



**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 |

# Global Market Confidence and Certification Specifications

| | |
|---|---|
| Document Id: | FIESTAIoT-WP2-D25-CertificationSpec-231215-V14 |
| File Name: | FIESTAIoT-WP2-D25-CertificationSpec-231215-V14.doc |
| Document reference: | Deliverable 2.5 |
| Version: | V14 |
| Editor: | Mengxuan Zhao (EGM) |
| Organisation: | Easy Global Market |
| Date: | 23 / 12 / 2015 |
| Document type: | Deliverable |
| Dissemination level: | PU |

# DOCUMENT HISTORY

| Rev. | Author(s) | Organisation(s) | Date | Comments |
|---|---|---|---|---|
| V01 | Martin Serrano | NUIG-Insight | 2015/02/01 | Initial Draft Proposal |
| V02 | Mengxuan Zhao | EGM | 2015/08/04 | Table of Content / Introduction |
| V04 | John Soldatos, Nikos Kefalakis | AIT | 2015/09/21 | Comments and Revisions of the Structure – Assignment of Contributors |
| V05 | Mengxuan Zhao, Paul Grace | EGM, ITINNOV | 2015/10/26 | Scope, Security and Quality auditing aspects, technical tools |
| V055 | John Soldatos, Nikos Kefalakis | AIT | 2015/10/27 | Initial AIT's Inputs (Background and Motivation in Section 3; Structure of the Certification Framework in Section 4; Description of Data Models and Interfaces) |
| V056 | Nikos Kefalakis | AIT | 2015/11/19 | Filled sections 3.4.2 and 3.7 |
| V060 | John Soldatos | AIT | 2015/11/24 | Section 3.4.1, various edits |
| V07 | Mengxuan Zhao | EGM | 2015/11/27 | Section 3.6, various edits |
| V10 | Amelie Gyrard Mengxuan Zhao | EGM, INSIGHT | 2015/12/04 | Reference for technical tools, Finalization |
| V11 | Paul Grace, Konstantinos Bountouris | ITINNOV, Com4Innov | 2015/12/20 | Technical Review |
| V12 | Luis Sanchez | UNNICAN | 2015/12/21 | Quality Review |
| V13 | Mengxuan Zhao, John Soldatos | EGM, AIT | 2015/12/22 | Modifications based on Technical and Quality review |
| V14 | Mengxuan Zhao | EGM | 2015/12/23 | Final version for approval |

# TABLE OF CONTENTS

**1 POSITIONING ..... 6**

1.1 FIESTA-IoT ..... 6
1.2 WP2 Overview ..... 8
1.3 Audience ..... 10
1.4 Terminology and Definitions ..... 11
1.5 Executive Summary ..... 13

**2 INTRODUCTION ..... 13**

2.1 Background and Scope ..... 13
2.2 Motivation ..... 14
*2.2.1 Federation of testbeds ..... 14*
*2.2.2 Certification and global market confidence program ..... 15*
2.3 Objectives ..... 15

**3 CERTIFICATION FRAMEWORK ..... 16**

3.1 Scope ..... 16
*3.1.1 Within FIESTA project ..... 16*
*3.1.2 Beyond FIESTA project ..... 16*
3.2 Certification Framework Stakeholders ..... 16
3.3 Structure of the Certification Framework ..... 17
3.4 Certification Aspects and Requirements ..... 18
*3.4.1 Data Models ..... 19*
*3.4.2 Interfaces and Services ..... 20*
3.4.2.1 Access Interfaces ..... 20
3.4.2.2 IoT Services ..... 21
*3.4.3 Security ..... 21*
*3.4.4 Quality Auditing Aspects ..... 23*
3.4.4.1 Quality of Service ..... 23
3.4.4.2 Best Practices & Blueprints ..... 24
3.5 Certification methodology ..... 24
*3.5.1 Questionnaires/scorecard ..... 24*
*3.5.2 Technical tools ..... 26*
3.6 Definition of indicator in scorecard ..... 27
3.7 Online self-assessment ScoreCard ..... 29

**4 REFERENCES ..... 34**

 

# LIST OF FIGURES

FIGURE 1 WP2 OVERVIEW ..... 8
FIGURE 2 RELATIONSHIP BETWEEN WP2 TASKS AND WITH OTHER WPS ..... 9
FIGURE 3 INTERACTIONS BETWEEN STAKEHOLDERS ..... 17
FIGURE 4 FIESTA MOCK-UP SCORECARD ..... 32
FIGURE 5 FIESTA SCORECARD MOCK-UP SAMPLE ..... 33

 

# LIST OF TABLES

TABLE 1 WP2 DELIVERABLES ..... 10
TABLE 2 TERMINOLOGY AND DEFINITIONS TABLE ..... 11
TABLE 3 INDICATIVE INTEROPERABILITY CLASSIFICATION ..... 18
TABLE 4 INTEROPERABILITY CERTIFICATION ASPECT ..... 19
TABLE 5 ACCESS INTERFACE CERTIFICATION ASPECT ..... 21
TABLE 6 SECURITY CERTIFICATION ASPECT ..... 22
TABLE 7 QUALITY AUDITING CERTIFICATION ASPECT ..... 23
TABLE 8 BEST PRACTICE CERTIFICATION ASPECT ..... 24
TABLE 9 INDICATORS FOR TESTBED CERTIFICATION ..... 27
TABLE 10 FIESTA SCORECARD CONTENT ..... 30
TABLE 11 FIESTA SCORECARD MOCK-UP RESULT/ADVICE GUIDE SAMPLE ..... 34

 

# TERMS AND ACRONYMS

| | |
|---|---|
| CEP | Complex Event Processing |
| EaaS | Experimentation-as-a-Service |
| ETSI | European Telecommunications Standards Institute |
| FIRE | Future Internet Research and Experimentation |
| ICT | Information and Communications Technology |
| IEC | International Electrotechnical Commission |
| IoT | Internet of Things |
| ISMS | Information Security Management Systems |
| ISO | International Standardization Organization |
| KPI | Key Performance Indicator |
| NGSI | Next Generation Services Interface |
| OCCI | Open Cloud Computing Interface |
| QoS | Quality of Service |
| SPARQL | SPARQL Protocol and RDF Query Language |
| SSN | Semantic Sensor Networks |

# 1 POSITIONING

## 1.1 FIESTA-IoT

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 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 establishes the Certification Programme Specifications that will drive the global market confidante and certification actions around IoT experimentation model.

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-IoT 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-IoT 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 WP2 Overview

This Work Package covers the FIESTA-IoT requirements engineering activities and will produce the requirements associated with testbed-agnostic experimentation, as well as with the Experiment-as-a-Service model to designing and conducting experiments. WP2 is composed of five different tasks (depicted in Figure 1), which tackle distinct aspects of the FIESTA-IoT EaaS Experimental Infrastructure:

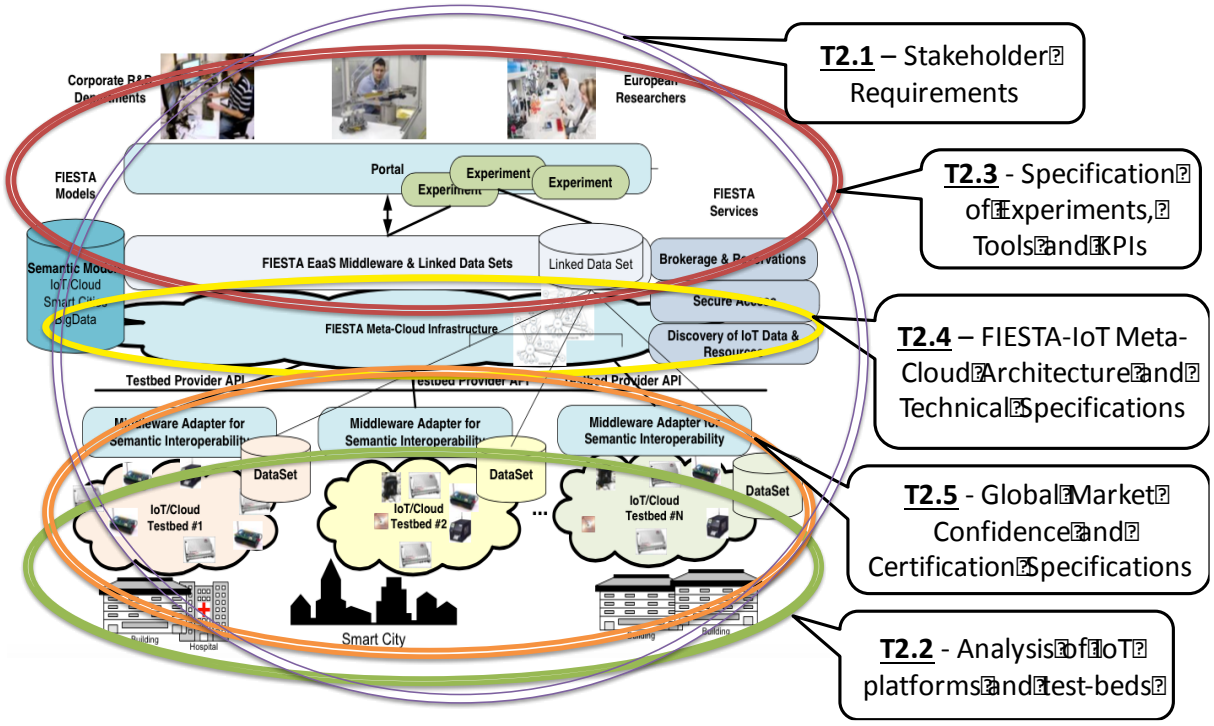


**Figure 1 WP2 Overview**

The WP2 Tasks cross all aspects of the FIESTA-IoT Infrastructure. They are:

Task 2.1. Stakeholder Requirements: This task is responsible for gathering and processing all Stakeholder requirements (using the Volere Requirements specifications (Volere) ). The involved stakeholders include: the IoT test-beds to be integrated, the experiment providers, and also researchers and experimenters. Also external projects (such as Open-IoT and Fed4Fire) will provide requirements so, to prepare FIESTA-IoT for the Open-calls. This task will produce a set of requirements that will be used by all other WP2 tasks.

Task 2.2. Analysis of IoT platforms and Test-beds: This task is focused on the Test-beds and IoT Platforms, analysing and describing what they do and how they do it. It will also use the set of test-bed requirements produced in T2.1 to better understand if each test-bed can fulfil the stakeholders' requirements. This task will then, model the Test-beds and IoT Platforms in functional blocks using the IoT ARM model from IoT-A project (IoT-A, 2013). It will gather what type of information they provide, and how they provide this information so that Task 2.4 can take this into account when developing the FIESTA-IoT Architecture. The outcome of this task will provide a basis for WP3.

 

Task 2.3. Specification of Experiments, Tools and KPIs: This task will specify all planned experiments and extrapolate from it the needed tools to execute those experiments. It will use the experiment related requirements produced in T2.1 and analyse them in terms of the tools that need to be provided from FIESTA-IoT to the experimenters. It will also specify the KPIs of each experiment so that later validation can occur. The result of this Task will be used as input to WP5.

Task 2.4. FIESTA-IoT Meta-Cloud Architecture and Technical Specifications: This Task will define the FIESTA-IoT Meta-Cloud Architecture, leveraging on the IoT-A ARM, and the technical specifications that will drive all the development work of the project. It will use information from previous tasks to identify the main building blocks, design & technology choices, and specify the functional blocks of the FIESTA-IoT architecture needed for achieving FIESTA-IoT's technical objectives. This architecture will serve as a base for all of the development phase of the project and more specifically for WP4.

Task 2.5. Global Market Confidence and Certification Specifications: This task is intended to study and define the global market confidence and certification specification. This means that this task is responsible to define the certification process, and the set of requirements that are required for a test-bed to comply, in order to be integrated into FIESTA-IoT. The outcome of this task will be used in WP6.

As described in the previous tasks description, the outcomes of each task will be used by other tasks of this WP2, or be used as inputs for the work in other WPs.

These relations between WP2 tasks and other WPs are depicted in Figure 2.

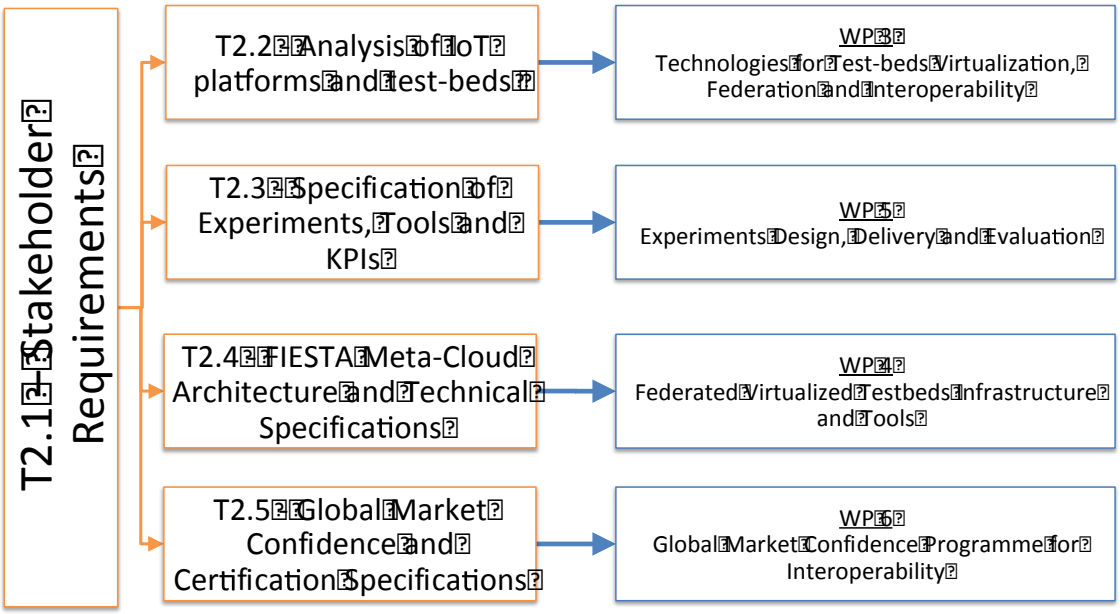


**Figure 2 Relationship between WP2 tasks and with other WPs**

In reference to the FIESTA-IoT project general objective(s), WP2 has a set of sub-objectives defined activities that are described as follow:

1) Determination of Stake Holder requirements.
2) Description of IoT Platforms and test-beds in order to facilitate their integration into FIESTA-IoT infrastructure.

 

3) Specification of planned experimentation and its executing tools, and the KPIs that will be used for validation.
4) Definition of the FIESTA-IoT Meta-Cloud architecture and the technical specifications required for the development WPs
5) Definition of the Global market confidence and Certification specifications

The Work Package 2 will also result in five deliverables, which will be directly linked with the objectives and tasks of the WP. Each Deliverable will be an outcome of each Task, meaning that Deliverable D2.1 will be provided at the end of T2.1 with the results of that specific task. The following table details the set of deliverables to be expected from WP2, with reference to the related tasks, the responsible partner for each deliverable and all other contributors.

**Table 1 WP2 Deliverables**

| No. | Deliverable | Responsible Partner | Contributors |
|---|---|---|---|
| D2.1 | Stakeholders Requirements | UNPARALLEL | NUIG-DERI, NEC, UNICAN, SODERCAN, SDR |
| D2.2 | IoT Platforms and Testbeds Analysis | Com4Innov | KETI, UNICAN, UNPARALLEL, AIT, NUIG-DERI, INRIA, NEC |
| D2.3 | Experiments, Tools and KPIs Specification | UNPARALLEL | UNICAN, INRIA, NEC, NUIG-DERI, AIT, ITINNOV, SODERCAN |
| D2.4 | FIESTA Meta-Cloud Architecture and Technical Specifications | UNIS | AIT, NUIG-DERI, UNICAN, ITINNOV, KETI |
| D2.5 | Global Market Confidence and Certification Programme Specifications | EGM | AIT, SODERCAN |

## 1.3 Audience

This deliverable addresses the following audiences:

- **Researchers and engineers within the FIESTA-IoT consortium**, which will take into account the various requirements in order to research, design and implement the architecture of the FIESTA-IoT Meta-Cloud Architecture.
- **Researchers on Future Internet Research and Experimentation (FIRE) focused on IoT and cloud computing systems experimenters at large**, given that the present deliverable could be a useful reading for researchers studying alternative IoT technologies and applications, along with indications and requirements towards building/establishing experimental architectures.

