D 2.4

Integration with FIRE Infrastructure

v 1.1 / 2015-03-31

Annika Sällström (LTU), Timotheos Kastrinogiannis (VELTI), Adrian Popescu (CEA)

This document provides a specification of the integration of the USEMP tools for FIRE facilities. The report highlights the relevant FIRE initiatives involving end-user data, FIRE integration principles and benefits offered by USEMP tools. Based on the identified requirements for integration by the FIRE initiative IoT Lab, the general structure for the API for USEMP integration with a standalone application is defined.

Project acronym	USEMP
Full title	User Empowerment for Enhanced Online Presence Management
Grant agreement number	611596
Funding scheme	Specific Targeted Research Project (STREP)
Work program topic	Objective ICT-2013.1.7 Future Internet Research Experimentation
Project start date	2013-10-01
Project Duration	36 months
Workpackage	WP2
Deliverable lead org.	LTU
Deliverable type	Report
Authors	Annika Sällström (LTU) Timotheos Kastrinogiannis (VELTI) Adrian Popescu (CEA)
Reviewers	Symeon Papadopoulos (CERTH) Laurence Claeys (iMinds)
Version	1.1
Status	Final
Dissemination level	PU
Due date	2014-09-30
Delivery date	2015-10-29
Revision date	2015-03-31

Version	Changes
0.1	First outline ToC
0.2	FIRE sections included and first definition of USEMP tool integration
0.3	Integration requirements and API specification included
0.4	Final version for internal review
1.0	Final version
1.1	Revised release after EC review

Table of Contents

1. **Introduction** 2
2. **FIRE – Future Internet Research and Experimentation** 3
    2.1. Fire and end-user data 3
        STEER 3
        Experimedia 3
        IoT Lab (www.iotlab.eu) 4
    2.2. FIRE integration mechanism – the IoT Lab example 5
        2.2.1. Testbeds 5
        2.2.2. Virtualization 6
        2.2.3. Interconnection 7
        2.2.4. Integration 7
        2.2.5. Cloudification 7
3. **USEMP tools for FIRE initiatives** 8
    3.1. Overview of the USEMP software 8
    3.2. Privacy aspects in IoT Lab 10
    3.3. Requirements for integration 12
        3.3.1. Alternative 1: Integrate the USEMP software at the IoT Lab application 12
        3.3.2. Alternatives 2 and 3: To download the USEMP software as a separate application and install it in the user browser or embedded in the IoT Lab platform for the privacy officer to use 13
4. **Specification of USEMP APIs for tools integration** 14
5. **Conclusions and future work** 16

Annex 1 17

1. Introduction

The purpose of this deliverable is to describe how FIRE testbeds can integrate and exploit the USEMP-tools in their initiatives involving user-data.

In the first section (Section 2) we introduce the FIRE programme and describe shortly projects in the current portfolio (June 2014) involving end-user data, as well as the more general FIRE integration mechanism.

In section 3 the USEMP tools are briefly introduced and then, the IoT Lab project is described as the prioritized project to capture requirements on the USEMP integration mechanisms. The IoT Lab has been selected as it clearly includes privacy aspects such as personal data collection and storage. It is in a period of its life cycle similar to USEMP (started in Oct 2013) and therefore fits best into the progress of USEMP. The section also details the requirements for integration.

In Section 4 the general structure for the API for USEMP-integration with a standalone application (e.g., smart phone Android app) is defined. Finally in Section 5 conclusions and future work are summarized.

2. FIRE – Future Internet Research and Experimentation

2.1. Fire and end-user data

The FIRE programme[1] (Future Internet Research and Experimentation) started in 2008 and has evolved into a marketplace of interconnected testbed facilities to respond to users' demands when researching and developing networks and services for the Future Internet.

FIRE has two interrelated dimensions:

1) FIRE experimental facility:

This is built to support research for the Future Internet, at different stages of the R&D cycle, based on the design principle of "open coordinated federation of testbeds".

2) FIRE experimentally-driven research:

This focuses on visionary multidisciplinary research, defining the challenges for and taking advantage of the FIRE Experimental Facility, consisting of iterative cycles of research, design and large-scale experimentation of new and innovative network and service architectures and paradigms for the Future Internet from an overall system perspective.

FIRE includes a wide set-up of different testbeds and usage initiatives. Technology domains covered include Internet of Things (IoT), Cloud and Wireless technologies, software-defined networking, etc. [2]

In the area of user privacy and personal data we have identified three FIRE initiatives involving end-user data:

STEER (http://fp7-steer.eu/)

STEER aims to explore the dynamic relationship between social information and networked media through experimentation. STEER addresses this *community-centric digitally-based ecosystem* which we refer to as "*Social Telemedia*", a cross-breeding of social networks and networked media. Social Telemedia will further intensify current societal practices and habits and they will flourish on a new *network middleware framework* that will combine *Social Informatics* and *Content Delivery*. To explore the Social Telemedia cyberspace, STEER has come up with two innovative use cases aspiring to cover the wide spectrum of community interactions that take place among members of dynamically instantiated communities while exploiting, discovering and correlating various forms of information. The uses cases will be deployed in the STEER experimental environment that is comprised of smart houses, ad-hoc communities and mobile devices combined with existing FIRE facilities such as OpenLab and EXPERIMEDIA.

