Specific Targeted Research Projects (STReP)

SOCIOTAL

Creating a socially aware citizen-centric Internet of Things

FP7 Contract Number: 609112

WP7 – Final Report

Deliverable report

Contractual date of delivery:
30/11/2016
Actual submission date: 15/11/2016

Deliverable ID:	**D7.4**
Deliverable Title:	**Final Report**
Responsible beneficiary:	UniS
Contributing beneficiaries:	All Partners

Start Date of the Project: 1 September 2013 Duration: 37 Months

Revision: Draft v0.8

Dissemination Level: Public unless otherwise stated

Document Information

Document ID: D7.4
Version: v0.8
Version Date: 15th September 2016
Authors: **Colin O'Reilly and the SocIoTal Consortium**
Security: **Public unless otherwise stated**

Approvals

	Name	Organization	Date	Visa
Project Management Team	Klaus MOESSNER	UNIS	14/11/2016	

Document history

Revision	Date	Modification	Authors
v0.1	30/09/2016	Initial draft created	C. O'Reilly
v0.2	07/10/2016	Contributions added	C. O'Reilly
v0.3	15/10/2016	Contributions added	C. O'Reilly
v0.4	24/10/2016	Contributions added	C. O'Reilly
v0.5	01/11/2016	Contributions added	C. O'Reilly
v0.6	09/11/2016	Contributions added	C. O'Reilly
v0.7	11/11/2016	Contributions added	C. Alais
v0.8	15/11/2016	Review updates	K.Moessner

Content

Executive summary

The SocIoTal EU FP7 project addressed the shortcomings of current IoT infrastructures, deployments and services by placing the citizen at the centre of the system and in control of their data with privacy and security deeply embedded. The project created a framework which can be used by local communities to manage devices and information streams with ease, while providing transparency to ensure that the user has knowledge of the service/operation, how it is occurring and control what of their information/data about them is being used. The framework was promoted and used with different communities.

In addition to the technological achievements of the SocIoTal project, the project explored the role of in the different stakeholders, from technology or service provider, developer to the end user.

The SocIoTal project recognised the importance having of users, developers and other IoT stakeholders such as cities and policy makers participating in the design and development of IoT deployments and services. From the beginning the project has ensured information and engagement with all of these stakeholders through meetups, co-creation workshops and pilot deployments. It helped to have this important group of people helping to shape the direction of the project by providing feedback during the course of the project which was then analysed and reacted to in the ongoing development and mirrored in the iterations of the framework.

From this engagement and the lessons that were learnt, the project developed, a stakeholder toolkit which provides those in governance with the necessary information to make informed decisions about IoT deployments. This toolkit was specifically designed to address and overcome the lack of knowledge and understanding by decision and policy makers which was identified during the lifetime of the project.

Section 1 - Summary description of the project and context

The Internet of Things (IoT) describes the networking and digital representation of physical devices which have sensors and actuators, in addition to their ability to communicate in a network. The formation of such a network allows the collection and exchange of information which can be provided and acted upon. So far, much attention has been focussed on the industrial and commercial exploitation of IoT, with examples including smart cities, smart factories and smart homes. However, there is still public reticence in the usage of IoT due to concerns about privacy, security and the in-transparency of what happens to private information of individuals.

1.1 Main aims

The SocIoTal project took steps to alleviate the concerns that the public has about IoT. The project builds on the foundations of emerging IoT technologies to introduce innovative technologies that ensure that privacy and trust are deeply embedded in the architecture. A summary of the achieved main aims of the project is:

- A governance, trust and reputation framework consisting of a set of innovative enablers that addresses the challenges of a community-based IoT infrastructure
- A privacy-preserving context-sensitive communication framework for IoT devices which includes security
- A detailed understanding of the technological and socio-economic barriers to citizen participation in an IoT
- 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
- Services piloted in two cities demonstrating the value of SocIoTal in the real-world.
- Engagement with users and developers

Figure 1 - Central Role of Communities in SocIoTal

Figure 1 details the central role of communities in SocIoTal and how the overall project leverages onto them to derive requirements, understanding needs and barriers, design use

cases and services and evaluate them with large pilots. It also shows how each project macro objective maps to a specific work package, the achievements of each are reported below.

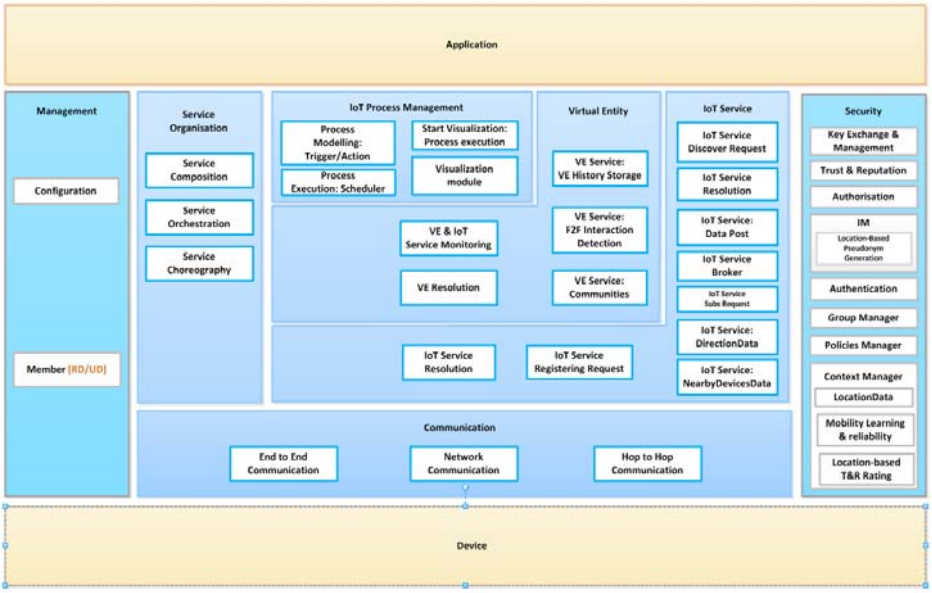


Figure 2: SocIoTal functional components

1.2 Current Issues

The private data and information flows that citizens provide to IoT infrastructures have a significant impact on people and societies, they can improve services, or enable innovative services in the first place (e.g. the traffic overlay in google maps relies on information (more or less voluntarily) provided by users. However, in order for this to occur there are a number of socio-economic and technological barriers that need to be overcome in order to enable IoT solutions that are inclusive to all of society. One particular aspect of IoT are the perceived privacy and security issues. It is critical to overcome these issues in order to enable a successful adoption of IoT in all areas of society. A high level of trust and confidence in IoT is crucial and therefore this is an important challenge which needs to be addressed.

In addition to trust, ease of management of an IoT system is critical in ensuring widespread uptake. This is necessary in order to provide sufficient motivation for citizens to contribute their devices and information flows to the system and therefore the community at large. Ensuring simplicity of the system will mean that it is easy for users to add manage the devices that provide information flows. In addition, it will provide a user with clear and immediate benefits which will provide motivation for the uptake of the architecture. In addition to ease of operation, the IoT system should provide transparency and adequate user control in order to ensure that a user has understanding of what is happening with the contributed devices and information flows. Transparency and user control ensures that the system is trusted.

1.3 Aims

The SocIoTal project addressed the issues related to trust, privacy and operability. The project designed a framework which encourages users to contribute their devices and information flows in order to unlock citizen centric information streams. This allows the creation of smart services which have high socio-economic value which address the needs and challenges of

individuals, communities and societies. Thus the project provided intuitive ways for users to contribute to and use the system while increasing the trust and confidence.

1.4 Achievements

Expanding the boundaries of its research beyond the limit of a single region or country and by reaching different European and non-EU realities, SocIoTal gained a deeper overview of current barriers to IoT adoption and proposes adequate strategies for effectively crossing them. SocIoTal research program has achieved the following objectives:

- Design of a socially-aware citizen centric architecture for an IoT framework providing services for cities, citizens and their communities. The designed SocIoTal platform ensures interoperability by proposing extensions to existing Architecture Reference Models (in particular the IoT-A ARM) and re-using existing components from other IoT platforms (such as FI-WARE and BUTLER).
- Specification and design of a governance, trust and reputation framework combining a set of innovative enablers that addresses the challenges of massive crowd-sourced IoT infrastructure.
- Research and development of a privacy-preserving context-sensitive communication framework for IoT devices with adequate security enablers to enhance security and privacy of users in discovering services and sharing their data.
- Support of citizen empowerment to easily manage access to IoT devices and information by specifying and designing an intuitive environment inspired by social media tools that provides increased awareness and controls. On the other side, addressing the design of a more powerful development environment allows IoT enabled citizen centric services to be created through open community APIs.
- Continuous support of proposed SocIoTal innovations with smart city trials evaluations and pilots of enhanced SocIoTal services in two cities thus demonstrating the value of SocIoTal to real word communities. Such services have been the result of citizens' involvement in the co-creation of rich use case scenarios of high societal value for their neighborhood, communities and cities.
- Continuously performing community engagement in order to understand the technological and socio-economic barriers for citizens' acceptance of IoT and participation to their services, by contributing to it with their devices and the data they generate.

