rdf-syntax-grammar

[15] http://www.w3.org/TR/rdf-testcases

[16] https://jena.apache.org/documentation/io/arp.html

[17] http://www.sparql.org/query-validator.html

SPARQL Query Validator

Input:

```
1 PREFIX iot-lite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
2 PREFIX ssn: <http://purl.oclc.org/NET/ssnx/ssn#>
3 SELECT *
4 WHERE {
5   ?resource a ssn:SensingDevice.
6 }order by asc(UCASE(str(?s)))
```

Formatted, parsed query:

```
1 PREFIX  iot-lite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>
2 PREFIX  ssn:  <http://purl.oclc.org/NET/ssnx/ssn#>
3
4 SELECT  *
5 WHERE
6   { ?resource <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> ssn:SensingDevice}
7 ORDER BY ASC(ucase(str(?s)))
```

Alebgra, with general triple optimizations:

```
1 (base <http://example/base/>
2   (prefix ((iot-lite: <http://purl.oclc.org/NET/UNIS/fiware/iot-lite#>)
3            (ssn: <http://purl.oclc.org/NET/ssnx/ssn#>))
4     (order ((asc (ucase (str ?s))))
5       (bgp (triple ?resource <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> ssn:SensingDevice)))))
```

Figure 18 SPARQL query validator example report

- **YASQE (Yes Another SPARQL Query Editor)** is a SPARQL query editor[18] which provides features such as:
  - Prefix auto completion using prefix.cc referencing ontology namespaces.
  - Property and class auto completion using Linked Open Vocabularies (LOV) API
  - An option to query SPARQL endpoints.
  - A SPARQL syntax highlighting and error checking.
  - Storage of SPARQL queries for further usage.

[18] http://yasqe.yasgui.org/

Figure 19: YASQE GUI

5.1.2 Ontology validators

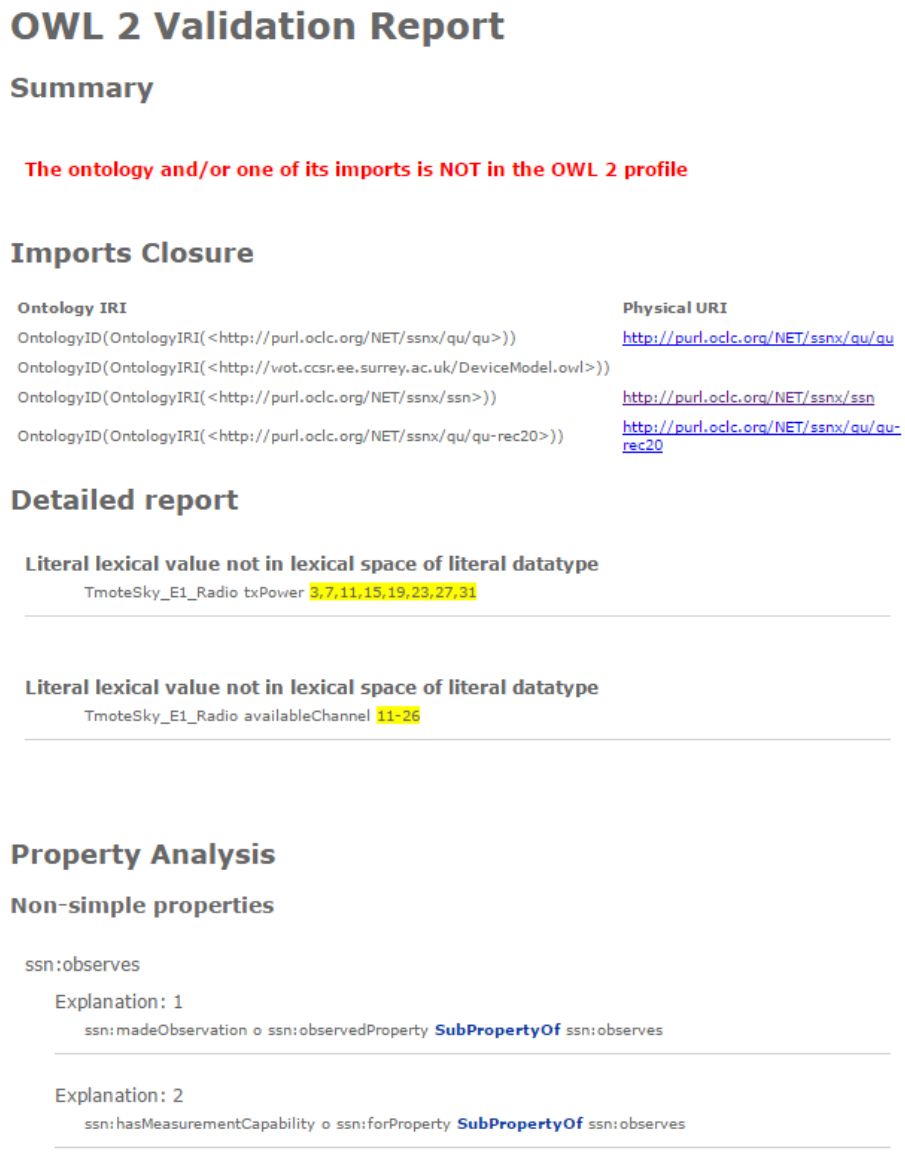
- Manchester OWL validator[19] checks problems in RDF model against the OWL 2[20] specifications, such as the compliance of the actual datatype of an instance against its declared datatype which is defined in OWL 2 specifications, or the global hierarchy restrictions defined in OWL 2. An example of validation report is shown in Figure 20. Its limitation is that it is not able to check against user-defined restrictions such as the compliance against a class or datatype defined in a "third-party" ontology (i.e. the Fiesta ontology). It has stopped updates since years ago and it lacks of documentation. It does not provide web API.