The project started in Oct 2012 and will end in September 2015.

Experimedia (www.experimedia.eu)

[1] http://www.ict-fire.eu/home.html

[2] http://www.ict-fire.eu/home/fire-projects.html

EXPERIMEDIA is a collaborative project aiming to accelerate research, development and exploitation of innovative Future Media Internet products and services through testbeds that support experimentation in the real world which explore new forms of social interaction and experience in online and real world communities EXPERIMEDIA will develop and operate a unique facility that offers researchers what they need for Future Media Internet experimentation. The aim is to explore new forms of social interaction and rich media experiences enabled by the Future Media Internet considering the demands of both online and real-world communities associated with Live Events. This will be achieved by research, development and operation of a unique FIRE facility targeting the Future Media Internet research community working with stakeholders such as venue management, broadcasters, content providers, application developers and service providers.

EXPERIMEDIA has significant user participation within experiments and therefore the systems under test build on many technologies within expected Future Internet systems.

The project ended on Aug 31 2014.

IoT Lab (www.iotlab.eu)

IoT Lab is a FIRE initiative which aims at researching the potential of crowdsourcing to extend IoT testbed infrastructures for multidisciplinary experiments with more end-user interaction.

Crowdsourcing can extend the capacities of existing testbeds with an almost unlimited number of distributed resources, without heavy investment, and with a flexible way to mutualize them. Moreover, crowdsourcing can provide direct interactions with a pool of potential end-users able to provide useful feedback and some sort of “collective intelligence”. It paves the way to a new research paradigm, placing the end-users at the centre of the research process, with a potential new model of “crowdsourcing driven research”.

The project covers several relevant topics including privacy and data ownership by design, reward models, reputation mechanisms, cloudification, quality of end-user experience and citizen involvement including crowdsourcing.

The project brings together technical and human sciences, enabling new multidisciplinary experiments, which address simultaneously the technology, the end-user and its environment. IoT Lab intends to move from traditional confined test bed to an extraverted testbed architecture involving a crowd of users and penetrating the society in its diversity across Europe, and eventually beyond.

The project will adopt a multidisciplinary approach and address issues such as privacy and personal data protection.

The project started in Oct 2013 and will end in Sept 2016

The IoT Lab initiative has been identified by the USEMP consortium as the first priority for USEMP software integration. This choice is determined by convergent objectives with respect to end-user privacy of the two projects but equally by a good synchronization of their lifecycle.

2.2. FIRE integration mechanism – the IoT Lab example

A key aspect in FIRE is the federation model implemented to integrate testbeds, which are also at the core of the IoT lab. Testbeds are experimentation platforms that contain a vast variety of devices and resources that are connected through different network protocols. They can serve many different purposes such as testing new protocols or enabling smart automations.

