Towards an Interoperability Certification Method for Semantic Federated Experimental IoT Testbeds

Mengxuan Zhao[1], Nikos Kefalakis[2], Paul Grace[3], John Soldatos[2], Franck Le-Gall[1]
and Philippe Cousin[1]

[1]Easy Global Market, Sophia Antipolis, Nice, France
`{firstname.surname}@eglobalmark.com`
[2]Athens Information Technology, Athens, Greece
`{nkef,jsol}@ait.gr`
[3]IT Innovation Centre, University of Southampton, Southampton, UK
`pjg@it-innovation.soton.ac.uk`

Abstract. IoT deployments and then related experiments tend to be highly heterogeneous leading to fragmented and non-interoperable silo solutions. Yet there is a growing need to interconnect such experiments to create rich infrastructures that will underpin the next generation of cross sector IoT applications in particular as using massive number of data. While research have been carried out for IoT test beds and interoperability for some infrastructures less has been done on the data. In this paper, we present the first step of the FIESTA certification method for federated semantic IoT test bed, which provides stakeholders with the means of assessing the interoperability of a given IoT testbed and how it can be federated with other ones to create large facility for experimenter. Focus is given on data and semantic context of the test beds and how they can interoperate together for larger experiments with data.

Keywords: Semantic Interoperability. Federation. Certification. Testbeds. IoT.

1 Introduction

The advent of the Internet-of-Things (IoT) paradigm has led to the emergence of a large number of context-aware human-centric applications that leverage data and services from sensors and other internet-connected objects. These applications are in several cases supported by IoT platforms, which facilitate the integration, and processing of IoT data streams, as well as their orchestration of IoT services in-line with the business requirements driving the IoT deployments [1]. Nevertheless, the vast majority of the platforms do not provide the means for building interoperable applications [2]. Hence, IoT deployments and also experiments tend to be fragmented and non-interoperable. This results in disaggregated and fragmented silo solutions, which can hardly be integrated into added-value applications [3].

One major aspect of the boom of IoT deployments is the growing and massive number of data which themselves can become non interoperable as data cannot be understood by different silos. It is therefore very important to provide environment such as test beds which can help to experiment the use of large data sets and get some tools to ensure data (semantic) interoperability [4]. Before providing techniques to ensure such data interoperability it is very important to provide large test facilities and

this is often provided by federation of testbeds. While federation of testbeds are promoted through regional program (i.e. GENI (https://www.geni.net) in US, FIRE and fed4FIRE [6] in EU), there is no specific federation techniques focusing on data and semantic interoperability.

To address this limitation the FIESTA project (http://www.fiesta-iot.eu) is developing a certification method for IoT interoperability, which provides testbed owners with the means to assess the interoperability features and capabilities of a given IoT testbed, while at the same time providing concrete guidelines to facilitate data interoperability. Such a certification method is motivated by the need to interconnect diverse IoT testbeds, to create richer experimental facilities.

The purpose of this paper is to introduce the FIESTA interoperability certification framework which is a set of tools and methodology. It is structured as follows: Section 2, following the present introduction provides more details about the framwork. Section 3 elaborates the methodology used to derive the suite, which included consultation with owners of IoT infrastructures and IoT software developers. Section 4 is devoted to the presentation of the suite, in the form of a scorecard, along with concrete examples of its use. Section 5 is the concluding section of the paper, which also highlights future work.

2   A Semantic Interoperability Certification Framework

The purpose of testbed is to provide an environment that allows experimentations and testing to be performed which can require the participation of selected end-users [5]. FIESTA is an experimental facility that is a federation of heterogeneous IoT testbeds. Experimenters can utilize tools and services to run IoT experiments across different testbeds (covering different heterogeneous technology domains) [6]. Interoperability is clearly at the heart of this federation. In order for testbeds and tools to participate in the federation—they must interoperate. Hence, the objective of the *certification framework* is to ensure that an individual testbed which applies to be a part of the federation conforms to the certification specifications in order to guarantee the service level of the federation. Such a framework ensures that the key stakeholders can behave as shown in Fig.1:

- **IoT Infrastructure Providers and Testbed Owners** provide the test environment, including resources and services (e.g. resource discovery, data access). The certification framework ensures that their testbed will gain wider visibility and will be used more extensively by applications and users.
- For **Experiments Developer and Integrators**. These are the people or organizations who develop and perform experimentations, which are in the form of new applications or services designed to get specific results, using the testing environment together with all available tools from the testbed. They 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.
- For **Experimenters / Researchers**. They are the people who use the experiments running on the test federation to obtain the results they want. They need the certification framework to get ensured about what testbeds are interoperable to be

used together, and what are the data accessible from the federation, in order to design their experiments and give the requirements to the experiments developer.

