IoT Lab
European Research Project

Researching crowdsourcing to extend IoT testbed infrastructure for multidisciplinary experiments, with more end-user interactions, flexibility, scalability, cost efficiency and societal added value

Grant agreement for: Collaborative project

Grant agreement no.: 610477

Start date of project: October 1st, 2013 (36 months duration)

Deliverable D1.4

Final IoT Lab Architecture and Components Specification

Contract Due Date	30/09/2016
Submission Date	20/10/2016
Version	v1.0
Use of Resources	This deliverable production is the result of Task 1.1 and Task 1.2 which has benefited from a collective effort of work from the partners of the consortium estimated to be about 7.91 PMs.
Responsible Partner	Aleksandra Rankov (DNET)
Author List	Aleksandra Rankov (DNET), João Fernandes (AI), Marios Karagiannis (Unige), Panagiotis Alexandrou (CTI), Theofanis Raptis (CTI), Gabriel Fillios (CTI), Sébastien Ziegler (MI), Cedric Crettaz (MI), Nikolaos Loumis (UNIS), Anna Ståhbröst (LTU), Riccardo Pozza (UNIS)
Dissemination level	PU
Keywords	Internet of Things, Crowdsourcing, Testbed, FIRE

Project Coordinator: Mandat International (MI)

Sébastien Ziegler <sziegler@mandint.org>

Abstract

This document reports on the final iteration of the IoT Lab platform architecture and its requirements which were established in the initially proposed platform architecture as provided in D1.2 Preliminary IoT Lab Architecture and Component Specification as well as on the updated platform architecture in D1.3 Updated IoT Lab Architecture and Component Specification. The final architecture reflects the feedback received on the implementation work carried out in the technical workpackages (WP2 Crowdsourced Augmented FIRE Infrastructure, WP3 Virtualization and Mobility and WP4 Cloudification for Multiple Testbeds Large Scale Integration). In addition, inputs from the non-technical workpackages (WP5 End-user and Societal added Value Analysis and WP6 Economic and Business Opportunity Analysis) on end-user and business angles respectively were also taken into account.

Acknowledgements

This deliverable is part of the IoT Lab European Research project, which has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under Grant Agreement no 610477.

Table of Contents

List of Tables

List of Figures

Abbreviations and acronyms

API	Application Program Interface
CA	Consortium Agreement
CPU	Central Processing Unit
DB	Database
EC	European Commission
ETL	Extract, Transform, Load
EU	European Union
FP7	Seventh Framework Programme
F4F	Federation for FIRE
FIRE	Future Internet Research and Experimentation
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GPRS	General packet radio service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
ID	Identifier
IoT	Internet of Things
IoT-A	Internet of Things Architecture
IP	Internet Protocol
IPC	Intellectual Property Committee
IPR	Intellectual Property Rights
IPSEC	Internet Protocol Security
IPSO AF	Internet Protocol for Smart Objects Application Framework
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organisation
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LSPI	Legal, Security and Privacy Issues
LTE	Long-Term Evolution, commonly marketed as 4G LTE
OML	Outline Markup Language
OS	Operating System
OSN	Online Social Network
PaaS	Platform as a Service

PC	Project Coordinator
PCP	Partner Contact Person
PDPO	Personal Data Protection Officer
PhD	Doctor of Philosophy
PM	Person Month
PMB	Project Management Board
PO	Project Officer
QoS	Quality of Service
QoE	Quality of Experience
RDI	Research, Development and Innovation
REST	Representational State Transfer
RESTful	Service based on REST
R&D	Research & Development SFA Slice based Federation Architecture
SLA	Service Level Agreement
SOTA (or SoA)	State Of the Art
SQL	Structured Query Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDG	Universal Device Gateway
UI	User Interface
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UPRAAT	Universal Privacy Risk Area Assessment Tool
URL	Uniform Resource Locator
US	United States
VoIP	Voice over Internet Protocol
WoT	Web of Trust
WP	Work Package
WPL	Work Package Leader
W3C	World Wide Web Consortium
XML	Extensible Markup Language

Executive Summary

This deliverable presents a detailed and comprehensive description of the final IoT Lab architecture, resulting from activities performed in different work packages. The IoT Lab architecture proposed in Y1 and further updated in the Y2 has been finalised in Y3 focusing on the realisation and practical implementation of the following remaining functionalities and components, interfaces and protocols supporting them:

- **Identity and role based access management (WP2):** Platform provides to its users a tailored information and role defined access rights to different platform functionalities. In this scheme, individual identifiers are assigned to all types of platform users that are used for their authentication, authorization and management of privileges across the platform. Six types of roles are implemented through the platform.
- **Trust management and users' privacy support (WP2):** Platform provides mechanisms that ensure trustworthiness of the platform in terms of privacy, open data and IP issues. The "Right to be Forgotten" is also supported for the mobile app users, which is as if the user never participated in the platform.
- **Security framework (WP2):** Security mechanisms have been implemented to ensure full protection of identities against the privacy risks, security of servers against any system instability or malfunction, data storage security against illegitimate access, network security against the risk of intrusion to the system infrastructure, viruses or similar intrusions as well as the security at the application level.
- **Incentives mechanisms, motivators and rewarding schemes (WP6):** To maximise end-users' motivation and participation in the crowd-driven research process, a thorough study has been performed resulting in the derivation of concrete requirements and the practical implementation of the relevant mechanisms i.e. related architectural components supporting the hybrid model identified in WP6 as most applicable to this platform.
- **Reputation framework (WP2):** To augment the user engagement with the platform, while at the same time evaluating his/her behaviour, a scoring mechanism called Reputation Scoring has been designed. This mechanism reflects the overall activity of users regardless of the type of their engagement and it is based on suitable ranking functions. Ratings are given to the crowd participants, researchers, proposed ideas, and for the platform based on the active feedback from users on crucial aspects of the platform.
- **Architectural adaptations** coming from end-user feedback (WP5)**:** received through the process of platform deployment and from a number of evaluation workshops organised with end users.

The process of final platform deployment followed the privacy by design principles.

1 Introduction

1.1 The IoT Lab project in brief

IoT Lab is a European research project exploring the potential of crowdsourcing to extend European IoT testbed infrastructure for multidisciplinary experiments with more end-user interactions. The project researches and develops:

1. Crowdsourcing mechanisms and tools enabling testbeds to use third parties resources (such as mobile phones), and to interact with distributed users (the crowd). The crowdsourcing enablers will address issues such as privacy by design, identity management, security, reputation mechanisms, and data ownership.

2. Virtualization of crowdsourcing and testbed components by using a meta-layer with an open interface, facilitating the integration and interaction with heterogeneous components. It should ease data integration and reduce the cost of deployment in a real environment.

3. Ubiquitous Interconnection and Cloudification of the testbeds resources. It will research the potential of IPv6 and network virtualization to interconnect heterogeneous and distributed resources through a Virtual IoT Network and will integrate them into the Cloud to provide an on-line platform of crowdsourcing Testbed as a Service (TBaaS) available to the research community.

4. End-user and societal value creation by analysing the potential end-users and crowdsourcing participants to propose an optimized model for end-user adoption and societal value creation.

5. “Crowdsourcing-driven research” as a new model in which the research can be initiated, guided and assessed by the crowd. It will compare it to other models.

6. Economic dimension of crowdsourcing testbed, by analysing the potential markets and business models able to monetize the provided resources with adequate incentives, in order to optimize the exploitation, costs, profitability and economic sustainability of such testbeds. It will also develop tools for future experiments.

7. Performing multidisciplinary experiments, including end-user driven experiments through crowdsourcing, in order to assess the added value of such an approach.

The project adopted a multidisciplinary approach and addressed issues such as privacy and personal data protection. To achieve these ambitious goals, the consortium consists of seven international academic or research partners and a SME that provides an expertise from complementary research areas, including Information and Communication Technologies, End-user interaction, and Economics.

1.2 Purpose and scope of the WP1

It is the purpose of WP1 Requirements and Architecture Design to identify relevant crowdsourcing scenarios and, requirements coming from the end-users in order to contribute to coherent platform architecture. This architecture considered inputs from other research projects (FIRE architectures) and extended them by taking into account the IoT Lab requirements. All this work has been in continuous alignment with the technical work carried out in all the other technical WPs where use cases and technical requirements serve as inputs. At the same time, the outcomes of these WPs were validated in the overall system architecture designed in WP1.

This work package is divided in two tasks, as follows:

- Task 1.1 Use Cases and Requirements Analysis: In this Task, completed in M6, a wide range of relevant crowdsourcing use cases were designed, as well as their derived functional and non-functional requirements.
- Task 1.2 Architecture Design: This Task investigated emerging architectures in European projects as well as novel extensions to those architectures. The design of the overall IoT Lab architecture also considers the requirements coming from Task 1.1.

WP1 coordinates and aligns the overall strategy and facilitates activities for the overall project.

