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

Certification Suite V2

Document Id:	FIESTAIoT-WP6-D63-CertificationSuiteV2-171206-Draft
File Name:	FIESTAIoT-WP6-D63-CertificationSuiteV2-171206-Draft.docx
Document reference:	Deliverable 6.3
Version:	Draft
Editor:	Mengxuan Zhao
Organisation:	Easy Global Market
Date:	06 / 12 / 2017
Document type:	Other
Dissemination level:	PU

DOCUMENT HISTORY

Rev.	Author(s)	Organisation(s)	Date	Comments
V01	Mengxuan Zhao Franck Le Gall	EGM	2017/09/01	TOC proposal
V02	Paul Grace, Nikolay Stanchev	ITINNOV	2017/10/10	Interoperability Testing tool – new contributions and portal integration text.
V03	Mengxuan Zhao Paul Grace	EGM ITINNOV	2017/11/28	Finalization
V03	Tarek Elsaleh Tiago Teixeira	UNIS UNPARALLEL	2017/11/30	TR and QR
V04	Mengxuan Zhao	EGM	2017/12/06	Ready for submission
Draft	Elias Tragos	NUIG	2017/12/08	Draft ready for submission

TABLE OF CONTENTS

LIST OF FIGURES

TERMS AND ACRONYMS

API	Application Programming Interface
EaaS	Experimentation-as-a-Service
FIRE	Future Internet Research and Experimentation
IoT	Internet of Things
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
OWL	Ontology Web Language
RA	Reference Architecture
RDF	Resource Description Framework
REST	Representational State Transfer
SDK	Software Development Kit
TPS	Testbed Provider Services
UI	User Interface
URI	Uniform Resource Identifier
WP	Work Package

1 INTRODUCTION

To address the issues of lack of practical tools and guidance in achieving semantic interoperability, the FIESTA-IoT Global Market Confidence Program is proposed and developed. The certification suite is one important part of the program which provides testing and certification tools.

The certification suite comprises three main components: the web portal which allows users to access all the tools from one unique entry point; the Scorecard which allows users to perform a self-assessment on semantic interoperability readiness; and the tools which allow users to actually test their product against semantic interoperability requirements.

At the end of the second year of the FIESTA-IoT project, the certification suite had already a good shape and was ready to perform a complete certification process on in-house testbeds which are semantic data providers of FIESTA-IoT. Due to limited time and experience, only basic functionalities were implemented to provide a service baseline. Optional features and improvement that make the certification suite more complete and easier to use, have been carried out in this version 2, which is the target of the present document.

This document begins with a reminder of what have been done until the end of the second FIESTA-IoT year in terms of tools and facilities of the certification suite. The third section will present the updates on the certification suite compared to the previous section. In section four, the user guide for the certification process will be explained, followed by the best practices to get the testbed efficiently certified compiled from our own experience and the feedback from Open Call users.

2 THE CERTIFICATION SUITE AND TOOLS (REMINDER)

We proposed the FIESTA-IoT global market confidence program in our previous work in the WP 6. It aims at certifying and labelling the products or data not only in the scope of the FIESTA-IoT project, but also for the IoT market in general. The main objectives of the certification and labelling program are:

1. Assist **researchers and experimenters** to develop robust and interoperable software that underpins cross-technology IoT experimentation.
2. Assist **standard delegates** to promote interoperability best practice supported by standards.
3. Provide the **marketplace** with tools to check conformity to best practices and standards.

It consists of four services:

1. **Online testing and certification tools**. These are the tools that can be accessed through the certification web portal. Following an online certification workflow, the user will be guided to use all or part of the tools to get a certificate.
2. **Consulting**. This service consists of providing expertise to help those who wish to make their product pass the certification tests and get a certification.
3. **Training**. This service consists of helping clients to attain the competence for making their product compliant to a certain specification to get a certificate.
4. **Solution design**. This service is an extension of Consulting in case that the client requires a ready-to-use solution for interoperability.

2.1 The certification suite overview

The certification consists of the first service that we provide in the global market certification program: the online testing and certification tools. Users can use this online certification suite to:

1. Test the semantic interoperability of their product regarding to a certain specification or standard during the development of a product.
2. Certify their product. A certification can promote the visibility and confidence of a product; Hence the provider has the interest to get their product certified. The certification suite will guide the user to complete the certification process and get the certificate if all the criteria have been satisfied.

2.1.1 Components

This certification suite is composed of the following components:

1. **Certification web portal**. Online tools are integrated and accessible from the web portal. Related information about the certification suite, such as: the guide to the certification process, and links to useful documentation like FIESTA-IoT deliverables, are also available on the web portal.
2. **Scorecard**. This is a score providing the maturity level of a product under test. A user can use this scorecard to evaluate his product by answering the questions.

3. **Online tests**. Addition to the self-assessment using the Scorecard, a user can use the online tests provided as a web service to prove the product's interoperability regarding to the specifications that he/she claimed compliant. The result will add more credibility to the interoperability level of the product (because it is tested by a reputable 3rd party—namely FIESTA-IoT), thus it brings the product to an upper certification level.

2.1.2 Certification process

The workflow of the certification process is illustrated in Figure 1.

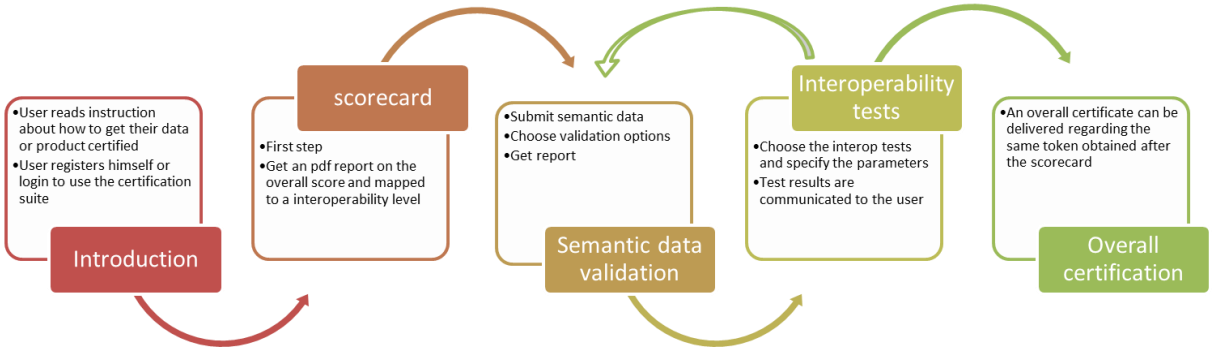

Figure 1 The Global Market Confidence Program certification workflow

1. The user should login or register him or herself on the certification suite in this step, to proceed the next steps.
2. The user is invited to fill in the self-assessment scorecard. A report is generated which contains the overall and per section scores, as well as the evaluated interoperability level of the product regarding the FIESTA-IoT Platform.
3. After the scorecard assessment, the user can choose to continue the certification process to achieve a higher certification level. At the end of each process, a report containing the testing result is generated.
4. After getting a report of the self-assessment scorecard, the user can choose to generate a certificate whenever he or she wants. The certificate contains the results of the scorecard and of the tests already performed.

2.2 Certification suite implementation V1

The first version of certification suite has been implemented and tested by the consortium partners. The objective of the intra-consortium test is to get feedback to improve the certification suite before launching it to the third-party users.

2.2.1 Access to the web portal

Users need to register an account to be able to use the portal. The FIESTA-IoT OpenAM credentials are not yet integrated to the certification portal (see Figure 2).

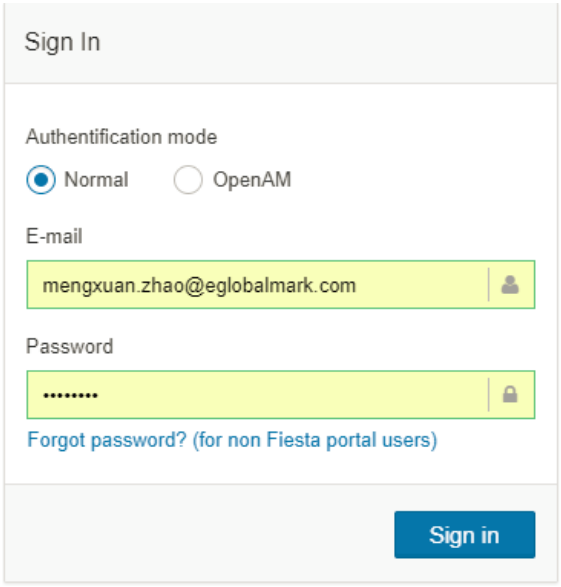

Figure 2 Authentication method using the account dedicated to the portal

2.2.2 Components implementation

The Scorecard and the ontology validation tests have been fully implemented in the first version, whereas the model-based interoperability testing tool has not yet been implemented for the TPS specifications. More details of the implementation are described in Deliverable D6.2.