The framework in available on GitHub (https://github.com/sociotal). The SocIoTal GitHub also includes a wiki with documentation and tutorials in order to provide support for developers and users. In addition, the SocIoTal consortium will provide further support through the GitHub "Issues" tab.

1.5 Expected impact

Technologically, SocIoTal contributes towards resilient and reliable IoT applications from citizen crowd-sourced IoT devices on a large scale. Novel reputation management mechanisms and trust models handle the reliability of IoT devices and respective data providers, thus automating derivation of reliability metrics of data sources or IoT devices. SocIoTal enablers for sensitive and privacy-aware communications, including the design of adequate security solutions, contribute to an overall increased confidentiality, authenticity, and integrity of the data sensed. The intuitive user environment allows ordinary citizens with little IT skills to develop resilient and reliable IoT applications, providing integrated support for confidentiality, authenticity, and secure exchange of data between selected circles of trust.

The SocIoTal project provides a methodology to enable the creation of community based smart city services that significantly contributes to a more sustainable and resource-aware society, by lowering the barriers for users adoption of IoT solution and their participation to co-creation of services.

This said, SocIoTal has the potential to unlock billions of citizen IoT device data streams to the Internet of Things, making them available for the exploitation of a growing European IoT solution and service economy. SocIoTal can thus open up new revenue streams for European suppliers for IoT based solutions and services to grow and expand their business on or for new innovative companies to emerge.

In fact, the possibility to commercially exploit its results and achievements appears already clear, in particular for the SMEs involved in the project. Some of the developed technologies, such as indoor positioning, face-to-face recognition and the intuitive user environment have the potential to reach the market either as a standalone product or integrated into existing ones, thus leading to the possibility of expanding existing business, for the involved SMEs, or establishing new ones, by spin-off activities from other consortium partners.

The dissemination of the results of the SocIoTal project has occurred through publications, talks and meetings with stakeholders. Academic publications have been one of the main channels for the dissemination of the results of the SocIoTal project. The results of the project have led to 28 conference publications, 22 journal publications and 2 book chapters including prestigious venues such as IEEE conferences. This number of publications shows the significant impact that the project has had within the academic community.

Further dissemination activities include presentations at workshops, of which there has been six. These have included the co-creation workshops with Nathalie Stambert. The co-creation workshops involved a varied audience of stakeholders, from representatives of tenants, councils and local communities to computer users and developers. The aim was for this varied audience to provide feedback and direction for the SocIoTal project.

Members of the SocIoTal project took part in 8 panel discussion at events such as IoT week. The topic of the discussions were the IoT field and current state-of-the-art and status of implementations.

Finally, the project has led to the filing of three patents.

Section 2 - Main Science & Technological Results and Foregrounds

The SocIoTal project introduced an IoT framework which is citizen-centric and provides privacy and security to the users' devices and information streams.

2.1 Framework

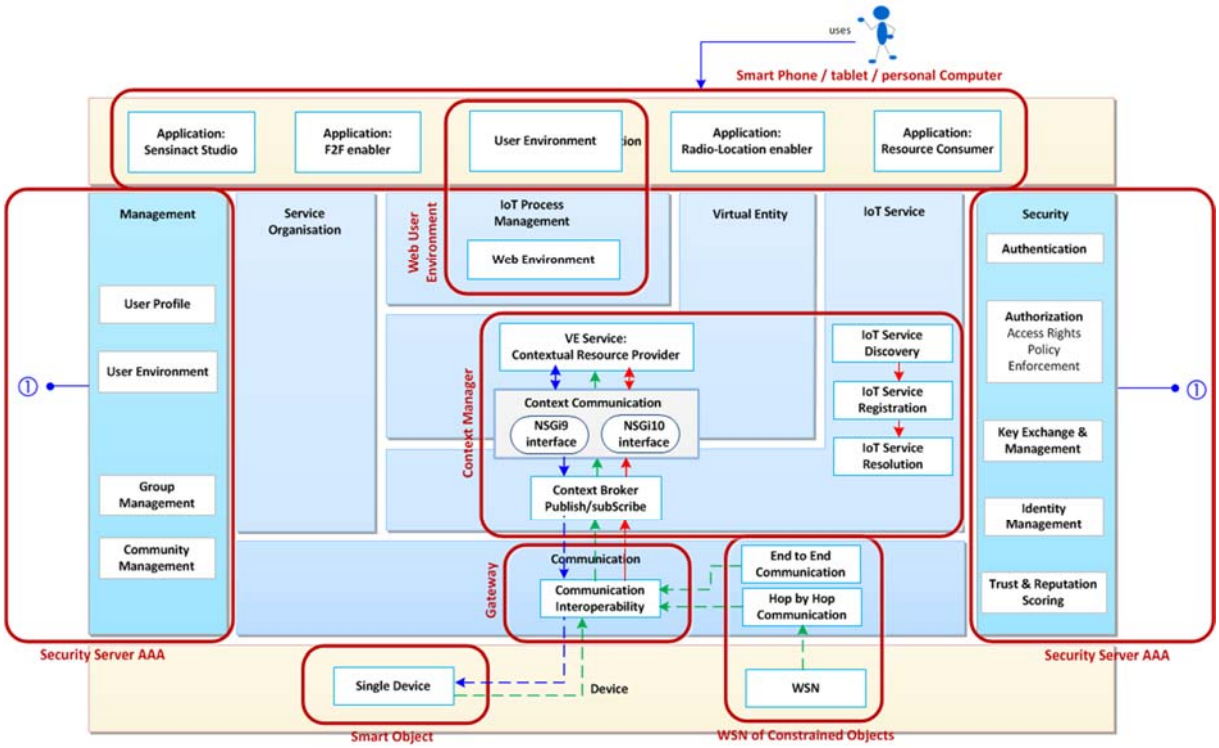


Figure 3: The architecture of the SocIoTal platform

2.1.1 Novelty

Today, a large number of different means are used to enable communication between heterogeneous devices. Furthermore, existing solutions do not address the scalability requirements for the future Internet of Things, they provide inappropriate models of governance and fundamentally neglect privacy and security in their design. IoT-A [12], the FP7 Internet-of-Things Architecture UE project, proposes the creation of an Architectural Reference Model (ARM) together with the definition of an initial set of key building blocks. Using an experimental paradigm, IoT-A combines top-down reasoning about architectural principles and design guidelines with simulation and prototyping to explore the technical consequences of architectural design choices. The architecture of the SocIoTal platform is based on the ARM framework provided by IoT-A. It provides several views with different levels of abstraction. Figure 1 shows the architectural view of an IoT system as defined by the ARM. It is composed of several blocks or Functional Groups (FG) supporting the various components involved in an IoT application and their interactions. The requirement process enables to derive the architectural views (Figure 3) from the application context.

The framework has been enhanced by the addition of frames (in red on the figure) that show the physical components that embed the underlying features in a goal of real deployment.

2.1.1.1 Results

With the project SocIoTal, new components and enablers compatible with Fi-Ware platform appear with the desire to ensure the functions of privacy by design in a user-friendly way for the user. The security server is enriched in order to manage the user identity, or rather its pseudonymity or his anonymity. The cryptographic algorithm “idemix“ implemented with the KeyRock component protects the privacy by the identity management embedded in the security server. Another component is the Trust & Reputation Manager, which allows to assign a “trust” rate to a user according to different criteria. This rate will be taken into account when assigning access rights to resources.

SocIoTal offers a user-centric scheme based on privacy. In this framework, the gateway does not anymore store the virtual resources. The resources are pooled and virtualized with their context by the Context Manager component. The security server enables a user to access securely to an authorized virtual resource ciphered and stored in the Context Broker, ensuring the confidentiality of the data within the SocIoTal platform.