1.3 Purpose and scope of the Task T1.2 on Architecture Design

In this Task, we design and describe the IoT Lab architecture based on the technical and end-user requirements defined in Task 1.1. The first approach considered is to analyse different emerging FIRE architectures as a basis for the architecture design and specification. The architecture also includes specific IoT Lab extensions in order to address the specific IoT Lab requirements. These extensions are meant to consider and support, for example, an ad-hoc organised, dynamic setup of an experimental infrastructure. This is to enable a simple mechanism while ensuring issues like reliability and privacy are handled efficiently in a collective environment of a small or large community. The architecture design plans to take into consideration built-in reputation and privacy mechanisms, as well as a dynamic selection of suitable crowd resources and optimal experiment scheduling. The architectural model is iteratively addressed taking into account work carried out in the technical work packages.

The architecture design needs to identify the main system components and their functionalities, interaction patterns, interfaces as well as the underlying communication links and mechanisms required for the maintenance of such systems.

Finally, the completion of Task 1.1 requirements defined and their evaluation is also part of this Task and contributes to the architecture design updates.

1.4 *Purpose and scope of the current document*

It is the objective of this document to describe the work carried out as part of Task 1.2 Architecture Design during the 3-year duration of the project. Due to D1.2 [1], as stated previously, an initial architecture reference model was initially developed based on inputs from various technical and non-technical WPs in Y1. The Y2 architecture included updates on the platform component developments, their interconnections, interfaces, standards, and network requirements, etc. Y3 architecture includes the final description of all implemented components, respective interconnections and interfaces resulting from the work in the following WPs:

- WP2 provided final inputs on Identity Management and Role based access control. It also provided reputation and scoring mechanisms based on ranking functions as well as the trust management and support of the users' privacy.
- WP3 provided inputs on interfaces and data exchange.
- WP4 provided inputs on Testbed as a Service (TBaaS) modularity as well as the End User Application Layer to enable users' interaction with the platform.
- WP5 provided inputs on end-user insights.
- WP6 provided inputs on Incentive Model Design Methodology and the Budget Management.

The following diagram depicts the sequences and interactions in Task 1.2 during Y3 of the project, which resulted in the final iteration of the platform architecture.

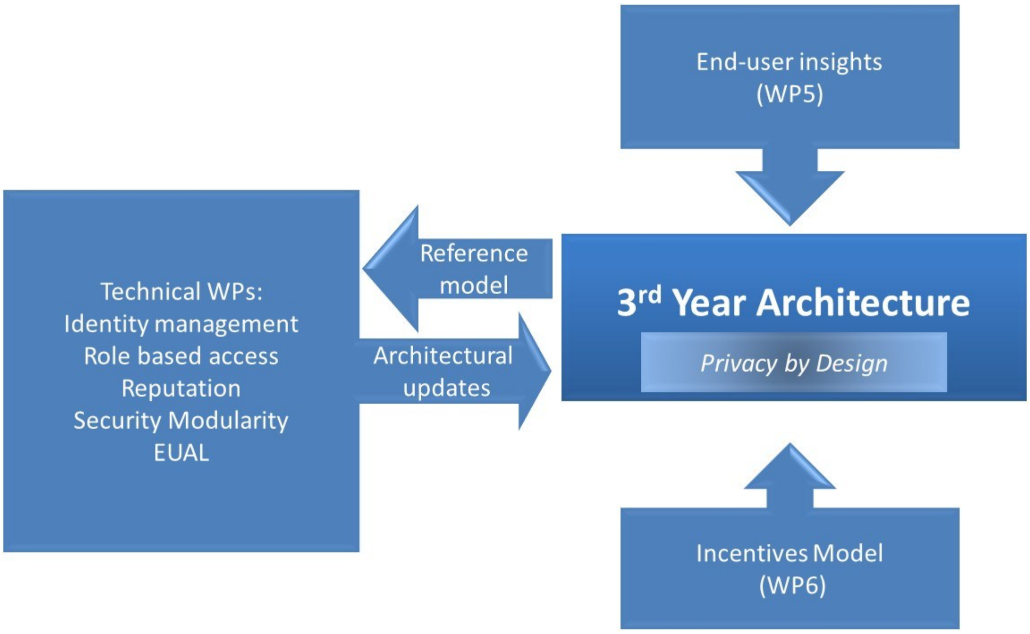


Figure 1: Platform development approach for Y3

The overall IoT Lab architecture as proposed in Y1 and Y2 has been revisited and then upgraded based on identified technical requirements (from planned and conducted use cases) as well as results achieved in the technical WPs. Deliverable D1.2 Preliminary and Updated IoT Lab Architecture and Component Specification was completed at the end of Y1 and Y2 respectively. The final iteration of the platform architecture as presented in this document is aligned with the principles of privacy by design.

1.5 Structure of the Document

The structure of the document is as follows: In Section 1, a brief overview of the IoT Lab project is given. In Section 0, we provide a brief overview of the architecture's development process referring to work in previous architecture deliverables (D1.2 and D1.3). Section 0 describes the main principles that were followed during the platform development including the aspects and measures undertaken to align with the privacy by design approach. This section also provides a brief overview of the use cases implemented during Y3 including their special requirements. Section 4 provides the final status of the architecture while Section 5 provides a detailed description of all integrated architectural components that have been developed and adjusted to support all identified requirements and functionalities. Section 5 presents the Conclusions and Future Work.

2 IoT Lab platform architecture – Development overview

This Section provides an overview of the IoT Lab platform development. The final platform architecture is in line with initial and updated architectures as well as with the planned architectural components as set during the first two years of the platform development.

The platform architecture design followed the guidance and recommendations established in the IoT-A Architecture Reference Model [2]. The Functional and Information view diagrams of this architecture originated in Y1 and illustrated below.

The Functional view of the IoT Lab architecture (Figure 2) shows the platform's main functional blocks and components.

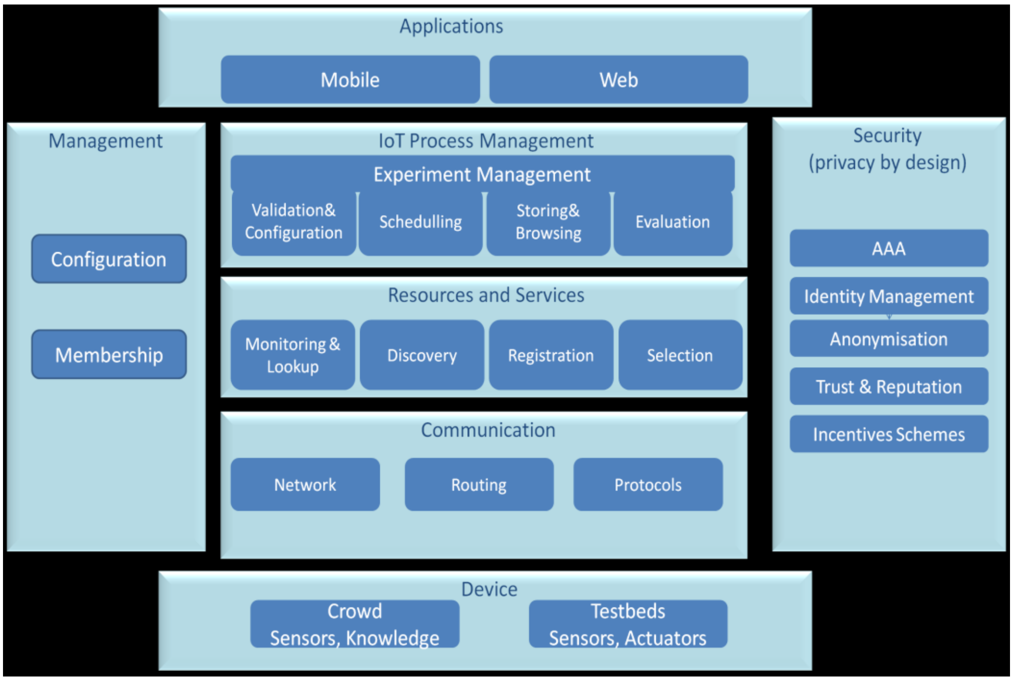


Figure 2: Functional view of IoT Lab architecture

The flow of data and interaction/dependency of the components in a general IoT Lab use case is illustrated by the information flow view presented in Figure 3. The actions involved include:

1. User registration/login
2. Post experiment to the validation and configuration component
3. Retrieve matched resources
4. Request for resource reservation
5. Data collection (crowdsourcing and crowdsensing data)
6. Experiment data analysis