- The W3C SSN ontology validation service [21] (Kolozali, Bermudez-Edo, Puschmann, Ganz, & Barnaghi, 2014) is a web application that allows ontology developers to validate their sensor descriptions that are based on the SSN ontology. Users can input their data either by uploading a file or directly inputting the data in the textbox. The validation service receives a description and compares it against the SSN ontology and other ontologies that are frequently associated with it, such as FOAF, RDF-Schema, Dolce Ultra-lite. The result given is a validation report that reports any inconsistencies with the data. The application also provides a tag cloud that illustrates the popularity of the terms that are used by all the data that has been submitted for validation. When a document is submitted to the service, the data is passed to the validator which uses the Jena Eyeball API. The document is then parsed via a SPARQL engine whereby the terms it contains are extracted and stored.

[19] http://mowl-power.cs.man.ac.uk:8080/validator/

[20] https://www.w3.org/TR/owl2-syntax/

[21] http://iot.ee.surrey.ac.uk/SSNValidation/about.html



OWL 2 Validation Report

Summary

The ontology and/or one of its imports is NOT in the OWL 2 profile

Imports Closure

Ontology IRI	Physical URI
OntologyID(OntologyIRI(<http://purl.oclc.org/NET/ssnx/qu/qu>))	http://purl.oclc.org/NET/ssnx/qu/qu
OntologyID(OntologyIRI(<http://wot.ccsr.ee.surrey.ac.uk/DeviceModel.owl>))	
OntologyID(OntologyIRI(<http://purl.oclc.org/NET/ssnx/ssn>))	http://purl.oclc.org/NET/ssnx/ssn
OntologyID(OntologyIRI(<http://purl.oclc.org/NET/ssnx/qu/qu-rec20>))	http://purl.oclc.org/NET/ssnx/qu/qu-rec20