3 UPDATE ON THE CERTIFICATION SUITE

3.1 Users and feedbacks

The first users of the certification suite implementation V1 are the FIESTA-IoT consortium members. We can observe two profiles of users:

1. **FIESTA ontology developer**. Some requirements of adding new concepts or enrich the taxonomy of the current FIESTA-IoT ontology were made by the Open Call testbeds. The FIESTA-IoT ontology developers considered these requirements and updated the ontology. They use the certification suite for the ontology validator to check the correctness of the updated FIESTA-IoT ontology before the official release.
2. **Testbed provider**. They use the certification suite for the complete functionality. They check their semantic annotation's conformance regarding to FIESTA-IoT ontology, check the API implementation regarding to the TPS specifications, and execute the full chain of certification process to get a certificate.

During the "alpha test" phase of the certification suite implementation, feedbacks are collected from intra-consortium channels, such as emails and Slack chats. Various bugs have been reported concerning the web portal functional anomalies, such as file upload failure, authentication error due to empty email address, etc.

The second users of the certification suite are the 1st Open Call testbed providers. They are required to use the certification suite to get their certificate before being able to join the FIESTA-IoT platform. They use the certification suite as the consortium testbed providers, however, their feedbacks are mostly collected through the FIESTA-IoT OC support email and the ticketing system. Their feedback was extremely valuable from a point of view external to the project. Apart from discovering new bugs and missing tiny components, we (the certification suite developer) realized that the process and the workflow were not 100% clear to the external users despite of some online help documents, which leaded us to create a step-by-step guide on "how to get your certification" that will be explained in details in section 4. From the feedbacks collected so far, we have also compiled a list of best practices that the users of the portal can follow to make their work more efficient.

3.2 Improved features and their implementation in V2

The certification suite first implementation aimed to provide a basic but functional implementation regarding to specifications in Deliverable 6.1. Optional functionalities and improvements have been carried out in version 2.

3.2.1 Authentication using FIESTA-IoT OpenAM credentials

The first version used a local authentication module with a dedicated user directory. It is not an ideal solution because the association of the certification result with the testbed identity distributed by the FIESTA-IoT consortium is needed. The FIESTA-IoT platform security module offers the authentication functionality and manages all the identities registered in the platform with the authorized rights based to their role such as *platform-observer, experimenter or testbed-provider*.

In version 2, thanks to the API provided by the FIESTA-IoT OpenAM instance, the authentication using the FIESTA-IoT OpenAM credentials is integrated to the certification portal (see Figure 3). A testbed provider no longer needs to create a new account on the certification portal. By using the FIESTA-IoT OpenAM authentication API, the certification suite is able to obtain automatically the account information such as username, the attached organization, the associated testbed and the role. This allows to associate the testbed provider identified in FIESTA-IoT platform to the generated certificate that proves the conformity of the underlined testbed regarding to the platform's requirements.

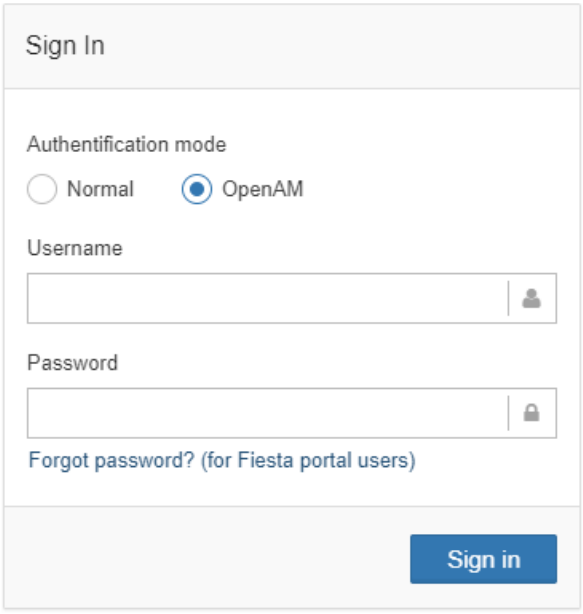

Figure 3 Login widget in using FIESTA-IoT OpenAM credentials

The FIESTA-IoT OpenAM account password recovery is also integrated in the certification portal. The link "Forget password?" redirects to the OpenAM password reset page for user to re-configure the password.

3.2.2 Interoperability tests on TPS

In section 4.3.5 of Deliverable D6.2, we described the initial design of the Model-based Interoperability Testing tool integrated into the FIESTA-IoT Certification Portal in order to carry out both interoperability and compliance tests to allow a Testbed provider to achieve certification that they interoperate successfully with the FIESTA-IoT platform and services.

The TPS Interoperability Tests

Four TPS testing models were developed and uploaded to the Model-based Interoperability Testing API of the certification portal (the API as reported in Table 4 of Deliverable D6.2 is unchanged and fully implemented and deployed):


```
TPS Methods (specified in Deliverable D3.4)
/getLastObservations
/getObservations
/pushLastObservations
/pushSingleObservation
```

In Deliverable 6.2, we described how different levels of certificate (gold, silver, or bronze) could be awarded based upon the number of operations from the list that are certified correct. However, it was decided that a testbed provider need only implement one TPS method to be allowed to integrate with the FIESTA-IoT platform, and there is no additional benefit to offering multiple method implementations. Hence, the Interoperability Testing certificate is awarded as follows:

- A Testbed provider implements one of the TPS methods from the TPS API specification.
- The testbed provider runs the certification test specific to that method.
- If the test passes, they are awarded the FIESTA-IoT TPS certificate.
- If the test fails, they are not awarded the certificate and the certification report provides pointers that can help identify issues.
    - Further, the report can be passed to the FIESTA-IoT support team for further help to achieve certification.

Certification Portal Integration

In Deliverable 6.2, the interoperability test had not yet been integrated into the Certification Portal; nor was it part of the full portal certification process (see Section 3 of this document). In this version, the portal front-end has been implemented – as shown in the following figures. Figure 4 shows that the list of TPS tests available can be selected by the end-user requesting a certificate.

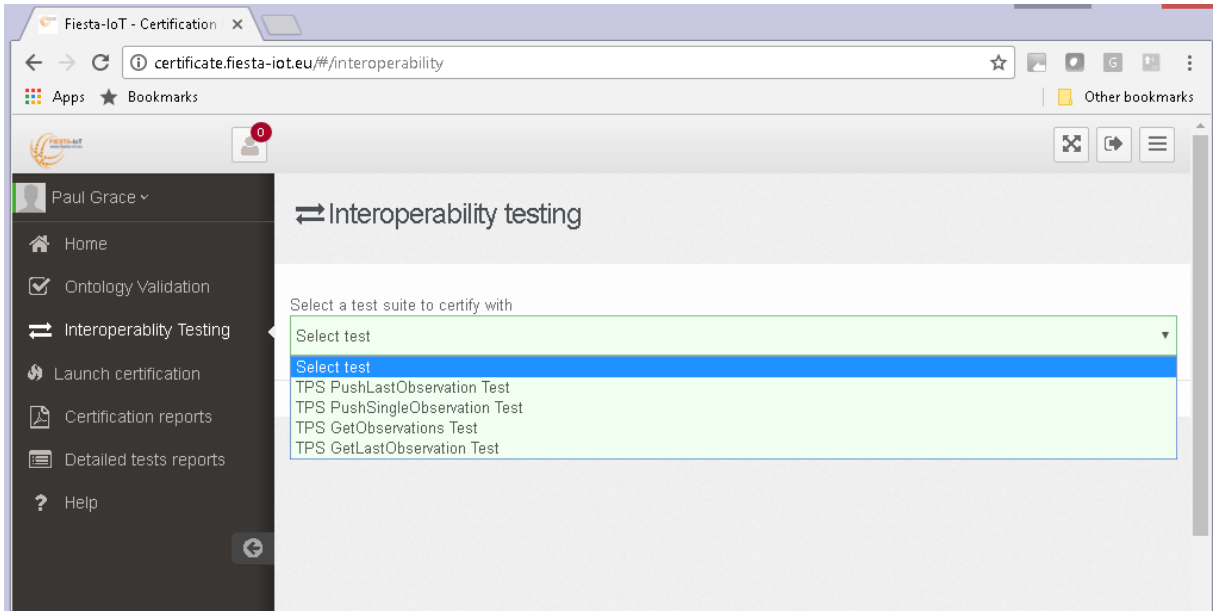

Figure 4: Interoperability Testing Portal – Select TPS Test

A page is then presented to the user as shown in Figure 5. Here there is a brief description of the test procedure (what it will test and how). It then displays the set of input values that must be provided by the user. These values are information about their testbed TPS implementation. For example, the user has selected GetLastObservation test and the following parameters are prompted:

- The API key (typically inserted into the HTTP Basic Authorization Field).
- The FIESTA-IoT identity of a sensor in their testbed.
- The Content-type of their annotated observation e.g. JSON-LD.
- The URL of their TPS.

Note, the portal is fully dynamic to work with newly created test models. When a model is uploaded to the Model-based Testing API, the portal works as follows:

- The drop-down list of tests will add this new model (a brief description is extracted from the model)
- If that test is selected, the certification portal analyses the model and extracts the input parameters (and their descriptions), creating text fields and text boxes for each.