 

- **Members of other Internet-of-Things (IoT) communities and projects (such as projects of the IERC cluster)**, which can find in this document a readily available requirements analysis for experimentation-like IoT services and tools. For these projects the document could provide insights into requirements and technological building blocks enabling the convergence between utility/cloud computing and the Internet-of-Things for enabling experimentation as a service.

## 1.4 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 |
|---|---|
| Characteristic | An inherent, possibly accidental, trait, quality, or property of resources (for example, arrival rates, formats, value ranges, or relationships between field values). |
| Device | Technical physical component (hardware) with communication capabilities to other Information technology (IT) systems. A device can be attached to, or embedded inside a physical entity, or monitor a physical entity in its vicinity (IoT-A, 2013). The device could be:<br>• **Sensor**: A sensor is a special device that perceives certain characteristics of the real world and transfers them into a digital representation (IoT-A, 2011).<br>• **Actuator**: An actuator is a mechanical device for moving or controlling a mechanism or system. It takes energy, usually transported by air, electric current, or liquid, and converts that into some kind of motion (IoT-A, 2011). |
| Discovery | Discovery is a service to find unknown resources/entities/services based on a rough specification of the desired result. It may be utilized by a human or another service. Credentials for authorization are considered when executing the discovery (IoT-A, 2013). |
| Domain | Refers to an application area where the meaning of data corresponds to the same semantic context. For instance, pressure in Water Management Domain may refer to water pressure on pipes while in Air Quality Domain it refers to atmospheric pressure |
| Information | Content of communication; data and metadata describing data. The material basis is raw data, which is processed into relevant information, including source information (e.g., analogue and state information) and derived information (e.g., statistical and historical information) (IEEE, 2007). |
| Measurement | The important data for the experimenter. It represents the minimum piece of information sent by a specific resource, which the experimenter needs in order to fulfil the objective of the experiment |

 

| | |
|---|---|
| Metadata | The metadata is the additional information associated with the measurement, facilitating its understanding. |
| Physical Entity | Any physical object that is relevant from a user or application perspective. (IoT-A, 2011). Physical Entities are the objects from the real world that can be sensed and measured and they are virtualized in cyber-space using Virtual Entities. |
| Requirement | A quantitative statement of business-need that must be met by a particular architecture or work package. (Haren, 2009) |
| Resource | Computational element that gives access to information about or actuation capabilities on a Physical Entity (IoT-A, 2011). |
| 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 (Project Management Institute, 2013) |
| 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 (Gavras, 2010) |
| 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 (Gavras, 2010) |
| Interoperability | The ability of two or more systems or components to exchange information and use the information that has been exchanged (IEEE, 1990) |
| 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 (MyFIRE, 2011) |
| 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 (Soukhanov, Ellis, & Severynse, 1992) |
| 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 |
| Virtual Entity | Computational or data element representing a Physical Entity. Virtual Entities can be either Active or Passive Digital Entities (IoT-A, 2013). |

 

## 1.5 Executive Summary

This deliverable analyzes the requirements and specifications identified as results of other tasks under the same work package. These inputs give us a clear reference against which we are going to certify the conformance of the participant testbeds.

In particular, this deliverable consists of an analysis of all the collected requirements and specifications on a FIESTA-compatible testbed, in order to define what a "FIESTA certified testbed" is and the certification process

# 2 INTRODUCTION

## 2.1 Background and Scope

A certification process refers typically to the validation and confirmation that a person, organization or infrastructure possesses certain characteristics. Beyond very common certifications of knowledge, competencies or professional capacities for people and organizations, when it comes to ICT infrastructures there are certifications of compliance to technical standards and capabilities. As a prominent example, cyber-security infrastructures are nowadays certified in terms of their compliance to the proliferating ISO/IEC 27000 family of standards for information security management systems (ISMS). Organizations such as ISO and ETSI provide the technical standards and processes that can drive similar certification processes. A main reason for this is that certifications are in several cases linked to standards.

There are also certification processes relating to two key concepts of the FIESTA project, namely experimental infrastructures and interoperability. Indeed, there are for example standards relating to the measurement aspects and quality of experimental infrastructures, such as the ISO 3534-1:2006, which defines general statistical terms and terms that can be used for auditing the measurement capabilities of experimental infrastructures. Likewise, several organizations deal with the certification of interoperability functionalities, in order to enable and validate the integration or interworking of heterogeneous systems and devices. A characteristics example is the certification of TETRA interoperability[1] features by the TETRA association.

In the area of IoT, the issue of interoperability is very high in the agenda of IoT evolution (Gyrard 2015). Recently we are witnessing both research and enterprise initiatives for IoT interoperability. For example, several of the ontologies that are surveyed in the scope of WP3 of the project represent efforts to define schemas for syntactic and semantic interoperability across IoT applications. Likewise, enterprises are defining techniques for the interoperable discovery and use of IoT resources (a prominent example being HyperCat[2]). Nevertheless, up to date there have been no systematic efforts to audit IoT infrastructures against such standards and initiatives (Serrano 2015). One of the main objectives of FIESTA is to define a certification process and relevant tools enabling stakeholders to assess the interoperability characteristics of an IoT platform, such as interoperability with market standards, interoperability with technologies identified in FIESTA, data interoperability at semantical level, etc. Due to its FIRE nature, FIESTA is focusing on IoT experimental

[1] http://www.tandcca.com/interop/page/12611

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

 

infrastructures (testbed), yet its methodology and tools could also serve as a basis for certifying the interoperability characteristics of a wider class of IoT platforms, such as smart city platforms (Schiele 2014).

## 2.2 Motivation

One of the big challenges in IoT today is the integration of the very heterogeneous data generated by diverse resources, as well as the combination and use of services stemming from different IoT systems (Barnaghi 2012). One of the main goals of FIESTA is to enable European experimenters/researchers to design, implement, execute and evaluate IoT experiments based on data from various IoT testbeds all over Europe, which were initially designed for different purposes and in different ways. To this end, FIESTA aims to provide a wide range of facilities for interconnecting and interoperating testbeds using semantic methods and tools, in order to achieve the Experiment-as-a-Service (EaaS) paradigm.

### 2.2.1 Federation of testbeds

The testbed federation is one approach to achieve the EaaS paradigm. Federation is understood to be: “an organization within which smaller divisions have some internal autonomy”[3]. In the context of the Internet of Things and testbeds, a federation considers that each testbed operates both individually and as part of a larger federation in order to gain value including:

- Expansion of the scope of applications/experiments that will be designed on the federation of diverse testbeds which are not possible with one single testbed.
- Possibility for large scale experiments.
- Attraction for experimenters to use.

The greater the number of testbeds federated, the richer experiments can be run on the federation in terms of scope, scale and available resources, and more attractive the federation is (Serrano 2015b). Therefore third parties are called to be involved in the project. The objective of the involvement of third-parties (c.f. section 3.1.2) will be two-fold:

- To ensure the design and integration (within FIESTA) of more innovative experiments, through the involvement of additional partners in the project (including SMEs). The additional experiments will focus on demonstrating the added-value functionalities of the FIESTA experimental infrastructure.
- To expand the FIESTA experimental infrastructure on the basis of additional testbeds. In this case the new partners will undertake to contribute additional testbeds and to demonstrate their blending and interoperability with other testbeds (already adapted to FIESTA).

