SocIoTal-The Development and Architecture of a Social IoT framework

Jorge Bernal Bernabe[‡], Ignacio Elicegui[†], Etienne Gandrille[‖], Nenad Gligoric[§], Alex Gluhak[††], Christine Hennebert[‖], Jose L. Hernandez-Ramos[‡], Carmen López[†], Andrea Manchinu[**], Klaus Möessner[*], Michele Nati[††], Colin O'Reilly[*], Niklas Palaghias[*], Antonio Pintus[**], Luis Sánchez[†], Alberto Serra[**], Antonio Skarmeta[‡], Rob van Kranenburg[¶]

[*]Centre for Communication Systems Research, University of Surrey, Guildford GU2 7XH, United Kingdom [‖]CEA- LETI, 17 rue des martyrs, 38000 Grenoble, France [**]CRS4, Technology Park of Sardinia, Building 1, Loc. Piscina Manna, 09010 Pula (CA), Sardinia, Italy [‡]Department of Information and Communications Engineering, University of Murcia [††]Digital Catapult, 101 Euston Rd, London NW1 2RA, United Kingdom [§]DunavNet, Antona Cehova 1, 21000 Novi Sad [¶]Resonance Design, Leo XIIIe straat 90j, 5046 KK Tilburg,The Netherlands [†]Universidad de Cantabria, Edificio de Ingeniería de Telecomunicación. Plaza de la Ciencia s/n, 39005 Santander, Spain

***Abstract*—In this paper the development and architecture of the SocIoTal platform is presented. SocIoTal is a European FP7 project which aims to create a socially-aware citizen-centric Internet of Things infrastructure. The aim of the project is to put trust, user-control and transparency at the heart of the system in order to gain the confidence of everyday users and developers. By providing adequate tools and mechanisms that simplify complexity and lower the barriers of entry, it will encourage citizen participation in the Internet of Things. This adds a novel and rich dimension to the emerging IoT ecosystem, providing a wealth of opportunities for the creation of new services and applications. These services and applications will be able to address the needs of society therefore improving the quality of life in cities and communities.**

In addition to technological innovation, the SocIoTal project sought to innovate the way in which users and developers interact and shape the direction of the project. The project worked on new formats in obtaining data, information and knowledge. The first step consisted of gaining input, feedback and information on IoT as a reality in business. This led to a validated iterative methodology which formed part of the SocIoTal toolkit and a best practices guide for local policy makers and cities.

I. Introduction

The concept of the Internet of Things (IoT) is the pervasive presence of sensors, actuators, smartphones and Radio-Frequency Identification (RFID) tags which are able to interact in order to achieve common goals. IoT uses a number of technologies to do this, including unique addressing schemes and wireless communication. Currently, there has been much focus on industrial and commercial exploitation with examples including smart homes, smart factories and smart cites. However, there is still public reticence concerning the usage of this infrastructure due to issues with privacy and security. The SocIoTal project builds on the foundations of emerging IoT architectures in order to address the issue of perceived privacy and security issues for end-users. The project introduces the following innovative key target outcomes, ensuring that privacy and trust are deeply embedded in the resulting architecture:

1) A governance, trust and reputation framework consisting of a set of innovative enablers that addresses the challenges of a community-based IoT infrastructure
2) A privacy-preserving context-sensitive communication framework for IoT devices which includes security
3) A detailed understanding of the technological and socio-economic barriers to citizen participation in an IoT
4) An intuitive environment that provides increased awareness and control and empowers citizens to easily manage access to IoT devices and information, while allowing IoT enabled citizen centric services to be created through open community APIs
5) Services piloted in two cities demonstrating the value of SocIoTal in the real-world.

In this paper, the development and final architecture of the SocIoTal platform is presented. In Section 2 the problem statement and motivation is detailed. In Section 3 the approach of SocIoTal is detailed. The overall architecture is described in Section 4 where the methodology used for the development of the platform is presented. Section 5 examines how the community was engaged. This section details how end-users and developers were engaged and how their input helped to shape the framework. Section 6 provides the conclusion and areas for future work.

II. Problem Statement and Motivation

IoT infrastructures where citizens provide IoT devices and contribute information flows will have a significant impact on people and societies. However, before this occurs there are a variety of technological and socio-economic barriers that need to be overcome in order to enable inclusive IoT solutions. One particular aspect is the perception of IoT which is critical to enable a successful uptake of IoT in all areas of society.

A high level of trust and confidence in IoT is crucial and this is therefore an important challenge which needs to be

Author Order Note: The authors of this publication are listed in alphabetical order.

addressed. IoT solutions are expected to operate seamlessly and act in the background, invisible to their users. To ensure a widespread update of IoT in all areas of society citizens must be provided with sufficient motivation to contribute their devices and information flows, making them available to their immediate community and to IoT at large. In addition, the IoT architecture and infrastructure should be sufficiently simple that citizens are easily able to add and manage the devices and information flows that they contribute. A system which is simple to operate and provides the user with immediate and clear benefits will provide sufficient motivation. However, the IoT system should be implemented to ensure that their is both transparency and adequate control for the user to allow a better understanding of what is happening with the devices and information flows the user has contributed. If transparency and control is not sufficient, there is a danger that the systems will be viewed with suspicion and mistrust, which may result in the opposition and refusal of the technology.