A certified testbed will help the other two stakeholders to have the confidence to concentrate on their core business without taking care of the details on the testing infrastructure. Conversely, once the two other stakeholders have confidence in the federation of certified testbeds, they will use more this testing infrastructure for their experiments. The **federator** (the FIESTA facility) is also a beneficiary of the certification framework that will provide guarantees that a given testbed complies and interoperates within the federation, thus being able to maintain the service level of the whole platform.
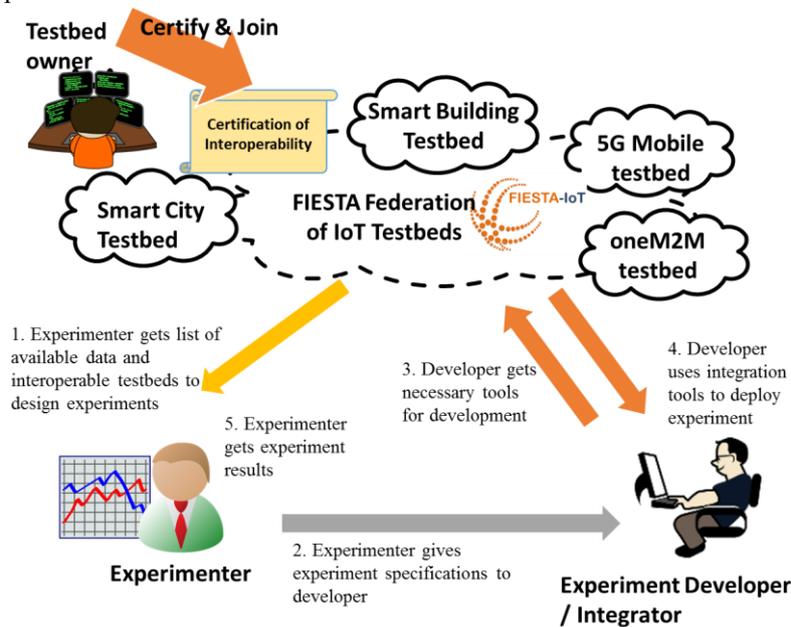
Fig. 1. Interactions between stakeholders in the certification framework

The structure of the certification framework comprises three elements:

- **Interoperability Aspects and Requirements**: The interoperability capabilities of each IoT platform or testbed will be defined in terms of a set of interoperability requirements (or capabilities) that it will have to fulfil. These requirements are discussed in the next paragraph.
- **Interoperability Scores:** Each of the requirements outlined above will give rise to scoring a testbed in terms of its interoperability features and capabilities. FIESTA will not define interoperability as an "all-or-nothing" value proposition. Rather, the project's certification framework foresees the assignment of an interoperability score to each IoT testbed, depending on the interoperability requirements/concerns that it addresses, as well as on the level/depth at which those requirements are addressed.
- **Classification and overall assessment**: The final outcome of the interoperability specification of a given testbed will be expressed also in terms of its classification

to an interoperability class signifying its interoperability level. However, there will also be testbeds that will be classified as non-interoperable ("fail" class) i.e. lacking essential features in order to be used in conjunction with other IoT platforms.

Table 1. Indicative Interoperability Classification.

Interoperability Class	Score (0-100) (example)	Explanation
"Platinum" (A)	S≥90	Excellent interoperability, exceeding the set of criteria.
"Gold" (B)	90>S≥80	Very good interoperability, fulfilling all the set of criteria.
"Silver" (C)	80>S≥70	Good interoperability, implementing most of the set interoperability criteria.
"Bronze" (D)	70>S≥60	Acceptable interoperability, providing support for a set of important requirements that enable interoperability
Fail (E)	60>S	The testbed has serious interoperability weaknesses and fails to meet essential interoperability requirements.