[3] OED, *federation n.* OED Online. March 2014. Oxford University Press. http://www.oed.com/view/Entry/68930?redirectedFrom=federation. Access on (March 28, 2014).

 

### 2.2.2 Certification and global market confidence program

Certification refers to a process that validates the compliance of certain characteristics of an object, person, or organization to a reference[4]. This compliance checking is often, but not always, provided by some form of external review, education, assessment, or audit.

In the framework of FIESTA, as the third-party testbeds are crucial to promote the federation, they need to certify their conformance to the federation specifications before being a member of the federation.

The project's global market confidence program focuses on providing a range of certification and compliance tools, aiming at auditing and ensuring the openness and interoperability of IoT platforms and technologies, including the project-scope certification process. From this program, different stakeholders in the project may have benefits:

- For the FIESTA consortium, the project's market confidence programme 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. Such guarantees are expected to be extremely useful for third-parties that will join the project as part of the FIESTA open calls.
- For testbed providers, the programme will ensure that their testbed will gain a better and wider visibility and that it will be used more extensively by applications and users, as the testbed will be capable of becoming federated with other testbeds in order to provide more interesting experiments with the same user experience, and to get the usage of other tools used within and outside FIESTA (i.e. HyperCat).For end user (experimenters), the programme will guarantee that the testbed under question is compatible with the federation that they can follow the same guideline/best practice provided by the federation to design/conduct experimentations. No or little cost of re-learning. They can enrich their experiments when new experiment capabilities are brought by new third-party testbed. As already outlined, this will directly benefit end-users participating in the FIESTA open calls project.

## 2.3 Objectives

The global market confidence and certification specifications which are the results of this deliverable will be used in WP 6 to design the global market confidence program. To give WP6 a good start point, the present document needs to:

- Define what is a certified testbed in terms IoT semantic interoperability.
- Define the needed requirements for certification.
- Define the methodology and tools of certification.
- Provide an initial tool, enabling testbed owners and end-users (experimenters) to understand the certification requirements and criteria.

These testbed related schemes will be transferred to WP6 which will adapt it to real cases of IoT deployments.

[4] Wikipedia, https://en.wikipedia.org/wiki/Certification

 

The FIESTA certification framework will belong among the exploitable assets of the project, since it will provide tools enabling IoT testbed owners and IoT system integrators to assess the interoperability features and capabilities of their systems as a means to improving them and guaranteeing their sustainability, technological longevity and wider use.

# 3 CERTIFICATION FRAMEWORK

## 3.1 Scope

### 3.1.1 Within FIESTA project

In the current project, four (4) testbeds are selected as initial participants, which help define a “FIESTA-compliant” testbed from their own requirements and specifications. They 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. Thus, these four (4) testbeds are the first targets to be certified for the conformance with specifications defined in this deliverable.

### 3.1.2 Beyond FIESTA project

Furthermore, the main target testbeds to be certified are the third-parties which want to be integrated into the federation, for example those who participate the open calls. In order to guarantee the service level of the federation, the individual testbeds need to be certified before to be federated, to make sure that they are conform to the certification specifications.

## 3.2 Certification Framework Stakeholders

- The FIESTA certification framework is primarily addressed to stakeholders of the IoT experimentation process, including providers of IoT experimental facilities, integrators of IoT experiments and experimenters (i.e. end-users) of the FIESTA federated experimental infrastructures. In particular: **IoT Infrastructure Providers and Testbed Owners**. As indicated by the name, they provide the test environment, including necessary services enablers, like resource discovery service enabler, technological enablers, like experimentation device connectivity enablers. They 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**. 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. Some experimentations need the participation of other people, which are the end users. 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.

- **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.

Figure 3 shows the interactions between the 3 identified stakeholders.

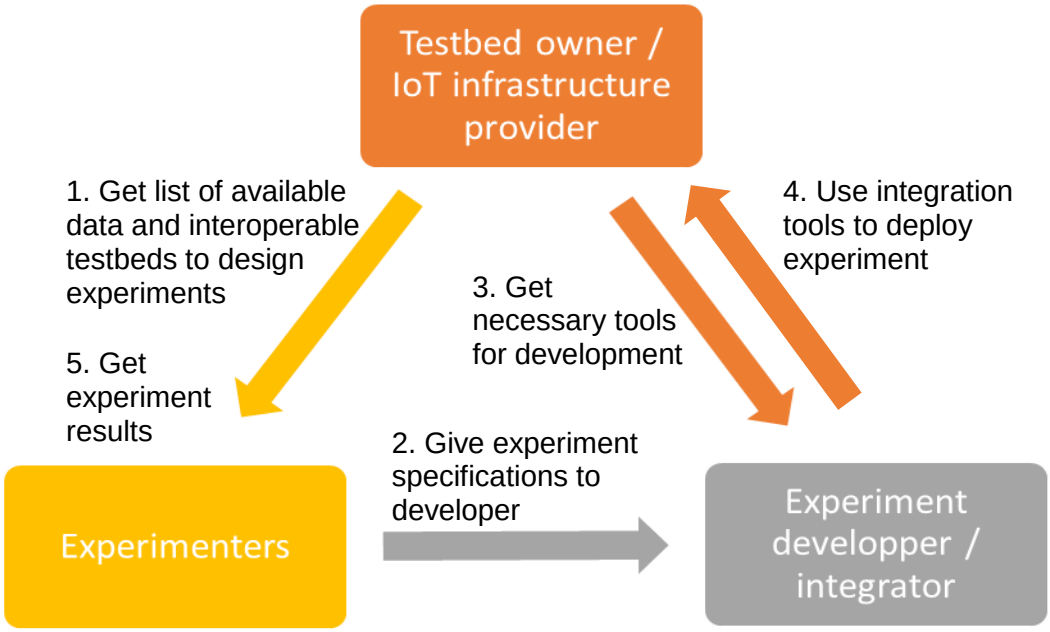


**Figure 3 Interactions between stakeholders**

As already outlined, as part of WP6 and the project's exploitation phase, the partners will attempt to expand the scope and applicability of the certification suite in order to address the broader set of IoT platform, IoT application integrators and end-users of IoT applications. This expansion will enable the applicability and use of the framework in the scope of the proliferating number of IoT applications and infrastructures, beyond experimental use. As part of such expansion, the role of IoT infrastructure providers will include the full range of IoT platform/system providers, while the experiments' integrator role will be enhanced in order to include the broader range of IoT solutions integrators. Finally, the expanded certification framework will address end-users of interoperable IoT applications rather than experimenters only.

## 3.3 Structure of the Certification Framework

The certification framework will be specified in terms of the following 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 (or platform) will be expressed not only in terms of its interoperability score, but also in terms of its classification to an interoperability class (e.g., A, B, C, D or platinum, gold, silver, bronze) signifying its interoperability level (e.g., excellent, very good, good, acceptable). 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. Note that the overall interoperability assessment of a testbed (or platform) will not be limited to an interoperability class and an accompanying score. Rather it will also provide an assessment of the lacking features.

**Table 3 Indicative Interoperability Classification**

| Interoperability Class | Score (0-100) (example) | Explanation |
|---|---|---|
| "Platinum" (A) | S≥90 | Excellent interoperability, exceeding the set of criteria. The testbed can directly be used in IoT applications in conjunction with other platforms and maximum likelihood to achieve interoperability. |
| "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 the use of the testbed in interoperable applications |
| Fail (E) | 60>S | The testbed has serious interoperability weaknesses and fails to meet essential interoperability requirements. |

## 3.4 Certification Aspects and Requirements

In this section, we take the general requirements which are described in D2.1[5] and try to map them into the four (4) following themes:

- **Data models**. It consists of the requirements for achieving interoperability by establishing and using semantic model for data in the federation.

[5] D2.1 « Stakeholder Requirements », FIESTA-IoT H2020 Grant agreement N° , 2015

 

- **Interfaces and services**. It consists of the requirements for available services and interfaces which should be provided by the federation and each testbeds.
- **Security**. It consists of the requirements on the security aspects that the testbeds and the federation should implement.
- **Quality Auditing Aspects**. It consists of the requirements on the evaluation of the testbeds.