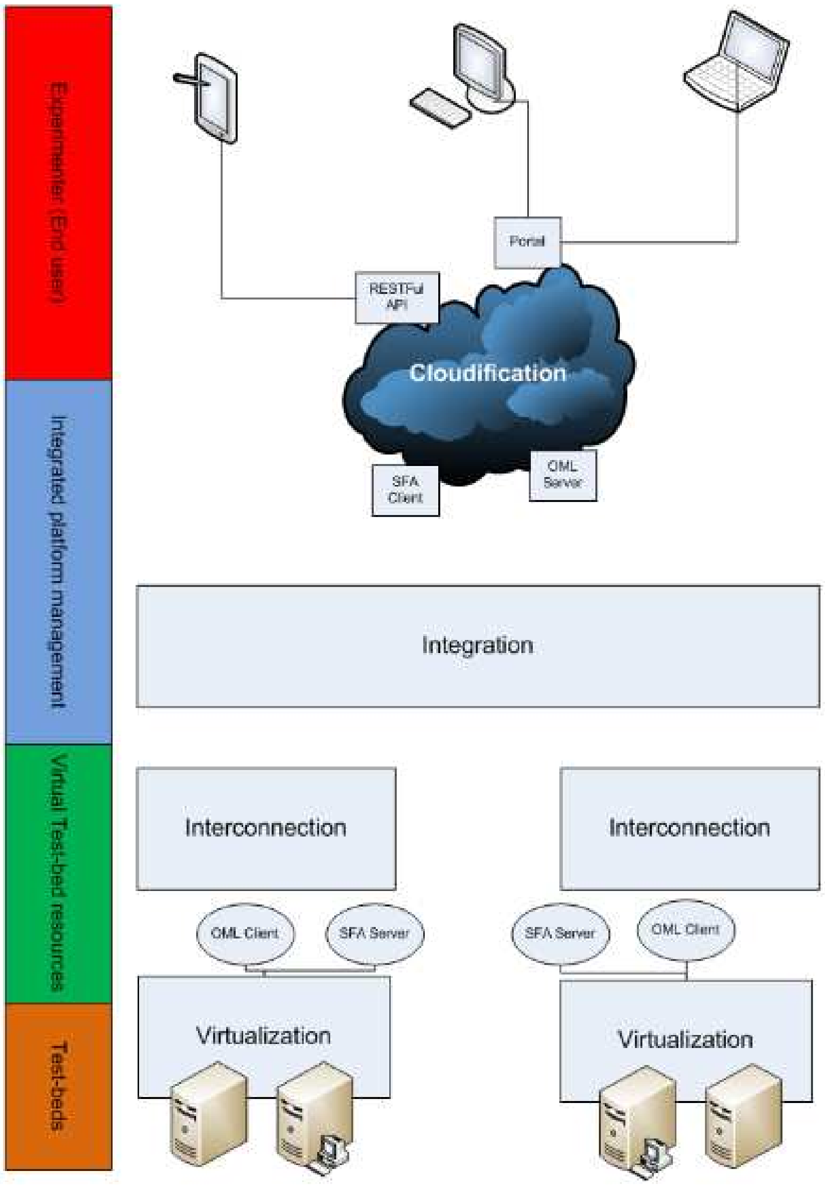

Figure 1.IoT Lab integration mechanism

The general architecture, illustrated in Figure 1, consists of the layers presented hereafter.

2.2.1. Testbeds

Testbeds are the core of IoT Lab. They are experimentation platforms that contain a large variety of devices and resources that are connected through different network protocols.

They can serve many different purposes such as testing new protocols or enabling smart automations.

The IoT Lab consortium gathers several FIRE-related research infrastructures: Hobnet, WISEBED and a Smart Santander node hosted by the University of Surrey, each of them with unique assets for IoT-enabled experimentation.

Hobnet stands for “Holistic Platform Design for Smart Buildings of the Future Internet”. It was set up to research the potential of the new Internet protocol (IPv6) to better manage buildings and reduce their energy consumption.

The WISEBED infrastructure within IoT Lab includes two different sites: the University of Geneva provides a wireless sensor networks for research purposes. This configuration provides the ability to massively and quickly flash nodes on the network using the USB connections as well as gather data and reports from all the nodes without using the wireless medium. The second WISEBED-site is at the Computer Technology Institute & Press "Diophantus" (CTI) consisting of 154 nodes of two different kinds (iSense and TelosB) in 8 rooms. Finally IoT Lab connects the Guildford testbed (a Smart Santnder node) that provides a Smart environment, based on an indoor sensor nodes deployment located in the Centre for Communication Systems Research (CCSR) at the University of Surrey. It serves Smart Campus experimentation.

2.2.2. Virtualization

At this layer a testbed abstraction is available through open interfaces. The resources of each testbed are virtualized in order to be accessible in a unified way. Each testbed uses its own mechanisms for resource discovery and reservation. In order to have the same mechanisms for all testbeds, tools such as SFA Wrap will be implemented on top of the local management system.

Moreover, each testbed will implement tools for data collection, such as OML in order to store and visualize data from experiments and measurements.

All the testbeds will then have the identical methods for resource discovery, reservation and provisioning.

In the case of IoT Lab they will use the ORBIT Measurement Library (OML) - a distributed software framework which enables the collection of data in real time in large distributed environments. OML provides a flexible and dynamic way in which data is collected and made available for real time access to the experimenters of a testbed facility. The OML server collects and stores measurements inside a database. The server is installed in the cloud application and will be assigned to a particular port. Devices that need to store their values or the results of the experiments on the cloud will have to use an OML client to send an OML stream to the server. The server listens on a TCP/IP socket for incoming OML streams.

In the testbeds there are different resources to be used by an experimenter. In IoT Lab they are implementing the Slice Federation Architecture (SFA) that provides a minimal interface to enable the federation of testbeds with different technologies and belonging to different administrators, while granting the control of the resources to their owners. This allows researchers to combine resources available in different testbeds, increasing the scale and diversity of their experiments. SFA is based on a set of high level concepts that define the actors and the resources that interact on the testbed, as well as defining an architecture with its interfaces and main data types to facilitate the federation of testbeds.

SFA is more of a specification of a standard rather than a specific implementation, and as a result there exist several different implementations (PlanetLab, ProtoGENI, OpenFlow). IoT Lab will most probably use the SFA Wrap to be adopted by IoT Lab facilities providers for discovery, reservation and provisioning of the resources of the IoT Lab testbed infrastructures.

2.2.3. Interconnection

At the interconnection layer, the testbeds are connected to a cloud application. The cloud application consists of tools that are capable of communicating with the testbed through the unified protocols and tools (SFA, OML).

2.2.4. Integration

The integration layer manages the input data from all the participating testbeds and then organizes and stores them.

2.2.5. Cloudification

The cloud application is a set of tools that orchestrate all the federated testbeds in order to provide unified access to them. The cloud application will offer to the end user the ability to run experiments on a variety of testbeds regardless of their different hardware and software technologies. Also, it gives control over the resources of each testbed. In other words the cloud application not only contains all the tools and procedures in order to handle the participating testbeds, but is also contains tools to pass that information easily to the end user in a unified way.