3   Certifying IoT Testbeds: Aspects and requirements

The production of the certification scorecard was developed by studying the interoperability requirements collected from our analysis of four testbeds aiming to integrate into the FIESTA federation (the requirements are documented [7]). These testbeds are not necessarily compliant with the FIESTA certified testbed definition from the beginning, because they may have different approaches or conflict of interest as they are independent. However, they should be the first to adapt the criteria of FIESTA testbed as soon as the definition of "FIESTA-compliant testbed", which is a mutual-agreement between them, is available, in order to establish the federation and enable first experiments running on the federation. This analysis of the requirements produced the following key themes where interoperability must be certified:

- **Data models**. Achieving interoperability by establishing and using a semantic model for the data in the federation.
- **Interfaces and services**. Certification of the services and interfaces which should be provided by the federation and each testbed.
- **Security.** Ensuring that testbeds maintain the end-to-end security properties of the federation.
- **Quality Auditing Aspects**. Ensuring that testbeds maintain the end-to-end Quality of Service Aspects of the federation.

3.1 Data models

A key interoperability characteristic of an IoT experimental infrastructure is its ability to represent and exchange data in standards-based models and formats. The rationale behind supporting such format is two-fold:

- **Syntactic Interoperability**: To facilitate developers in accessing and processing data, on the basis of popular, mainstream and widely use standards such as REST and JSON. This is a major step towards syntactic interoperability across IoT applications that use/leverage data from multiple testbeds.
- **Semantic Interoperability**: To ensure that IoT applications leveraging data from multiple testbeds have compatible semantics, thanks to their compliance to a common (standards-based) data model or ontology. The interoperability score of a testbed will be defined on the basis of the number and type of supported data models and ontologies

3.2 Interfaces and Services

Another interoperability feature of a testbed relates to the interfaces that it supports for accessing its IoT services and resources. The support of a standards-based interface can facilitate third-parties (i.e. integrators of IoT experiments) to develop interoperable applications, on the basis of the principle: "Build once and interface across multiple testbeds".

Interfaces. Apart from the provision of support for access interface, a testbed's interoperability is affected by the type of IoT services that it supports, such as for example services for discovery of resources (e.g., services, sensors) and data processing functionalities (e.g., CEP). To facilitate the FIESTA platform access across multiple testbeds some of the most known IoT and/or proprietary interfaces are going to be utilized:
- **SPARQL interface** : SPARQL Protocol and RDF Query Language interface is a web service for conveying SPARQL queries to an SPARQL query processing service and returning the query results to the entity that requested them
- **NGSI**: Next Generation Services Interface is a RESTful API via HTTP. Its purpose is to exchange context information.
- **OCCI**: Open Cloud Computing Interface is a Protocol and API for Management tasks. It can serve models in addition to IaaS, including e.g. PaaS and SaaS.
- **IoT-A Virtual Entity end point**: virtual entities representing physical entities can be discovered
- **Relational DB end poin**t.
- **Document DB end point**.

IoT Services. Some of the testbeds could provide additional services that will enable the experimenter and the FIESTA platform of having more advanced interaction with it. These services include:
- **Resource Discovery**: this service will enable FIESTA platform to discover available resources of the testbed and list them to the experimenter.
- **Direct access to sensors through services**: this service will enable the experimenter, based on an agreed access policy, to access the data feed of the sensor directly for retrieving real time data.
- **Actuation true offered services**: will enable the experimenter, based on an agreed access policy, to control a sensor/actuator by exposing its control interface.

3.3 Security

Security must be considered in an end-to-end manner across the federation. Interoperability covers both functional and non-functional properties. Each testbed that joins and participates in the FIESTA federation must comply with the security technologies, protocols and practices in order that it interoperates with the same secure characteristics. A fully interoperable testbed (syntactically and semantically) at both the data and interface/service levels still cannot operate within the FIESTA federation without considering conformance with the security architecture and requirements (and indeed other non-functional properties). For a testbed to be considered maintaining security compliance it must achieve the following elements:

- **Secure encrypted communication channel** between all testbed interfaces and FIESTA. The testbed must implement fully secure interface endpoints. That is all communication between the testbed and systems in the federation are encrypted.
- **Authentication**. The testbed must trust the FIESTA federation to identify and authenticate experimenters on its behalf. A request received by a testbed in the federation is deemed to be authentic.
- **Identity Management** (optional). A testbed may wish to determine who is using what features of the testbed, e.g. for accounting purposes.
- **Authorization**. The testbed may trust FIESTA to authorize users on its behalf. The testbed must then provide FIESTA a set of access policies for its resources.
- **Testbed-based Access Control** (optional). A testbed can choose to perform local access control decisions and enforcement. n

By conforming to these security features the key requirements of the federation are maintained: i) single-sign of experimenters to use all testbeds and services in the federations; ii) authorized access to resources; and iii) secure and protected communication in the federation.