As already outlined, while FIESTA will primarily focus on the interoperability of IoT experimental infrastructures (testbeds), yet its certification framework will be directly expandable to a wider class of IoT platforms (beyond experimentation). This will be evident in WP6, where the certification framework will be substantiated and used not only for IoT testbeds certification, but also for third-party IoT platforms.

### 3.4.1 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. Hence, testbeds supporting mainstream format and standards for their APIs will score higher in terms of interoperability comparing to those that do not offer such APIs.
- **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. In the scope of FIESTA, semantic interoperability will be ensured based on compliance to the ontologies that are under specification in WP3 of the project. The interoperability score of a testbed will be defined on the basis of the number and type of supported data models and ontologies. Full compliance to the FIESTA ontologies should yield the highest semantic interoperability scoring. Different scales may be however applied when considering the certification framework outside the scope of the FIESTA project: The more standards-based models and ontologies supported, the highest the score.

**Table 4 Interoperability certification aspect**

| Id | Indicator | Related requirement | Description |
|---|---|---|---|
| INT-01 | Syntactic interoperability | 54_NFR_INT_Interop_between_fiesta_testbeds | Mainstream format and standards APIs supported by testbed |
| INT-02 | Semantic Interoperability | 72_NFR_SEM_Semantic_annotations_data<br>73_NFR_SEM_Mapping_semantic_model | Data model and ontologies defined in Fiesta should be used to the testbed data |

While both syntactic and semantic interoperability are crucial for building data intensive interoperable IoT applications, the semantic interoperability aspect is relatively more important when compared to syntactic interoperability. This is mainly

 

due to the fact that most IoT platforms and system support already APIs, while support for semantic data models is much less frequent.

4 maps the 2 above interoperability aspect indicators to the requirements from D2.1[5].

### 3.4.2 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”. In the scope of the FIESTA project compliance boils down to supporting the testbed interfaces to be specified in WP4. However, the certification framework will specify a wider list of standards-based APIs (such as OCCI), which if supported would increase the interoperability capabilities of the testbed.

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).

#### *3.4.2.1Access Interfaces*

To facilitate the FIESTA platform access across multiple testbeds some of the most known IoT and/or proprietary interfaces are going to be utilized and mapped to the FIESTA data structure. Some of these access interfaces are:

- **SPARQL interface**[6]: 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**[7] : Next Generation Services Interface is a RESTful API via HTTP. Its purpose is to exchange context information. The three main interaction types are
    - one-time queries for context information
    - subscriptions for context information updates (and the corresponding notifications)
    - unsolicited updates (invoked by context providers)
- **OCCI**[8]: Open Cloud Computing Interface is a Protocol and API for Management tasks. OCCI is a flexible API with a strong focus on integration, portability, interoperability and innovation while still offering a high degree of extensibility. It can serve models in addition to IaaS, including e.g. PaaS and SaaS.

[6] http://www.w3.org/TR/rdf-sparql-protocol/

[7]http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/ngsi-v1-0

[8] http://occi-wg.org/

 

- **IoT-A Virtual Entity[9] end point**: virtual entities[10] representing physical entities can be discovered
- **Relational DB end point**: is an endpoint for accessing the relational database of the testbed if available.
- **Document DB end point**: is an endpoint for accessing the document database of the testbed if available.

#### *3.4.2.2IoT 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**: this service will enable the experimenter, based on an agreed access policy, to control a sensor/actuator by exposing its control interface.

Table 5 summarizes the indicators derived from Section 3.4.2.

**Table 5 Access Interface certification aspect**

| Id | Indicator | Related requirement | Description |
|---|---|---|---|
| INT-03 | Access interfaces | 06_FR_ACC_Querying_data_compositions<br>24_NFR_ACC_Tools_planning_auto_tasks<br>45_NFR_PLA_Orchestration_of_resources | Testbed should support at least one standard API in the list of several most-known interfaces |
| INT-04 | IoT services | 02_FR_ACC_Resources_available<br>04_FR_ACC_Discover_info_independent_testbed<br>05_FR_ACC_Dynamic_discovery_resources<br>13_FR_ACC_Expose_testbed_actuation_capabilities | Resource discovery, direct access to sensor data and actuation should be supported by the testbed through IoT services |

### 3.4.3 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. A fully interoperable testbed (syntactically and semantically) at both the data and interface/service levels still cannot operate within the FIESTA federation without

[9] http://www.iot-a.eu/public/terminology

[10] http://www.meet-iot.eu/deliverables-IOTA/D4_3.pdf

 

considering conformance with the security architecture and requirements (and indeed other non-functional properties). The following list describes the key requirements that a testbed must comply with:

- **Secure encrypted communication channel** between all testbed interfaces and FIESTA. The testbed must implement fully secure interface endpoints. That is all communication from FIESTA and to FIESTA is encrypted. To achieve this 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 in order to initiate the secure and trusted channels.
- **Authentication**. The testbed must trust FIESTA to identify and authenticate experimenters on its behalf. A request received by a FIESTA member is deemed to be authentic (n.b. FIESTA is authenticated in the previous step).
- **Identity Management (optional)**. A testbed may wish to determine who is using what features of the testbed, e.g. for accounting purposes. In order to interoperate with the FIESTA identify management services, the 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 may trust FIESTA to authorize users on its behalf. The testbed must then provide FIESTA a set of access policies for its resources. These policies are described in the UMA[11] specification. They can be entered manually via the FIESTA management portal; or they can be programmatic where the testbed complies with the UMA APIs and protocols.
- **Testbed-based Access Control (optional).** A testbed can choose to perform local access control decisions and enforcement. For this its interface endpoints must be able to read HTTP messages and extract the authorization token from the message and then utilise the OpenID Connect APIS as described previously. FIESTA recommends deploying a UMA access control compliant software to perform the policy decision based on UMA policies. However, the testbed is free to choose the software (There is no further compliance after the request has been received).

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.

Table 6 summarizes the above security aspect indicators that should be verified if a testbed wants to join FIESTA, with the related requirements extracted from D2.1[5].

**Table 6 Security certification aspect**

| Id | Indicator | Related requirement | Description |
|---|---|---|---|
| SEC-01 | Secure encrypted communication channel | 18_FR_SEC_Testbed_authentication_mechanisms | All communication from FIESTA and to FIESTA is encrypted |

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

 

| | | | |
|---|---|---|---|
| SEC-02 | Testbed authentication | 18_FR_SEC_Testbed_authentication_mechanisms<br>20_FR_SEC_Experimenter_single-sign-on | FIESTA authenticates experimenters on the behalf of testbed |
| SEC-03 | Identity Management (option) | 18_FR_SEC_Testbed_authentication_mechanisms<br>20_FR_SEC_Experimenter_single-sign-on | Testbed interoperate with FIESTA with OpenID-Connect and OAUTH protocol to use FIESTA's identity management API |
| SEC-04 | Authorization | 19_FR_SEC_Testbed_manage_privil edges<br>21_FR_SEC_Tool_manage_users<br>69_NFR_SEC_Verify_authorise_user_actions | Testbed trusts FIESTA to authorize users on its behalf |
| SEC-05 | Testbed-based Access Control (optional) | 19_FR_SEC_Testbed_manage_privil edges | Testbed can perform local access control on FIESTA requests |

### 3.4.4 Quality Auditing Aspects

Quality expectations depend on the evaluated subject. As clarified at the beginning of the document; the general objective of this task is to define what a "FIESTA certified testbed" is and the certification process, the target of evaluation in the scope of this section is the testbeds.

Testbeds aim to provide better services to attract experimenters to run experiments on it. In a given testbed, most important impacts on the quality of service are the technological and service enablers that experimenters and developers use directly to implement the experiments.

#### *3.4.4.1Quality of Service*

Quality of Service (QoS) aims at evaluating the end to end service delivery quality and correlating it with the users' quality of experience.

Note: QoS is not about what function or what capability is provided by the service, but is about at what level of satisfaction this service is brought out to the users, good, medium or poor[12].