2.2 Context Manager

The SocIoTal Context Manager (CM) supports the platform’s entities directory plus context information storage, accessed and managed through an implemented OMA NGSI9/10 compliant API rest interface. Since all SocIoTal platform components rely, one way or another, on context information provided by registered context entities, CM becomes one of the core blocks of integration within SocIoTal Platform.

2.2.1 Novelty

SocIoTal CM is based on OMA NGSI context models and interfaces and its core relies on FIWARE platform. From this point of view, the most novelties introduced by the SocIoTal CM come from the integration with the rest of SocIoTal components, providing support for F2F recognition, trust management or location information and the SocIoTal Security Framework, which involves:

- Integration with/support of Community-Tokens, which allows the organization of the registered entities within communities and restricts its access/management to community members.
- Integration with/support of Capability-Tokens, limiting the access to context information and management capabilities according the SocIoTal policies defined within the Security Framework
- Bubbles support that encrypts context information, granting access only to consumers that matches the attributes the bubble requires in every moment.

2.2.2 Results

SocIoTal project has released Version 3 of its Context Manager. This Open Sourced code allows users to download and install their own instance of SocIoTal CM with full support for context entities registration and management plus information sharing. Tutorials and detailed documentation is provided for final users to install and operate it, including integration with other SocIoTal components that allow full support for security functionalities and enablers’ context information.

The SocIoTal CM V3 has been also deployed in SocIoTal Platform Cloud instance, so a full working implementation of the SocIoTal Platform, including all features and web interfaces, can be tested and evaluated by end users and developers.

2.3 Privacy and Security

SocIoTal has designed different security technologies to deal with identity management, authorization, authentication, trust management and data sharing in IoT. These technologies have been designed, implemented and integrated altogether as part of the SocIoTal security framework. In the end, it enables a suitable, holistic and privacy-preserving security solution for IoT environments, which is based on innovative security technologies.

2.3.1 Novelty

The design and implementation of the security framework have been realized through the convergence of different technologies, that have been adapted and integrated with other SocIoTal components. The authorization is performed by implementing the novel concept of capability based access control augmented by the usage of security policies. The Identity management and authentication processes for IoT have been carried out by means of the adoption of a disruptive privacy-preserving mechanism based on private-ABC (Attribute Based Credential), i.e. Idemix, which was not applied to IoT scenarios so far. Regarding secure group data sharing among users, SocIoTal has developed, integrated and evaluated an innovative mechanism to perform the encryption based on attribute based cryptographic, which is also a trendy technology to cope with the data sharing in groups.

2.3.2 Results

Authorization

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

The authorization system is composed of the following sub-components. The Capability Client allows making request to the Capability Manager to obtain capability tokens, which are used to get access to resources hosted by other devices. The Capability Evaluator is a library intended to evaluate capability tokens. Such evaluation is based on the action and device being requested and the use of KeyRock authentication credentials. Capability Manager accepts requests for capability tokens generation and request authorization decisions to the Policy Decision Point (PDP) that makes the access control decision based on XACML policies defined through the Policy Administration Point (PAP), which, in turn, is an UI that allows users can define XACML policies in user-friendly way.

Identity Management and Authentication

The Identity Management (IdM) system follows a claim-based approach with Attribute Based Credentials (ABC). The IdM relies on the Idemix cryptographic library from IBM, providing additional means to deal with IoT scenarios where consumers and providers' can be not only traditional computers, but also smart objects (e.g. smartphones). The IdM endows users and smart objects with means to control and manage their private data in their smartphone, defining partial identities over their whole identity, which is derived from the credential obtained from

de Issuer. The usage of partial identities ensures a privacy-preserving solution with minimal disclosure of personal information. SocIoTal IdM has been recently integrated with Fi-Ware Keyrock IdM to support traditional Identity management operations in scenarios where claim-based accesses are not needed.

The Identity Management is composed of the following sub-components. The Android-Client that allows obtaining Idemix credentials from the Issuer server. It also allows interact with the Verifier server which can validate the partial identity derived from the credential. The Issuer-Server is a web application which allows generating Idemix credentials for clients. Communications are done by https. The client must be authenticated against the Issuer using a valid certificate. The Issuer also supports the verification functionality. The Verifier-Server is a web application, which can validate partial identities presented by the client application. The IdM-Enabled-Capability Manager allows users to obtain capability tokens using their partial identities. In other words, it allows authenticating and demonstrating their attributes by means of Idemix proofs of having a valid credential issued by the Issuer. Finally, the IdM KeyRock Client Java library provides a basic API for identity management by implementing a client to interact with the FIWARE KeyRock server. To carry out such communication, the SCIM 2.0 and Identity API v3 interfaces provided by this IdM are used.

Secure Group Sharing and KEM

The SocIoTal Group Manager component is based on the Attribute Based Encryption, namely CP-ABE cryptographic technology, which is 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 (also known as Attribute Authority (AA) or Key Manager(KEM)), and the Group Manager Client. The former accepts requests for CP-ABE keys generation. CP-ABE keys that are generated by the AA are associated to the attributes stored in the Keyrock IdM. The later allows obtaining cryptographic material (keys) form the AA, encrypt, decrypt as well as sharing encrypted information through the Context Manager. In addition, SocIoTal has developed an android App that allows secure data sharing procedures within SocIoTal bubbles based on CP-ABE cryptographic scheme by using the Group manager libraries.

2.4 Trust Management

SocIoTal Trust Manager is framework for quantification of trust taking into account contexts coming from different SocIoTal Trust components, i.e. location based trust, trust from the F2F enabler; but supports any additional context from the Context Manager to be included into the reputation score calculation. This component automatically subscribes to *on value change* in the Context Manager and re-computes the score maintaining the trust value updated and ready to be used by other application/services/components.

2.4.1 Novelty

SocIoTal Trust Manager is core trust component of the SocIoTal platform enabling user to use trust from different sensed phenomenon as an input for building the score for his application. Accordingly, this is the main innovation: provisioning of the trust quantification framework and it integration with other trust components in the platform, offering several layers of security as follows:

- Security by design achieved by utilizing Privacy and Security SocIoTal framework
- Application level security for building custom third party services based on different context values used as an input into the general model for the Trust framework

2.4.2 Results

This component is developed and deployed in the SocIoTal platform with documented API for adding rules that are used by the generic model to compute the trust score and push it to the Context Manager. Trust Manager is integrated with the Context Manager and it automatically subscribes to attribute value changes to continuously maintain the updated version of score in respect to last attribute in the Context Manager.

2.5 Communities and Bubbles

2.5.1 Communities

A SocIoTal Community defines a closed environment where only registered users and entities can share information: registered resources/entities will publish data that only registered users will be able to read. The original idea refers to a SocIoTal Community, created and managed by a SocIoTal user, as a group of users and resources with a common objective or inquisitiveness. A role set definition will decide who can do what within the community.

2.5.1.1 Novelty

The project defines and provides a platform-based communities structure, established between users and entities connected to the same infrastructure network. This structure, managed by the SocIoTal Communities Manager and built in SocIoTal Integrated Platform, provides centralized services to SocIoTal users, as creation and definition of communities, registering and management of users, adding information sources, roles management and so on. The entities and their associated context information added/registered within a community will be accessible only to registered users

2.5.1.2 Results

The developed Communities Manager (V1) provides mechanisms to register users, manage communities, assign resources (Context Entities) and request and validate Community-Tokens. These mechanisms are presented as a HTTP/HTTPS RESTful API divided into three main set of methods:

- Users API: groups the functionalities related to the users' creation and management. This set of functionalities are directly linked to SocIoTal IdM, using the provided JAVA API and its SCIM compliant interface. This way, all SocIoTal components link to the same shared user's directory.
- Communities API: contains the methods to create (and manage) communities and assign users and roles. It is implemented through the Keystone V3 API provided by the Keyrock instance of SocIoTal, shared also by the SocIoTal IdM. This way, SocIoTal IdM will have access also to the domains/communities schema created by the Communities Manager.
- Community-Tokens API: includes the request and retrieve community-tokens operations and the community-tokens validation. It is implemented over the same token schema SocIoTal IdM uses to validate users by user/password mechanism, so community-token can be also used to authenticate users

SocIoTal Communities Manager is available to download through SocIoTal GitHub. A complete tutorial to operate with communities, users and context entities is also provided.

2.5.2 Bubbles

A bubble comprises an interconnected collection of users and smart objects sharing the same set of trust policies, based on the existence of a strong relationship among them. Opportunistic Bubble is a kind of dynamic sharing group composed of a set of members that could be unknown each other. To be a member of a bubble, each member must satisfy a particular set of identity attributes given by the fact of possessing specific attributes in its credentials.