III. SocIoTal Approach

The aim of the SocIoTal project is to create a reliable and secure IoT environment which encourages citizens to contribute their devices and information flows. This provides the foundation to unlock a significant number of new citizen-centric information streams which will be available for the creation of new services that will have high socio-economic value. The combination of devices and information flows with an IoT deployment will allow the creation of smart services addressing the needs and challenges of individuals, communities and societies. A key research theme of the SocIoTal project is to increase the trust and confidence in IoT systems while providing simple and intuitive ways for users to contribute to and use the system. This will further encourage the creation of services with high socio-economic value.

To implement the vision and research objectives of SocIoTal, several approaches are taken. A set of technological innovations and tools were developed to increase trust and confidence in IoT, and to provide a secure environment with transparency and control. In addition, the technological barrier to participation was lowered through tools to simplify participation and enable an environment for the easy production and consumption of value added services. In order to ensure the impact of the research, SocIoTal closely engaged with people, services developers and other IoT stakeholders such as city councils and policy makers throughout the lifetime of the project.

The following sections detail the components which were designed and implemented. The SocIoTal platform is freely available, details of how to obtain it are given in Section V.

IV. SocIoTal Architecture

The architecture of the SocIoTal platform is designed thanks to the Architecture Reference Model (ARM) [1] provided by the EU project IoT-A that enables the generation of user-centric IoT platforms. The abstraction level offered by some of the views enables to consider the security and privacy objectives with a lot of flexibility in a rigorous framework based on the design process.

The SocIoTal platform, Figure1, is built around a central component, the Context Manager that holds the database with the contextual information. All the components and enablers will interact with the Context Manager to access data in a confidential manner.

A. Context Manager

The Internet of Things environment is usually visualized as a number of entities providing information that, after some management or treatment, can be used to create new value added services. In order to manage such a volume of data, there is a need to harmonize this, by nature, heterogeneous environment; so all the entities, called Context Entities, and the information they provide, called Context Information, have to be homogeneously represented by a common data model.

The SocIoTal Data Model representation is based on the OMA reference NGSI9 and NGSI10 specifications [2]. This way, all Context Entities and Context Information can be modeled through an identifier and a set of attributes that describe their capabilities and the nature of the information. As previously mentioned, the component in charge of the context management in the SocIoTal platform is the SocIoTal Context Manager (SCM). This SCM can be seen as the core of the platform, acting as the context entities directory, and context information storage, allowing the storage and retrieval of the last values of all the information sent by the registered devices. These functionalities, and other related ones, allow the user to perform a very complete management of the information and can be accessed through the corresponding NGSI9 and NGSI10 interfaces, implemented as RESTful APIs and documented [3]. Through these interfaces, the users are able to easily register their devices in the platform, configure them to send their information to the platform, and to retrieve that information when needed, while either performing a direct request of a resource or performing a subscription to the data.

In addition to the aforementioned functionalities, the SCM plays a key role in the context awareness concept of SocIoTal since it gathers, in addition to the ordinary context of an entity, all the special context information provided by the SocIoTal enablers which enrich the stored information of the registered Context Entities. This extra information can be used by other components which need to know as much as possible about the context of the entity in order to provide the best service.

B. Privacy and Security

Increasing trust and confidence is not an easy task in a distributed and uncontrolled IoT environment with diverse end-user participation. In particular, to unlock the potential from IoT, it is necessary to minimize the risks that are associated with security and privacy concerns by considering technologies-independent architectures [4]. Indeed, the aim of SocIoTal was to use emerging architectural models as starting points and then to introduce innovative enablers that strengthen the existing architectural foundations to ensure that privacy and trust are deeply embedded in the resulting architecture.

Security and privacy aspects are handled in SocIoTal by the security framework. Such a framework provides a