In Table 7, we take the requirements from D2.1[5] related to QoS to identify necessary indicators for the certification framework. Some requirements target the FIESTA platform not the testbeds, however, we estimate that in order to achieve some quality for the federation platform, each component, including the federated testbeds, should also achieve the requested quality.

**Table 7 Quality auditing certification aspect**

| Id | Indicator | Related requirement | Description |
|---|---|---|---|

[12] D4.2 «Evaluation framework», FESTIVAL H2020 Grant agreement N° 643275, 2015, http://www.festival-project.eu/wp-content/uploads/2015/10/FESTIVAL-D4.2-Evaluation-Framework-v1.0.pdf

 

| | | | |
|---|---|---|---|
| QoS-01 | Response time | 28_NFR_ACC_Response_delay_controlled | Response delay should be controlled in a tolerated interval |
| QoS-02 | Processing time | 41_NFR_PLA_Minimise_processing_delay | Request from experiment should be processed as quick as possible |
| QoS-03 | Computational assets | 43_NFR_PLA_Optimise_computational_assets | Resources for computing should be optimized |
| QoS-04 | Service prioritization | 44_NFR_PLA_Prioritization_of_services | If testbed provides several services, it should support the execution of services with different priorities |
| QoS-05 | Reliability | 51_NFR_PLA_FIESTA_highly_reliable | Testbed should be enough reliable |

#### *3.4.4.2Best Practices & Blueprints*

Best practice is a guide for platform/framework users, in the present case the developers using the testbed, 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.

Table 8 shows the identified indicators mapped to the requirements from D2.1[5] related to this topic.

**Table 8 Best practice certification aspect**

| Id | Indicator | Related requirement | Description |
|---|---|---|---|
| BP-01 | Documentation | 30_NFR_ACC_FIESTA_well_documented | Documentation should be available to users |
| BP-02 | Description interface | 31_NFR_ACC_Describe_IoT_services_and_applications | High-level interface aiding users to describe applications and services |
| BP-03 | Tools | 32_NFR_ACC_Provide_dev_deploy_manag_config_tools | Development, deployment and management tools should be available for users |

## 3.5 Certification methodology

### 3.5.1 Questionnaires/scorecard

One of the main interoperability certification tools of the project will be provided in the form of a scorecard. The scorecard will provide the means of realizing the interoperability classification listed in **Error! Reference source not found.**. It will comprise a set of questions that will be linked to interoperability criteria and features (such as supported data models and security functionalities), notably the criteria outlined in earlier paragraphs. Note that the scorecard will be typically used by testbed owners and/or IoT solution providers prior to engaging to any development or deployment tasks that involves the interfacing or interconnection of multiple IoT

 

testbeds. For example, in the scope of FIESTA experimentation, testbed owners can use the scorecard in order to assess the feasibility and the effort required to interconnect their testbed with the FIESTA infrastructure. As another example, a provider of IoT solutions can use the scorecard in order to assess the effort needed to interconnect two different IoT infrastructures for the purpose of data analysis or data-intensive experimentation.

The inputs and outputs of the scorecard are envisaged to be as follows:

- **Inputs**: Scorecard user, which can be testbed owner, FIESTA platform, experimenter, etc. as defined in **Error! Reference source not found.** in "target user" column, responses to a set of questions that are related to interoperability features. Based on each question, the user will have the opportunity to provide information on whether and at what extend a testbed supports some interoperability feature. Interoperability features (and associated questions) will be clustered in categories (e.g., data models, interfaces, security), based on the classification of interoperability features that have been presented in earlier paragraphs.
- **Output**: Based on the responses to the various questions, the scorecard will compute, compile and provide as output:
    - The classification of the testbed, in terms of their interoperability characteristics (Table 3).
    - An interoperability score, which will be used as a metric for comparing different testbeds in terms of their interoperability capabilities. The score will be indicative of the effort required to customize the testbed in order to become interoperable with other IoT infrastructures.
    - A set of comments, which will accompany and illustrate the assessment. These comments could be taken into account by users wishing to use the testbed in interoperability scenarios or even development applications that ask for interoperability characteristics.

The scorecard will be primarily administered to testbed owners, who will be able to complete in order to assess their IoT infrastructure in terms of interoperability. Beyond testbed owners and administrators, the scorecard will be a very useful utility for interoperability consultants and solution integrators. Specifically, the users of the scorecard will be:

- **Testbed Owners/administrators**: Testbed owners will be using the scorecard in order to assess the interoperability characteristics and capabilities of their IoT infrastructure. Based on the assessment they will be also able to derive comments about weaknesses and limitations, along with information towards remedying them.
- **Interoperability Consultants**: Interoperability consultants are likely to use the scorecard in order to assess the suitability of a given infrastructure for the implementation of applications and services that involve data and services stemming from multiple heterogeneous IoT infrastructures. As already outlined, the scorecard will also provide insights regarding the required effort and steps. The role of interoperability consultant can be seen as a new stakeholder role, which will be substantiated in the scope of the FIESTA testbed certification process in WP6. We expect such consultants to perform

 

interoperability assessments on behalf of testbed owners and/or IoT solution providers engaging in the integration of diverse testbeds.

- **Integrators of IoT solutions**: IoT solution integrators are expected to use the scorecard in order to assess the effort needed to integrate a given IoT infrastructure as part of interoperability scenarios, notably scenarios involving data and services from multiple testbeds.

### 3.5.2 Technical tools

Technical tools are made to give objective evaluations on given topics.

- **Online tools** (Gyrard 2015). These are light-weight tools for general purpose, for example, to validate an RDF file against the RDF syntax. These tools are generally not designed for a specific target (e.g. a given ontology, a given testbed) and are used for a preliminary offline validation before the target being integrated into the running system or federation (e.g. the fact that the ontology of testbed A is validated by the online tool against the testbed federation ontology does not necessarily mean all its datasets are annotated by this ontology). Some examples of online tools are:
  - **RDF validator**[13] for checking the syntactical correctness of an RDF document;
  - **HyperThing**[14] for checking validity of URIs and the resource type behind the URIs themselves (a document or a thing);
  - **OOPS**[15] for checking common ontology pitfalls which are defined in several recommended ontology development guidelines;
  - **SSN validator**[16] for checking conformance of ontologies against a reference ontology.
- **Monitoring/control tools**. These tools are mostly developed with the given testbeds to provide testbed runtime monitoring data and the possible control commands. They are mostly testbed specific, but can provide APIs for third party applications to get data and send authorized commands with configurable parameters. In the current certification framework, these tools will be used for quality auditing aspect certification.
- **Test suites**. A test suite is a collection of test cases to validate a system according to specified behaviors. They are developed for specific purpose and contain structured and detailed instructions, steps and goals for the test cases. In the current certification framework, test cases can cover the above certification topics, and other potential topics including some testbed specific ones.
- **Security aspect related tools**. Available tools can be applied to ensure that a testbed complies with the security requirements of FIESTA. For example,

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

[14] http://hyperthing.org

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

[16] http://iot3.ee.surrey.ac.uk/SSNValidation/

 

Interoperability testing tool to check if HTTPS is in place to ensure the encrypted communication channel, and compliance testing tool to check if the exposed endpoint of a testbed compliant with OAUTH which means the identity manager is in place. In project OWASP[17], a list of available security testing tools are identified for various security aspects in the released Testing Guide[18].