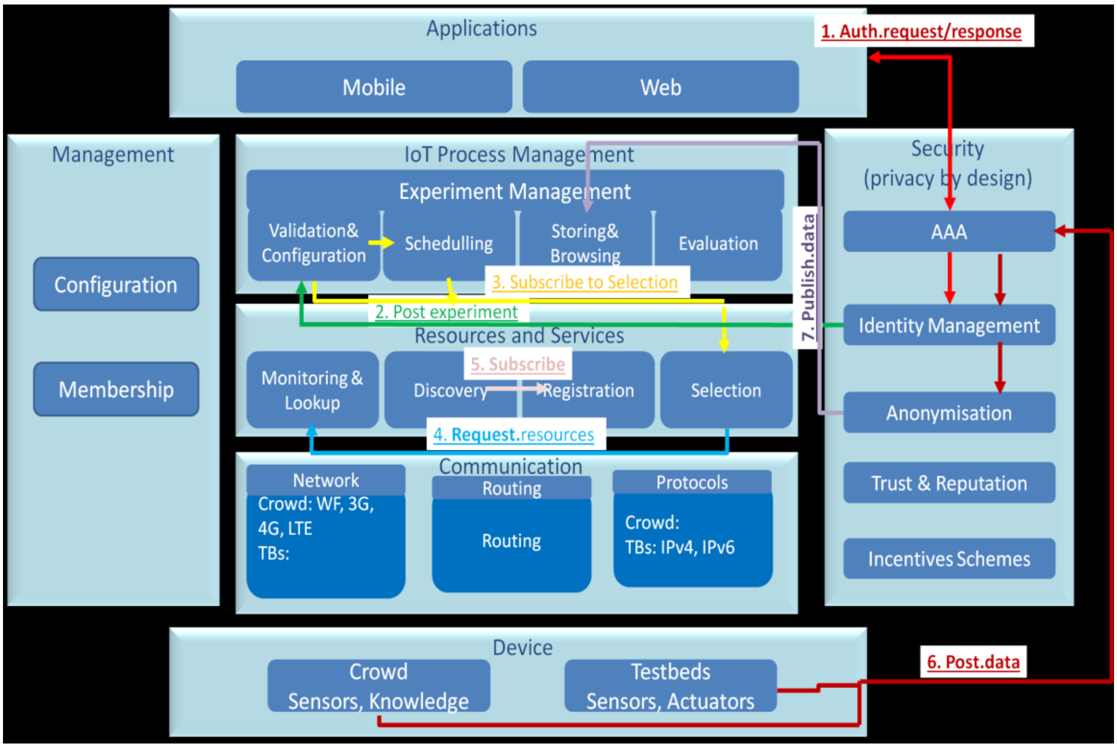


Figure 3: IoT Lab: Information flow view

A detailed analysis of requirements is performed through a range of representative use cases proposed in Y1 and Y2. These interactions and data flows based on the IoT-A diagrams in Figure 3 above resulted in a Deployment View as seen in Figure 4 of the concrete architecture proposed at the end of Y2 in D1.3 Updated IoT Lab Architecture and Component Specification. This provided a reference point for the further development, refinement and implementation of components carried out in Y3 (components not implemented in first two years are marked yellow).

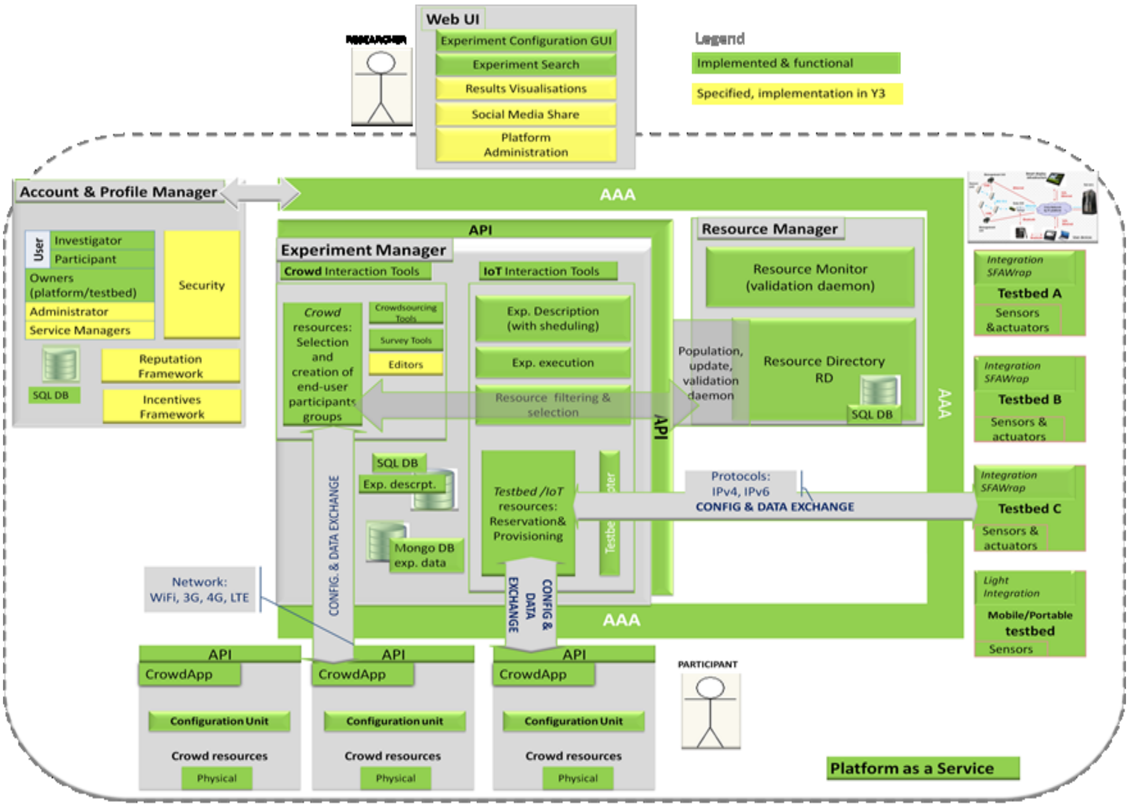
The key components identified at the top-level view of the platform are:

- **IoT Lab Accounts Manager**: Sets-up and manages the participants' accounts, including personal accounts and role-based access to the platform.
- **IoT Resources Management Interface**: Based on Fed4FIRE enablers enabling interactions with IoT components from various types of testbeds and smart phones.
- **Crowd Interaction Management Interface**: Handles the interaction with participants, including tools to set up a survey, design ad hoc experimentation GUI, and access to collected data, etc. This part is completely independent from Fed4FIRE.

Our approach and activities undertaken in the final iteration of platform development during the final project year are described in the next section. The focus is on:

- Development and implementation work towards deployment of all remaining architectural components and update of existing ones.

- Continuous alignment with the main principles as described in Section 0 focusing on privacy by design.
- Integration of the whole system to meet requirements of all planned used cases including the ones implemented in Y3 and to address feedback received from users of the platform.



Note: There is only one SQL DB which stores data related to all resources and experiment description. For visual purposes it is presented on this figure as 3 separate DBs.

Figure 4: IoT Lab Architecture – A Deployment view and implementation status of the Y2 architecture (marked yellow missing components)

3 IoT Lab platform - Development principles and activities

The development principles followed during Y2 have also been followed in this final year of platform development. The identified gaps have been addressed to meet the latest set of requirements. The aspects of the platform that required special considerations were:

- Privacy by design
- Support of selected set of representative Use Cases
- Integration of heterogeneous technologies
- FIRE compliance
- Platform modularity and architectural extensions
- Support for incentives and motivators

Some of the specific requirements also considered in the platform development include: ad-hoc organised dynamic setup of the experiments' infrastructure and resource scheduling among multiple users.

The following sub-sections provide the final status of each of the above points and their effect on the final IoT Lab platform architecture.

3.1 Privacy by design

A key priority during Y3 of the project has been to ensure that the architecture was fully compliant with the privacy by design approach. WP2 performed a detailed and systematic analysis of potential risks related to personal data protection. The adoption of the General Data Protection Regulation (GDPR) in April 2016 has been carefully analyzed and studied in order to ensure complete compliance.

Privacy by design is ensured through concepts of full transparency, prior informed consent, the Right to be Forgotten and anonymity definition.

The architecture is now aligned with the adopted strategy, which consists in differentiating the crowd participants' data process from the research data process as explained in D2.3 Identity Management and Reputation Mechanisms Report. The former is intended to be fully and irreversibly anonymized, while the latter is publicly visible for transparency requirements. Hence, support for the users' privacy protection is approached from two sides: the crowd side (anonymized) and the researcher side (including any other stakeholder providing the personal data to the platform).

In order to fully align with the privacy by design approach the following had to be ensured for each side:

Crowd participants: Data provided by the crowd is effectively anonymous which means that no identifying information about the participant can be entered or stored on a platform. Interfaces accepting direct input from users do not ask for any identifying information about them. Furthermore, the collection of personal data through any indirect means, such as surveys is forbidden and the community is invited to report any breach of this obligation to the platform administrator.

Researchers and other stakeholders: It is considered by the platform that the crowd has the right to get clear and transparent information about the leaders of the researches that they wish to join. The personal data obligation applies in this case to researchers and any other stakeholders who would provide the personal data to the platform.

Data considered as sensitive by the platform are listed in Table 1 below together with the measures that have been undertaken to ensure privacy protection. Detailed analysis of privacy risks is provided in D2.3 Identity Management and Reputation Mechanisms Report and the most important ones are listed below.