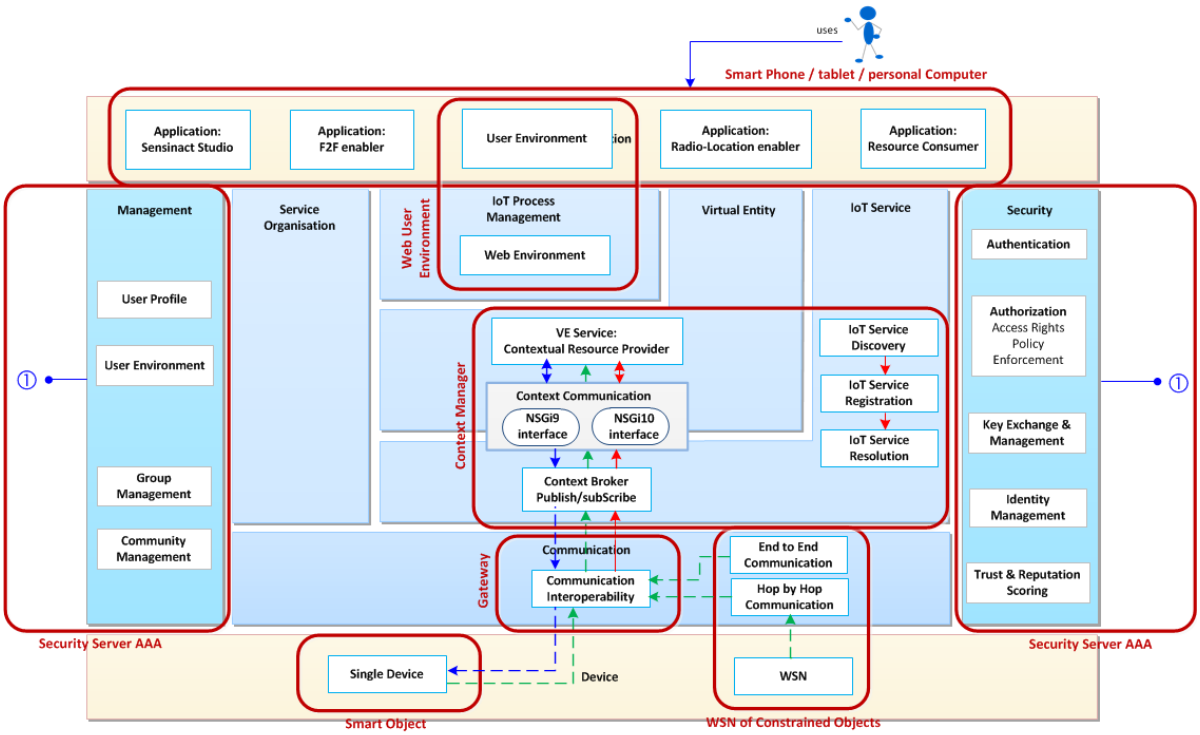

Fig. 1. The architecture of the SocIoTal platform

holistic security and privacy-preserving solution that has been implemented and validated in the scope of the project. The different components are introduced below.

The SocIoTal Authorization component is designed as a combination of different authorization technologies and tools in order to enable a suitable solution for IoT environments. Such a system is based on the use of XACML [5] access control policies, which are employed to generate authorization credentials in the form of capability tokens [6]. Then, such tokens include the access rights and are used by smart objects to get access to services being provided by other IoT entities and services.

The SocIoTal Identity Management (IdM) component follows a claim-based approach with Attribute Based Credentials (ABC). The IdM relies on the Idemix [7] cryptographic library from IBM, providing a privacy-preserving solution which allow dealing with IoT scenarios where consumers and providers can be not only traditional computers, but also smart objects (e.g. smartphones). In addition, the SocIoTal IdM has been integrated with Fi-Ware Keyrock IdM to support traditional IdM management operations in scenarios where claim-based accesses are not needed.

The SocIoTal Group Manager component is based on the CP-ABE cryptographic scheme [8], as a flexible scheme to enable a secure group data sharing mechanism. The functionality of this component is mainly split into two entities: the Group Manager Server or Attribute Authority (AA), and the Group Manager Client. The Group Manager client API allows obtaining cryptographic material, encryption, decryption as well as sharing encrypted information through the Context Manger.

The Authentication component provides different ways of authentication. Firstly, a claim-based approach using Idemix presentation protocol, secondly traditional login-password by relying on Keyrock and thirdly eID authentication with x509 certificates. The Key Management Component is implemented as an Attribute Authority (AA) that accepts requests for CP-ABE keys generation. The CP-ABE keys that are generated by the AA according to the associated attributes stored in the Keyrock IdM

C. Trust Management

There are a lot of definitions of trust management and trust-reputation systems generally. Although each of them has a separate model and methodology, the goal of quantification of the reputation and transferring separate context meanings into one reputation score, persists. Trust Management is defined as the activity of collecting, encoding, analyzing and presenting evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships [9].

The trust and reputation systems are mainly based on model defining, trust score computing and management of reputation data, respectively providing secure and efficient data recovery [10] and methods for quantification of entitys value that other consumers in the system realize as a measure of trustworthiness. In general, trust can be generated by using trust matrix and reputation vector [11]; by aggregating values for some specific scenarios such as peer-to-peer network [12];

or by implementing a rule-based agent that takes input from reputation model [13].

The Trust Manager is a REST component based on a generic rules model that utilize simplified level of score quantification by assigning weights for each examined rule. The Trust Manager is developed as a component that will enable user by using generic model for trust and reputation to add, remove and manage his own set of rules that will be used to quantify a final reputation score for his application. This component utilizes and relies on other SocIoTal platform components, more specifically on SocIoTal Context Manager to receive/push the updated version of the entity values which is used for building the reputation score. Subscription enables the Trust Manager to on demand recompute reputation score only for application that consumes certain context in the quantification process.

D. Communities and Bubbles

One of the most difficult barriers to overcome in the Internet of Things users acceptance is data privacy. Usually, when users share information about themselves, their devices or their surroundings, they are very distrustful about the possibility that the information could be disclosed to other people or entities without their permission. In order to provide users with tools which allow them to have overall control of their data, the SocIoTal Communities Manager and SocIoTal Bubbles have been developed.

The Communities Manager (ComM) tool allows users to share their entities and their related information only with those users, organized in groups or communities, to whom they grant access. Through the ComM, the users will firstly be able to register themselves within the SocIoTal platform. Once the user has been registered, they will be able to create communities where they can register new devices and add new users with whom to share that devices and its information. If the creator of the community, the owner, accepts a new user within the community, they will have to provide the new member with a role that will specify the kind of actions permitted within the community. All this information related to the users and the role they have within a concrete community is represented by a community-token. This token will have to be attached to any request for action performed by a user against the SocIoTal Context Manager, this way the platform will be able to determine if a specific user is able to perform a specific action over a resource (access or modification) within a specific community. This tool is available through a set of APIs that, can be found in [14] with the corresponding documentation.

In addition to communities, SocIoTal bubbles are considered as groups of objects that share their information under a set of security and privacy restrictions. SocIoTal bubbles are defined as a common entity in the Context Manager that, in turn, has a list of associated entities. Furthermore, each bubble is bound to a specific CP-ABE policy that is used by all entities within the same bubble to encrypt their data. Users are empowered to define bubbles and these properties through the Web User Environment. The use of SocIoTal provides two key advantages. On the one hand, the use of CP-ABE provides a simple and scalable key management process for IoT environments, since entities do not need new keys to participate in different bubbles. On the other hand, the confidentiality of the data is maintained in an end-to-end manner, which means that entities that do not belong to a certain bubble will not be able to decrypt the exchanged information (including the Context Manager).