Detailed report

Literal lexical value not in lexical space of literal datatype

TmoteSky_E1_Radio txPower 3,7,11,15,19,23,27,31

Literal lexical value not in lexical space of literal datatype

TmoteSky_E1_Radio availableChannel 11-26

Property Analysis

Non-simple properties

ssn:observes

Explanation: 1

ssn:madeObservation o ssn:observedProperty **SubPropertyOf** ssn:observes

Explanation: 2

ssn:hasMeasurementCapability o ssn:forProperty **SubPropertyOf** ssn:observes

Figure 20: Manchester OWL validator report example

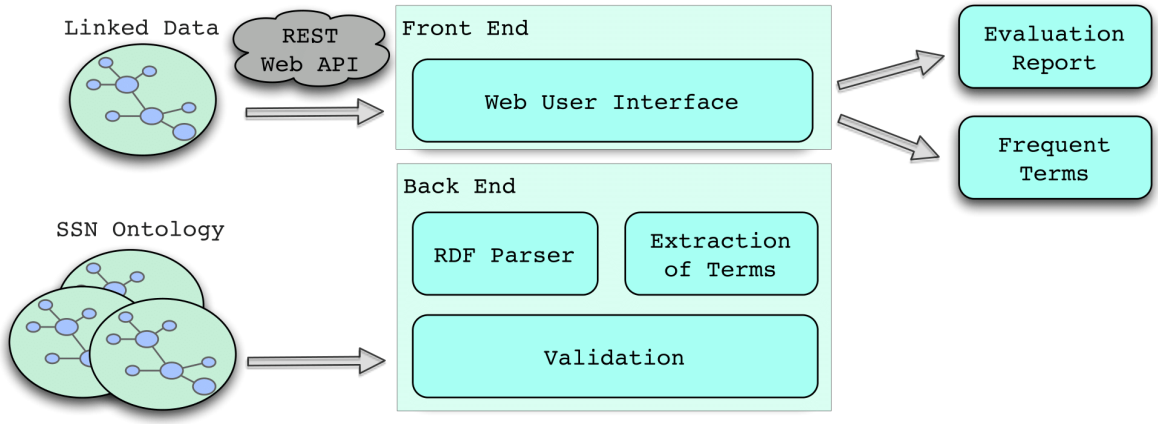


Figure 21: SSN validator architecture

5.1.3 Reasoning tools

A reasoner is a key component for working with OWL ontologies. In fact, virtually all querying of an OWL ontology (and its imports closure) should be done using a reasoner. This is because knowledge in an ontology might not be explicit and a reasoner is required to deduce implicit knowledge so that the correct query results are obtained.

Several reasoners exist for logical consistency checking, such as Pellet[22], FaCT++[23], HermiT[24]. They all implement the OWL API[25] which is a Java interface and implementation for the W3C Web Ontology Language (OWL), used to represent Semantic Web ontologies. Given an OWL file, they can determine whether or not the ontology is consistent, identify subsumption relationships between classes, etc.

Jena provides light-weight OWL reasoners[26] that could be described as instance-based reasoners which means it works on instance data and the reasoning about classes is done indirectly. It is anticipated that OWL rule reasoner will be most suited to applications involving primarily instance reasoning with relatively simple, regular ontologies and least suited to applications involving large rich ontologies, for which the more complex reasoners based on more sophisticated Description Logic reasoning such as listed above are more suitable.

5.1.4 Best Practices

Encouraging the use of best practices such as Oops[27] [25]. here it aims to assist ontology developers to avoid pitfalls in their ontology that can cause problems when applying reasoning. It also looks into avoiding maintainability issues and improves accessibility and clarity. This includes detecting polysemic concepts, synonymous classes, unconnected ontology concepts, and cycles in classes to name a few. Although thus type of tool is useful for mature ontologies, it may not be useful for ontologies that are intended to be “lite”.

5.1.5 Checking deferenceable URIs

Although not mandatory, it is essential that RDF resources are accessible through their URIs if they are to regarded as linked open data. Unfortunately, there are many declared resources in the web that are not reachable by the URI. Vapour[28] [26] is a web application that can be used to check the reachability of linked open web resources using their URIs. It also checks web application’s handling of content negotiation from HTTP requests with accept types for HTML descriptions or RDF variants for the targeted web resource.