Table 1: Privacy by design: Sensitive data and protection measures

No	Sensitive data/communication	Protection measures
1	Personal identifiers: Phone number, email address, name, postal address, MAC address, IP address.	Not requested/stored in IoT Lab database. Shared obligation not to request any of these data and in case of any breach of this obligation to inform the IoT Lab platform immediately.
2	IP addresses: • There is potential risk to identify person through IP address. • Useful for getting approximate geolocation.	There is no IP address stored in the IoT Lab database. ▪ An anonymous token is stored in a database to enable any communication between the user and the platform. ▪ Anonymization of IP addresses through telco operators (access possible only to *“NATed”* IP addresses). LimeSurvey can collect IP addresses. However: ▪ Logged IP addresses are the ones of the network operator, which are natting and hiding the mobile phone IP addresses. ▪ Logging IP address is optional. ▪ IoT Lab can prevent any collection by running a script that deletes all collected IP addresses when a survey is posted.
3	Socio-economic profile of users stored in a DB that can be considered as sensitive data.	Can be deleted based on user’s request from the mobile app.
4	Mobile phone ID.	Use of unique database identifiers that cannot be linked to a physical user by reasonable means.
5	Participants’ sensor data that could indirectly expose his/her identity following the data analysis (spatial and temporal correlations) and in combination with other data.	Altering participants’ data through randomisation and generalization techniques

6	Collection of GPS location of participants.	Platform ensures a low enough granularity of collected geo-location to prevent any identification of participant but at the same time high enough to provide useful data for the researcher.
7	Mobile app settings.	Default options set to opted-out preventing any data collection.
8	Enabled sensors in mobile app.	Notification automatically sent to the users.
9	Sensors started to be used in experiment.	Notification automatically sent to the users – use of slice based consent.
10	Collection biometric data (face, heart rate)	Platform is not designed to handle biometric data which was a strategic decision.

3.1.1 Other aspects of trustworthiness

In addition to providing support for the users' privacy protection, IoT Lab platform has also provided support for the following:

- **Open data**
  The IoT Lab consortium decided not to authorize sharing any data from third parties collected from the crowd smart devices and their belonging sensors, which is in line with requirements for the personal data protection and participant's consent with respect to data re-use. Data collected from testbeds (not from crowd) can be made available to third parties.
- **IPR policy**
  Experiments performed on IoT Lab are likely to generate Intellectual Property that may be protected. A clear IPR policy and strategy has been adopted that ensures that results of researches developed with IoT Lab can be freely exploited by SMEs and industrial partners:
  - Each experiment provides a clear description of its objectives and discloses the lead researcher in charge of it, including its expected exploitation results.
  - Each participant can choose, filter and control to what experiments he/she will contribute.
  - Each participant is free to use or not use the application. A clear prior informed consent process is stated, which explains that the data provided to the platform, once anonymized, are given away to the researchers, including the exploitation of any innovation based on the research results.

If the research developed and performed on IoT Lab platform generates IPR and the researcher is not interested in protecting or exploiting it, IoT Lab association can do it for them. IoT Lab platform will also encourage transparent access to the research results and make available non-sensitive results as openly accessible as possible.

- **Right to be Forgotten**
  The Right to Be Forgotten is also supported for the mobile app users, which can request it, and have certain data deleted so that third persons can no longer trace them as if they never participated in the platform.

3.2 *Use cases support*

In addition to finalizing development and implementation of a number of remaining platform components, Y3 had also a great deal of activities related to the fine tuning of the platform components to provide support for the use cases' realization. These use cases were proposed in Y2 to be used as a validation vehicle for the platform and demonstrate its value to potential users.

The implemented use cases and identified special requirements are listed in Table 2 including the implementation status of the listed requirements.

Table 2: Use cases and special requirements

Use case description	Special Requirements	Implementation status
Energy efficiency This use case is set in a building in which the building manager aims to incentivize the crowd to provide their smartphone sensor data during a time window in order to properly configure the room/building device actuators and achieve a high level of both energy efficiency and user comfort in a room/building.	• Survey composition within the Web portal • Resource filtering • Survey list creation • Incentive mechanism in place • Triggering location data and sending to the database	All requirements implemented
Smart Hepia This use case aims to find new innovative scenarios concerning the building energy efficiency using the ideas provided by the HEPIA students through the mobile application and to apply these scenarios using the TBaaS.	• IoT Lab platform administrator account • Survey composition within the Web portal • Pushing a survey to a list of users • Proposition of new ideas • Evaluation of the new ideas • Download of experiments results • QR code for the mobile application • Geo-fencing for the mobile app • French translation of the mobile app • Cancellation of a resource reservation • Cancellation of an experimentation	All requirements implemented
Brewery This use case took place in the premises of the largest beer factory of the Balkan area. It focuses on energy efficiency via	• Cancellation of an experiment • Download of experimental results • Integration of client type resources	All requirements implemented

indoor lights actuation based on external environmental conditions (e.g. sunlight)	• Associate resources with users	
ekoNET Novi Sad This use case aims to understand the correlation between the air quality in cities and people's emotions including their subjective perception of air quality	• Survey and experiment composition • Filtering users via research code • Pushing survey to selected group of participants • Sharing GPS location at the time of survey submission • Relating survey responses with socio-economic data • Merging survey and sensor data	All requirements implemented
Jumpology This use case has two purposes. Firstly, to test the test process when implementing a test that involves the mobile application, a survey and the TBaaS system. Here, the objective was to promote the system and the test to an unknown crowd of users to see identify adoption opportunities and barriers. Secondly, this use case aims at understanding human behavior and actual practice in the case of jumping.	• Identifying invited crowd through identification: Unique research project identification numbers to be used as identificator of crowd • Selecting invited crowd, and inviting them in different rounds of experiment • Selecting crowd with a specific socio-economic profile (from the invited people) • Adding/removing participants to an ongoing experiment • Testing the survey and the experiments before it is launched to the participants. • Packaging the research project as a whole, containing sensors, questionnaires, users and descriptions to be sent to the mobile application • Communicating with crowd by pushing information related to the experiment • Combining sensor data with socio-economic profile • Follow up of e.g. drop-outs, data sharing, survey answers from the crowd	All requirements implemented

3.3 Integration of heterogeneous technologies

The RESTful nature of developed and implemented APIs allows their ease of use and adoption. This has been proven by the ease of integrating new testbeds within the platform and through the handling of multi-disciplinary resources ranging from mobile phones to low power sensor motes. The platform currently unifies four static testbeds under the IoT Lab flag provided by CTI, UNIGE, UNIS and MI, all of them using a different technology as described in D1.2. In addition to the static testbeds, the mobile and portable ekoNET testbed has a moving sensor network mounted on a city bus to monitor air pollution, which is federated along with a number of mobile phones based on an Android application. All these resources are handled in the same way.

MI contributed to further develop and extend the platform to heterogeneous IoT devices using diverse communication protocols by using the Universal Device Gateway (UDG) framework. It also contributed to extend the HEPIA testbed with both sensing and actuation mechanisms on a smart building environment.

The architecture of the main four testbeds is provided in the Y1 document D1.2, whilst the ekoNET testbed architecture and integration process is provided in D3.2 [3] and D7.2 [4] respectively. A brief description of the mobile application is provided below.

3.3.1 Mobile phone resources

The mobile phone application has been restricted for the duration of the project to the Android platform. This design choice has limited any integration of interoperation issues that usually occur when using different platforms. The development of iOS and other mobile platforms is anticipated in order to allow a wider range of participants. In this case, the IoT Lab architecture defines system independent APIs so that it will ensure interoperability between the testbed(s) backend(s) and mobile devices.

A detailed definition of requirements for devices to be used in IoT Lab experiments is provided in D3.3 [5].

3.4 Alignment with FIRE platforms and projects

Fed4FIRE provides a set of tools enabling easy configuration and execution of experimental set-ups on a wide range of Fed4FIRE testbeds. These testbeds cover various technology domains including, but not limited to cloud computing, wireless and wired networking, sensor networks, and software defined networking. Fed4FIRE testbeds can be fully operated remotely, where the only technical requirement for experimenters is to have standard Internet connectivity.