E. Enablers

The aim of enablers is to provide users with an easy way to interact with the SocIoTal framework, thus reducing technological barriers for users. The enablers provide information streams from sources such as sensors or smart phones which is communicated to the Context Manager through protocols such as REST. Once it is stored in the Context Manager it can be queried by other components which can use the information to provide services. Three enablers were designed and implemented on the Android platform, the Face-to-Face Enabler, the Gait Recognition Enabler and the Geo-Localization Enabler.

The Face-to-Face (F2F) enabler aims to detect social interactions by utilising commercial off-the-shelf mobile phones, in an opportunistic and non-intrusive manner [15]. The data collection process is based on integrated sensors and communication interfaces of todays smartphones. A novel machine-learning model was developed that leverages the Bluetooth Received Signal Strength Indicator to estimate the interpersonal distance among the users in vicinity. A state-of-the-art technique for estimating users facing direction [16] was implemented to extract the relative orientation of the users based on users walking locomotion. To enable the ad-hoc communication among the devices, a collaborative sensing scheme was developed that operates in an opportunistic and distributed manner. The above components were integrated into a coherent system that infers the existence of real-world F2F interactions without the users involvement [17]. Each smartphone that belongs to the SocIoTal platform, runs in the background the F2F enabler and logs internally all the detected social interactions. A RESTful communication interface that follows the NGS10 interface was developed to allow the F2F enabler to publish the detected social interactions to the Context Manager, so that other components could utilise the provided information. The F2F enabler publishes to the Context Manager contextual information related to the F2F interactions such as the users involved in the interaction, their social relation, the timestamp and the location of the interaction.

The Gait Recognition Enabler is used to authenticate users based on their walking pattern. The aim was to provide a continuous passive authentication scheme for a smart phone. The enabler uses the accelerometer data to provide measurements of the users walking pattern, also know as their gait. It is known that gaits are unique to each user, and therefore this can be used to identify as user. The enabler has two phases, a training phase and a testing phase. During the training phase sensor data is gathered from the accelerometer and this is used to construct a model of the users walking pattern. Once the training phase is complete, the testing phase begins where every 2 minutes of walking the current users gait is compared to the model. If the walking pattern differs significantly, it is

determined that a different user has the phone, an imposter, and this is reported to the Context Manager. If the current gait is similar to the model, it is determined that the rightful user is in possession of the phone, and this is reported to the Context Manager. This information is used by the Trust Manager in the calculation of trust scores. The Gait Recognition Enabler was implemented as an Android App.

The geo-localization enabler [18] is used to follow the movement of people in an indoor environment. This enables the generation of statistics in an office building for instance to know the room most visited at given hours and to adapt the temperature heating accordingly. This component provides real-time, time-stamped location information of users and user devices within an indoor environment. It relies on a pre-established Wireless Sensor Network (WSN).

The user wears a so-called mobile node, which can be a constrained object or device that has the ability to communicate wirelessly within the WSN. The network is comprised of static nodes, which act as location anchors, and possibly other mobile nodes belonging to other users of the network. By using an ad-hoc protocol, the mobile node has the ability to estimate its distance from other nodes and then sends this information to the gateway. The gateway then computes the user location based on the data received from users mobile nodes and stores it in the Context Manager for further processing and/or querying.

A web application enables the user to visualize their real-time location on a map of the building. This application can be hosted on the gateway or any third-party infrastructure that has the ability to query the Context Manager.

F. Web And Mobile User Environments

One of the main SocIoTal objectives is to provide citizens and service developers a set of tools and techniques to manage, use, mix and compose services, data and physical devices in an IoT digital ecosystem. From an end user perspective, a personal dashboard plays a central role for the citizens in order to manage/share devices in social circles, providing intuitive mechanisms to the user for expressing the way in which they want their mixed physical-virtual environment to behave.

The SocIoTal User Environment is the tool specifically designed for and targeted to end-users. It is composed of the Web User Environment and the Mobile User Environment. These complementary tools are targeted to unskilled people, users and citizens, as they expose simpler features through user-friendly, modern and intuitive user interfaces.

The Web User Environment provides to non-experts users an intuitive tool to manage their personal or communal IoT. The tool integrates other SocIoTal platform components in order to provide a simple-to-use, secure and privacy-aware personal dashboard (see Figure 2). Through it, users can manage their connected devices, share them with other people in joined communities and to set trigger-action rules to build simple alerts and personal micro-apps. The Mobile User Environment is a mobile application with a subset of operations provided by the web environment; more specifically it consumes the Web User Environment API to enable the addition and removal of devices to/from the users workspace, watching the readings from the devices, receiving push messages from the Web environment, etc.

Adding a device to the user environment workspace can be done by scanning a QR code with the mobile app. The QR code can be generated manually by the user, but must contain predefined elements that are going to be extracted, i.e. SocIoTal ID, device name, description and value type.

G. Developer Environment

The Developer Environment (Figure 3) is an Eclipse based studio which facilitates the browsing of available SocIoTal assets and eases the development of applications.

A map provides a visual feedback using pinpoints. It allows rapid geolocated browsing of all the assets. Clicking on a pinpoint, a popup displays assets information and current sensors values. On the left, a tree viewer displays an exhaustive list of the assets, including those which are non geolocated or not currently visible on the map because of the zoom level. The color of the elements is based on their trust and reputation score. Below this view, an area can receive drag and drop of sensors displayed in the tree viewer. This interaction triggers the creation of a realtime graph, which displays the evolution of the sensor value which has been chosen.