## 3.6 Definition of indicator in scorecard

Certification aspect evaluation indicators which have been identified in the previous section are summarized in Table 9 with more information:

- Id: the id number assigned to each indicator in previous tables
- Indicator: the name of the indicator, identical as assigned in previous tables
- Description: a short description of the indicator
- Target user: who should provide the evaluation of the current indicator
- Criteria/score range: the evaluation criteria, or a score range if the evaluation requires a rating from the user
- Score: the result of evaluation according to the criteria/score range

**Table 9 Indicators for testbed certification**

| Id | Indicator | Description | Target user | Criteria/score | Score |
|---|---|---|---|---|---|

[17] https://www.owasp.org/index.php/Main_Page

[18] https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

 

| | | | | **range** | |
|---|---|---|---|---|---|
| INT-01 | Syntactic interoperability | Mainstream format and standards APIs supported by testbed | Testbed provider | If common data format and APIs supported | Yes/No |
| INT-02 | Semantic Interoperability | Data model and ontologies defined in Fiesta should be used to the testbed data | Testbed provider | If ontologies and data model used | Yes/No |
| INT-03 | Access interfaces | Testbed should support at least one standard API in the list of several most-known interfaces | Testbed provider | If standard APIs supported | Yes/No |
| INT-04 | IoT services | Resource discovery, direct access to sensor data and actuation should be supported by the testbed through IoT services | Testbed provider | If these services supported | Yes/No |
| SEC-01 | Secure encrypted communication channel | All communication from FIESTA and to FIESTA is encrypted | Testbed provider, FIESTA platform | If applied | Yes/No |
| SEC-02 | Testbed authentication | FIESTA authenticates experimenters on the behalf of testbed | Testbed provider | If applied | Yes/No |
| SEC-03 | Identity Management (option) | Testbed interoperate with FIESTA with OpenID-Connect and OAUTH | Testbed provider, FIESTA platform | If supported | Yes/No |
| SEC-04 | Authorization | Testbed trusts FIESTA to authorize users on its behalf | Testbed provider | If applied | Yes/No |

 

| | | | | | |
|---|---|---|---|---|---|
| SEC-05 | Testbed-based Access Control (optional) | Testbed can perform local access control on FIESTA requests | Testbed provider | If available | Yes/No |
| QoS-01 | Response time | Response delay should be controlled in a tolerated interval | experimenters | Max delay | Respect or not the max delay |
| QoS-02 | Processing time | Request from experiment should be processed as quick as possible | experimenters | Max processing time | Respect or not the max processing time |
| QoS-03 | Computational assets | Resources for computing should be optimized | Testbed provider | Optimization score (1 to 10) | |
| QoS-04 | Service prioritization | If testbed provides several services, it should support the execution of services with different priorities | Testbed provider | If supported | Yes/no |
| QoS-05 | Reliability | Testbed should be enough reliable | Testbed provider | Percentage of reliability | To be specified (ex. 90%) |
| BP-01 | Documentation | Documentation should be available to users | experimenters | Users' satisfaction of the usefulness of provided documentation | To be specified (ex. 90% of users think the documentation is useful and enough ) |
| BP-02 | Description interface | High-level interface aiding users to describe applications and services | experimenters | If available | Yes/no |
| BP-03 | Tools | Development, deployment and management tools should be available for users | experimenters | Users' satisfaction of the usefulness of provided tools | To be specified (ex. 90% of users think the tools are useful and enough ) |

 

## 3.7 Online self-assessment ScoreCard

Based on the items presented in the previous sections we have generated a mock-up scorecard (Table 10) in an Excel file that will provide a score to the testbed owner based on the features that is capable to provide. The self-assessment scorecard is divided into five main categories:

- Data Models: which includes the items that are related to data storage, data formatting and data retrieval.
- Interfaces and Services: which is includes the items related with the offered interfaces with data consuming clients of the testbed
- Security: which includes the security related features that are offered from a testbed
- Quality Auditing Aspects: which includes the items related to the quality of services provided from a testbed.
- Generic: which includes whatever is not related with the above categories.

**Table 10 FIESTA 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 |
| Proprietery 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 an OMA Next Generation Services Interface (NGSI) |
| OCCI Interface | Does the Testbed offer an Open Cloud Computing Interface (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) |
| Addittional DB | Can the testbed replicate/annotate its current data to the FIESTA format in a local Database |

Taking in consideration the categories and items provided in Table 10 above we have generated an Excel file (XLSM) based scorecard which is depicted in Figure 4 below.

 

| Testbed/FIESTA Interoperability | | | Overall Score: | 0,0% | |
|---|---|---|---|---|---|
| # | Check Items (double click topics to expand / collapse) | Descriptions | Yes (double click to | Partially (double click to | No (double click to |
| 1.2 | FIESTA Ontology | Does the testbed supports the FIESTA ontology | ☐ | ☐ | ☐ |
| 1.3 | SensorML | Does the testbed supports SensorML language to represent the sensor | ☐ | ☐ | ☐ |
| 1.4 | SWE | Does the testbed supports Sensor Web Enablement (SWE) language to represent the sensor data | ☐ | ☐ | ☐ |
| 1.5 | Proprietery Format | Does the testbed supports a proprietary language to represent the sensor | ☐ | ☐ | ☐ |
| 1.6 | Data Extraction | Does the testbed provides the ability to extractr data in a document format (i.e. CSV, Excel, XML, RDF, JSON, etch) | ☐ | ☐ | ☐ |
| 1.7 | Graph Database | Does the testbed store its data in a Graph Database | ☐ | ☐ | ☐ |
| 1.8 | Document Database | Does the testbed store its data in a Document Database | ☐ | ☐ | ☐ |
| 1.9 | Relational Database | Does the testbed store its data in a Relational Database | ☐ | ☐ | ☐ |
| 2 | Interfaces and Services | | ☐ | ☐ | ☐ |
| 2.1 | SPARQL End Point | Does the Testbed offer a SPARQL (Graph DB) endpoint | ☐ | ☐ | ☐ |
| 2.2 | NGSI Interface | Does the Testbed offer an OMA Next Generation Services Interface | ☐ | ☐ | ☐ |
| 2.3 | OCCI Interface | Does the Testbed offer an Open Cloud Computing Interface | ☐ | ☐ | ☐ |
| 2.4 | Virtual Entity Endpoint | Does the Testbed offer an Virtual Entity end point | ☐ | ☐ | ☐ |
| 2.5 | Relational Database End Point | Does the Testbed offer a Relational DB endpoint | ☐ | ☐ | ☐ |
| 2.6 | Document DB Endpoint | Does the Testbed offer a document DB endpoint | ☐ | ☐ | ☐ |
| 2.7 | IoT Services End Point | Resource Discovery | ☐ | ☐ | ☐ |
| | | Direct access to sensors thru services | ☐ | ☐ | ☐ |
| | | Actuation thru offered services | ☐ | ☐ | ☐ |
| 3 | Security | | ☐ | ☐ | ☐ |
| 3.1 | Data Encryption | Offer secure encrypted communication channel between all testbed interfaces and FIESTA | ☐ | ☐ | ☐ |
| 3.2 | Authentication | Can trust FIESTA to identify and authenticate experimenters on its behalf | ☐ | ☐ | ☐ |
| 3.3 | Identity Management | determine who is using what features of the testbed | ☐ | ☐ | ☐ |
| 3.4 | Authorization | Is the testbed able to specify access rights to specific resources | ☐ | ☐ | ☐ |
| 3.5 | Testbed-based Access Control | Can the testbed choose to perform local access control decisions and enforcement. | ☐ | ☐ | ☐ |
| 4 | Quality Auditing Aspects | | ☐ | ☐ | ☐ |
| 4.1 | Response time | Do you control or set a threshold before which your testbed must give a response to the received request? | ☐ | ☐ | ☐ |
| 4.2 | Processing time | Do you control or set a threshold before which your testbed must finish | ☐ | ☐ | ☐ |
| 4.3 | Computational assets | Does your testbed implement any resource optimizing mechanism? | ☐ | ☐ | ☐ |
| 4.4 | Service prioritization | Does the Testbed support the execution of services with different | ☐ | ☐ | ☐ |
| 4.5 | Reliability | Do you define a ratio of failure time/working time that the testbed must respect? | ☐ | ☐ | ☐ |
| 5 | Generic | | ☐ | ☐ | ☐ |
| 5.1 | Documentation | Does the Testbed provide Documentation | ☐ | ☐ | ☐ |
| 5.2 | Tools | Does the testbed provide development, deployment and management | ☐ | ☐ | ☐ |
| 5.3 | Adaptors | Can the Testbed offer the abbility to run third party software (i.e. FIESTA | ☐ | ☐ | ☐ |
| 5.4 | Addittional DB | Can the testbed replicate/anotate it's current data to the FIESTA format in | ☐ | ☐ | ☐ |

**Figure 4 FIESTA mock-up Scorecard**

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 (upper right) of the testbed/FIESTA Interoperability. The items will have different weights that could be configurable by the scorecard owner, which will be based on FIESTA consortium experience, and will contribute in the overall score. Different levels of interoperability with the FIESTA platform will be defined and will be mapped with specific score level. We also investigate the generation of an automated report with a results/advice guide on what a testbed could easily further support or what needs to be done for it to be interoperable with the FIESTA platform. An example of a filled up scorecard with the relevant mock-up result/advice guide is provided below.