3.4 Quality Auditing Aspects

Quality expectations depend on the evaluated subject which is testbed in the current case clarified earlier. Testbeds aim to provide better services to attract experimenters. In a given testbed, the most important impacts on the quality of service are the technological and service enablers that experimenters and developers use directly to implement the experiments.

Quality of Service (QoS) aims at evaluating the end to end service delivery quality and correlating it with the users' quality of experience. From [7], we identify the QoS-related indicators for the certification framework which are:
- **Response time**. The maximum delay to give a response to a received request.
- **Processing time**. The maximum delay that the testbed must finish the processing even in the most complex case.
- **Computational assets**. Resource assignment for computing should be optimized.
- **Service prioritization**. If a testbed provide several services, as resources are limited, it should be able to prioritize some services.
- **Reliability**. The testbed should be enough reliable to not interrupt experiments too often.

Good quality of a testbed is also related to how easy and clear that an experimenter can develop and deploy their experiments on it. **Best practice** such a support which is a guide for platform/framework users to design and run services/applications conform to the specifications in an efficient way. It helps to improve the reusability of the testbed for conducting various experiments on it. This guide will also help other testbeds in the federation to understand and cooperate with the current testbed. This is a part of the whole documentation. In a similar way, we identify the best practice-related indications from the requirement document of Fiesta.

- **Documentation**. The most essential part of the best practice about a platform.
- **High level interface description**. This will guide the users to use provided services.
- **Tools**. Available tools will help development, deployment and management of experiments.

4   Testbed Interoperability ScoreCard

Based on the items presented in the previous sections we have generated a scorecard, based on the criteria presented in Table 2, which was implemented in an Excel file and when completed during the certification process will provide a score to the testbed owner based on the features that is capable to provide.

Table 2.   The interoperability scorecard content

Testbed/FIESTA Interoperability	
Items	**Description**
Data Models	
SSN Ontology	Does the testbed supports the SSN ontology
FIESTA Ontology	Does the testbed supports the FIESTA ontology
SensorML	Does the testbed supports SensorML language to represent the sensor data
SWE	Does the testbed supports Sensor Web Enablement (SWE) language to represent the sensor data
Proprietary Format	Does the testbed supports a proprietary language to represent the sensor data
Data Extraction	Does the testbed provides the ability to extract data in a document format (i.e. CSV, Excel, XML, RDF, JSON, etch)
Graph Database	Does the testbed store its data in a Graph Database
Document Database	Does the testbed store its data in a Document Database
Relational Database	Does the testbed store its data in a Relational Database
Interfaces and Services	
SPARQL End Point	Does the Testbed offer a SPARQL (Graph DB) endpoint
NGSI Interface	Does the Testbed offer NGSI
OCCI Interface	Does the Testbed offer OCCI
Virtual Entity Endpoint	Does the Testbed offer an Virtual Entity end point
Relational Database End Point	Does the Testbed offer a Relational DB endpoint
Document DB Endpoint	Does the Testbed offer a document DB endpoint
IoT Services End Point	Resource Discovery, Direct access to sensors thru services, Actuation true offered services

Security	
Data Encryption	Offer secure encrypted communication channel between all testbed interfaces and FIESTA
Authentication	Can trust FIESTA to identify and authenticate experimenters on its behalf
Identity Management	Determine who is using what features of the testbed
Authorization	Is the testbed able to specify access rights to specific resources?
Testbed-based Access Control	Can the testbed choose to perform local access control decisions and enforcement?
Quality Auditing Aspects	
Response time	Do you control or set a threshold before which your testbed must give a response to the received request?
Processing time	Do you control or set a threshold before which your testbed must finish processing the request in the most complex case?
Computational assets	Does your testbed implement any resource optimizing mechanism?
Service prioritization	Does the testbed support the execution of services with different priorities?
Reliability	Do you define a ratio of failure time/working time that the testbed must respect?
Generic	
Documentation	Does the Testbed provide Documentation
Tools	Does the testbed provide development, deployment and management tools
Adaptors	Can the Testbed offer the ability to run third party software (i.e. FIESTA adaptors)
Additional DB	Can the testbed replicate/annotate its current data to the FIESTA format in a local Database