3. USEMP tools for FIRE initiatives

3.1. Overview of the USEMP software

The USEMP Platform helps the end users to obtain feedback about their privacy status on social networks or identify potential trackers of the web-based services that service providers deliver and to get insights about the monetary value of their personal data Users' personal and behavioural data generated, explicitly or implicitly, via the web browsers are given as input to the multimedia and social network mining algorithms, which assess potential privacy risks related to data shared on the Web. Based on dimensions which are indicated as potentially sensitive by the user, the outputs of the algorithms present warnings and hints about the user's level of privacy. Through the use of automatic algorithms, USEMP will give OSN users (e.g., Facebook users) improved awareness and control over the content and information they explicitly share online that can be observed and/or can be inferred. This control implies handing the users a series of tools for assessing and changing the visibility of sensitive content towards other users and the availability to the online social network.

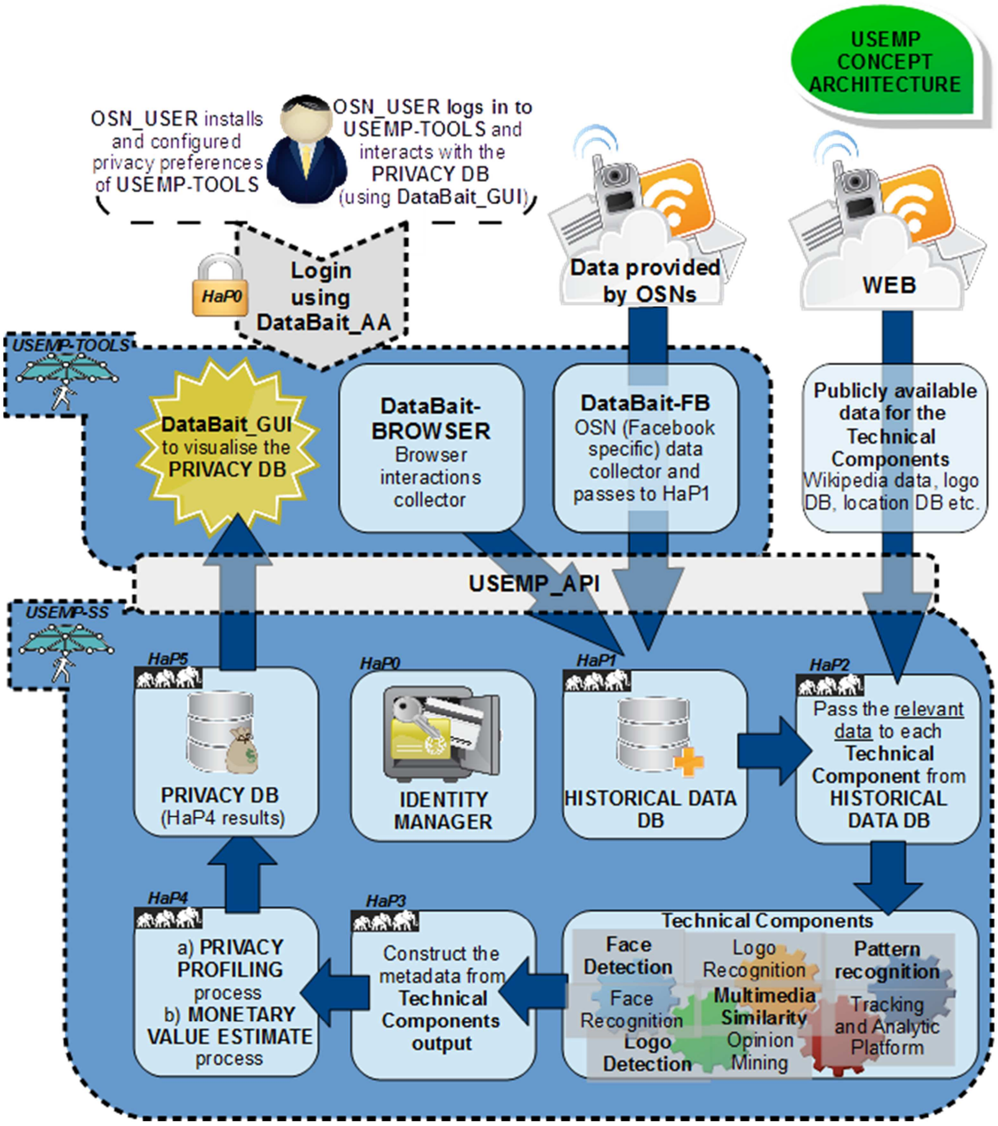
USEMP CONCEPT ARCHITECTURE
OSN_USER installs and configured privacy preferences of USEMP-TOOLS
OSN_USER logs in to USEMP-TOOLS and interacts with the PRIVACY DB (using DataBait_GUI)
HaP0
Login using DataBait_AA
Data provided by OSNs
WEB
USEMP-TOOLS
DataBait_GUI to visualise the PRIVACY DB
DataBait-BROWSER Browser interactions collector
DataBait-FB OSN (Facebook specific) data collector and passes to HaP1
Publicly available data for the Technical Components Wikipedia data, logo DB, location DB etc.
USEMP_API
USEMP-SS
HaP5
PRIVACY DB (HaP4 results)
HaP0
IDENTITY MANAGER
HaP1
HISTORICAL DATA DB
HaP2
Pass the relevant data to each Technical Component from HISTORICAL DATA DB
HaP4
a) PRIVACY PROFILING process b) MONETARY VALUE ESTIMATE process
HaP3
Construct the metadata from Technical Components output
Technical Components
Face Detection
Logo Recognition
Pattern recognition
Face Recognition
Multimedia Similarity
Tracking and Analytic Platform
Logo Detection
Opinion Mining

Figure 2. USEMP Concept Architecture

The USEMP Web Browser software plugin also tracks third party online tracking and analytics services that monitor and collect the end-users' digital trails on their web browser(s), providing them the capability to dynamically disable or enable trackers (i.e., define fine-grained "do not track rules").