On the bottom right corner of the studio, an XText based editor allows rapid prototyping of applications. Using syntax validation, code completion and syntax highlighting, the developer is guided and can focus on the application logic.

V. Engaging the Community

During the creation of the SocIoTal project it was recognized that there was a requirement to have concrete engagement with the community of users and developers that were seen as the users of the framework. Therefore an aim of SocIoTal was to closely engage with people, service developers and other IoT stakeholders such as cities and policy makers throughout the lifetime of the project. Several steps were taken in the development and evaluation phase to ensure that both users and developers had input into the design and implementation of the framework. This input was provided in the form of Meetups, co-creation workshops, pilots and hackathons. SocIoTal research identified as main barriers to broad IoT adoption in 'smart' cities:

- lack of understanding by SME's and City Councils
- lack of third party trust providers
- lack of involvement of end-users in building use-cases and developing news services

The lack of understanding is addressed in Meetups, introducing research questions and listening to the local stakeholders. The lack of involvement of citizens was addressed in co-creation workshops with researchers from UC, Santander and Novi Sad. The co-creation workshops were prepared and executed with the help of the methodology of Nathalie Stembert.

The aim of Meetups was to engage with the local community of users and developers. Over the course of the project meetings were organized where aspects of the project were presented and discussed. In addition, other presenters were brought in to discuss the latest developments in the field. Meetups are