2.5.2.1 Novelty

The SocIoTal user environment allows defining group of users and devices as part of a **bubble**. Likewise, SocIoTal has devised a mechanism for sharing information within bubbles in a secure and privacy-preserving way, by giving users full control over their personal data disclosure. The Group Manager component of the SocIoTal security framework is based on the use of the CP-ABE cryptographic scheme in order to enable a secure data sharing mechanism with groups of entities belonging to a bubble. The disseminated data is encrypted under an attribute policy so that only those entities fulfilling the policy (i.e. members of the bubble), can decrypt and access the shared data. The data is shared by means of the Context Manager that in this case acts as data broker.

2.5.2.2 Results

The Group Manager component has implemented and integrated in SocIoTal and it enables secure data sharing between members of the bubbles defined by the web user environment. The Group Manager is based on the CP-ABE cryptographic 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. In addition, SocIoTal has developed an android App that allows secure data sharing procedures within SocIoTal bubbles based on CP-ABE cryptographic scheme by using the Group manager libraries.

2.6 Enablers

Three enablers were created for the SocIoTal project. The aim of the enablers was to use novel technology in order to perform an action. Three enablers were designed for the project. The *face-to-face enabler* determines social interaction based on proximity. The *gait recognition enabler* authenticates using the walking style of the user. The *location-based enabler* determines the current location of a person indoors.

2.6.1 Face-to-face enabler

The face-to-face enabler [D3.1.1] [D3.1.2] was designed in order to infer and categorize human inter-actions and then translate this into a machine readable format. In order to detect face-to-face interactions, the enabler keeps track of user's facing direction and detects nearby devices by performing Bluetooth discovery. The knowledge of the users' interpersonal distance estimation and relative orientation computation is combined to infer if the users are performing a face-to-face interaction. Through the novel use of the Bluetooth signal in smartphones, human interactions are placed into three categories, Public, Social and Personal, and from this, trust relationships are inferred. The communication of these relationships are communicated to the Trust Manager in order to be used in the trust calculation.

2.6.1.1 Novelty

As opposed to previous approaches, we designed, implemented and evaluated a novel approach for detecting face-to-face interactions by using only off-the-shelf mobile phones. The first contribution relates to collaborative sensing and inference, where the devices sense, exchange that data and infers based on the retrieved data. The system operates in a fully distributed way, without the need of any centralized coordinator. Each device performs the inference online in order to eliminate any privacy issues and does not transmit the data to third parties. The logged data are available only at the user's disposal. Regarding the inference that is performed, the system detects nearby devices, estimates their interpersonal distance with respect to each user through a novel machine-learning technique based on Bluetooth RSSI and computes the relative orientation of the users based on their facing direction. In particular, the application detects the on-body position of the device, estimates the direction of the user and keeps track of it. It exchanges with the nearby devices the direction of the user, calculates the relative orientation and proximity with each user and finally performs classification, depending on the selected target class, about the occurrence of face-to-face interaction. Currently to our knowledge, there is no work that detects face-to-face interactions based on collaborative sensing, proximity detection and relative orientation in real-time without restrictions about specific on-body position, firmware modifications or third party system to perform the inference which preserves the user's privacy.

2.6.1.2 Results

The enabler was evaluated in a lab environment and in real-world environment. The real-world environment experiment [D3.1.1] served the sole purpose of evaluating and proving the viability and robustness of face-to-face enabler in a real-world situation. The online analysis of inter-action zone and proximity detection provided a solid investigation regarding the accuracy of the method. Subsequently the online analysis of the system was implemented to substantiate the sustainability of user direction combined with the proposed proximity detection model for face-to-face interaction detection. The enabler as a coherent system detected accurately 81.40% of the interactions in a real-world environment, similar accuracy to a state-of-the art technique based on RFID-tags that is more obtrusive. In addition, the novel interpersonal distance estimation technique was evaluated in an office environment [D3.1.2] to understand its accuracy against the state-of-the-art techniques. 48000 Bluetooth signal samples were collected in a normal office environment, where water-filled bottles were used to simulate the effect of human body. The proposed interpersonal distance estimation technique outperformed the state-of-the-art solutions and achieve up to 93.52% accuracy for interaction zone quantification and 88.5 for proximity detection.

2.6.2 Gait recognition enabler

The gait recognition enabler was designed to establish the trustworthiness of the data stream coming from a smartphone. In an environment where smart phones are performing both sensitive transactions and are producers of sensitive data, it is important to know whether the phone is in the hands of the *rightful user* or an *imposter*. The gait recognition enabler uses the accelerometer sensor to obtain data on the walking pattern of the user. It uses this to determine whether the current holder of the phone is the *rightful user* or an *imposter*. This information is communicated to the Context Manager and is then used by the Trust Manager in order to be used in the trust calculation.

2.6.2.1 Novelty

The aim of the gait recognition enabler is to provide a novel method to authenticate users. The enabler authenticates users *passively* without them having to perform an action such as

entering a password or providing their thumb for fingerprint recognition. This enables authentication to take place in the background and to even occur when the user is not physically using the phone.

The novelty of the algorithm to perform gait recognition is that it uses a phase space to represent the dynamical system that is formed from the accelerometer readings while the smart phone is in the user's pocket. A lower-dimensional manifold on which the data lies is then identified in the phase space. This manifold is used to distinguish the *rightful user* from the *imposter.*

2.6.2.2 Results

The gait recognition enabler was evaluated in both the laboratory and real-world environments. In D2.3 the performance of the gait recognition algorithm was compared with another gait recognition algorithm and it was shown to exceed it in terms of performance. D2.3 also detailed the performance of the algorithm in a real-world environment with ten users. Ten users were used to evaluate the performance of the algorithm in an urban environment. The results showed that the algorithm was able to differentiated between the *rightful user* and the *imposter* based on the walking pattern of the user.

Further evaluations occurred in D5.2 where the enabler was trialled with 10 users. The trial involved an extended test in a real-world environment with a larger number of users than previous tests. Users invited to participate in the trial were issued with an HTC One S smart phone with the Gait Recognition Enabler installed. They were instructed to walk home from work with the App activated, following any route they desired. During this time, the Gait Recognition Enabler would construct a model of their normal walking pattern using one sequence of walking data. After the model is constructed, The Gait Recognition Enabler would then authenticate the subsequent walking sequences using the previously constructed model.

Upon returning the phone, all the data was extracted. The data was then used to construct the models of normal walking for each user, and then, to test the system in detecting imposters, the user data of the remaining subjects was applied to the model to determine the number of anomalies detected. This evaluation included user feedback which was requested once the users had been given the results. Feedback from the users stated that they trusted the application, with an average users trust score of 8.4/10.

In summary, the Gait Recognition Enabler is able to provide a novel authentication method that will authenticate passively with no interaction from the user. The algorithm that performs the gait recognition was evaluated on walking data sets in the laboratory and is shown to have performance that exceeds state of the art. The enabler was also trialled in a real-world environment twice and it is shown to operate as expected and that users have a high level of trust in the application.

2.6.3 Location-based enabler

2.6.3.1 Novelty

The geo-localization enabler is used to follow the displacements 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 and calibrated 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 algorithm, the mobile node has the ability to estimate its distance from each anchor node 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 transmits this information to the Context Manager to be stored and available 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.

2.6.3.2 Results

The enabler has been deployed and tested in the offices of the CEA, at the first floor of the building. Nine anchors have been placed in the corridor and in the meeting room. A person wearing a sink node is moving in the building according to his activities. The collected raw information is sent to the fixed gateway located on the same floor and processed to compute the coordinates localizing the person within the building. This information is ciphered and pushed to the context manager to be stored. An end user sharing the secret key is able to get the information and deciphering the coordinates. By this way, the moving of the person that wears the sink node can be followed on a map of the building.
This enable to optimize some parameters as the temperature or the air conditioned for the wellbeing of the occupant and to save energy by heating only the rooms that are living.
A video is available to show the performance of the whole system and its reactivity.

2.7 Web and Mobile User Environment

The complementary Web and Mobile User Environments were conceived and designed to provide intuitive mechanisms and tools to the users, for expressing the way in which they want their IoT environment behave. In particular, the Web User Environment provides a complete personal dashboard as a user-friendly and intuitive workspace in which every user can compose data coming from sensors, devices and services. It allows also to manage registered smartphones and to set simple data-based devices composition using a WHEN event DO action a paradigm. Finally, it is capable to analyse in near real-time the data produced by devices to report potential anomalies detected on them. The Web User Environment integrates all the developed platform security-related components and also allows managing physical objects in a user's social circles (communities), under well-defined privacy and security policies. A set of Web API completes the range of available features in order to provide an open platform and tool to developers.