Application of scorecard to certify a testbed. Figure 2 is shows an example of a filled up scorecard with the relevant mock-up result/advice guide. This example is from the input and feedbacks from the Santander Smart City testbed. In the generated Excel file, the testbed owner is able to choose the level of support for the listed items above by ticking the appropriate box on the right and as soon as it finishes it can get an overall score (72.7/100 on upper right) of the testbed/FIESTA Interoperability. In the current case, a "Yes" give a score of 1.35, a "Partially" gives 0.75 and a "No" gives 0. It should be noted here that for the reason of ease of use for the scorecard users, some criteria in Table 2 are split into several finer items. We also investigate to generate automatically a report with a results/advice guide on what a testbed could easily support further or what needs to be done to make it interoperable with the FIESTA platform. according to specific items (i.e. "The testbed could adapt FIESTA ontology with some effort" (in data models category in Table 2)) is an advice given based on the "NO" answer of "Does the testbed supports the FIESTA ontology?"), or according to a score calculated within a category (i.e. "The testbed provides satisfactory quality of service" is given based on the scored calculated from the answers to items in the category "Quality Auditing Aspects"). It is mapped to the interoperability class "Sliver (C)" to give the testbed owner an intuitive information about how much effort to investigate in the future to make the testbed interoperable regarding to FIESTA.

Fig. 2. An interoperability scorecard mock-up sample

Table 3. An interoperability scorecard mock-up result/advice guide sample

Data Models
The testbed could adapt FIESTA ontology with some effort
Interfaces and Services
The testbed could adapt FIESTA architecture by implementing SPARQL endpoint
The testbed could utilize the FIESTA adaptors thru NGSI interface.
The testbed can provide direct access to sensors and actuators thru its own interfaces
Security
The testbed provides satisfactory level of security
The testbed can only provide complete access to one user type which will be controlled by FIESTA
One Fiesta User will require to be created to access the Data offered by the testbed
Quality Auditing Aspects
The testbed provides satisfactory quality of service
Generic
The testbed could offer FIESTA compliant database without the need of additional software

5   Conclusions and outlook

As part of this paper we have highlighted the importance of federating IoT test beds to ensure data interoperability experiments, along with the need of a framework for auditing IoT applications against their interoperability characteristics. The framework addresses a wide range of aspects that underpin interoperability, including

supported interfaces, data models, security mechanisms and more. Special emphasis is given in the provision of support for standards, which is an aspect that can greatly facilitate interoperability. The certification framework is currently provided in the form of a scorecard, which has been subject to small scale validation on the basis of the involvement of few testbed owners and IoT developers. As part of on-going work we are transforming the scorecard to an interactive on-line tool, which will facilitate its use by stakeholders, while at the same time enabling the reception of feedback for fine-tuning the implementation. Furthermore, a larger scale validation targeting owners and administrators of commercial IoT infrastructures (rather than experimental testbeds only) is also planned. This future work is expected to increase the number and scope of the potential beneficiaries of the certification framework, which will be provided as an on-line service. Furthermore the framework currently addressing test beds will be extended to the whole data IoT interoperability world where there are a lot of expectations in particular within Standards organizations such as ETSI or oneM2M, just to mention few ones.

References

1. Soldatos J, Serrano M, Hauswirth M.: Convergence of utility computing with the internet-of-things. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on. 4-6 July, 2012, Palermo, Italy, IEEE (2012)
2. Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J. P., Riahi, M., Aberer, K., Jayaraman, P. P., Zaslavsky, A., Zarko, I. P., Skorin-Kapov, L., Herzog, R.: OpenIoT: Open Source Internet-of-Things in the Cloud. Lecture Notes in Computer Science, invited paper, vol. 9001, (2015)
3. Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R. Bughin, J., Aharon, D.: Unlocking the Potential of the Internet of Things. McKinsey Global Institute, June (2015)
4. Serrano, M., Quoc, H. N. M., Le Phuoc, D., Hauswirth, M., Soldatos, J., Kefalakis, N., Jayaraman, P. P., Zaslavsky, A.: Defining the Stack for Service Delivery Models and Interoperability in the Internet of Things: A Practical Case With OpenIoTVDK. IEEE Journal on Selected Areas in Communications 33(4): 676-689 (2015)
5. MyFire project (http://www.my-fire.eu) deliverable D1.2-taxonomy on common interpretation of testing, testing approaches and test bed models
6. Fed4Fire project (http://www.fed4fire.eu) deliverable D2.3 First sustainability plan
7. Fiesta project deliverable D2.1 «Stakeholders Requirements»,