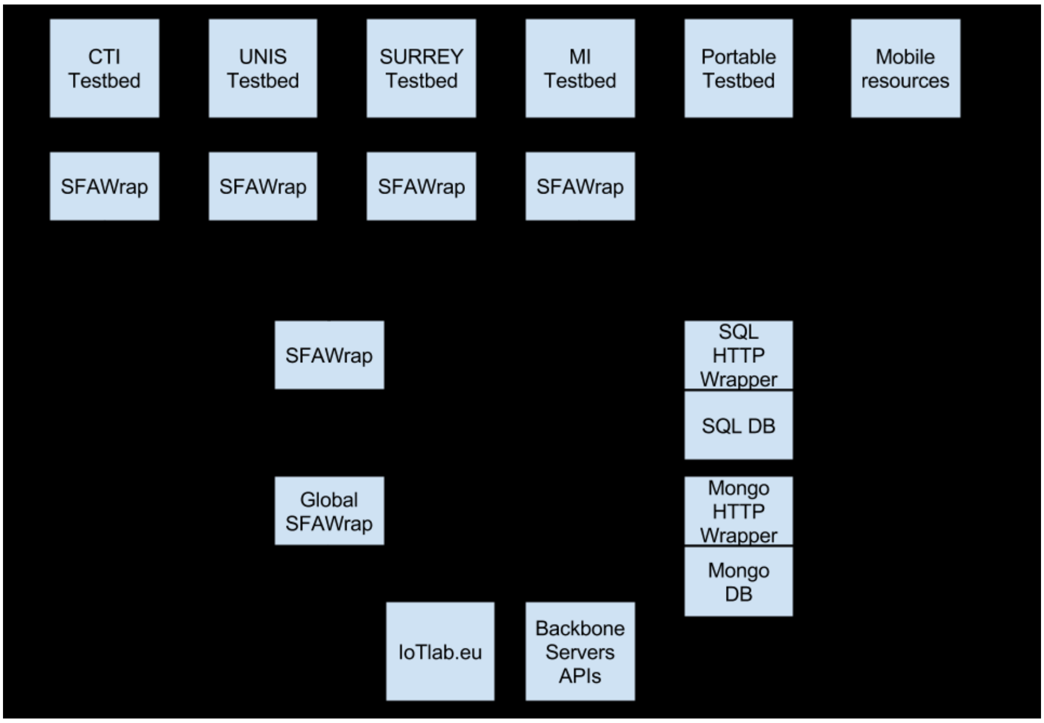


Figure 5: Overview of the IoT Lab architecture defining the federation strategy. The platform components are depicted.

Fed4FIRE offers three degrees of federation: associated, light and advance. The current IoT Lab architecture opts for a light federation with the option of moving towards an advanced one in the future. To achieve this light degree of federation, it is required to accept all certified Fed4FIRE users into the IoT Lab platform and give them an access to a subpart of IoT Lab functionalities. From the federation provided tools and architectural concepts, IoT Lab uses the Aggregate Manager (AM) as a way to discover resources, RSpec to describe them and the SFI client to populate the SQL resource database. The Aggregate Manager's compatibility with Fed4FIRE standards was tested with jFed tools provided by the Fed4FIRE federation as described in D7.2 Intermediary Integration and Tests Report. The IoT Lab also uses SFA Wrap as a layer between the static testbeds and database and as a layer between the platform and the Fed4FIRE community. The global SFA Wrap, as shown in Figure 5, advertises all IoT Lab resources - static testbeds, portable testbeds and mobile phone devices.

IoT Lab has maintained an ongoing collaboration with Fed4FIRE and has initiated two joint projects that will support the ongoing convergence between IoT Lab and Fed4FIRE architecture:

- F-Interop: F-Interop (www.f-interop.eu) is a three years H2020 European research project. It is researching and developing online interoperability and performance test tools supporting emerging IoT-related technologies from standardization to market. It intends to support researchers, product development by SME, and standardization processes. It brings together IoT Lab, Fed4FIRE and OneLab testbeds into a common interoperable framework for testbed as a service.
- Fed4FIRE+: Fed4FIRE is a 5 years H2020 research project that will start in January 2017 of which MI is a partner. It will support the convergence and integration of the IoT Lab platform with the mainstream Fed4FIRE architecture.

3.5 Platform modularity and architectural extensions

A modular architecture enables the evolution of individual components without impacting the whole architecture.

IoT Lab uses the RSpec format for establishing communication and exchanging information among its various modules. Initially, the RSpec format was designed to address the needs of testbed facilities that focus on regular computer networks. However, the IoT Lab provisions resources whose nature greatly differs. In particular, the entire IoT Lab platform federated testbeds focuses on the domain of IoT and Smart Buildings and provisions crowdsourced resources, i.e. devices and sensors that are provided by the general public; e.g. smartphones and tablets. IoT Lab also provisions experiments that are conducted in the form of surveys and questionnaires. The initial definition of the RSpec format could not effectively address the ephemeral and ad-hoc nature of such resources.

In order to mitigate this issue, we have extended RSpec to support the description of IoT resources by incorporating the IPSO Application Framework (IPSO AF) [6]. IPSO AF defines a RESTful design for use in IP smart object systems such as Home Automation, Building Automation and other M2M applications. This design defines sets of REST interfaces that could be used by a smart object to represent its available resources, interact with other smart objects and backend services.

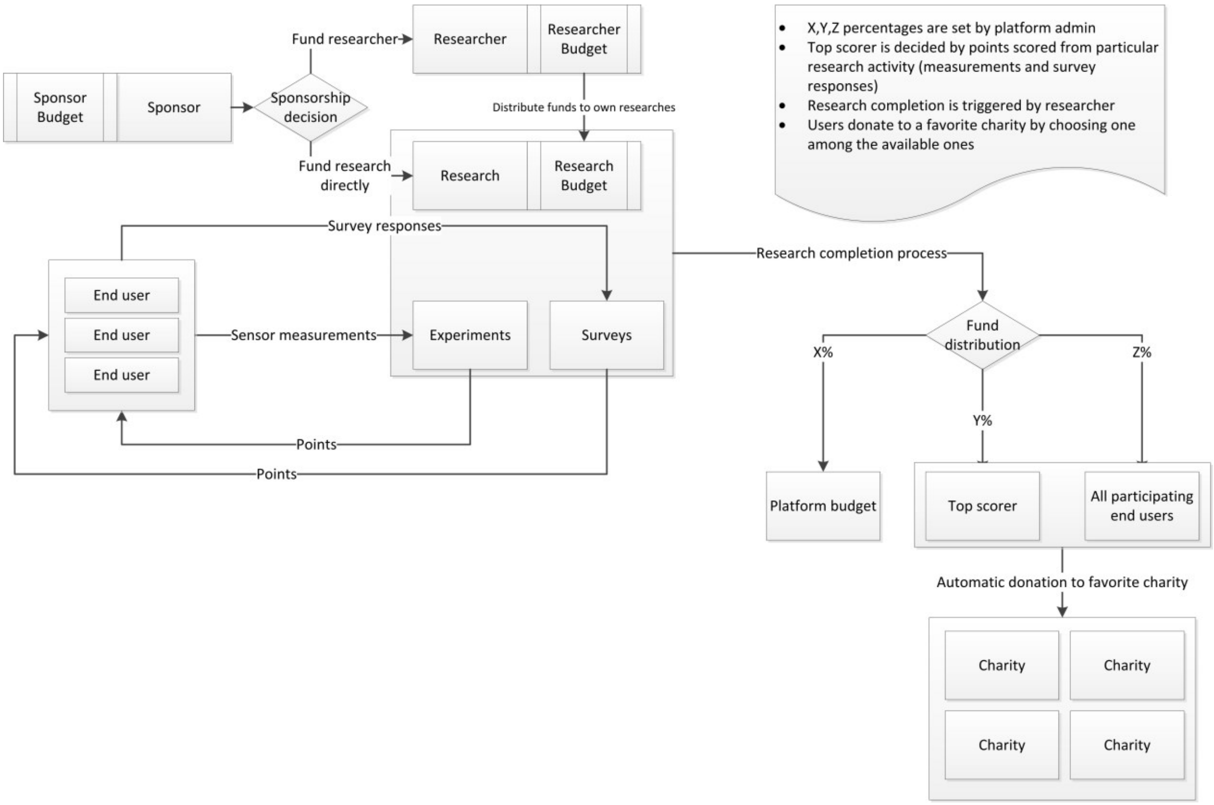
While the components are able to exchange information with each other with the use of RSpec documents, they expose their functionalities via RESTful APIs and Web services at the same time. This way, the particular implementation details of each component are hidden, thus obfuscating any changes that may take place as part of their evolvement in the IoT Lab platform. As an example, the Measurements Database (the database where all collected data is being stored) was initially designed as a relational database. However, it has proven to be a wrong design decision due to the fact that as a relational database, it needed to become extremely complex and difficult to maintain. Thus, we opted to change the underlying technology and port the database in a NoSQL technology, which was a radical change. We used MongoDB over other popular choices such as Redis, Cassandra and ElasticSearch. IoT interactions and data management need a variety of dynamic queries. In addition, as the platform grew, the size of the data collected grew as well. For these two reasons, namely the need for variety of dynamic queries and performance over a large database we selected MongoDB. However, as the services and the functionalities were exposed as a set of function calls, this change did not propagate to other components of the IoT Lab platform that accessed the DB (database); e.g. the mobile application. Figure 5, already shown in Section 0, depicts the components of the IoT Lab platform and how they are connected in terms of information and services exchange. Further details on the federation strategy and the particular mechanisms developed can be found in D4.2 Mixed testbed and Testbed as a Service report.

3.6 Support for incentives and motivators

In order to better motivate the crowd to participate in the experimentation process of IoT Lab, we performed an extensive study on motivators and incentives as part of WP5 End User and Societal Added Value Analysis and WP6 Economic and Business Opportunity Analysis. As an outcome of the survey on motivators [7] made by WP5, it is clear that both intrinsic and extrinsic types of motivators are relevant to the crowd. Therefore, IoT Lab architecture is designed to support both types of incentives. WP6 [8] suggests following a hybrid approach where a sponsor allocates a budget to a research directly or to a researcher who can then freely distribute these funds to their researches, but research participants are not directly rewarded by this budget. They have instead the possibility to exchange earned and allocated points for money donations to a charity of their choice. Part of the budget (set by the platform administrator) is used for platform maintenance, whereas the rest is allocated proportionally to the charities based on credits/points distribution.