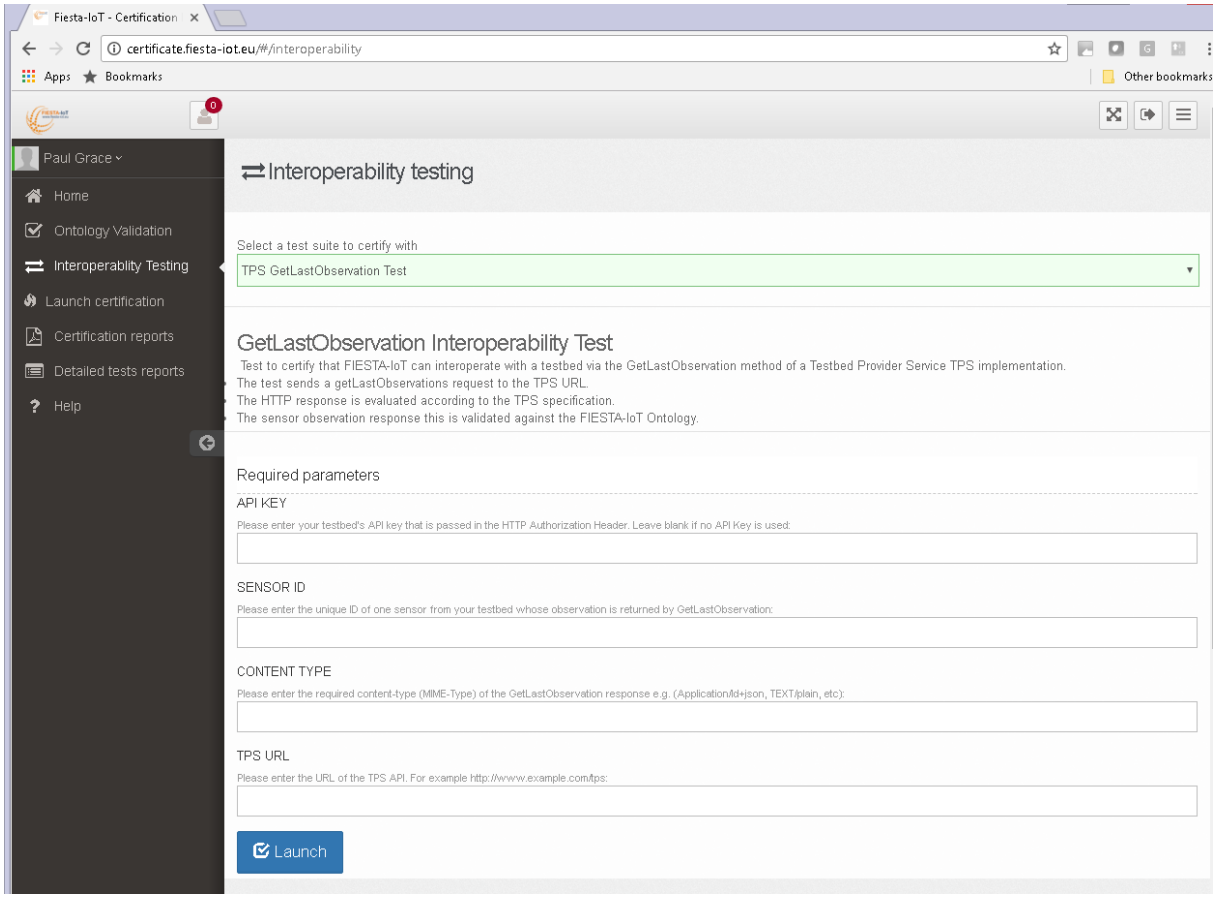

Figure 5: Enter the TPS test parameters

After completing the fields, the user starts the TPS test by selecting the “Launch” button. This executes the interoperability test on the server, and the results are returned and displayed to the user as shown in Figure 6. Here, the top part of the page indicates the outcome of the test (either Pass or Fail). While the bottom “Result” section lists the full output of the test in terms of the individual steps executed as part of the model-based test.

The usage of this service by external parties (testbed providers from the 1st and 2nd Open Calls) led to improvements based upon their feedback:

- When the test failed, the provided report was not clear as to why this happened and how they can rectify the problem.

Therefore, we extended the underlying interoperability testing model to model failures. We briefly explain this extension here using a simple example. Figure 7 highlights that a test transition of *http.code=200* passes and goes to a successful end state to complete the test. However, previously with only this information, if this test failed there would be no other information other than code equals another value. So instead we model more information, i.e. alternative error transitions that move to false end states. If the test hits one of these states the report information is attached to the output to the user, to add additional explanation about why they have not succeeded with their interoperability test.

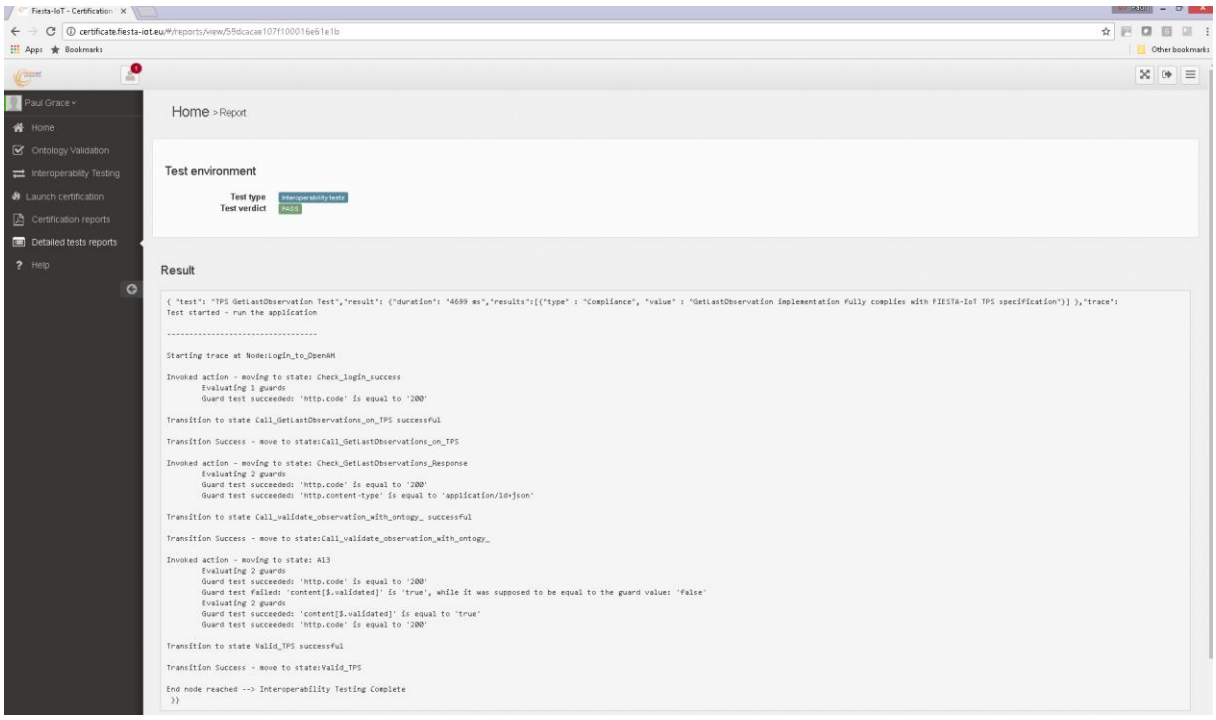

Figure 6: TPS test results

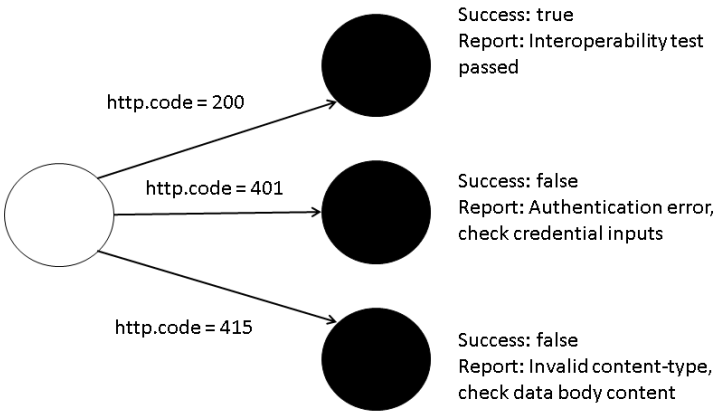

Figure 7: Interoperability Model Extension – reporting error states

Summary

In Deliverable 6.2 we defined four requirements for the interoperability testing part of the certification suite. Requirement number 4 was as follows:

- ***Req-4: An online service for performing interoperability certification tests***
    - *A web service for running interoperability tests whose results inform a certification report that can then be used to generate interoperability certificates.*

We have shown in this section, that this requirement has been fully implemented and realised by the following:

- Online interoperability testing service deployed on the FIESTA-IoT service platform machines, and accessible with a fully documented RESTful API.
- Certification Web Portal to select, execute and report on interoperability tests.
- Use of certification portal by external 3rd party tools.

However, although the requirement has been achieved we will continue to look to improve the interoperability testing tool based upon feedback received from users of the tools.

3.2.3 Model-based Interoperability Testing Tool Improvements and Extensions

In this Deliverable, we report on the improvements and extensions made to the interoperability testing tool (MBT tool) that forms part of the suite of certification and testing tools provided by FIESTA-IoT. An early version of the MBT tool was presented in Deliverable 6.2; and we now list in turn the extensions that have been carried out in the period since.