The Mobile User Environment is an extension of the Web User Environment providing a mean for a user to acquire the device profile via QR code to his workspace, views to manage operations on the mobile, extract latest measurements, removing device from the workspace as well as to receive push notification that could be generated as a triggers from the Web Environment.

2.7.1 Novelty

The Web User Environment provides a user-friendly workspace specifically targeted to final users and not to skilled people. On some aspects it uses simple paradigms also adopted by consumer products like IFTTT (like in connections mechanism) whereas it integrates all the

security and privacy aspects required by a modern, secure, consumer-friendly IoT Web application.

Moreover, supporting by default social circles as communities it allows to securely share devices, other physical "things" and data with other people in the same community.
The responsive and documented workspace makes simple managing users' connected "things" and starting collecting produced data. The anomaly detection feature represents another novelty included in an IoT Web environment: a Three-Sigma Rule algorithm is automatically applied in near real-time as data flows from devices and it allows to immediately detect and report anomalies on data to the user, in a visual way.

A main innovation of the Mobile User Environment beside the integrated security and privacy mechanisms provided by the platforms and enablers is the co-creation aspect and the fact that the application is built by using the feedback from the end-users. The RRI (Responsible Research and Innovation) methodology was used with the attempt to indirectly tackle the possible uncertainties that may arise when developing the product which will be used by a target group.

2.7.2 Results

Web and Mobile User Environments are the main tools of the SocIoTal platform targeted to final (not experts) users.

They have been used during all the project dissemination activities involving citizens and developers, like during several Meetups, workshops and evaluation sessions. In particular, thanks to the feedback received from attendees, the tools have been greatly improved concerning both exposed features and user experience (UX), sometimes resulting in re-design from scratch of the UI and UX, like in the case of the Web User Environment.

The latter allowed people to use it as the entry-point to the SocIoTal platform. The Web User Environment allowed them to connect devices and services to build new, simple and secure personal IoT applications based on SocIoTal, or to experiment with devices and produced data.

As a result of the above mentioned approach, the provided User Environment has been released and already used in some pilots as well as in research and startup community. The Hackathon organized during the project lifetime was fertile ground for experimenting and evaluating the User Environment which resulted with release of services such as Alcohol Breath Analyser, Air quality monitoring, Green Area monitoring, Fire detector, etc; all built mainly using User Environment components by users and citizens with no developer expertise. The Alcohol Breath Analyser grown into startup involving more interested parties into this third party project based. Another startup was using SocIoTal components for the project Noise pollution monitoring

2.8 Developer Environment

2.8.1 Novelty

The developer environment developed by CEA, namely sensiNact Studio, is a tool that allows developing, deploying and managing IoT applications interacting with the devices connected to the sensiNact platform. It is based on Eclipse and built as a rich-client platform application. The Graphical User Interface (GUI) is developed using the views mechanism from Eclipse.

Thus, it proposes many view related to browse devices, locate devices on a map and interact with devices, i.e. get value from sensors or perform an action on an actuator.

The Studio is also dedicated to the creation of IoT application without particular knowledge of any specific software development language. Written in a Domain Specific Language (DSL), an IoT application includes an Event-Condition-Action (ECA) rule, which defines the behavior of devices in the case of the occurrence of event and the verification of one or several conditions.

2.8.2 Results

The sensiNact Studio eases the development of applications for developers. The application can be deployed and monitored in a few clicks, which gives a rapid feedback, essential for rapid prototyping of IoT applications. The tool has been successfully integrated with the SocIoTal core platform. A specific NGSI communication bridge has been built for the integration. The tool can be used to retrieve SocIoTal assets including with their trust and reputation scoring. The tool also support the encryption process of data soted in the SocIoTal Context Manager.

2.9 Engaging the Community

Community engagement formed a key aspect of the SocIoTal project. Throughout the lifetime of the project, users and developers have been engaged with the project in innovative ways in order to maximize their input and stake in the project

2.9.1 Novelty

The project included the role of Community Manager, who's role it was to engage with developers and users. This allowed input from users and developers into the direction of the project at an early stage. The role of the Community Manager was to drive the interactions and perform studies in order to identify barriers. For example, the project performed a study in order to determine the technological and socio-economic barriers to participation in IoT.

2.9.2 Results

The study determined that there were three main barriers, these are

- Lack of third party trust providers
- Lack of oversight for SME's in the technological landscape and success stories
- Lack of rich scenarios

The SocIoTal project created and delivered a citizen-centric socially-aware Internet of Things by leveraging composite ecosystem of stakeholders involving different actors. The Community Manager engaged with stakeholders from city councils, developers and SMEs and citizens. From the identified barriers to their inclusion in IoT, a set of incentive and engagement strategy was defined. Lowering the barriers to inclusion using methods such as Meetup and co-creation workshops ensured that the SocIoTal project involved and listened to a broad range of stakeholders and they added direction to the project.

2.10 Pilots

Based on the SocIoTal architecture and SocIoTal developed platform (including SocIoTal core components and enablers), one of the project's target was to implement at least two different services in Novi Sad (Serbia) and Santander (Spain) in order to demonstrate, as field trials, the new SocIoTal Integrated Platform capabilities whilst creating new value added services for citizens. This also provided an evaluation of all platform components, involving real users, facing all the constraints and limitations that a complex society can pose in these kinds of deployments.

2.10.1 Novelty

The final implementation of the selected services involves two remarkable aspects: the deployment of the SocIoTal tools in the real and dynamic environment of a city, and the final involvement of the users, citizens and developers, who actually evaluated SocIoTal novelties. The first task has been undertaken relying on the previous integration processes, the trials of the different components of the platform and new implementations to shape the final scenarios. Regarding the involvement of the citizens, it has been the result of the work accomplished within SocIoTal and related to engagement activities such as Meetups, information meetings, presentations, tutorials, etc.

In order to come full circle, a complete evaluation process has been performed by gathering feedback from end users, with different profiles, and realising the correspondents quantitative and qualitative analysis of the tools.

2.10.2 Results

As a result of the above mentioned processes, SocIoTal defined, developed and evaluated, involving end users, 4 pilots:

- DisApp [Santander City] (Adapted route calculation for disabled people) pilot, that provides disabled citizens with an application to go from one place to another in the city, avoiding barriers along their journey (works, road closed, narrow sidewalk, etc.), creating a community of users that feeds the application by uploading and sharing information about obstacles.
- Sharing Info [Santander City] pilot, oriented to developers and the whole SocIoTal capabilities exploitation, by providing this collective with the required tools, tutorials and workshops to access and use them. With this, the target of the pilot is to reach the maximum groups of developers and get them to propose ideas, build simple apps and/or include their own sets of devices.
- Mood of the City [Novi Sad City] pilot, where the mood of the city is measured by taking multiple parameters as an input, emotions (neutral, sadness, surprise, happiness, anger, contempt, disgust and fear), age and gender. The final Mood of the city value is computed as an index using aggregated users' data, i.e. users' mood detected from camera. A deployed "Smile of the city" totem, invites potential users to smile and download mobile applications to get involved in numerous activities related to development of Novi Sad into a smart city.
- Elevator supervisor [Novi Sad City] pilot, that enables tenants to monitor elevator distance travelled between inspections and to alert them when the malfunction happens. In order to engage testers, there were two events with end-users from different associations to invite them to participate in the pilot.

The results obtained from end users' feedback provided the information to be able to mine the conclusions about what are the strengths and weaknesses of the whole platform, thus extracting the lessons learnt for future implementations and deployments

2.11 Science & Technological Objectives

In this section, the S & T objectives are detailed and how the project addresses them.

2.11.1 Objective 1: To design a socially-aware citizen centric architecture for an IoT eco-system providing services for cities, citizens and their communities.

The design of the SocIoTal platform has made significant advances in the design of citizen centric architectures. The architecture design is based on the ARM framework provided by IoT-A. The architecture is aimed at being citizen centric by providing services which are easily set-up and maintained by both developers and non-developers. This is performed through the use of innovative web and mobile applications and underpinned by the Context Manager. The security framework in the architecture ensures that the information flow in the eco-system in secure and can be easily set-up and maintained by users.

2.11.2 Objective 2: To explore a robust and distributed IoT governance framework based on IoT identity models that encompasses the notion of dynamically changing communities and take into consideration their impact on privacy and trust relation.