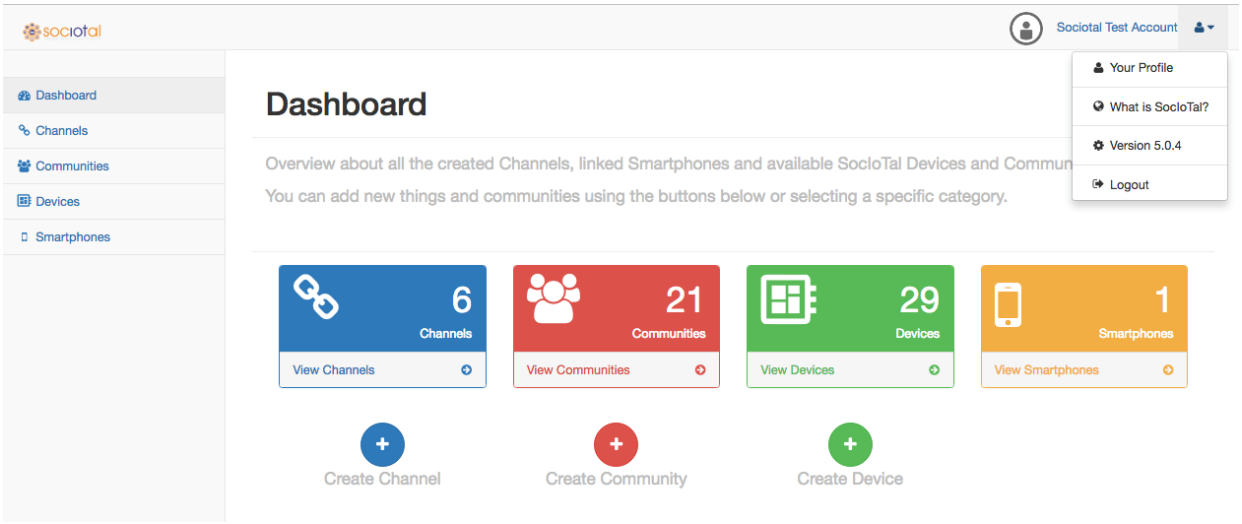

Fig. 2. The Web User Environment of the SocIoTal platform, the dashboard

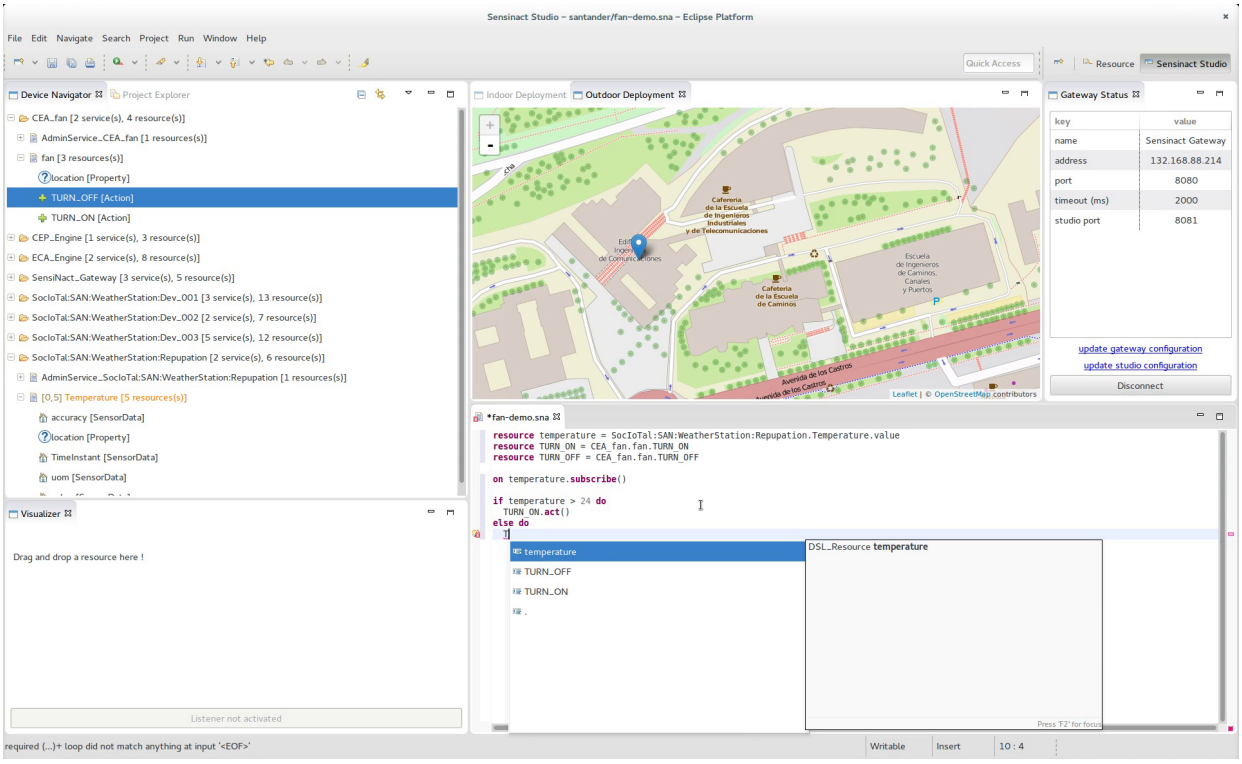

Fig. 3. The developer user environment of the SocIoTal platform

among the fastest growing form of organizational meetings where people gather around a topic. In total SocIoTal held 71 Meetups in 3 years in 5 cities (Santander, Ghent, Guildford, Novi Sad and Grenoble) with 1594 members to date and 1534 attendances. In order to account for the no-shows and people that show up unregistered, experience shows us we must subtract about 15 % of this total. That leaves us with 1309 attendances. The main achievement is to build a local context that will stay after the projects lifetime. Meetups are informal gatherings of prosumers, interested amateur experts, local SME and IT business and lone coders and hackers who engage in two or three 5 to 10 minute presentations and have a beer afterwards. Meetups are practical and pragmatic affairs that can benefit from academic input if that is interfaced correctly, not in theoretical chunks but in real world advice.

Citizen engagement does not only needs to addressed during the course of a process or project but from the very beginning. In the requirements phase citizens need to be involved in order to create buy-in and enthusiasm for technology in their homes, streets and cities. Co-creation workshops are highly structured ways to extract feedback from citizens, developers, city councils and any kind of stakeholder in such a form that requirements

can be made quite quickly in the technical context of the use case. The outcomes of the co-creation workshops confirm that the granularity of data quality is one of the most important factors in bridging IoT to end-users. If applications are not meaningful for real everyday problems then the added value of a sensor grid that is monitoring obvious situations is not seen as relevant to the work being done in the SocIoTal project and also obtain feedback on the development.

Hackathon events were used as a wheel for the evaluation of the platform and user engagement as well as for interaction and integration with other projects. There were three Hackathons organized during the project lifetime, two during SenZations Summer School [19] and one held during the IoT Week 2016 in Belgrade.

In Tips for City Authorities How to Avoid Citizen Engagement Pitfalls, Dr. Mazlan Abbas, CEO of REDtone IOT, asks: "Many citizen engagement mobile apps (example identifying pothole, drainage faulty traffic light, illegal parking, unattended, etc. issues) failed simply because it is unable to sustain the popularity, usage, and continuous enhancement. Why?" [20]. During the project's lifetime we found that all stakeholders are uncertain as there is very little to none best practice. Citizens question privacy and security, as well as added value. Companies are slow to adopt to new business models or get pushed by Over The Top players without a real strategic view. A New Electronics survey of 187 councils from across England, Northern Ireland, Wales and Scotland by DJS Research found that many local governments across the U.K. lack the capability, leadership and budget to implement smart city projects. This comes as an increasing number of cities worldwide throw resources behind smart city projects to improve their budgets and livability. A report by Lucy Zodion [21], a street lighting firm, states that more than 80% of councils had little or no engagement with smart city planning. Furthermore, the report states that there is a need for leadership from government to enable local authorities to provide the delivery and leadership required to create a strategy for smart cities. The report identifies issues such as poor funding, little evidence, insufficient collaboration and low confidence in smart projects as the main barriers to success.

The SocIoTal toolkit is addressing these issues. The graphic toolkit has five sections: on security and the SocioTal tools, relevance, ecosystem, compliance and mega trends in smart cities. The Stakeholder Coordinator Toolkit addresses the barriers and incentives that were identified during the projects lifetime. The toolkit is an external service offered as part of the general consultancy and workshop offerings of Council, theinternetofthings.eu, which is part of Resonance Design, one of the two SME companies in SocIoTal. The issues identified are strongly aligned while every city has its own areas of focus. The SocIoTal toolkit is available to download [22].

A. Platform Implementation and APIs

The above proposed architecture was fully implemented over the lifetime of the project and is available on GitHub [23]. Here the framework, in terms of libraries and applications, can be downloaded. A wiki provides API information and tutorials on how to setup and use the platform. In addition, public instances of the platform are available. These are instances that are open to public use in order to evaluate and test the APIs and other aspects of the project. The details of the public instance can be found on the SocIoTal website [24].