[22] https://github.com/complexible/pellet

[23] http://owl.man.ac.uk/factplusplus/

[24] http://www.hermit-reasoner.com/

[25] http://owlapi.sourceforge.net/source.html

[26] https://jena.apache.org/documentation/inference/#owl

[27] http://oops.linkeddata.es/

[28] http://linkeddata.uriburner.com:8000/vapour

5.2 Interoperability and Compliance Testing Tools

5.2.1 Model-based Interoperability Testing Tool

The Model-based Interoperability Testing Tool [27] allows a system developer to create, use, and re-use “models of interoperability" to reduce development complexity in line with the following requirements to ensure interoperability is correctly achieved. In particular it supports:

- Specification compliance; to check that systems comply with particular specifications, e.g. an IoT sensor produces event data according to the NSGI specification, or streamed data content complies with a data format specification uploaded to the HyperCAT[29] catalogue).
- Interoperability testing; monitors the interaction between multiple systems to test whether they interoperate with one another, identifying the specific issues to be resolved where there is failure.

The tool supports the compliance and interoperability testing of HTTP-based protocols i.e. it can test the format, sequence and exchange of HTTP messages. It also tests the correctness and compliance of data in terms of schema checks (of JSON schema and XML schema); further it can test the content of fields complies with a specified value (using JSONPath[30] and XPath[31] expressions).

The Modelling tool is illustrated by the screen-shot in Figure 6. The tool offers two key functions to the user: i) a graphical editor providing drag and drop functionality to create the compliance and interoperability models; ii) a monitoring and testing environment to execute the real systems against the model to test their compliance and interoperability. The tool reports the results back to the user. The tool is open source (LGPL v3 Licence) and is fully available to be used, changed and extended in the context of FIESTA.

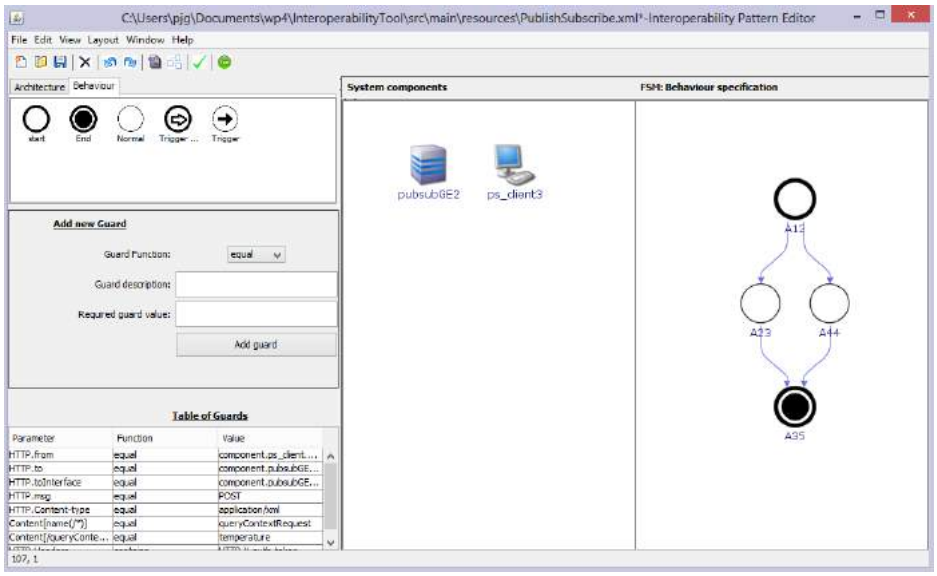


Figure 22: Model-based Interoperability Testing Tool

[29] http://www.hypercat.io/

[30] https://code.google.com/archive/p/json-path/

[31] http://www.w3.org/TR/xpath20/

Such a tool can be used by the FIESTA confidence programme in the following ways:

- Market Confidence Programme Developers (as part of the Certificate Authority) can model the compliance requirements or the interoperability requirements for a given standard e.g. OneM2M or NSGi. The software for these tests can then be generated automatically to be used by the FIESTA market confidence programme testing tools.
- The certification body tests the compliance and interoperability of a submitted product to test. This tool can be pointed at the submitted product, the compliance and interoperability tests will be run. The produced report then forms the input to the certification generation (e.g. it complies).