In general the end users that generate data are often unaware about how and where their information is used. Hence, they cannot estimate the (monetary) value of their personal data. Another part of the USEMP platform will help the end users to increase their awareness about how their data are used, about the valuation of their personal data as well as the criteria employed to assess and control the level of risk for their privacy.

The USEMP software will be made available through an easy to use application. End users will visit a web application (i.e., via a URL) to sign up to the service. Then they will download and install the software plugin to the web browser for data collection necessary in order to return privacy cues. The *web application* will be used by the end users to access the above mentioned services and features i.e., awareness and control over their personal data, as well as for visualization purposes.

High level steps/functions for a FIRE-specific use case

Post Condition: The USEMP browser software (i.e. plug-in) has been downloaded and installed in the browser of the end user. The latter has been successfully registered at the USEMP platform

1. The user accesses the web application and logs-in to her account.
2. The web sites (or specific domains) that the end user visits are monitored, while the data she uploads (e.g., photos, videos) are collected and analysed, using the above mentioned browser plugin.
3. Based on the collected data, USEMP increases end user awareness about the personal data that have been made available online (e.g., in terms of sensitivity level, time, etc.), identifying potential privacy leaks.
4. The user receives notifications or hints about privacy issues that may arise from a post or from information submitted to a web site, proposing her to apply specific actions.
5. Third party online trackers that monitor and collect the behavior and the digital trail of an end user on her web browser(s) are detected.
6. The user has the capability to dynamically disable or enable the trackers of the web sites that she visits.
7. In general, the user gains useful insights on the value of her digital data that she either directly shares or indirectly collects by various network actors that track her activities on her web browser.

Benefits for involved parties using the USEMP Platform

The **end users** will manage the use of their personal data (e.g., used for marketing, advertising, etc.) in a transparent way and will gain useful insights on the value and potential monetization of their digital personal data. On the other hand, service providers or application publishers will benefit from trust and loyalty that will be built between them and the end users.

3.2. Privacy aspects in IoT Lab

Within the scope of the work of the IoT Lab, the main goal is to develop a crowd sourcing platform that will support the chosen experiment scenarios with suitable privacy preserving mechanisms in order to attract users and assure them regarding the respect of their privacy, i.e. that no personal information beyond the sensed data will be revealed to the experimenters.

Organizing a successful crowd sourcing experiment involves two main tasks: (i) attracting as many volunteers as possible possessing suitable devices equipped with the sensors of interest, and (ii) gathering and processing sensor data which are sufficiently useful and numerous to satisfy the goals of the experiment.

The crowdsourcing participants in IoT Lab, will provide the following information through a Web form channeled over SSH (https) connection to the user's mobile device:

- Pseudonym
- Password
- Optional Email address to be contacted
- Optional basic socio-economic profile.

Those data will be managed as anonymous data and will be used for the socio-economic analysis of the multidisciplinary experiments. The profile could include data such as:

- Gender
- Year of birth (or class of age)
- Education level (such as: elementary school, college, university)
- Professional profile
    - Sector: (such as : Education; Public administration; Company/SME; NGO; other)
    - Position (such as: Director/manager; employee; independent; student; other)
- Country of residency
- Living in: urban area; rural area.

The socio-economic profile will be kept as fully anonymous. The researchers will not access individual profiles, but only the statistics of aggregated results and correlations. The email address will be stored in a separate table from the profile and other collected data in order to enable complete dissociation of data from the email address.

For the IoT Lab, we have identified two specific possibilities for the use of the USEMP tools by two different types of users: the IoT Lab end-users and the IoT Lab privacy officer. The added value for the IoT Lab would be to raise its credibility, trust and confidence level by the end-users.

1. USEMP tools for the IoT Lab end-users

- Track IoT Lab end-users' personal and sensing data generated and/or disseminated via the IoT Lab applications (e.g., Android app). Such data can be real-time and should be fed into the USEMP back-end system.

- Track IoT Lab users (end-users, researchers) personal and/or behavioural data generated via their web browser(s) and feed the latter into the USEMP back-end system via the USEMP API.
- Visualisation of user Privacy Leaks, Privacy Notifications (pop-ups).

2. USEMP tools to be used by the IoT Lab privacy officer [3]

- Identify the IoT Lab users' trackers (e.g., researchers), in terms of 3rd party online tracking and analytics services, that monitor and collect users digital trail on their web browser(s).
- Propose or define fine-grained do not track (DNT) rules.
- Visualisation of user Trackers Identification, filtering and Do Not Track Policies Creations.