Almost all developed architectural components expose an Application Programming Interface (API). The APIs role in the SocIoTal architecture is twofold: to provide a large set of IoT functionalities to third-party application developers through an open community API, thus instrumenting and fostering them to build new applications for smart neighborhood, communities and cities; to provide all the needed endpoints and libraries targeted to the internal system integration, intra-modules communications and future platform extensions. Basically, the provided SocIoTal APIs are of two types: software libraries (e.g., written in Java language) to be linked to requiring applications, like those available, for example, for Authorization and Identity Managers; Web APIs (adopting a REST principle) and programming language agnostic, like the endpoints exposed by the User Environment, the Context Manager, the Trust Manager and others. All the APIs documentation is open and available through a unique access point, the related and updated, API documentation hub [25].

B. Pilots

Pilots of SocIoTal are deployed in two European cities Novi Sad (Serbia) and Santander (Spain).

Novi Sad has deployed two pilots running on the SocIoTal platform leveraging services and functionalities from different components and enabler.

1) Mood Of The City - This pilot is deployed in one of the largest public shopping mall in Novi Sad and its measures happiness of the city by taking multiple parameters as an input, emotions (neutral, sadness, surprise, happiness, anger, contempt, disgust and fear), age and gender.
   The totem "Smile of the City" which promotes the concept of smart cities through detection of smiles of passing citizens, invites them to smile and download mobile applications and get involved in numerous activities related to development of Novi Sad into a smart city. The final Mood of the city value is computed as an index using aggregated users data, i.e. users mood detected from an image, answers to a subjective happiness questionnaire, users selections from a predefined mood list and environmental data (current temperature, humidity, etc; that is scientifically proven to influence the people mood).
2) Elevator supervisor - The Elevator supervisor is depicted for deployment during the co-creation workshops held with citizens. A main motivation for building this service was a feedback from the citizens that suggested that there is no information about the distance that elevator can reach between the scheduled inspections as well as no alert that can arise in case of malfunction. This trial enables tenants to monitor elevator distance travelled between inspections and to alert them when the malfunction happens. The SocIoTal Mobile Environment

Fig. 4. The mood of the city piloted in the city of Novi Sad, Serbia.

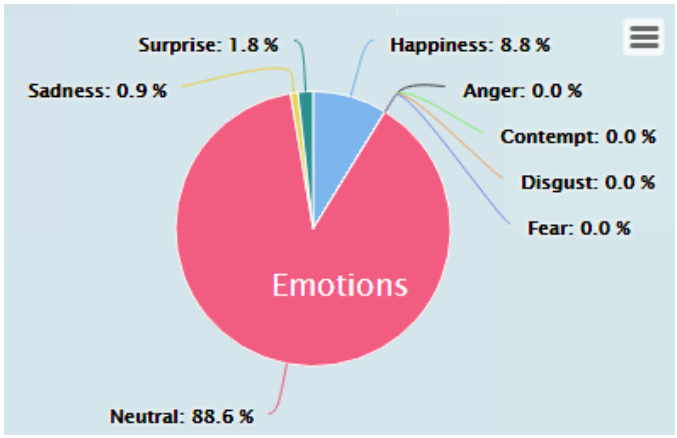

Fig. 5. The emotions

is used by tenants to receive alerts when elevator reaches limit and needs an inspection. Each user that adds the Web User Environment to his circle of users can see the elevator data in his mobile and web workspace. All data are sent from the Raspberry Pi device with accelerometer sensor to the SocIoTal Context Manager.

Santander City, sheltered in the north of Spain, have deployed two of the SocIoTal pilots providing new value added services to the citizens by using the components and tools developed in the SocIoTal project. It is interesting to highlight the importance of the citizens involvement during the life cycle of the pilot: when selecting the use cases, when gathering requirements and during the final testing of the services. Initially, both pilots were born from ideas proposed by citizens and developers through the Santander City Council platform called Santander City Brain [26], where citizens are invited to share ideas to improve the quality of life in the city. After an initial ideas selection, a co-creation workshop with citizens was set in order to gather a set of requirements that really fulfill their needs and expectations. Finally, users were also invited to participate in the pilots in order to test the final provided services.

1) Enabling Santander - This pilot provides citizens with an application, called DisApp, to obtain routes from one place in the city to another avoiding the different obstacles that could be difficult for users to move around. This can be described as a collaborative tool where all users can enrich the application by adding new obstacles that could present a problem for users with mobility problems. Because of this, although the target group of the application was the disabled community in the city, and people with mobility problems (temporary injuries, prams, etc.), all citizens are invited to collaborate with their reports.
   As previously mentioned, the DisApp application is based on the use of different SocIoTal tools. The Communities Manager tool is accessed when a user wants to create a new account, being created as a new user in the platform and being added to the DisApp community. Also, when the user logs in, the Communities Manager tool will ensure that the user has an account in SocIoTal and that they belong to the DisApp community.
   Once logged in, the user is able to find routes between two points in the city avoiding (if they want) points that have been reported by other users as possible obstacles. When a user is walking and find something that can present a problem for a person with mobility problems, they can upload to the platform information of the obstacle by completing a form with data about the location, photo, description, duration, etc. This information is uploaded to and managed by the SocIoTal Context Manager and can be presented in the application through maps and markers. In the case that an obstacle is presented in the initial route provided by the application, the users can check the information of the obstacle, and if it is a problem for their mobility they can select the obstacle as a no-go point and a new route will be calculated avoiding it.
2) Sharing Information - This pilot was born as a need to fulfill the interest of users and developers of being participants of the IoT environment without renouncing control of their data. Within the framework of the SocIoTal project, different IoT Meetups were set and many of the citizens attending showed much interest about the Internet of Things. During the first meetings, citizens were introduced to the concept of IoT and were given presentations of some regional IoT projects. The next natural step was to teach them how to create their own IoT devices. After that, the SocIoTal platform was introduced through the Web User Environment and its mobile version, the Mobile User Environment, in order to provide citizens with tools to easily manage that devices. This management is conducted by the functionalities provided by the SocIoTal Context Manager and SocIoTal Communities Manager and presented to the user through the Web User Environment. From this user friendly interface, users are able to register themselves in the platform, register their devices, subscribe to the values that the devices report, create communities which share the information they consider with those users they

consider, etc. For citizens with a more technical profile this pilot also involved the provision and training of SocIoTal components APIs. This way, developers can easily include the SocIoTal functionalities within their developments.