While the tool does not consider semantic data (a key feature of the FIESTA market confidence programme) - FIESTA will investigate how the results of such semantic testing can be integrated with this tool to provide complete coverage of the testing requirements.

6 FIESTA GLOBAL MARKET CONFIDENCE PROGRAMME PROPOSAL

6.1 The way we will offer the programme

The Internet of Things has been on the market for years. Technologies have been the focus of development to enable the connection between things. Strategies, standards and implementations supporting the technical interoperability are generally available as the standards organizations, alliances and consortia treated it with priority. However, the IoT is not only about connecting things, new networking technologies, it's also about high level communication across multi-domains. Thus the informational level interoperability, more specifically the semantic interoperability, is indispensable for the IoT evolution. Unfortunately, this subject is less mature in terms of development. Several projects have worked on this subject facing the semantic interoperability challenge.

The market demand for semantic interoperability solution has been expressed since years such as in IERC AC4 document [28] and followed up by the AIoTI WG3 on Standardisation [29] who address the semantic interoperability as a main challenge in the IoT. Currently, activities in IoT interoperability is highly focussed on Semantic interoperability and in particular as discussed within SDOs such as:

- SAREF reference ontology from ETSI SmartM2M. This ontology is built upon from more than 40 existing ontologies in the Home and Energy domain and will serve as a reference of unified data model for upcoming IoT systems.
- oneM2M semantic activities. Very active discussions and proposals are taking place in oneM2M MAS (Management, Abstraction and Semantic) WG. Some of them have been already included in the architecture and implementation specifications, such as a specific resource type "semantic descriptor" [30].
- W3C Web of Things. This initiative aims to provide a shared semantics for discovery, interoperability, scaling and layering on top of existing protocols and platforms. Things are described in RDF by using metadata which are further grouped into core and domain-specific metadata. SSN ontology is also a result from W3C's effort on the semantics.

- ITU is also convinced that semantic technologies are promising candidates to meet the current requirements for the IoT infrastructure, such as the automation, interoperability, reusability of large volume of data. It released very recently a recommendation Y2076 [31] on semantic requirements and framework of IoT.

All these discussions and activities with the various community working on IoT interoperability lead to have identified a MAJOR need for semantic interoperability best practices but also tools. Unfortunately, the valuable results and experience from these projects and communities stay experimental limited to the research domain, with complex configuration and not-so-friendly user interface that bound the further exploitation of their value.

Given the current status, Fiesta-IoT aims to more elaborate this informational interoperability to be able to bring it to the market by providing main tools that facilitate the access to semantic technologies. FIESTA will look at not only the testbeds providers, experimenters, researchers which could interact within the FIRE community, but more important will look at the overall market demand for IoT tests and interoperability. Therefore main objective of the certification and labelling programme with best practices and tools is

1. to assist researchers and experimenters
2. to assist standardisers to promote interoperability best practice supported by standards
3. most **important**, to provide to market place tools to check conformity to best practices and standards

In term of operational development, the Global Market Confidence programme will be implemented over two phases:

1. **Within the Fiesta project's timeframe**. The stakeholders will be those from the consortium, including the initial partners and the new partners from the open calls who bring their own testbeds into the Fiesta federation in a semantic interoperable way. During this phase, regular meetings are organized to set up a communication way between the programme implementers and the users (in the current case, the testbed owns). Especially during the period of tool integration and fine tuning, the interactions between the first testbeds and us will be close and frequent to improve the project's programme together, in order to provide a service quasi-mature and stable for open calls. In this phase, the programme will offer only **online tools**, including scorecard and testing tools, integrated in a web portal. Other forms of service, such as consulting and training, will not be distinguished from the **intra-project communications** as planned in the DoW. Experimenters and test beds owners available after the open calls will be asked to use the labeling programme and will help also to collect feedbacks and improve process
2. **Beyond the Fiesta-IoT project**. After the end of the project, we plan to maintain and extend the programme to fit the **IoT market in general**. The main stakeholders will be not only other individual testbeds who wish to join the functional and proved Fiesta Platform, but also other platforms who wish to implement similar programme, and experimenter and application developers who wish to know how to get use of such promising platforms. The service will be provided always with **online tools** integrated in a web portal and necessary

documentation and **material**, along with parallel support such as **training**, **consulting** and complete **commercial solution**.