The diagram in Figure 6 depicts performance of the Incentives Framework as implemented within the IoT Lab platform showing the typical interaction between involved actors/entities namely sponsors, experimenters (researchers), participants and the IoT Lab platform.

In the diagram, the Sponsor finds a research he or she is interested in and supports it by giving a defined contribution. They also have the choice of sponsoring a researcher instead and giving them the freedom to fund their current or future researches with the funds provided. By using the IoT Lab platform, the Sponsor indicates details about his or her contribution and the platform creates the budget for the research and informs the researcher about the details. In this way, the researcher defines or allocates the budget by specifying within the platform the type of actions the participants should perform in order to be given a specific credit. During the research execution and while the crowd is providing data, the IoT Lab platform provides information back to the participants regarding their point gains for performing certain actions. The number of points for specific actions are set by the platform administrator.



- X,Y,Z percentages are set by platform admin
- Top scorer is decided by points scored from particular research activity (measurements and survey responses)
- Research completion is triggered by researcher
- Users donate to a favorite charity by choosing one among the available ones

Figure 6: Incentives framework

Upon completion of a research, the researcher triggers the research completion action. When this is triggered, the platform automatically distributes the available funds for this research to three different recipients: the platform budget for maintenance, the top scorer of all the participating users and to all users proportionally depending on the points gathered. During the lifetime of the particular research, points are given to participating users by having them complete actions (providing sensor measurements and/or providing survey responses). Points are given on a research-basis and are used only for distributing funds upon the end of the research.

In summary, the support for the depicted model for incentives as implemented within the platform is using the following functionalities**:**

- The IoT Lab platform provides ways to allow sponsors to back researches or researchers by providing their contributions to the research projects or researchers.
- The IoT Lab platform provides ways that allow researchers to allocate budgets to their researches, specifying the type of actions and the credits research participants are given for performing those actions.
- The IoT Lab platform provides ways to monitor and record crowd participants' contributions to experiments.

- The IoT Lab has up-to-date information on the contribution of a participant, providing the overall accumulated credits for each of them for a particular research.
- The IoT Lab platform provides ways that allow researchers to distribute the available research funds automatically when a research is finished.
- The IoT Lab platform can execute payments in the form of donations to different charities;

4 Platform integration

Various testbeds have been federated and integrated within the platform and all planned architectural components have been implemented enabling the fully supported experimentation through both crowd and IoT interactions.

As shown in D1.2 and D1.3 on Preliminary and Updated IoT Lab Architecture and Component Specification respectively in Y1 and Y2, the main architectural components of the IoT Lab platform are grouped into following functional units corresponding to the IoT-A Architecture Reference Model [1]:

- Account and Profile Manager
- Resources Manager
- Experiment Manager
- User Interface (Web and Mobile app)
- Testbeds (static, portable/mobile, smartphone and modelled) as devices
- Communication
- Security and Privacy

The following Figure 6 illustrates the final view of the architecture indicating completion of development and the implementation of each functional unit and its corresponding components.

A detailed final description of each functional unit, their components and communication/interaction interfaces is provided in Section 5. All this is a direct result of research and development activities realised in other WPs.

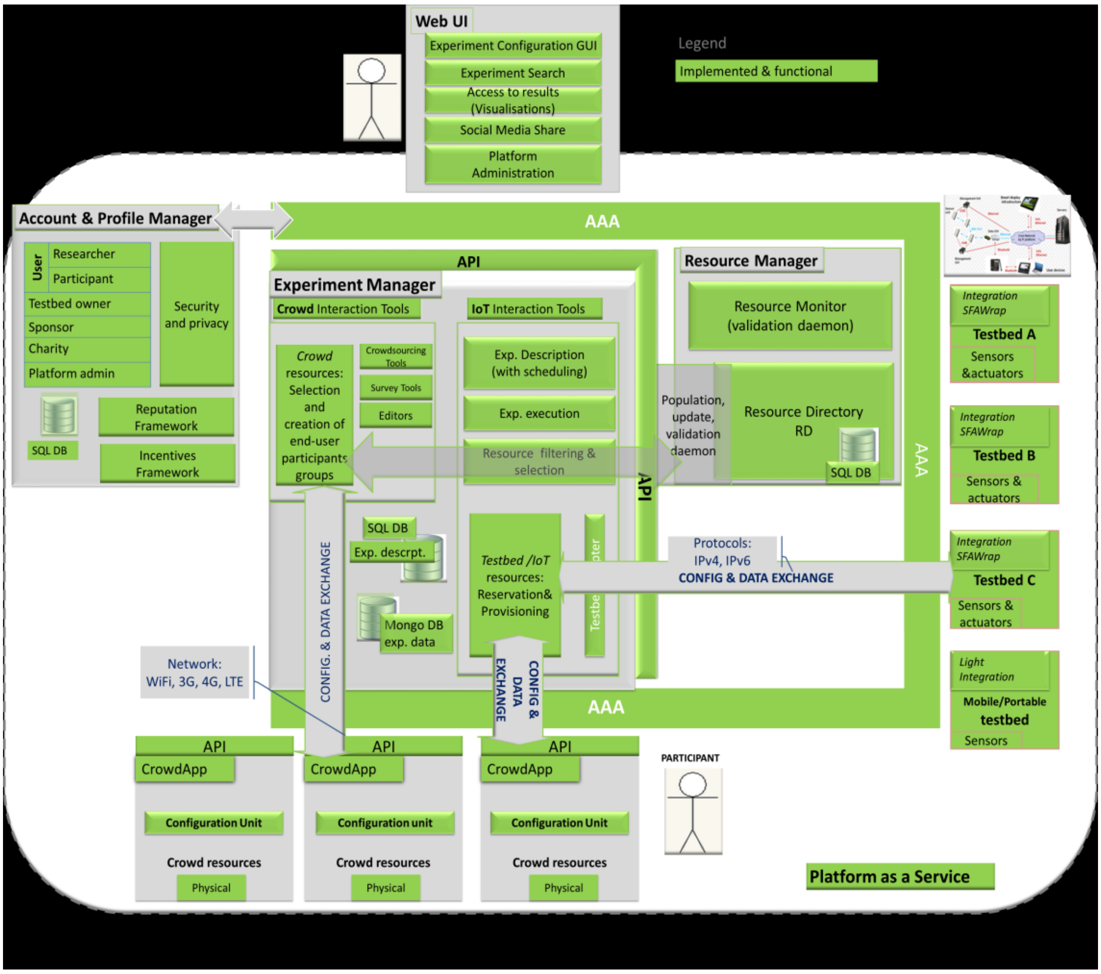


Figure 6: IoT Lab platform. Status of the final platform deployment (all planned functionalities implemented)

5 Architectural Components – Final Development Status

The final status of each functional unit of the IoT Lab Platform is provided in this section. The purpose of each architectural component is described and the available functionalities are listed and explained. Plans for further improvement of each component are also included based on gaps identified through evaluation and validation process as well as the feedback received from users.

5.1 Account & Profile Manager Unit

This unit encompasses the following components:

- User account/profile and identity management with the role based access control
- Security and privacy aspects
- Incentives framework
- Reputation framework

5.1.1 User profile and Identity Management

Purpose	An identity management scheme is implemented with a role-based authentication and authorisation policy. In this scheme, individual identifiers are assigned to all the types of users of the platform that are used for their authentication, authorization and management of privileges across the platform. For all types of users, individual identifiers (username and password) are used by them for accessing the platform. The access rights differ from user to user, depending on the role of the user (e.g. administrator, researcher, participant, sponsor, charity, etc.).
Final implementation status	The distinct roles that a user can have ultimately determine the functionalities and access rights this user has on the system. Each user is assigned a role during registration and this role defines the user's platform access rights for the lifetime of the account. Multiple roles cannot be assigned to a single user account. If this is necessary, then multiple registrations to the platform, one for each role, are required. The existing roles for the IoT Lab platform are the following: ***Crowd participants*** • Can get involved in contributing to the platform (proposing research ideas, providing their mobile device's sensor data, providing data/knowledge/information through their participation in surveys). • Can provide anonymously their socio-economic profiles, which are then made available to researchers to analyse correlations between results and socio-economic dimensions. • Depending on their contributions (e.g. quality and quantity of provided data/information/ideas) to the platform, they receive points and achieve badges that they can exchange for donations to their favorite charities that they selected among an offered list.

- All data/information provided by the users are anonymised by design and thus cannot be linked to them later.