IoT Lab alternatives with USEMP software	Advantages	Disadvantages	Benefits for IoT lab users
Integrate the USEMP software with the IoT Lab application	User's personal and sensed data collected in real-time. End users could potentially control the type of data that will provide to the IoT platform.	Large amount of information should be sent to the USEMP back-end. Web applications are not checked. This would require a lot of development efforts	Increase users' awareness and trust towards IoT lab for the usage and value of collected/sensed data.
Download the USEMP software as a separate application and install it at IoT users' browser	Enable users to forbid Specific Online Tracking Services (embedded to a web site) from tracking their personal data. Notification towards informing users (e.g., end-users, researchers) on potential personal data privacy leaks and compromises.	The data collected by standalone applications e.g., Android apps are not taken into account. The end-users do not have actual control on the web apps that researchers use to experiment or view IoT Lab data.	Increase end-users' trust, since the web apps that researchers/experimenters use are monitored regarding web sites trackers and potentially about uploaded pictures/texts.
Use the USEMP software as an internal "watch-dog" embedded in the IoT Lab platform	The IoT Privacy officer is aware about the value of the data of end users as well as about the privacy leaks (e.g., trackers) of the researchers Notification about users (researchers, experimenters) personal data privacy leaks and compromises based on data stored at the IoT lab.	IoT Privacy officer is responsible for informing the users about privacy issues, while the users have no real-time control over their data.	Increase end users confidence for the IoT lab infrastructure, since the IoT privacy officer is aware about privacy issues related to the end users and the researchers.

Table 1. Summary different alternatives for IoT Lab with the USEMP software

[3] The IoT Lab privacy officer is a person in charge to protect IoT Lab users from privacy violation

In Table 1, we summarize the different advantages, disadvantages and benefits from the three different alternatives identified for integration of USEMP with the IoT Lab platform:

- 1st Alternative: Integrate the USEMP software at IoT Lab application.
- 2nd Alternative: The IoT Lab users (e.g., end user, researchers) download the USEMP software as a separate application and install it at his/her browser.

3rd Alternative: Use the USEMP software as an internal "watch-dog" embedded in the IoT Lab platform to ensure that neither the researcher nor the experimenter is transmitting personal/private data. This would be a tool for the Privacy officer of IoT.

3.3. Requirements for integration

The integration between the USEMP software and the IoT Lab infrastructure is driven by the privacy needs that arise in the context of the IoT Lab, as described in the previous section. Taking into consideration the above, three alternatives have been identified as requirements for the integration of the USEMP software with the IoT lab infrastructure.

3.3.1. Alternative 1: Integrate the USEMP software at the IoT Lab application

The following technical and functional requirements have been identified for the first alternative:

IoT Lab

- o Provide the structure and the data model of the IoT Lab monitoring data.
- o Associate the monitored data with each specific user.
- o Registration to the USEMP platform in order to receive USEMP credentials.
- o Develop and integrate the login functionality for the authentication and authorization with USEMP credentials.
- o Transmit monitored/sensed data to the USEMP back-end functionality.
- o The output of the USEMP processing (e.g., privacy leaks, behaviours identifications) could be visualized from the USEMP web platform.

USEMP

- o Provide a communication stream between the USEMP back-end infrastructure and the IoT Lab for the transmission of data that IoT Lab applications monitor or provide (extend the USEMP API).
- o Study the collected data by the IoT Lab in order to discover the type and categories of personal or behavioural information.
- o Adapt USEMP algorithms (i.e., training) based on the structure of the IoT Lab data.
- o Update of the USEMP metadata that is he output of the USEMP Technical components.

3.3.2. Alternatives 2 and 3: To download the USEMP software as a separate application and install it in the user browser or embedded in the IoT Lab platform for the privacy officer to use

The following technical and functional requirements have been identified for the second and the third alternative:

IoT Lab

- Provide the URLs of web pages for the case that publicly available information is used by the IoT Lab.
- Indicate the domains that should be filtered by the USEMP browser plugin.
- Registration to the USEMP platform in order to receive USEMP credentials.
- The output of the USEMP processing (e.g., trackers and control over identified trackers) could be visualized from the USEMP web platform as well as directly from the Browser plugin.

USEMP

- Adapt the USEMP browser plugin in order to filter the specific domain or URLs that are used by the IoT Lab infrastructure.

Update of the USEMP metadata that is the output of the USEMP Technical components.

4. Specification of USEMP APIs for tools integration

In the case of a web-based application there is no need for the specification of any API between the USEMP applications and the IoT Lab. In this case all necessary information will be retrieved by the web browser add-on that will be installed as described above. A browser plug-in or add-on, is a computer program that extends the functionality of a web browser in some way (Figure 3).The output of USEMP processing will be available through the USEMP web-site.