3.2.3.1 Remote Certification

While the Certification Portal provides one solution to testing and certifying that a system complies with and interoperates with given interoperability standards—it is not fit for all situations and users. This is because:

- The portal requires that all systems to be testbed are made accessible through a public interface, e.g. an external HTTP URL. However, many testers may not wish to adhere to this condition. Such behaviour is expensive and time consuming to configure (particularly if the system under test will never be made externally accessible). Further, due to security issues, or intellectual property concerns—the tester may not be happy to have testing carried out by an unknown external service.
- The system under test wishes to test the interactions between two systems deployed in a given domain. Without injecting an external agent into that domain then a remote testing service cannot observe and test these interactions.

Therefore, there is a strong requirement for a certification process to support testing tools that a user can use locally themselves to achieve certification.

Here we describe the extension to the MBT tool to allow a user to use the Graphical MBT tool on their own machines, but still safely and securely achieve certification with the FIESTA-IoT Certification Process.

The first step is to select **"Certification->Download Model"** from the Tool menu (left side of Figure 8). The user will then be shown the list of test models available (here we use the certification portal API, so the list of TPS tests, described previously, are returned to the user) as seen in the right screen of Figure 8.

After selecting a model (e.g. GetLastObservation) the model will be loaded into the tool (as seen in Figure 9) and the user can then execute the test using the local instance of the tool. The user executes the test and the tool displays the Interoperability report on screen; based upon this information, they can then request a certificate. They do this by selecting **"Certification->Request Certificate"** from the tool menu.

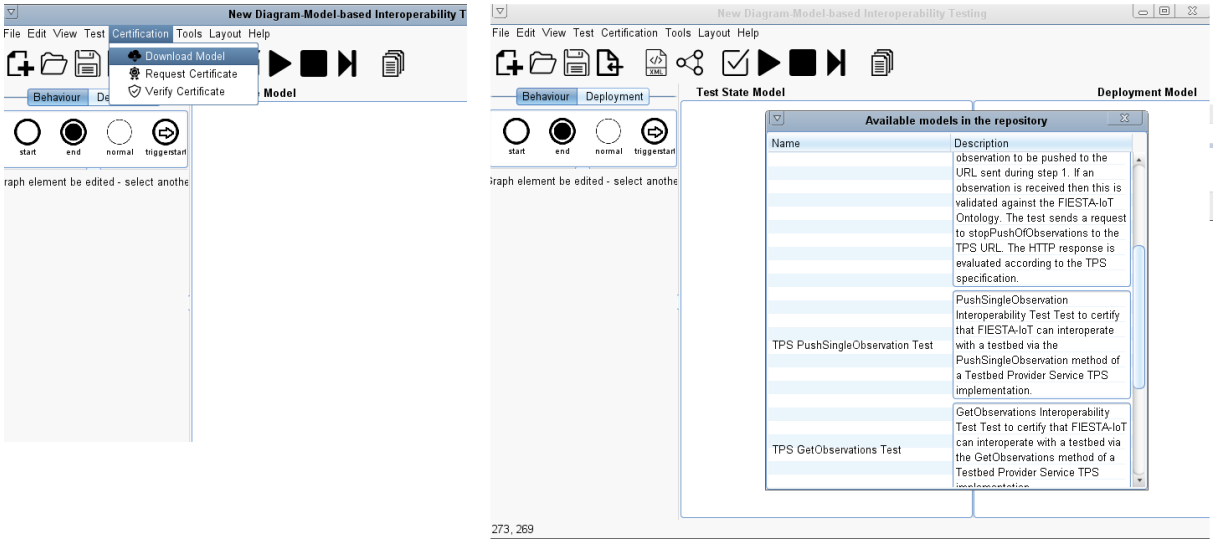

Figure 8: Selecting a Certification model in the MBT tool

When the certificate is requested, a number of checks must be made:

- The tool must ensure that the test has not been changed/tampered with in order that the system passes and achieves a successful result without having implemented the system correctly. To avoid this, the MBT tool creates a hash of the original test; and then when the test result is submitted, the executed test is also hashed using a similar algorithm. The two are compared and if they differ then the test has been altered and the tool will not proceed with certification.

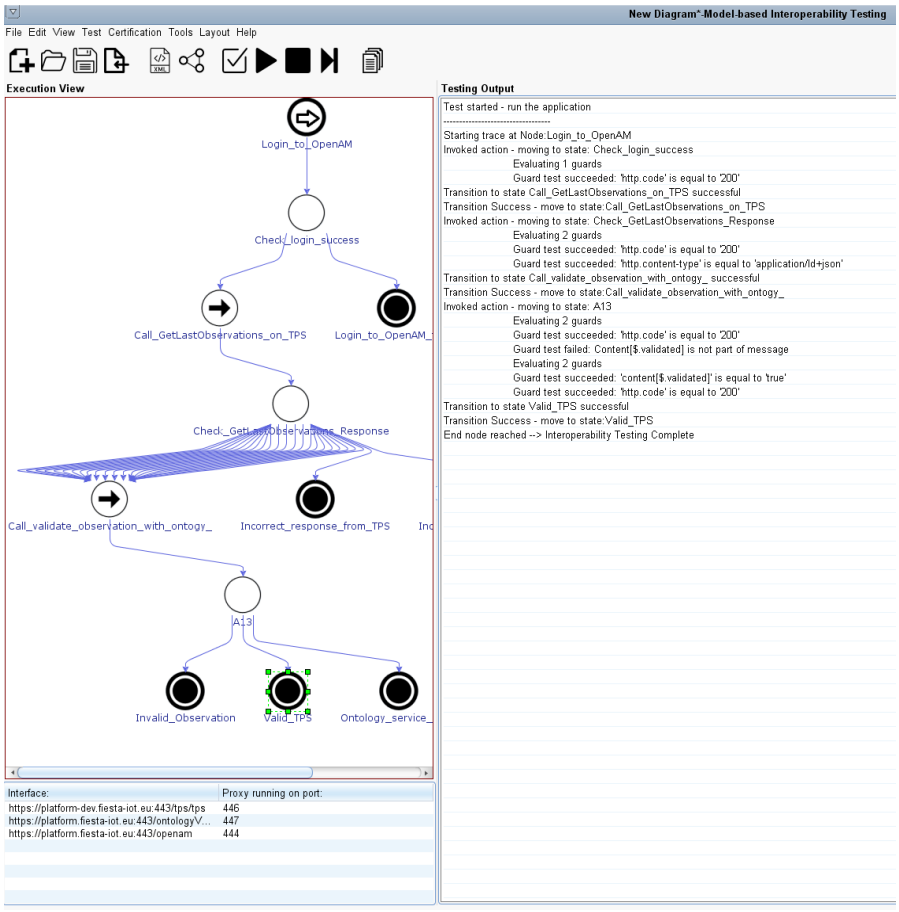

Figure 9: Execution of the certification model

When the certification is successful then a PDF certificate is generated (shown in Figure 10). This can be used as evidence for supporting certification equivalent to the portal certification. For example, the portal certification is complete except for the interoperability testing. The user can then add this PDF as additional evidence.