In this example, the weight attributed to each item is as follows: “Yes” gets 1.35, “Partially” gets 0.85 and “No” gets 0. A testbed owner fills the scorecard by ticking the item that suites the best for his testbed on every item. An overall score 66.5 is given when the scorecard is filled up and the advice/result guide is given according to specific items (i.e. “The testbed could choose to host the FIESTA annotated data locally” (in data models category in Table 11) ) is an advice given based on the “YES” answer of “Does the testbed store its data in a graph data base?”), 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”).

**Testbed/FIESTA Interoperability** — Overall Score: 66,5%

| # | Check Items (double click topics to expand / collapse) | Descriptions | Yes (double click to | Partially (double click to | No (double click to |
|---|---|---|---|---|---|
| 1 | **Data Models** | | ▣ | ▣ | ▣ |
| 1.1 | SSN Ontology | Does the testbed supports the SSN ontology | ☐ | ☑ | ☐ |
| 1.2 | FIESTA Ontology | Does the testbed supports the FIESTA ontology | ☐ | ☐ | ☑ |
| 1.3 | SensorML | Does the testbed supports SensorML language to represent the sensor | ☐ | ☐ | ☑ |
| 1.4 | SWE | Does the testbed supports Sensor Web Enablement (SWE) language to represent the sensor data | ☐ | ☐ | ☑ |
| 1.5 | Proprietery Format | Does the testbed supports a proprietary language to represent the sensor | ☐ | ☐ | ☑ |
| 1.6 | Data Extraction | Does the testbed provides the ability to extractr data in a document format (i.e. CSV, Excel, XML, RDF, JSON, etch) | ☐ | ☑ | ☐ |
| 1.7 | Graph Database | Does the testbed store its data in a Graph Database | ☑ | ☐ | ☐ |
| 1.8 | Document Database | Does the testbed store its data in a Document Database | ☐ | ☐ | ☑ |
| 1.9 | Relational Database | Does the testbed store its data in a Relational Database | ☐ | ☐ | ☑ |
| 2 | **Interfaces and Services** | | ▣ | ▣ | ▣ |
| 2.1 | SPARQL End Point | Does the Testbed offer a SPARQL (Graph DB) endpoint | ☑ | ☐ | ☐ |
| 2.2 | NGSI Interface | Does the Testbed offer an OMA Next Generation Services Interface | ☐ | ☑ | ☐ |
| 2.3 | OCCI Interface | Does the Testbed offer an Open Cloud Computing Interface | ☐ | ☐ | ☑ |
| 2.4 | Virtual Entity Endpoint | Does the Testbed offer an Virtual Entity end point | ☐ | ☐ | ☑ |
| 2.5 | Relational Database End Point | Does the Testbed offer a Relational DB endpoint | ☐ | ☐ | ☑ |
| 2.6 | Document DB Endpoint | Does the Testbed offer a document DB endpoint | ☐ | ☐ | ☑ |
| 2.7 | IoT Services End Point | Resource Discovery | ☑ | ☐ | ☐ |
| | | Direct access to sensors thru services | ☑ | ☐ | ☐ |
| | | Actuation thru offered services | ☑ | ☐ | ☐ |
| 3 | **Security** | | ▣ | ☐ | ▣ |
| 3.1 | Data Encryption | Offer secure encrypted communication channel between all testbed interfaces and FIESTA | ☑ | ☐ | ☐ |
| 3.2 | Authentication | Can trust FIESTA to identify and authenticate experimenters on its behalf | ☑ | ☐ | ☐ |
| 3.3 | Identity Management | determine who is using what features of the testbed | ☐ | ☐ | ☑ |
| 3.4 | Authorization | Is the testbed able to specify access rights to specific resources | ☑ | ☐ | ☐ |
| 3.5 | Testbed-based Access Control | Can the testbed choose to perform local access control decisions and enforcement. | ☐ | ☐ | ☑ |
| 4 | **Quality Auditing Aspects** | | ▣ | ▣ | ☐ |
| 4.1 | Response time | Do you control or set a threshold before which your testbed must give a response to the received request? | ☑ | ☐ | ☐ |
| 4.2 | Processing time | Do you control or set a threshold before which your testbed must finish | ☑ | ☐ | ☐ |
| 4.3 | Computational assets | Does your testbed implement any resource optimizing mechanism? | ☑ | ☐ | ☐ |
| 4.4 | Service prioritization | Does the Testbed support the execution of services with different | ☐ | ☑ | ☐ |
| 4.5 | Reliability | Do you define a ratio of failure time/working time that the testbed must respect? | ☐ | ☑ | ☐ |
| 5 | **Generic** | | ▣ | ▣ | ▣ |
| 5.1 | Documentation | Does the Testbed provide Documentation | ☐ | ☑ | ☐ |
| 5.2 | Tools | Does the testbed provide development, deployment and management | ☑ | ☐ | ☐ |
| 5.3 | Adaptors | Can the Testbed offer the abbility to run third party software (i.e. FIESTA | ☑ | ☐ | ☐ |
| 5.4 | Addittional DB | Can the testbed replicate/anotate it's current data to the FIESTA format in | ☐ | ☐ | ☑ |

**Figure 5 FIESTA Scorecard mock-up sample**

 

**Table 11 FIESTA Scorecard mock-up result/advice guide sample**

| **Data Models** |
|---|
| The testbed could adapt FIESTA ontology with some effort<br>The testbed could choose to host the FIESTA annotated data locally |
| **Interfaces and Services** |
| The testbed could be directly accessed from the current SPARQL endpoint<br>The testbed could utilize the FIESTA adaptors thru NGSI interface.<br>The testbed can provide direct access to sensors and actuators thru its own interfaces |
| **Security** |
| The testbed provides satisfactory level of security<br>The testbed can only provide complete access to one user type which will be controlled by FIESTA<br>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 provide better documentation to the end users<br>The testbed could offer FIESTA compliant database without the need of additional software |

# 4 REFERENCES

(Barnaghi 2012) P. Barnaghi, W. Wang, C. Henson, K. Taylor, "Semantics for the Internet of Things: early progress and back to the future", International Journal on Semantic Web and Information Systems (special issue on sensor networks, Internet of Things and smart devices), September 2012.

(Schiele 2014) Gregor Schiele, John Soldatos, Nathalie Mitton, “Moving Towards Interoperable Internet-of-Things Deployments in Smart Cities”, ERCIM News 2014(98) (2014).

(Serrano 2015a) Martín Serrano, Payam Barnaghi, Francois Carrez, Philippe Cousin, Ovidiu Vermesan (eds), “IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps” White Paper of the 4th Activity Chain of the EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS (IERC), March, 2015

(Serrano 2015b) Martin Serrano, John Soldatos, Philippe Cousin, Pedro Malo, “Internet of Things Experimentation: Linked-Data, Sensing-as-a-Service, Ecosystems and IoT Data Stores”, Building the Hyperconnected Society - Internet of Things Research and Innovation - Value Chains, Ecosystem and Markets, River Publishers Series in Communication 2015 (page. 261-277)

(Gyrard 2015) Amelie Gyrard, Martin Serrano, Ghislain Atemezing, “Semantic Web Methodologies, Best Practices and Ontology Engineering Applied to Internet of Things”, IEEE World Forum on Internet of Things (WF-IoT), Milan, Italy, December 14-16, 2015

 