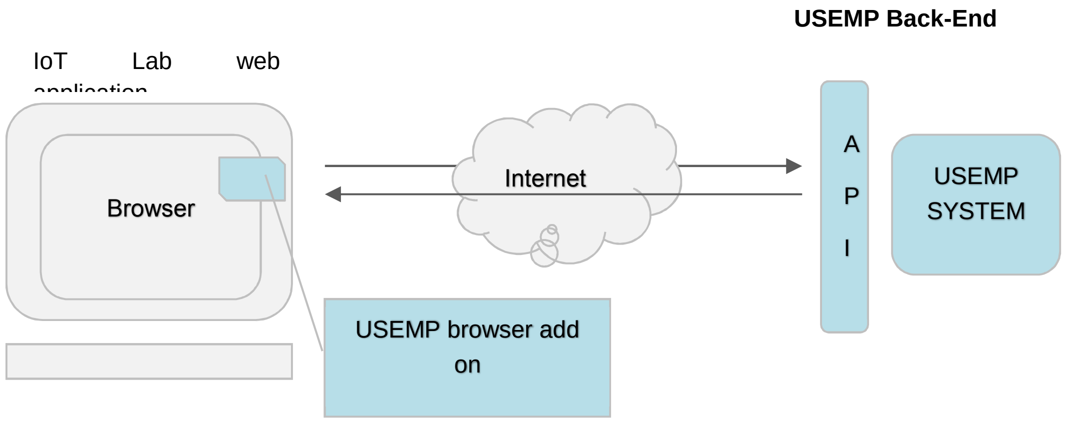

Figure 3. USEMP and IoT Lab integration through a web based application

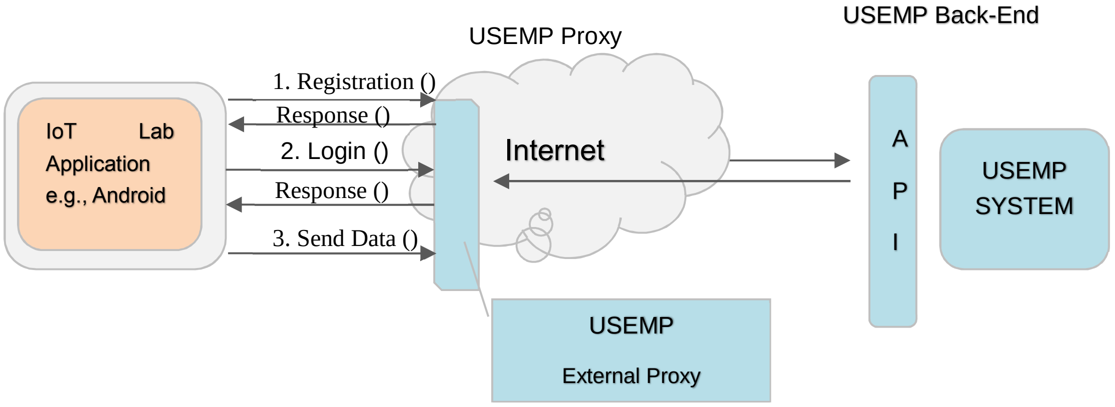

Figure 4. USEMP and IoT Lab in the case of a standalone application

In the case of a standalone application (e.g., smart phone Android app), APIs should be specified between the USEMP platform and the IoT Lab applications (Figure 4), and the development of a proxy server is required. The proxy server will provide, at least, the following interfaces, which will be used by the IoT app:

- Registration(): The IoT Lab user registers to the USEMP platform the first time that she uses the app or when she wants to enable the USEMP privacy functionality.
- Login(): The IoT Lab user provides her credentials (username and password) to initiate the collection and the analysis of her data. The login process is repeated every time that she opens the IoT Lab app.
- Send Data(): The IoT Lab application transmits to the USEMP proxy the data that the user provides or senses (e.g., monitoring, media, and text). These data are forwarded to the USEMP back-end, which undertakes to process them and identify e.g., privacy leaks.

In that case the output and the visualization of the USEMP processing are provided by the USEMP web site. Alternatively, additional APIs should be defined and provided to the IoT Lab app from the USEMP external proxy.

Finally, an additional solution that could be selected for the interaction between the IoT Lab and the USEMP infrastructures is the specification of the APIs between the IoT Lab back-end and the USEMP back-end (Figure 5). In that case both the web-based application and standalone application (e.g., smart phone android app) is not necessary to interact directly with the USEMP platform. The IoT Lab back-end infrastructure undertakes to authenticate the IoT Lab user to the USEMP platform, using the credentials of the IoT Lab. In addition the IoT Lab periodically provides to the USEMP platform collected data or personal data of the experimenters or the users of the IoT Lab. The output of processing is accessed via the USEMP web-site.

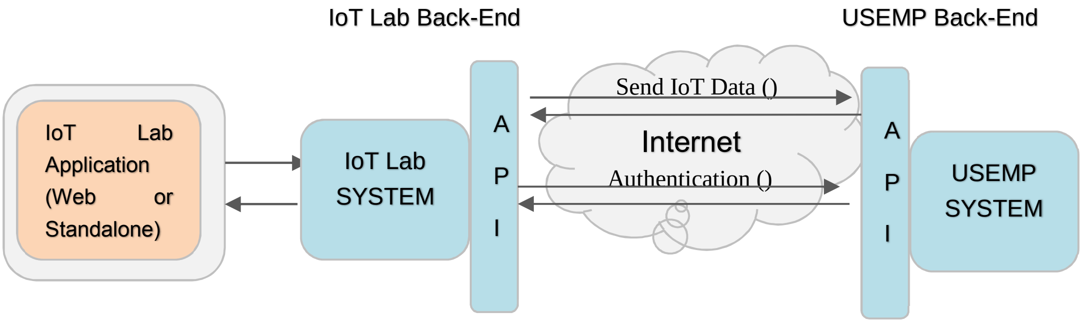

Figure 5. USEMP and IoT Lab back-end interaction

The alternatives presented in section 3.3 and the associated solutions will be evaluated together with the IoT Lab partners in order to jointly decide whether any of the above could be prioritized, taking always into account the individual roadmaps of each project.