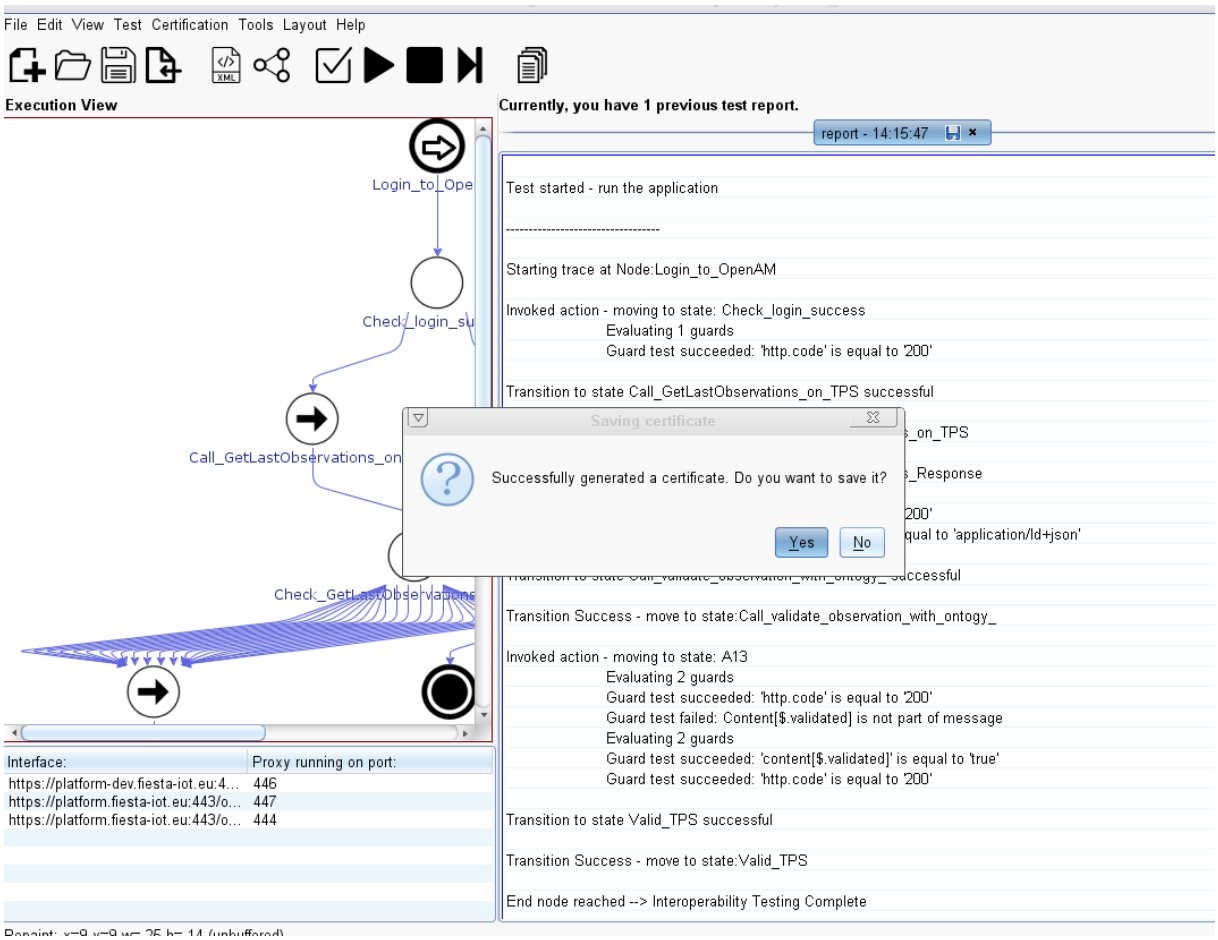

Figure 10: PDF certificate produced

The final step is to ensure that submitted PDFs are verified as correctly produced by the FIESTA-IoT testing tool; and again, no content in the PDF has been altered to cheat certification. For this, the PDF is digitally signed by FIESTA-IoT and this stamp is added to the certificate (as seen in Figure 11).

The MBT certificate portal service provides a remote operation to verify digitally signed PDFs. The PDF is passed, and the service will detect if any changes to the PDF content have been made unauthorized parties.

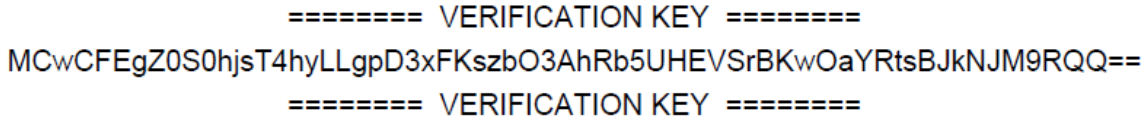

Figure 11: Certificate Digital Signature

3.2.3.2 Improved Usability

To make the tool more usable by software testers, the following extensions have been provided:

- **Helpers.** Every text input field, where a user must enter rule tests has helper wizards that can help the user build the model. For example, when creating a test

on a HTTP header field the user can select from the pre-defined set of common HTTP headers.

- **JSONPath and XPath Wizards.** Where testing rules test on values in JSON and XML data, the user previously had to enter the XPATH expression manually. Now the tool quickly helps them identify the correct expression and inserts it into the model for them. The tool opens the pop-p as shown in Figure 12 and the user then inputs the XML. They click on a tag/value in the XML and the XPath expression is generated.

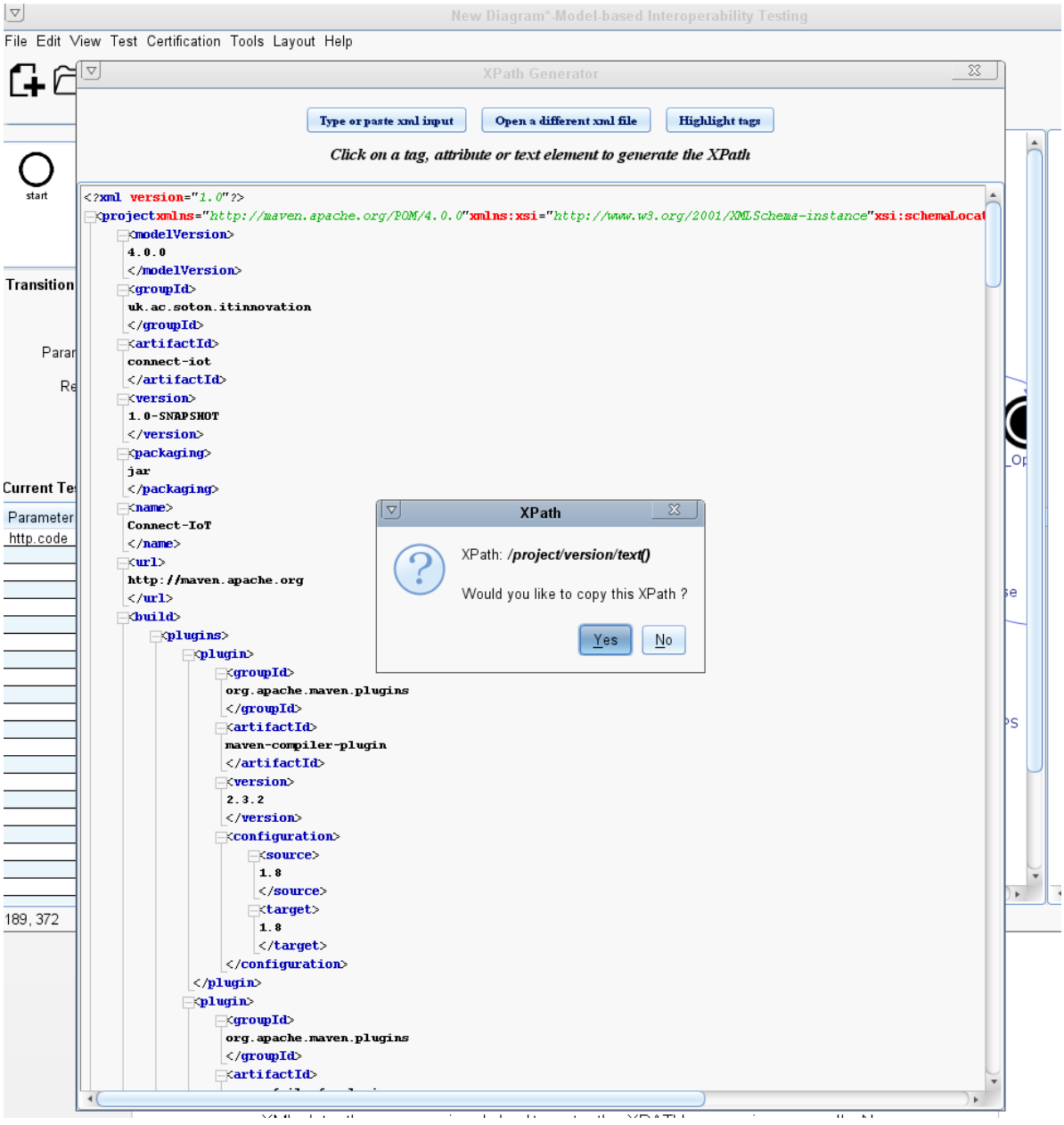

Figure 12: XPATH helper

- **Step-by-Step Debugging.** The user can now execute the interoperability test one step at a time. To better understand where tests succeed, and where they fail-why they fail. When they run the test, they select the “step-by-step” option and then the test is displayed as presented in Figure 13. To the left, the current position of the test sequence is displayed (via the highlighted state) and the report is displayed to

the right as each transition is made. To move to the next step, the user selects the "Next Step" button from the toolbar.