The SocIoTal project designed a framework for IoT governance which enables citizens to easily add devices and information streams. The governance framework developed as part of the SocIoTal project aims to provide security and privacy while maintaining user control and ease of operation. Innovative approaches to context storage and security management have lowered the technological skills required for users providing a system which is set up and managed more easily.

The notion of easily sharing information with subsets of users is managed using the concepts of communities and bubbles. The SocIoTal framework allows devices to easily share information based on intuitive concepts such as communities and bubbles. The framework provides an easy interface with which to manage communities through the web user environment. In addition, bubbles form more temporary sets with which to exchange information by exploiting temporal aspects such as proximity.

Issues of trust relationships are managed with the enablers and the trust manager. These components ensure that citizens are able to easily control access to the information streams using intuitive and novel applications such as the face-to-face enabler.

2.11.3 Objective 3: To enable more automated forms of discovery and specification of trust relationships between humans and a translation of those to their devices as well as the establishment of reputation of IoT devices/data providers.

The aim of this objective was to reduce the technological barriers by simplifying the setup and management of the IoT infrastructure. This was performed through three enablers, face-to-face, gait recognition and location-based, were implemented as Android Apps and aimed to provide a user with a simple. For example, the face-to-face enabler provides a translation of human relationships into a machine interpretable setting, allowing the SocIoTal framework to

detect relationships in the real-world and then to infer trust from them. The gait recognition enabler ensures that the current users of the phone is the correct user, this ensure that information streams from the phone are actually from the user identified with the phone and not an imposter.

The Trust Manager provides the analysis for the metrics produced by the enablers. It is the role of the trust manager to interpret disparate scores from different events and provide a level of trust. By subscribing to events from the Context Manager, the Trust Manager is able to obtain the latest events registered by the enablers to determine the current level of trust.

2.11.4 Objective 4: Enabling secure, context-sensitive, privacy-preserving communication between IoT devices through a framework and novel security enablers

This objective was fulfilled by devising and implementing a context-aware security Framework comprised of different security and privacy-by-design mechanisms and enablers, such as, trust management, authorization, Identity Management and group management.

The authorization is performed by implementing the novel concept of capability based access control augmented by the usage of XACML security policies. The Identity management and authentication processes for IoT have been carried out by means of the adoption of a disruptive privacy-preserving mechanism based on private-ABC (Attribute Based Credential), which was not applied to IoT scenarios so far. Regarding secure group data sharing among users and smart objects, SocIoTal has developed, integrated and evaluated an innovative mechanism to perform End-To-End data encryption based on attribute based cryptographic, which is also a trendy technology to cope with the data sharing in groups.

SocIoTal has designed and implemented a privacy-preserving Identity Management system based on Idemix, that has been integrated with Fiware IdM (Keyrock) and other components of the framework (like the Authorization and Group Manager). It enables that the security in changing communities and bubbles can be tackled through the dynamic attributes hold in the IdM along with the usage of attribute based encryption mechanisms. Moreover, users can preserve their privacy when are authenticated and access to target devices and services using their attribute based credentials, as the IdM endows them with means to control and manage their private data in their smartphone, defining partial identities over their whole identity, which is derived from the credential obtained from de Issuer.

2.11.5 Objective 5: To investigate mechanisms and corresponding tools to empower citizens to manage and share their IoT devices with others in different circles of trust and to provide them with an increased awareness and control. SOCIOTAL aims to provide tools for citizens to create, network and share their personal IoT, making it organic

SocIoTal defined the concept of “Communities” based on the types of relationships among smart objects and users. In this case, the usual driver of communities is the common interest relationship, putting together users and information related to a similar target or application. This way, a community is a secure cooperation between different producer users, making entities (devices, services, events, resources etc.) available to selected consumer users (community members), to achieving a common objective. A SocIoTal Community, created and managed by a SocIoTal user, provides a closed environment where only registered users and entities can share information: registered resources/entities will publish data that only

registered users will be able to read. A role set definition will decide who can do what within the community.

The Communities Manager component, developed and published by SocIoTal, provides the end user with the functionalities to create and manage communities. It is integrated with SocIoTal IdM, so SocIoTal Communities are linked to SocIoTal registered users thus allowing the community's members definition, and with the SocIoTal Context Manager, so registered context entities can be associated to existing communities, restricting its access to community members.

2.11.6 Objective 6: To understand the technological and socio-economic barriers for a citizen participation in the Internet of Things and the nature of incentives that would encourage an increased citizen engagement.

The SocIoTal project undertook a study to understand the barriers to citizen participation in IoT. The study found that although IoT has huge potential, there were three main barriers towards sustainable public adoption of IoT. The first is lack of trust. The SocIoTal project addressed this by offering a secure platform that individual citizens can use to expose their own IoT devices to a community of users that they choose. The second barrier is lack of inspiring use-case. The SocIoTal project addressed this by using co-creation workshops early in the project to produce use-cases which are relevant to citizens. The third barrier is the lack of awareness of citizens. The project addressed this by setting up Meetups in five cities and investigating the kind of activities that could be host and the relationships that could be established. This is documented in Deliverables D6.1 and D6.3.

In addition to the study, the project undertook direct involvement with citizens through co-creation workshops and meetups. This allowed citizens to have a direct participation in the project and allow the understanding of the technological and socio-economic barriers that citizens face. For example, Meetups hosted in five cities allowed both developers and non-developers to access and use the platform, providing feedback on the technology and opinions about usability. Co-creation workshops were used to allow citizens to provide use cases for the technology that the SocIoTal project was creating. Discussions at the co-creation workshops allow the identification of current barriers. These included a mentality change for citizens, where members of a local community consider the local amenities as belonging to them rather than the local authority. In addition, a mixing of responsibilities between the public and private organizations so that citizens do not feel that everything has been determined without consultation.

A product of the project is the "Stakeholder Coordinator Toolkit". The SocIoTal toolkit addresses, in the form of a workshop, the three main barriers to broad adoption of Internet of Things that were identified in the project: lack of understanding by SME's and City Councils, lack of third party trust providers and lack of involvement of end-users in building use-cases and developing news services. For each of these three main barriers, the workshop offers solutions.

2.11.7 Objective 7: To realise and trial innovative services of high societal value based on citizen/city centric IoT infrastructure with clear benefits for communities and their citizens.

In order to provide citizens with tools and mechanisms to lower the barriers of participation in the IoT domain, the WP5 focuses its work on the design, deployment and coordination of different pilot services, thus demonstrating the applicability of the tools and techniques

developed in the rest of work packages and finally bringing the experiment to the citizens, creating each corresponding field trial that will also collect the involved citizens' feedback. Through co-creation workshops, meet-ups and previous initiatives, such Santander City Brain, SocIoTal collected citizens needs and requirements in order to define a set of potential services to be developed on top of SocIoTal platform and oriented to offer end users new innovative services based on IoT and information sharing. After a thorough evaluation of the different options, a final set of four pilots, including developed services and their corresponding field trials where implemented and evaluated by final users in two cities: DisApp pilot, that provides information to disabled people, uploaded by disabled people (making use of the Communities concept); Sharing info, that fosters developers' adoption of SocIoTal functionalities; Mood of the City that exploits SocIoTal features within SmartCity environment; and Elevator supervisor application, making use of SocIoTal user's interfaces to manage information gathered from sensors in an elevator.

2.12 Key Performance Indicators

Key performance indicators (KPIs) were defined during the project proposal in order to determine the success of SocIoTal in reaching its goals. The KPIs were revisited during the second year of the project in order to adapt them to the direction of the project. The KPIs are listed in .