In terms of implementation the requirements for supporting Android and WEB-based clients developed in IoT Labs or other FIRE testbeds for integration with the USEMP platform as described above (registration/login/authentication/sendData) will be included in USEMP platform revised backend architecture (D7.4). The implementation of the FIRE integration toolkit will be scheduled as part of the updated USEMP platform as part of WP7, (D7.6).

5.Conclusions and future work

The USEMP software can provide added value for other initiatives involving private data. From cooperation with the IoT Lab initiative three different possibilities have been highlighted:

1. To integrate the USEMP software at the IoT Lab application
2. To download the USEMP software as a separate application and install it in IoT Lab user browser
3. To use the USEMP software as an internal “watch-dog” embedded in the IoT Lab platform.

Of course the IoT Lab and the FIRE initiatives are only one example of external actors who could benefit from the USEMP software. To continue the actual integration and by this validate the usefulness of the USEMP software the next steps will be for IoT Lab to decide on the “way to go”. Discussions are ongoing with the technical partners of IoT Lab as well as the privacy officer on what would be the best alternative. A key aspect will be to avoid too much complexity and dependence and therefore it will be most probably to either provide the USEMP software for the IoT Lab users for them to download and install and/or to integrate the USEMP software into the management component of the IoT Lab platform. From the USEMP project, we have offered to support the IoT Lab integration on our side as their use-case could really be beneficial for both validating the USEMP software outside our own environment but also serve the exploitation activities of the project.

What also should be highlighted as an outcome of this task is the establishment of a joint agreement between USEMP and IoT Lab to bring our projects together and to align our privacy strategy, and this will be open to others to join. This would mean to share experience, ideas and strategies to improve and implement a high standard privacy policy on a wider scale. A first step will be a memorandum of understanding to be signed by both parties (the signing is in progress, cf. Annex 1). This memorandum of understanding has the purpose to strengthen and accelerate the mission in both projects to protect the privacy rights of individuals. It is also targeting to establish a “Privacy interest-group” or similar open to a wider public as we both have identified privacy as a highly prioritized domain for future Research and innovation initiatives – not only in the scope of testbeds, IoT and social media.

Additionally the flows/requirements for integration of the USEMP tools with IoT Labs and other similar FIRE testbeds presented in section 4 will be integrated to the design of the USEMP platform as a FIRE USEMP integration toolkit (D7.4). Their implementation in an an experimental version (as set of backend APIs) will be provided as part of WP7 work (D7.6).

Annex 1

Memorandum of Understanding

Memorandum of Understanding

Between

IoT Lab (EC 610477)

and

USEMP (EC 611596)

This Memorandum of Understanding (MOU) sets for the terms and understanding between the IoT Lab and USEMP to align our privacy strategies and to establish a common initiative for wider outreach and engagement.

Background
IoT Lab and USEMP are both EC-supported STREP projects initialized in 2013 including privacy and personal data protection.

IoT Lab is an initiative on crowdsource driven research. The project develops a smart phone application to enable both crowdsourcing and crowdsensing. IoT Lab has performed a systemic analysis on privacy risk and personal data protection to identify critical aspects that need to be addressed throughout the project.

USEMP is developing tools for privacy in social media. The solution will help end-users to identify privacy leaks or potential trackers. The project also includes data valuation mechanisms and how social networks monetize user data.

Purpose and implementation
This MOU has the purpose to strengthen and accelerate the mission in both projects to protect the privacy rights of individuals.

The above goals will be accomplished by undertaking the following activities:
- share experiences to improve our privacy strategies with the intention to implement a high standard policy
- joint outreach actions including to actively invite other initiatives to join with the intention to establish a “Privacy interest-group” or similar

Funding
This MOU is not a commitment of funds

Duration
This MOU is at-will and may be modified by mutual consent of authorized officials from Mandat International (representing IoT Lab) and CEA (representing USEMP) This MOU shall become effective upon signature by the authorized officials from Mandat International and CEA and will remain in effect until modified or terminated by any one of the partners by mutual consent. In the absence of mutual agreement by the authorized officials from the partners this MOU shall end on 2014-12-01.

Contact Information

IoT lab project coordinator:
IoT Lab c/o Mandat International
Sébastien Ziegler, Director
3 chemin Champ-Baron
1209 Geneva
Swizerland
+41 79 750 53 83
sziegler@mandint.org

The elected IoT Lab representative for the privacy interest group:
Annika Sällström
Luleå university of technology, Sweden

The elected USEMP representative for the privacy interest group: (tbc)
Laurence Claeys
iMinds, Belgium

USEMP project coordinator:
CEA
Adrian Popescu

________________________ Date:
(Partner signature)
(Partner name, organization, position)

________________________ Date:
(Partner signature)
(Partner name, organization, position)