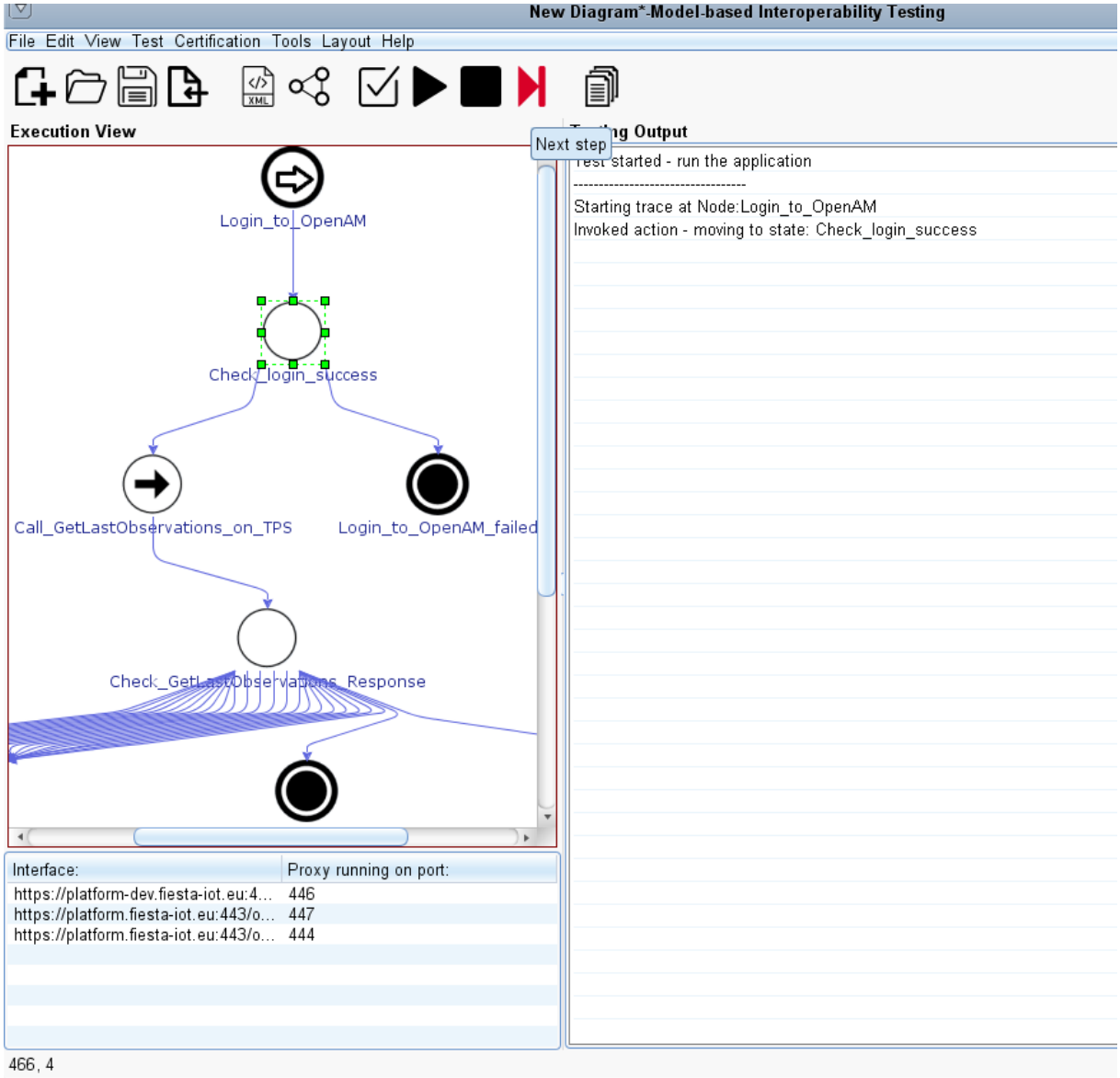

Figure 13: Step-by-Step debugging

3.2.3.3 Additional Protocols

To support a broader range of testing, the testing tool now supports more protocols beyond HTTP. These protocols are:

- **The Constrained Application Protocol**[1] (**CoAP**). This is prevalent in many IoT standards (importantly OneM2M) and the ability to use the MBT tool to test the interoperability of complete systems whose elements use both HTTP and COAP offer a unique selling point for the tool.

[1] https://tools.ietf.org/html/rfc7252

- **SOAP**, or the Simple Object Access Protocol[2] is a protocol used by Web services with XML used to encode messages. This ensures that the tool has broader coverage across the Web Services deployments that tie IoT with online services and cloud computing interfaces.

[2] https://www.w3.org/TR/soap/

4 CERTIFICATION PROCESS PRACTICE

To help the third-party users to use the certification portal to get their testbed certified before joining into the FIESTA-IoT platform, a user-guide has been developed. The content has been transformed to HTML format and available on the Moodle platform[3] that users can consult as frequently as they want.

The user guide has three main parts:

1. **Prerequisites**. It specifies at which stage the user should come to the certification portal to get their certificate.
2. **Login and Authentication**. A certificate only makes sense when it targets a specific and identified subject. The authentication is a crucial step in the certification process.
3. **Certification process**. It is a step-by-step guide for users to get the certificate.

We do not try to replicate the content of the user guide in this document. It is provided in the Annex I. The web portal is designed to be intuitive and self-contained, which makes the guide easy to follow. No negative feedback was received about the certification process from the users.

The FIESTA-IoT consortium decides to allow only those testbeds who have successfully completed all the three tests (the Scorecard, the semantic data validation and the TPS interoperability tests). A certificate issued by the certification portal indicating that the underlined testbed succeeded all the tests is a must for joining FIESTA-IoT platform.

4.1 Best practice to get the testbed certified by FIESTA-IoT

This section summarizes the best practices to successfully get the certificate from the consortium's experience and the interaction/feedback with each Open Call partners.

1. Use the AaaS (Annotator as a Service) or follow the example annotations of the in-house testbeds to avoid errors in the semantic annotation of resources and observations.

2. Use the TPS skeleton provided on GitHub to better understand the TPS API and the required interactions with the FIESTA-IoT platform.

3. Use the online tools (ontology validator and MBT interoperability testing tool) to check the annotation and the TPS implementation as often as possible during the development. It helps to identify the errors (if any) as soon as possible

4. Talk to FIESTA-IoT consortium whenever there is an obstacle for the development. The consortium makes a lot of effort to provide a feedback as soon as possible.

[3] http://moodle.fiesta-iot.eu/mod/book/view.php?id=96&chapterid=85

5 CONCLUSION

In this deliverable, we firstly reviewed the status of the certification suite and tools at the end of the second year. At this moment, the main framework, including the certification process, the components and the expected results, were already in good shape. The main work regarding this certification framework during this year, has been to improve several functionalities, such as the authentication method, the interoperability tests, and most importantly, to invite participants to try the certification suite and tools.

For this purpose, we had two parallel activities:

1. Enhance and improve the online certification suite and tools. We implemented the authentication method using the unique FIESTA-IoT OpenAM credentials, which makes the users to manage less credentials to access all the FIESTA-IoT services, and makes the FIESTA-IoT technical team to have less work to maintain the mapping between the certificate and the actual platform access. The TPS interoperability tests have been successfully integrated to the certification portal, which has made the test suite for getting the certificate complete.
2. Provide documentation and manual for correctly and efficiently using the certification suite and tools. The manual and related documentation are available on the Moodle training platform[4].

The next step of the work for the following months of the project is mainly about maintaining the certification suite and tools and help users to get their certificates. The Model-based interoperability tools aims also to integrate more market-oriented tests such as oneM2M and NGSI API tests (to be reported in the future Deliverable D6.5). It also aims to release an “offline” extension of the tool to help those applications which do not have an Internet connection. This will help the FIESTA-IoT tool to be ready for more market challenges.

[4] http://moodle.fiesta-iot.eu/mod/book/view.php?id=96&chapterid=85

APPENDIX I – THE CERTIFICATION PROCESS MANUAL

Prerequisites

To succeed your certification process and get a valid certificate, you need to prepare your FIESTA-IoT account and your testbed

- The certification process must be conducted with your FIESTA-IoT account. This account makes the proof of the identity of the testbed under certification. If you do not have one yet, please refer to the handbook[5] to get one.
- The output data must be semantically annotated using the FIESTA-IoT ontology. You need also to be aware of the serialization format of your semantic data (i.e. RDF/XML, JSON-LD) and be able to extract one sample of your data stream which constitute a stand-alone semantic-annotated piece of information (i.e. with requested prefix used in the annotation, complete data graph). This "stand-alone" sample need to pass the ontology validation to make your certification process progress.
- You must implement at least one of the four TPS API methods and the endpoint must be accessible for FIESTA-IoT platform. This is crucial for FIESTA-IoT to get data from your testbed. For more information of the TPS, please refer to the handbook and the sample code[6].

A.1. Login to the certification portal

Go to the certification portal (http://certificate.FIESTA-iot.eu/). Choose "OpenAM" as Authentication mode, and use your FIESTA-IoT OpenAM credentials to login.

[5]http://moodle.fiesta-iot.eu/pluginfile.php/711/mod_resource/content/2/FIESTA-IoT_Handbook4ThirdParties_v1.0.pdf