VI. Conclusion

This paper provided details of the work done as part of SocIoTal, a European FP7 funded project. The aim of the project was create an IoT ecosystem centred on trust, user control and transparency. In addition, the aim was to provide users and developers with input into the design and features of the infrastructure through concepts such as Meetups and co-creation workshops. Tools and mechanisms were used to lower the technological knowledge required to operate the system in order to further encourage users to contribute devices and information streams. This provides an opportunity for the construction of services to add soci-economic value to the community.

Although the SocIoTal project is drawing to a close, the components and concepts are being exploited and improved in other projects with the aim to further progress the idea of a social Internet of Things.

Acknowledgment

This work was supported by the SocIoTal project under grant agreement No 609112.

References

[1] "Introduction to the Architectural Reference Model for the Internet of Things," http://www.iot-a.eu/public/public-documents/copy_of_d1.2/view, accessed: Sept. 20, 2016.

[2] "NGSI Context Management," http://technical.openmobilealliance.org/Technical/release_program/docs/NGSI/V1_0-20101207-C/OMA-TS-NGSI_Context_Management-V1_0-20100803-C.pdf, accessed: Sept. 20, 2016.

[3] "SocIoTal Context Manager API," https://github.com/sociotal/SOCIOTAL/wiki/SocIoTal-Context-Manager, accessed: Sept. 20, 2016.

[4] J. L. Hernández-Ramos, J. B. Bernabe, and A. Skarmeta, "Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 28–35, September 2016.

[5] T. Moses *et al.*, "Extensible access control markup language (xacml) version 2.0," *Oasis Standard*, vol. 200502, 2005.

[6] J. L. Hernández-Ramos, J. B. Bernabe, M. Moreno, and A. F. Skarmeta, "Preserving smart objects privacy through anonymous and accountable access control for a m2m-enabled internet of things," *Sensors*, vol. 15, no. 7, pp. 15 611–15 639, 2015.

[7] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 21–30.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*. IEEE, 2007, pp. 321–334.

[9] T. Grandison, "Trust Management for Internet Applications," Ph.D. dissertation, Imperial College London, 2003.

[10] P. Bonatti, C. Duma, D. Olmedilla, and N. Shahmehri, "An integration of reputation-based and policy-based trust management," *networks*, vol. 2, no. 14, p. 10, 2007.

[11] C. de Kerchove and P. Van Dooren, "Iterative filtering for a dynamical reputation system," *arXiv preprint arXiv:0711.3964*, 2007.

[12] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003, pp. 640–651.

[13] A. Paschke, R. Alnemr, and C. Meinel, "The rule responder distributed reputation management system for the semantic web." in *RuleML Challenge*. Citeseer, 2010.

[14] "SocIoTal Communities Manager API," https://github.com/sociotal/SOCIOTAL/wiki/SocIoTal-Communities-Manager, accessed: Sept. 20, 2016.

[15] N. Palaghias, S. A. Hoseinitabatabaei, M. Nati, A. Gluhak, and K. Moessner, "A survey on mobile social signal processing," *ACM Computing Surveys (CSUR)*, vol. 48, no. 4, p. 57, 2016.

[16] S. A. Hoseinitabatabaei, A. Gluhak, R. Tafazolli, and W. Headley, "Design, realization, and evaluation of udirect-an approach for pervasive observation of user facing direction on mobile phones," *IEEE Transactions on Mobile Computing*, vol. 13, no. 9, pp. 1981–1994, 2014.

[17] N. Palaghias, S. A. Hoseinitabatabaei, M. Nati, A. Gluhak, and K. Moessner, "Accurate detection of real-world social interactions with smartphones," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 579–585.

[18] I. Tunaru, B. Denis, and B. Uguen, "Location-based pseudonyms for identity reinforcement in wireless ad hoc networks," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–5.

[19] "Summer School on IoT and its Applications," http://www.senzations.net, accessed: Sept. 20, 2016.

[20] "Tips for City Authorities How to Avoid Citizen Engagement Pitfalls," https://iotworld.co/2016/08/01/tips-for-city-authorities-how-to-avoid-citizen-engagement-pitfalls/, accessed: Sept. 20, 2016.

[21] "Smart City White Paper: Lucy Zodion," http://www.citihorizons.com/resources/lucy-zodion-white-paper, accessed: Sept. 20, 2016.

[22] "SocIoTal Toolkit," http:/http://www.theinternetofthings.eu/smartcityworkshop, accessed: Sept. 20, 2016.

[23] "Sociotal github," September, https://github.com/sociotal.

[24] "Sociotal webpage," September 2017, http://sociotal.eu.

[25] "SocIoTal wiki," https://github.com/sociotal/SOCIOTAL/wiki, accessed: Sept. 20, 2016.

[26] "Santander City Brain," http://www.santandercitybrain.com/, accessed: Sept. 20, 2016.