As mentioned above, the services within the programme will be provided the following four forms:

- **Online tools**. These are tools that can be used through the web portal. Users can either access to them individually to test a specific aspect, or choose several of them to establish an automatic testing chain for certification.
- **Consulting**. This kind of service consists of providing expertise to help those who wish to make their product (i.e. testbed, experiment, application) interoperable with the Fiesta-IoT platform (1st phase) and other IoT platforms (2nd phase). how to make testbed/experiment/application compliant -> solution design
- **Training**. This kind of service consists of helping clients to get the competence for their product that they require
- **Solution design**. This kind of service is an extension of consulting in case that the client wish a ready-to-use solution for interoperability.

6.2 Plan for integrating of tools from other WPs and open source communities

We have identified for the programme the subjects to validate and some related tools to test their conformance and interoperability against the Fiesta specifications on the subjects. Among the tools listed in 5, we can group them in 2 categories:

1. Mandatory tools for conformance and interoperability testing.
   - Ontology: ontology validator
   - Semantic annotation: ontology validator
   - Reasoning: reasoners
   - SPARQL: SPARQL validator, YASQE, Vapour
   - Interoperability: Model-based Interoperability Testing Tool
2. Assisting and supportive tools for making and improving the conformity and interoperability.
   - Syntax: RDF validator, OWL validator
   - Best practice: Oops
   - URI checking: Vapour

Tools in both categories will be hosted as web service in Fiesta-IoT meta-cloud and accessible from the web portal. The integration priority will be given to the mandatory tool category.

6.3 The portal / web site to be developed for this purpose

Fiesta-IoT portal aims to incorporate comprehensive information to bring it to the people and by providing main tools that facilitates the access to semantic technologies for experimentation. The main objective of the portal and tools is

1. Describe requirements and provide specifications
2. Communicate information that is for public domain and community
3. Announce any development and integration plans

7 REFERENCES

[1] V. Haren, *TOGAF Version 9.0,* 2009.

[2] IoT-A, «Deliverable D1.2: Initial Architectural Reference Model for IoT,» 2011.

[3] Project Management Institute, "A Guide to the Project Management Body of Knowledge (5th Edition ed.)," 2013.

[4] A. Gavras, «Experimentally Driven Research White Paper,» 2010.

[5] IEEE, "IEEE Standard Glossary of Software Engineering Terminology," 1990. [Online]. Available: http://goo.gl/svqXqB. [Accessed 31 03 2016].

[6] MyFIRE, 05 2011. [Online]. Available: http://www.my-fire.eu/documents/11433/38630/D1.2+-+taxonomy+on+common+interpretation+of+testing%2c%20testing+approaches+and+test+bed+models?version=1.0. [Accessed 06 07 2015].

[7] A. H. Soukhanov, K. Ellis et M. Severynse, The american heritage dictionary of the english language, Boston: Houghton Mifflin, 1992.

[8] Fiesta-IoT, «Deliverable 2.4: FIESTA-IoT Meta Cloud Architecture,» 2015.

[9] Fiesta-IoT, «Deliverable 2.5: Global Market Confidence and Certification Specifications,» 2015.

[10] ISO/IEC, *ISO/IEC Guide 2:2004, Standardization and related activities -- General vocabulary.*

[11] M. Serrano, P. Barnaghi, F. Carrez, P. Cousin, O. Vermesan et P. Friess, «IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps,» *EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS,* 03 2015.

[12] P. Middleton, P. Kjeldsen et J. Tully, «Forecast: The internet of things, worldwide, 2013,» *Gartner Research,* 2013.