[6] https://github.com/fiesta-iot

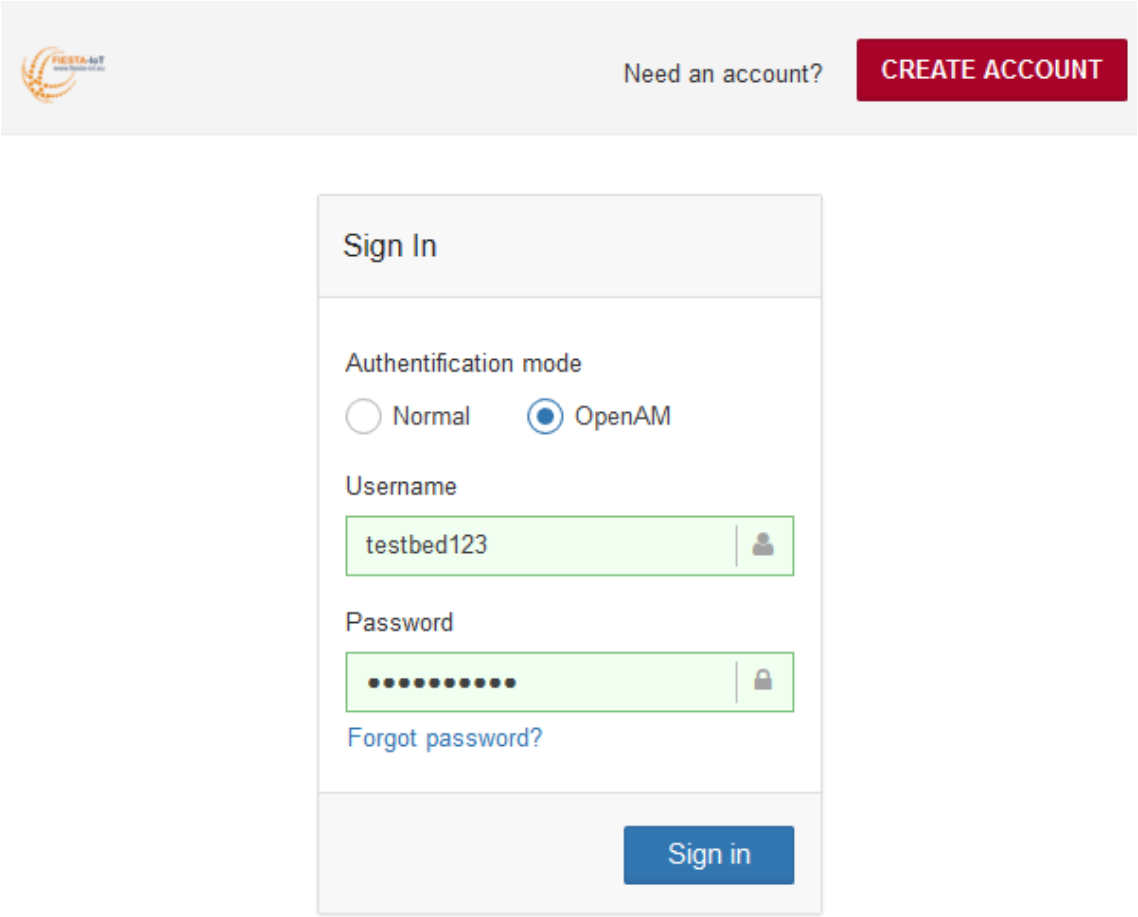

Figure 14. Log in to the FIESTA-IoT certification portal using OpenAM credentials

A.2. Launch the certification process

Just after the log in, you are on your home page where historical test reports and certifications are displayed. To launch a certification process, just click on “Launch certification” in the menu and you should see the following web page.

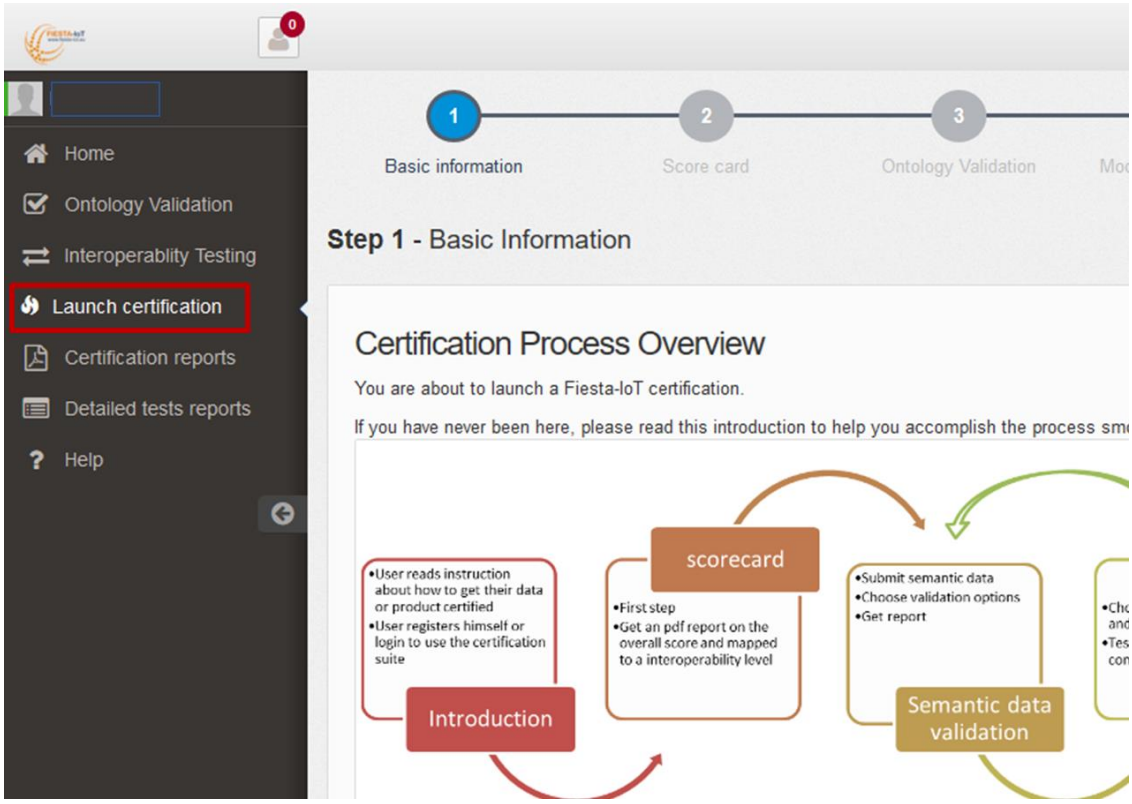

Figure 15 Launch a certification process

On this page, the certification process is explained. Follow the instructions on the page. It contains 3 assessment/tests that you **MUST** to perform to get a valid certification for joining FIESTA-IoT.

1. Self-assessment scorecard. This scorecard is a questionnaire covering several aspects of your testbed. Answer it regarding to your testbed
2. Ontology validator. You need to prove that your annotated data are conform to the FIESTA-IoT ontology[7]. You need to provide a sample of your annotation and validate it against the FIESTA-IoT ontology. More details will be given in the following section.
3. Interoperability testing. You need to prove that your TPS implementation is compliant with the TPS specification. According to the FIESTA-IoT TPS specification, your testbed needs to implement at least one TPS API methods to be able to provide your semantic data. Choose one among the four TPS API tests regarding to your implementation in the drop-down menu. More details will be given in the following section.

A.2.1. Use the ontology validator

In step 3 ontology validator, you need to give one example of the semantic annotation, either an annotation of a resource, or an annotation of a piece of observation. You can choose either upload your semantic annotation as a file, or copy-paste directly the annotation using “Direct input”. If you choose “Direct input”, you need to also specify the serialization type using the drop-down menu.

[7] http://ontology.fiesta-iot.eu/ontologyDocs/fiesta-iot.owl

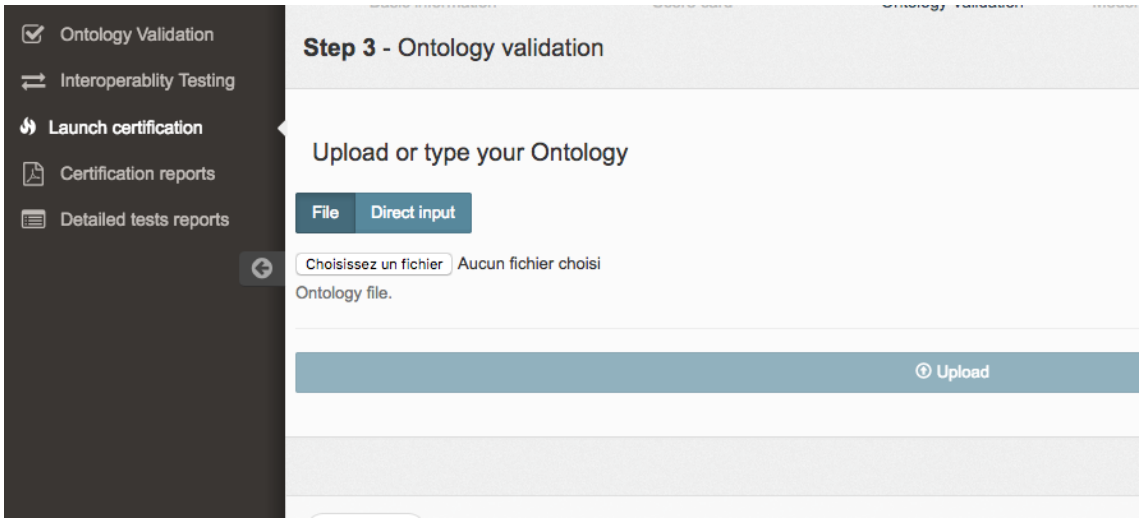

Figure 16 Upload a file containing your semantic annotation

Figure 17 Direct input your semantic annotation in textbox

On the next page, you need to choose only FIESTA-IoT as reference ontology, and check all the four types of errors.