Researchers

- Must be registered to the platform in order to be able to use its resources. This is required to guard against overloading the system with open access to all while it also protects from malicious misuse since researchers are not anonymous.
- Must be registered with their full identities, in order to comply with transparency requirements with the participants.
- Can initiate experiments and execute them either through IoT interactions (experiments that use sensor data, either from fixed/portable testbeds or from the mobile app sensors) or through crowd interactions (refers to compiling and distributing surveys to end-users of targeted socio-economic groups who provide the required information/opinion/knowledge back to the platform).
- Access to all the data collected to support their experiment and research to be able to conduct analysis and report the results.
- Can be recipients of sponsorship funds and be able to allocate them to support their experiments and research goals.

Platform Administrator

- Responsible for the supervision of all activities related to the platform and the management of user accounts.
- Manages all platform user accounts including validation/approval, suspension or rejection of researchers' or other platform users' access to the platform and carrying out a global data deletion request in order to realize the "Right to be Forgotten" functionality requirement.
- Role assumes access to all data produced by experiments, all (current, past and future) experiment resource reservations and surveys from all participating mobile phones and researchers.

Testbed owners

- Role is assigned to users that belong to the entities that make physical testbeds available (universities, companies, foundations etc.) and have been given the right to grant them for use to the IoT Lab platform.
- They are responsible for maintaining their testbed resources in a coherent way, which refers to inserting/updating new resources, and specifying the resource accessibility using related database APIs.
- Access to all the data and reservations of the resources that belong to the specific testbed they own.

	Sponsors • Users who wish to make donations (sponsorships) to specific researchers or directly to researches. When a sponsorship is given to a researcher instead of a research, the researcher can then choose the way the donation will be distributed to his/her researches. • Access to the list of all researchers that applied for donations (with all the relevant data about that researcher and its research) and to a list of all researches that opted for donations (with an access to the research description, objectives, timescale etc.). • Can select a specific research or researcher from the list and donate the money directly via PayPal. • Access to the list of all of his or her sponsored researchers and researches. ***Charity*** • This role is given to users that represent registered charities. Charities have to provide all the information necessary to prove their legal status (formal paperwork, banking information etc.) because, ultimately, they are the intended recipients of sponsorship funds donated to the platform. They also need to provide detailed descriptions of their activities and goals. • The Charity role has no real interaction with the IoT Lab platform but charities appear in a list given to end users from which the end users can select who they would prefer to receive donations because of the end user’s participation in sponsored experiment, following the approval of the charity registration.
Identified gaps/required extensions	Based on individual or group identities and IoT platform utilisation and preference setting, the IoT Lab platform could extract a range of useful statistical information.
WP relation	Updates to the description of this component relates to the Identity Management as result of the work carried out in WP2, Task 2.3.
Further plans	Further extensions/updates/adaptations will be considered from the feedback collected from the platform evaluation and validation.

5.1.2 Security and Privacy framework

Purpose	The identities of the users are protected against various privacy risks by means of specific measures we have taken, within the context of the overall security of the platform.
Final implementation status	The privacy of user participants is a high priority for the IoT Lab. Our implementation is based on the privacy by design approach, where all data/information provided by the users are anonymised, by default, and thus cannot be linked to them at a later time. • The database is not storing the phone number or IP address of the participant. • For all communications originating from the platform to the participant's mobile device, an anonymous token is stored in the database to enable this communication. • Other personal data that are entered by the user as part of their socio-economic profile are stored in the database but can be deleted at any time from within the mobile application or using the "forget me" functionality. • Each mobile phone connected to the platform is identified through a unique identifier, which cannot be reversed. • The system has been designed to ensure that the database identifier cannot be linked to a physical user through “reasonable means” as stated by the European GDPR (recital 26) and in line with Working Party 29 interpretation in Opinion 5/2014 on anonymization techniques. In order to reduce the effects of the risks on the users and the platform, we have taken a number of security measures. These measures are taken at different levels across the IoT Lab system: • Security of Servers (enabled firewalls, disabled ports, strong passwords, updates for the system, backup policy, penetration tools run periodically, etc.). • Data storage security (database access control policies through a username/password based authentication mechanism, several user classes with different database access privileges). • Network security (ports of firewall are closed for all unused services, in cases where remote access to a server is required a demilitarized zone network configuration is employed and Intrusion Detection System tools are used). • Security at the application level including secure communication (developers follow all the customary, important security guidelines recommended by experts for the development of the IoT platform applications and services).
WP relation	Updates to the description of this component relate to Protection of Identities as result of the work carried out in WP2, Task 2.3. The risks we have to handle are presented in depth in D2.3, where a systematic risk analysis is presented for the most common identified

	threats.
Further plans	Further extensions/updates/adaptations will be considered from the feedback collected from the platform evaluation and validation.

5.1.3 Incentives Framework

Purpose	The purpose of this component is to increase the number of participants and their motivation for participating in the research process. Therefore, the IoT Lab platform provides functionalities that allow the use of motivators both intrinsic and extrinsic in exchange for their participation in researches.
Final implementation status	The Incentives Framework has been implemented following a simple and elegant approach. The most important of the functionalities have been specified to support the hybrid model identified by WP6, D6.3 as the most applicable to the platform. The functionalities of this framework that have been implemented enable: • Sponsors to back a specific research, specifying the amount of their contribution, which is transferred to the platform and allocated to the research. • Sponsors to back specific researchers, effectively giving them the option to distribute funds to their researches as they best see fit • Participants to choose between available charities or their favourite charity and allow automatic donations to them when researches are concluded that include them contributing sensor or survey data. • The participant having access to information regarding his/her contribution(s). • The automatic distribution of funds to participants (and then to their favourite charities) when a research is concluded. This is according to their contribution to each research in a survey and sensor data (weights for each can be set by the platform administrator) and according to percentages that the platform administrator sets for each class (best contributor, all contributors etc.). • The end users to rate the experiments that they have participated in or their experience with the whole platform, through the crowdsourcing tool directly or by answering a survey via their smart device.
WP relation	Design and implementation of this component was directly influenced by the work and results achieved in WP5 and WP6.
Further plans	This component will be further upgraded and fine-tuned in line with the users' requirements/feedback.

5.1.4 Reputation Framework

Purpose	In order to motivate and engage a large number of users to participate in the research process, reputation mechanisms have been developed that can provide more information and statistics about the researchers, participants and the platform performance itself. The main purpose of this component is to monitor the user activity and then estimate the user rating in a semi-automatic way. The reliability rate of the users is calculated for both investigators and participants through different functions and mechanisms.
Final Implementation status	An enumeration of implemented ranking functions follows: • Rating for the Crowd participants, which is calculated from the number of sensors provided to experiments, the number of experiments they have participated in, the surveys they have responded to, the ratings earned for proposing ideas and the research points gathered from application of the Incentive Model. • Rating for the experimenters, which is based on the research projects created using IoT Lab and the number of days the platform is used for running experiments. • Rating for the proposed ideas for new experiments, which is based on the average rating from users, the rating received by users and the idea's 'freshness'. • Rating for the Quality of Service, which is based on the platform's uptime, responsiveness and the amount of up to date resources.
Identified gaps/required extensions	IoT interactions used initially a cache component for mobile phone measurements. As additional experiments and use-cases were proposed with more demanding requirements, the component was discarded. This forced redesigning the Quality of Service rating.
WP relation	The description of this component relates to the work carried out in Task T2.3 in WP2.
Further plans	Further extensions/updates/adaptations will be considered from the feedback collected from the platform evaluation and validation.

5.2 Resource Management Unit

Purpose	This unit is responsible for storing the information about resources and monitoring their status and availability.
Final implementation status	A detailed status of implemented functionalities within this functional unit are: • Resource Directory component, represented by a SQL database and its HTTP Wrapper, as described in D4.2, maintains a description of all resources available in the IoT Lab platform; their type, the way to access or interact with them. It also includes the information on entities and their roles (e.g. testbed provider, researcher, participant, etc.), ongoing research projects and their leaders, status of experiments and participants involved. • SFA Wrap interface, as a Fed4FIRE enabler is used to virtualise static resources of our testbeds whilst the global SFA Wrapper wrapped around the database is used to advertise all integrated resources (static, portable, mobile and crowdsourced resources) to third party entities as shown in Figure 5. • All the information stored in the Resource Directory can be accessed by authorised entities using the corresponding APIs also described in detail in D4.2. • Implemented APIs provide also the advanced functions such as resource filtering based on different criteria (resource type, etc.). • A validation Daemon as described in D4.2. which keeps the real time information on availability of resources in the system. • Resource discovery mechanism able to announce the available resources on testbeds is accomplished by the update and Population Daemons described in D4.2
Identified gaps/required extensions	At this moment, we do not use OML as we opted for the light federation. However, OML may be used in the future, if we plan to pursue a deeper degree of federation.
WP relation	Development and implementation work with databases, integration and virtualisation of resources and APIs performed in WP4, provided an input to this component.
Further plans	Proceed further with alignment with F4F and implement OML for data collection from testbeds and crowdsourced devices.

5.3 Experiment Management Unit

The experiment management unit controls the functioning of two tools, namely the IoT interaction tools and Crowd interaction tools. All the components in the Experiment Manager are accessible through the Experiment Manager RESTful API. The status for each of these tools and their corresponding components are provided below.