Description of Work			Updated KPIs to be used for the measurement of project success		
Category	**KPI**	**Initial Threshold**	**KPI Description**	**KPI Threshold**	**Achieved**
Citizen participation	# Followers	1,000	# People involved in meetups and co-creation workshops	1000	1635
	# Active users	100	# Field trial participants	50	165
	# contributed IoT devices or streams	800	# Sensors, mobile devices, users and entities supplying data to the platform	500	231
Services	# Services realised in project trials	4	# Services created by modular components of SocIoTal	4	6
	# Services from developer community	4	# Projects developed from hackathons	4	3
Developer participation	# Followers	100	# Developers exposed to SocIoTal tools	100	88
External to the consortium	# Registered developers	20	# Active developer participants (use and extend the framework)	50	16
	# Active projects	5	# External projects using the platform	5	5
Wider community uptake	# No cities interested in SocIoTal replica	5	# Organizations in the platform	5	0
	# Projects contributing in new IERC AC	5	# No. of contributions of SocIoTal to IERC activities	5	0
2nd and 3rd year feedback	Not in DoW		# Questions from developers regarding APIs	100	35
	Not in DoW		# Users involved in incentive mechanisms	NA	42
	Not in DoW		Qualitative feedback from users based on questionnaires on utility of pilot services	NA	5
	Not in DoW		# Qualitative feedback from users on intuitive user environment	20	25
	Not in DoW		Qualitative feedback from developers	50	36
Security KPIs	# Users using security and privacy functionalities by default	75%	# Users using security and privacy functionalities by default	100%	100%
	# Users providing feedback about the security and privacy	30	# Users providing feedback about the security and privacy	40	12
	Number of services that use secure communication among devices	4	Number of services that use secure communication among devices	6	6
	Number of device centric enablers supporting secure establishment and trust management	2	Number of device centric enablers supporting secure establishment and trust management	3	3
	% of coverage of different kind of SOCIOTAL entities in secure group communications	100	% of coverage of different kind of SOCIOTAL entities in secure group communications	75	75
	Number of secure and privacy components envisaged to be developed	4	Number of secure and privacy components envisaged to be developed	5	5

Table 1: KPIs for the SocIoTal project

The KPIs have been used to measure the impact of the project in 7 categories; citizen participation, services, developer participation, external to the consortium, wider community uptake, 2nd and 3rd year feedback and finally security. The results show that the project has been successful in meeting the pre-determined KPIs and has therefore had the desired impact.

Section 3 - Impact

One of the aims of the project was to maximize the impact of the project through as many channels as possible.

3.1 Exploitation

The results and components from the projects will continue to be exploited beyond the end of the project.

3.1.1 University of Surrey

The enablers created as part of the SocIoTal project will further exploited in future projects. The technology that underlies the face-to-face enabler is being exploited in the TagItSmart EU project in order to determine proximity to items. This will aid in context-aware scanning of smart codes. The gait recognition app will also be used in the TagItSmart project in order to provide authentication. The method will be further refined and used in conjunction with other authentication methods to provide multimodal authentication.

The trials of the components designed by UniS has led to improved knowledge in building IoT infrastructures and solutions that are socially acceptable. This knowledge will be exploited in future projects in order to align technology more with the requirements and acceptability of end-users and developers.

The SocIoTal project has enabled UniS to identify further research challenges that need addressing the field of IoT. This knowledge has already been used in one EU project proposal and will be used in further research and project proposals in the future.

The project has strengthened the knowledge of sensing using smartphones. This will be applied to the H2020 TagItSmart project and in future EU project proposals.

3.1.2 COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES

The geo-localization demonstrator is a proof of concept implemented with nodes from openMote technology using IEEE 802.15.4 wireless radio, which incorporates both end-to-end security and the confidentiality of the data stored in the cloud. Several applications may be derived, in particular in the field of Smart Building, in indoor, for intelligent energy management, including the heating.
The precision of the geo-localization system can be further improved by the use of technologies as Lora or Bespoon instead of openMote. However, the algorithms for computing coordinates from the collected RSSI measurements are performant including in an embedded environment.

The techniques to generate and manage pseudonyms for the MAC addresses can be used for many applications of the IoT where the confidentiality of the installation is required. Still under development and tests, these techniques can be deployed shortly on a PoC and integrated into a complete system IoT. They present the advantage of being very light and show unprecedented performance so far. They carry a real potential.

sensiNact Studio is a tool to develop, deploy, supervise and manage IoT applications. It is based on Eclipse framework and integrated with the sensiNact open platform, which will be released as an open source project within the Eclipse community.
The objective is to allow a community of developers to continue improving the tool and to reach to industrial adoption of the platform within the Eclipse business community. The tool will be

released as the Eclipse Public License (EPL). Value added add-ons on top of the tools will be provided by CEA to its industrial partners under proprietary license. We expect to improve the tool by adding properties such as dependability and robustness in further research. The main impact we expect is that the sensiNact platform and tool used by an increasing number (more than 100) of developers, SMEs, startups for commercial exploitation within a time frame of 2 years)

The patented secret key generation and distribution method aims at securing wireless communications in small groups of wireless devices in a decentralized and ad hoc way. Accordingly, it is applicable into many contexts, including IoT and WSN applications or device-to-device communications (e.g., in WiFi Direct, 5G D2D, smartphone-based physical social applications, IoT “bubbles of trust”...)... Even if initially designed for (and particularly suitable to) wide-bandwidth systems, it can be easily adapted to various radio technologies and standards, including narrow-band ones. This technique, which has been mostly validated through realistic simulations so far (including ray-tracing predictions), shall be further tested through experiments internally and in the frame of upcoming collaborative research projects. Relying on the filled patent, the proposed technique might be transferred in turn to industry.

3.1.3 CENTRO DI RICERCA, SVILUPPO E STUDI SUPERIORI IN SARDEGNA

The Web User Environment platform, created as part of the SocIoTal project, along with some of the modules developed and adopted solutions, will further exploited in future projects. That, in order to experiment and build more socially acceptable and trusted modern IoT platforms and solutions, in particular stressing the social aspects and investigating how to improve the overall experience for end users. Moreover, the security paradigms adopted during the platform integration will be a foundation pattern to be further investigated in future, in designing and developing secure platforms for the IoT.

Some selected and adopted best-practices in API design have proven their validity and will be used also for future, API-based, software modules and integrations.
Generally, the developed knowledge has already been used in one EU project proposal and the existing prototype will be used to attract new research partners and to successfully apply to other international funding programs.

Finally, the evaluation methodology defined and applied during the SocIoTal project will be a solid tool for out-of-the-lab future evaluations of developed applications. That methodology has been validated involving real users, developers and citizen, in order to collect their feedback. Feedback that driven the continuous, iterative improvement of the SocIoTal tools.

3.1.4 DRUSTVO ZA KONSALTING, RAZVOJ I IMPLEMENTACIJU INFORMACIONIH I KOMUNIKACIONIH TEHNOLOGIJA DUNAVNET DOO

The experience and outcomes of the project will be exploited in following manner:
Engaging users and co-creation process: this is expertise acquired during the project. The methodology and activities done in the project have proved to be successful and we are now using this approach when interacting with our (potential) customers. This is in particular applicable to the process of definition of system requirements. Further to this, thanks to the activities done on the engagement of SocIoTal stakeholders (in particular meetups), the company significantly raised its profile not only in the research community, but also in the business domain as well as general public.

FIWARE experience: Implementation of SocIoTal platform helped us to further strengthen our FIWARE competence which will contribute to more efficient implementation of our FIWARE based solutions in the smart city and smart agriculture domains. Further to this, SocIoTal platform components are now considered for inclusion into our cityNET and agroNET solutions. Module for trust and reputation is being considered for integration with our myNS smartphone application. The Smiling kiosk pilot is deployed in Novi Sad as a permanent installation and is now being offered to other cities and organizations.

3.1.5 Resonance Design

The SocIoTal Stakeholder Coordination toolkit, a solution to the identified barriers, is made available as a commercial offering by Council in the form of a smart city workshop in order to systematically engage with the different identified SocIoTal stakeholders and to continue to design new rich use cases, based on effective business moments, thus generating potential value for each involved actor.

See http://www.theinternetofthings.eu/smartcityworkshop

3.1.6 UNIVERSIDAD DE CANTABRIA

SocIoTal integrated platform, as one of the main outcomes obtained from the project, will be used to promote IoT usage among end users (citizens and external developers) by including it as an option in open calls belonging to projects where UC is involved (such Organicity) or reusing part of it in concrete developments, as in Wise-IoT. In this line, it will be also included within University of Cantabria courses, as part of specific IoT and smartcity labs and promoted in vocational training, as IoT guided activities. To achieve this, UC, as SocIoTal technical partner, will provide support in those events and activities where it promotes SocIoTal Integrated Platform.

Specific SocIoTal components developed by UC, such SocIoTal Communities Manager, will be enhanced to be included as part of Santander Smart City set of functionalities, oriented to exploit the concept of SocIoTal Communities and secure information sharing in oncoming IoT initiatives. These functionalities will be also offered as part of the Santander smartcity testbed.

Experience in Co-Creation workshops and the Santander IoT Meetups structure will also leverage future citizens and developers' engagement, as well as to obtain new use cases and pilots to be developed.