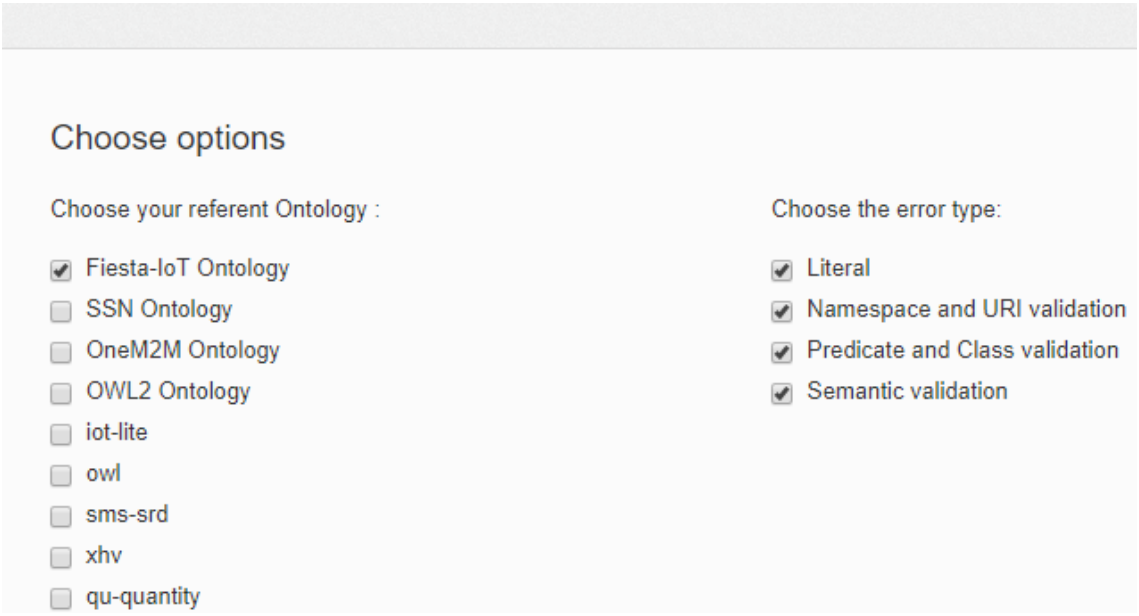

Figure 18 Choose FIESTA-IoT Ontology as reference ontology and check all the validation types

Click on the blue button “Validate” to launch the validation

A.2.2. Perform the Interoperability tests

In the drop-down list, there are four TPS interoperability tests. According to your implementation, choose one among them to be tested. For example, if you have implemented both getObservations() and getLastObservation() API, you can either choose “tps GetObservations test” or “tps GetLastObservation test”.

The text fields below are automatically adapted to the test you just chose. Following the tooltip next to each text field title, you are invited to provide the information about the testbed to make the interoperability tests able to be executed on your testbeds. In principle, the tests will test the correct implementation of the interactions between the testbed and FIESTA-IoT.

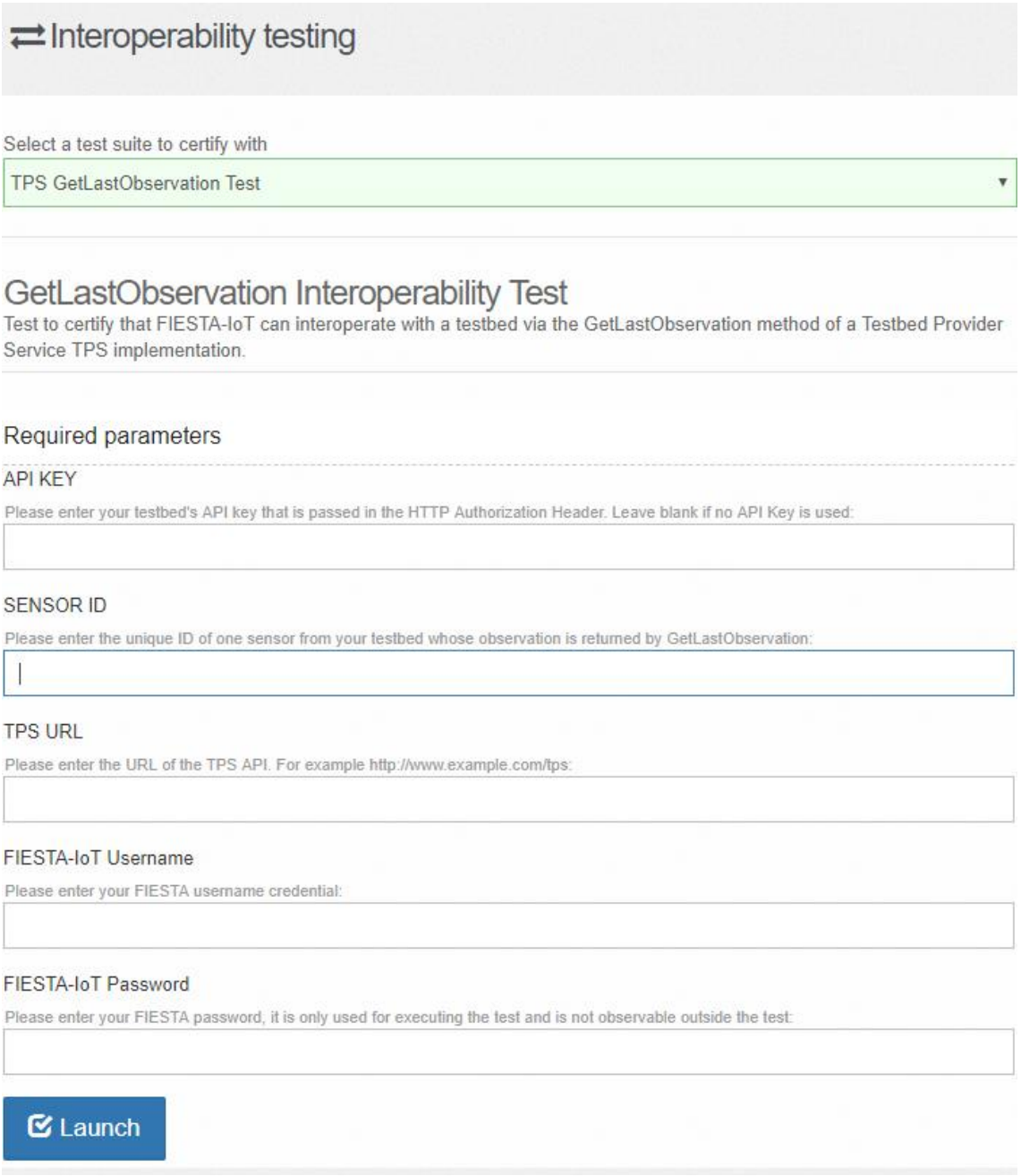

Figure 19 Enter information required for interoperability test

A.2.3. Get the certification

After having passed all the three assessment/tests, you are directed to the certification result page as the following figure:

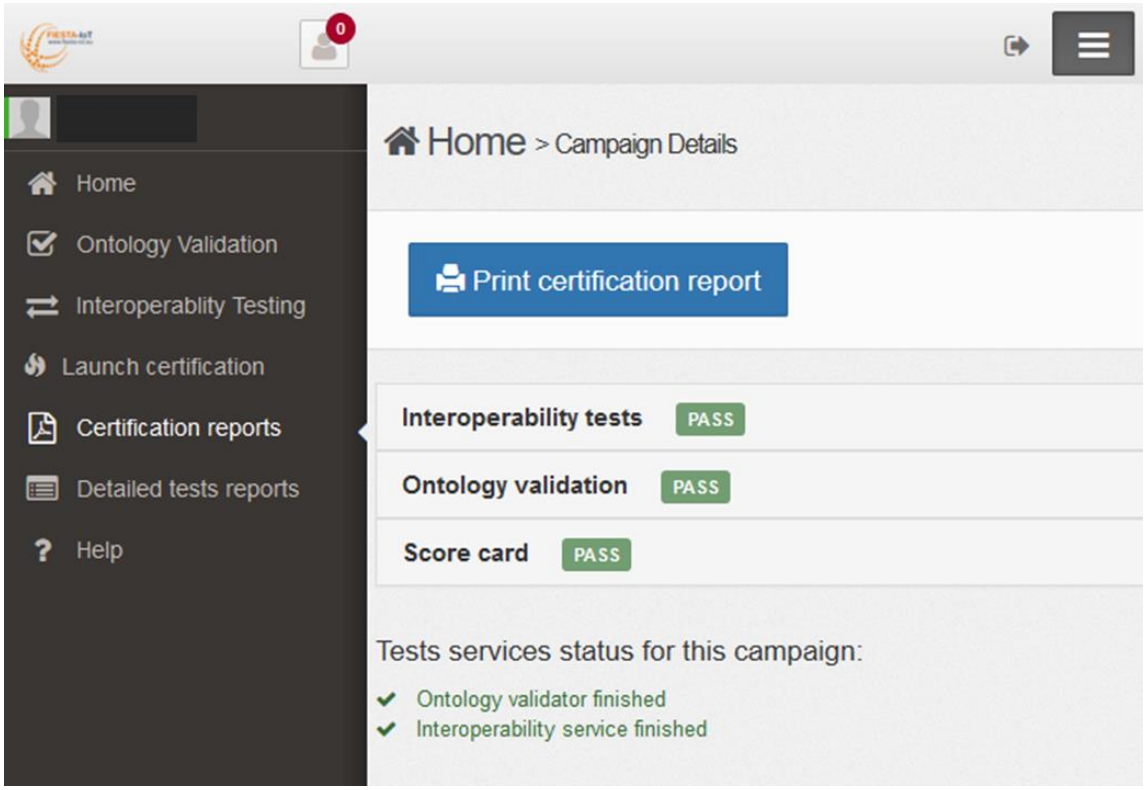

Figure 20 Print your certification

You need to click on the blue button “Print certification report” to get your certificate in PDF format and send it to the FIESTA-IoT support team (oc-support@FIESTA-iot.eu). The certification report includes all the information that you need to communicate to the FIESTA-IoT support team to get you the account promotion. You are not requested to add any extra information.

If you do not have **all the three tests passed**, i.e. if you see a red or yellow flag rather than a green one, you can still click the button to print the report, but it will not be considered as a valid certification to be able to join FIESTA-IoT platform.