5.3.1 IoT Interaction tools

Purpose	The purpose of this tool is to enable conduction of experiments involving resources such as sensors and actuators on static and portable/mobile testbeds or on smart-phone devices that can reliably describe a high number of envisaged scenarios.
Final implementation status	• Experiment Composition Module receives a standardised abstract experiment representation and validates the experiment definition so it can be executed by the Experiment Running Module. • Experiment Composition and Description Module is based on 'if this then that' logical expressions that can define how resources will be used in the specific scenario. • Description of the IoT interaction experiment is stored in the SQL database upon launching the experiment. • Experiments are conducted on top of different testbeds. • No testbed or mobile phone offers the capability to have a code/programme running on them. Their functionalities include taking the measurements as defined in the Experiment Composition Module and pulling the measurements on demand. • As explained in Section 3.2, discovery of new resources is done by the Population Daemon, which takes an RSpec from all testbed resources through the AM of SFA Wrap and then parses it and interacts as necessary with the database. The experiment composition tool gets all active resources directly from the SQL Resource DB. • Reservation and provisioning of testbed resources is performed through the HTTP Wrapper of the SQL database (see D4.2) • All data provided by the experiment is collected in the MongoDB. (see D4.2) • The experimenter has the option of terminating the experiment as discussed in D4.2
Identified gaps/required extensions	Currently, once an experiment involving IoT resources has begun, the experimenter has the option of terminating it, but not to change its parameters whilst running.
WP relation	Development and implementation work with experiment composition, description and execution has been a part of WP4.

Further plans	The creation of a new type of dynamic IoT experiment. Dynamic experiments follow a different life cycle than the current experiment schema. The experimenter will not have to provision mobile sensors beforehand. The crowd will be prompted to join the experiment by scanning a QR code.

5.3.2 Crowd Interaction tools

Purpose	The purpose of this tool is to enable interaction with the crowd through surveys enabling the collection of the crowd knowledge, opinions and information on a specific subject specified in a survey.
Final Implementation status	• The survey tool is implemented and can be used by the researcher. It includes the following functionalities: • Participant/Resource Selection Component uses APIs to detect and select available resources in the SQL database that match the specified query. Participant/resource filtering can be done based on socio-economic profile of participants, their geo-location (geo-fencing) or research code entered by the participant if they wish to take part in a specific experiment. • Exposing the crowd resources: IoT Lab Experimenting Platform exposes crowd resources in a standardised way via SFA Wrap. • The discovery - creation of new mobile resources is done directly through the SQL database (see D2.2) • Crowd Interaction Management Interface handles the interaction with the participants. • All data provided through the survey is saved in LimeSurvey and collected in the MongoDB. (Info D4.2). • Merging IoT Lab data with LimeSurvey data: Socio-economic profile of end users (if available, since they are optional) participating in surveys can be merged with the corresponding responses saved in LimeSurvey tool. • Exchange of messages between the crowd participant and the researcher is available ensuring the full anonymity of the end user participant. • Notifications can be pushed to crowd participants using different filtering options (e.g. geofencing based, research code based etc.).
Identified gaps/required extensions	This tool currently requires a separate user account for accessing the LimeSurvey hosted on the IoT Lab server. An option that will be considered is to provide IoT Lab platform users with the possibility to automatically access the LimeSurvey with IoT Lab credentials.
WP relation	The main inputs for a development of this tool came from activities in WP2 and WP4.
Further plans	Further extensions/updates/adaptations will be considered from the

	feedback collected from the platform evaluation and validation.

5.4 User Interface - End User Application Layer

Users of IoT Lab platform can access the platform and its functionalities in two ways, using:

- Web application
- Mobile application

5.4.1 Web App User Interface

Purpose	This component enables the IoT Lab user to interact with the IoT Lab platform (TBaaS) through the Web GUI. It is meant to be used by users having different roles such as IoT Lab researchers, platform administrators, testbed owners and sponsors.
Implementation status	The current list of functionalities implemented per each role is: ***Researcher:*** • Registration/login • Research project profile creation • Survey creation • Participants group creation • Pushing survey towards all; a selected group of participants and/or geographic area • Pushing notifications • Select and reserve new resources • Experiment composition and execution at the back end of the platform • Data/results storage in the measurement DB (MongoDB) • Access to results (raw data) • Export of experimental and survey data into excel format where they can be visualised • Update for testbed resources ***Platform administrator*** • Management of researches, researchers and other users' accounts • Management of experiments • Management of incentives – platform settings ***Testbed Owners***

	• Management of their testbed resources and reservations ***Sponsors*** • Money donations to selected researchers or researches ***All*** • Search for ongoing researches and access to results were provided • Social media share of interesting researches/experiments to increase the platform visibility
WP relation	Implementation of these components is related to the work and results achieved in WP4 (APIs development).
Further plans	Further extensions/updates/adaptations will be considered from the feedback collected from the platform evaluation and validation.

5.4.2 Mobile App User Interface

Purpose	This component enables the IoT Lab user to interact with the IoT Lab platform (TBaaS) through the mobile app GUI as a participant.
Full implementation status	These are the functionalities for the end-user participant: • Validation of terms of use • Personal data protection through anonymization • Optional socio economic profile • User defined control settings (defining a degree of involvement in the experiment) • Notification icon if any sensor data collection is ongoing • Proposal of research ideas • Voting for research ideas • Checking ranking of ideas • Searching of ideas and researches according to criteria • Participation in research through: ○ Smartphone sensor data provision ○ Survey participation • Access to My Researches • Bi-directional communication with the researcher (without revealing any identity/privacy related data) • Choice of favourite charity
WP relation	Implementation of this component has resulted from the work and activities performed in WP4 (APIs development) and WP2 (crowdsourcing tools).
Further plans	Further extensions/updates will be considered from the feedback from the users.

5.5 Testbeds – Integration and Virtualisation

Purpose	Unification of the resource discovery and reservation process.
Implementation status	All testbeds have been integrated and their resources can be advertised: • Static testbeds have been integrated and virtualised through F4F SFAWrap • Mobile testbed ekoNET lightly integrated • Crowdsourcing devices (smartphones) • Modelled testbeds and virtual resources All registered resources are stored in a SQL database.
WP relation	This work resulted from activities in WP3, WP4 and WP7.
Further plans	Feedback from implemented use cases will provide input for required extensions/updates.

5.6 Support for end-user feedback

Purpose	To improve usability and quality of experience for platform users. To align with requirements for the new use cases.
Implementation status	Various channels were provided to ensure feedback from users in order to permanently improve the platform performance and usability, to include new features and functionalities and to improve UX. These include: • Surveys • Use Cases • Direct Messaging from End Users to Researchers (Anonymous) • Feedback to the Website (Email, Forms) • Evaluation Workshops
WP relation	WP5 related evaluation workshops and feedback from both expert and user evaluation, and WP7 test use cases.
Further plans	To continue adapting the platform in co-creation with end users.

6 Conclusions and Future Work

This document presents the final IoT Lab architecture resulting from the work successfully performed in other technical WPs, end-user insights, adopted Incentives Model as well as from the final updated set of requirements resulted from the use cases implemented in Y3.

Novel components and functionalities implemented during this final year include:

- Identity management and role based access control
- Trust management and users' privacy support
- Security framework
- Incentives framework including motivators and rewarding schemes
- Reputation framework

Components implemented in previous stages of the project were updated and upgraded to align with the final set of requirements identified. These components are:

- Resources management
- Experiments management with related tools for IoT and crowd interactions
- User interfaces
- Testbed integration

Work was performed to address the end user feedback received from evaluations workshops.

Architectural adaptations have been performed to address potential privacy concerns identified throughout the platform implementation process and to ensure that privacy by design principles have been followed.

Lessons learned and general feedback from the implementation work, as well as from implemented use case scenarios were also considered as a useful input for future upgrades of the platform.

Future work on platform and developed tools will also include:

- Adaptations to support a deeper degree of federation with Fed4Fire
- Enabling dynamic IoT experiments without need to provision mobile sensors beforehand
- Continuously consider and address the feedback received from users to make the platform more user friendly and adopted by a larger number of people.

References and end-notes

[1] IoT Lab D1.2 & D1.3 – Preliminary/Updated IoT Lab architecture and component specification

[2] IoT-A: Internet of Things – Architecture, www.iot-a.eu/

[3] IoT Lab D3.2 – Mobile testbeds virtualisation report

[4] IoT Lab D7.2 –Intermediary integration and tests report

[5] IoT Lab D3.3 – Modelled testbeds virtualisation report

[6] IPSO Application Framework http://www.ipso-alliance.org/wp-content/uploads/2016/01/draft-ipso-app-framework-04.pdf

[7] Survey on motivators - https://www.surveymonkey.com/r/?sm=IBb4nt0S6fC8pQTHTF5L%2bg%3d%3d

[8] IoT Lab D6.2 – Cost and efficiency monitoring tools

[9] 3G and 4G bandwidths- http://www.diffen.com/difference/3G_vs_4G

[10] 802.11b bandwidth - https://en.wikipedia.org/wiki/IEEE_802.11