[13] M. Bauer, P. Chartier, K. Moessner, N. S. Cosmin, C. Pastrone, J. X. Parreira et R. Rees, «IERC-AC2-Deliverable 1,» 2011.

[14] K. Taylor, «Semantic Sensor Networks: The W3C SSN-XG Ontology and How,» chez *proceedings of 2011 Semantic Technology Conference*, San Francisco CA, USA, 2011.

[15] M. Compton, P. Barnaghi, L. Bermudez, R. G. Castro, O. Corcho, S. Cox et et.al, «The SSN Ontology of the Semantic Sensor Networks Incubator Group,» *Journal of Web Semantics: Science, Services and Agents on the World Wide Web,* 2012.

[16] Fiesta-IoT, «Delivrable 3.1.1: Semantic Model, Interoperability and Mobility support, Best Practices,» 2015.

[17] S. Kolozali, M. Bermudez-Edo, D. Puschmann, F. Ganz et P. Barnaghi, «A Knowledge-Based Approach for Real-Time IoT Data Stream Annotation and Processing,» chez *IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom), and IEEE Cyber, Physical and Social Computing (CPSCom)*, 2014.

[18] A. Gyrard, M. Serrano et G. A. Atemezing, «Semantic web methodologies, best practices and ontology engineering applied to Internet of Things,» chez *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, 2015.

[19] P. Staroch, A weather ontology for predictive control in smart home, Master Thesis, 2013.

[20] A. Gyrard, S. K. Datta, C. Bonnet et K. Boudaoud, «Standardizing Generic Cross-Domain Applications in Internet of Things,» chez *IEEE Globecom WOrkshop (GC wkshps)*, 2014.

[21] A. Gyrard, Designing Cross-Domain Semantic Web of Things Applications, PhD Thesis, 2015.

[22] N. Rozanski et E. Woods, Software systems architecture: working with stakeholders using viewpoints and perspectives, Addison-Wesley, 2012.

[23] A. Gyrard et M. Serrano, «A Unified Semantic Engine for Internet of Things and Smart Cities: From Sensor Data to End-Users Applications,» chez *2015 IEEE International Conference on Data Science and Data Intensive Systems*, 2015.

[24] A. Gyrard et C. Bonnet, «Semantic Web Best Practices: Semantic Web Guidelines for Domain Knowledge Interoperability to Build the Semantic Web of Things,» chez *oneM2M*, 2014.

[25] M. Poveda-Villalon, A. Gomez-Perez et M. C. Suarez-Figueroa, «Oops!(ontology pitfall scanner!): An on-line tool for ontology evaluation,» *International Journal on Semantic Web and Information Systems (IJSWIS),* vol. 10, n° %12, pp. 7--34, 2014.

[26] D. Berrueta, S. Fernandez et I. Frade, «Cooking http content negotiation with vapour,» chez *Proceedings of 4th Workshop on Scripting for the Semantic Web (SFSW2008).*, 2008.

[27] P. Grace, B. Pickering et M. Surridge, «Model-driven interoperability: engineering heterogeneous IoT systems,» *Annales des Télécommunications,* pp. 141-150, 2016.

[28] P. Cousin, M. Serrano et J. Soldatos, «Internet of Things Research on Semantic Interoperability to address Manufacturing Challenges,» 2014.

[29] AIOTI WG03 - IoT standardization, «Semantic Interoperability, Release 2.0,» 2015.

[30] oneM2M, *oneM2M TS-0001: "Functional Architecture",* 2015.

[31] ITU-T, *T-REC-Y.4111/Y.2076: Semantics based requirements and framework of the Internet of things,* 2016.

[32] Ahmed Loubiri, Abdel Obaid, and Fatiha Sadat. An ontology based system for social networking for health application support. In *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2013.

[33] Antonio J Jara, Miguel A Zamora-Izquierdo, and Antonio F Gomez-Skarmeta. An ambient assisted living system for telemedicine with detection of symptoms. In *Bioinspired Applications in Artificial and Natural Computation*, pages 75–84. Springer, 2009.