3.1.7 UNIVERSITY OF MELBOURNE

Australia is an urbanized society and more than 89% of the population lives in cities and this trend is expected to further increase in the future. The possible applications of future Internet technologies in cities are diverse, ranging from sustainable management of transport, constrained resources and utilities for managing ecological impact on the environment, and providing improved health and social care, and citizen engagement in decision-making. The Internet of Things (IoT) technology enables devices to be connect, communicate, decide in the cyber world, and eventually control the physical world. We have setup Internet of Things (IoT) testbed for real-time environment monitoring in the City of Melbourne. Specifically, we have deployed sensor nodes at two technically-strategic locations: Fitzroy Gardens (five sensor nodes) and Docklands Library (four sensor nodes). Each node measures temperature, light and humidity levels. The sensors were deployed near tree canopy cover to measure the effect

of tree canopy coverage against the urban heat island. The deployments were made in consultation with the Urban Forest Monitoring team from the City of Melbourne city council.

The data was collected for over a calendar year continuously ZigBee communication between sensor nodes and base stations. 4G communication was used to push the data from base stations to a central cloud server. Using the City of Melbourne's Open Data Platform, the data was made available to citizens. The IoT testbed and the algorithms developed will be used to analyse co-related data as well as consider geo-spatial and temporal data sources. For example, analysing vehicular traffic, temperature, air quality, pollen levels, and other situations in the city all at the same time. The solutions developed will be used to detect anomalous events, such as traffic jam, high levels of pollen, and predict the future events in near real-time, more suitably for IoT applications. Further, the IoT testbed will be used to analyse the security and privacy of the collected data, storage, processing and providing related semantics to decision makers. Further, the testbed will be used to analyse the quality of service (QoS) requirement, time delay and bandwidth requirements for different applications and environments.

http://issnip.unimelb.edu.au/research_program/Internet_of_Things/iot_deployment

3.1.8 UNIVERSIDAD DE MURCIA

The results of the project developed as part of UMU results like the DCapBAC and the Secure Group Sharing based on CP-ABE are actually being considered as componentes to be integrated in other platforms for Smart City like FiWARE in order to support secure management of IoT data and its possible usage in further EU projects. Work on IdeMix it is also now part of the proposal evaluated under the CHISTERA call for further research for privacy preserving IoT solutions. Also the results will be exploit in the context of new PhD (2 already done in the context of SocIoTal) and master thesis in order to generate new knowledge and publications. Additionally research carried in the context of SocIoTal like Trust and Reputation Models will be worked on the context of extension of IoT Architectural discussion on different fora. Finally we must mention that the results associated to security protocols and algorithms like DCapBAC and CP-ABE are being exploited through the spin-off company Odin Solution www.odins.es that it is focused on Smart Infrastructure solutions and design of gateways and sensors for IoT based solution.

3.1.9 AYUNTAMIENTO DE SANTANDER

Santander has been characterized by its eagerness to provide a more efficient city management closer to the citizens through the use of Information and Communication Technologies. Santander is in the vanguard of innovation when talking about smart cities.The city is trying to consolidate this position, convinced that high levels of innovation will generate positive results for businesses and contribute to the growth of our economy. The General Plan for Innovation 2020 shows the model of Santander as integral Smart City and it favours an open innovation ecosystem in which citizens, entrepreneurs and local businesses participate.

In this context, some important lessons learnt coming from SocIoTal project, that are, IoT Meetups structure and Co-Creation workshops, will be reused in the future to disseminate innovation activities in the city and also to facilitate people's participation in Santander as a living lab.

In terms of sustainability some components of SocIoTal platform, developed by University of Cantabria, will be used by education local entities for teaching IoT technologies. In addition,

SocIoTal platform will be used by the Municipal Training Workshop to continue developing new functionalities in the mobile application DisAPP developed during Santander pilot, using some components of SocIoTal platform after the end of project. This developpe is supported by the councillor in charge of promoting the integration of disabled people.

3.1.10 CITY OF NOVI SAD

SocIoTal has been the first smart-city project deployed by the City of Novi Sad which helped us gain valuable experience in engaging users and available tools in co-creation process: this is arguably one of the most significant outcomes of the project. Creation of the SocIoTal ecosystem through conferences, workshops, meetups, provoked increased interaction between public administration and citizens in creating and monitoring development of the city.

Together with DNET and PUC "Informatics", we initiated Smart City as a concept for further city's development. A number of Smart City projects soon followed as a direct consequence of SocIoTal and especially CLIPS project (http://www.clips-project.eu) and WeLive project (http://www.welive.eu) which are being regarded as a direct continuation of the SocIoTal.

In December 2015 the Sustainable Development Strategy (2016 – 2020) was adopted defining fundamental vision and key priorities of development in the next five years and in the thematic area titled "good governance", one entire segment covers the topic of the smart city, which among others, deservingly owing to the pioneering project SocIoTal, now defines framework for the smart city, open innovation and public administration modernization (e-government) http://www.novisadinvest.rs/sites/default/files/dokumenti/Strategija%20odr%C5%BEivog%20razvoja%20GNS%20-%20PDF.pdf (Serbian version only).

On more general level the City of Novi Sad has significantly raised its profile as being the pioneering City in the context of Serbia in implementing Smart City projects aimed at open collaborative innovation for more efficient and less expensive public services.

SocIoTal platform components: module for trust and reputation is being considered for integration with DNET's myNS smartphone application.

The Smiling kiosk pilot is deployed in Novi Sad as a permanent installation and is now being offered to other cities and organizations.

3.2 The Pilots

During the last year of the SocIoTal project, WP5 focused its work on the deployment and coordination of different pilot services, thus demonstrating the applicability of the tools and techniques developed in the rest of work packages and finally bringing the experiment to the citizens, creating each corresponding field trial that will also collect the involved citizens' feedback. This work resulted in four pilots, based on previous requirements and needs collected from citizens and played in two cities. These pilots intended to present the SocIoTal Platform features to developers and end users while gather their impressions, suggestions and corrections.

The pilots also played and evaluated the different engagement techniques developed within SocIoTal, based on workshops, co-creation events, meet-ups, hackathons and so on. As main outcomes of these executed pilots, SocIoTal achieved:

- A wide number of end users, involving non-technical users and developers, that evaluated the platform features and application developed from different points of view and provided valuable feedback that allowed SocIoTal partners to evolve platform components, tune them to real user's needs and learn lessons about how to bring IoT to citizens.
- Close contact with other EU IoT projects that contribute to SocIoTal grow up by proposing new features and/or using SocIoTal components. Examples of these are RERUM, Organicity and Wise-IoT.
- External users/developers commitments to evolve pilots (case of DisApp), supported by SocIoTal partners and to use SocIoTal Integrated Platform as part of IoT insertion on Vocational training courses.

3.3 Academic Dissemination

The dissemination of the results of the SocIoTal project has occurred through publications, talks and meetings with stakeholders. Academic publications have been one of the main channels for the dissemination of the results of the SocIoTal project. The results of the project have led to 28 conference publications, 22 journal publications and 2 book chapters including prestigious venues such as IEEE conferences. This number of publications shows the significant impact that the project has had within the academic community.

Further dissemination activities include presentations at workshops, of which there has been six. These have included the co-creation workshops with Nathalie Stambert. The co-creation workshops involved a varied audience of stakeholders, from representatives of tenants, councils and local communities to computer users and developers. The aim was for this varied audience to provide feedback and direction for the SocIoTal project.

Members of the SocIoTal project took part in 8 panel discussion at events such as IoT week. The topic of the discussions were the IoT field and current state-of-the-art and status of implementations. Finally, the project has led to the filing of three patents.

3.4 Community Interaction

In years 1 and 2, the SocIoTal research identified as main barriers to broad IoT adoption:

1. A lack of understanding by SME's and City Councils
2. A lack of third party trust providers
3. A lack of involvement of end-users in building use-cases and developing new services

In the year 1 and 2 community interaction deliverables, we described how we addressed issue #1-3 in co-creation workshops, dedicated developer sessions, introducing research questions and listening to all local stakeholders. In year 3 we used the Meetups as Developer Focus Groups of the software tools, related to issue #2. We brought all issues together in a Stakeholder Coordinator Toolkit.

Throughout the project, the total Meetup community engagement was 74 Meetups, 1637 members 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:

- Ghent, 24 Meetups, 561 Members, 557 attendances
- Guildford 19 Meetups, 355 Members, 423 attendances

- Novi Sad 11 Meetups, 260 Members 231 attendances
- Grenoble 10 Meetups, 260 Members, 183 attendances
- Santander 7 Meetups, 201 Members, 140 attendances

Meetups were organized in five cities in order to disseminate the work of the project to users and developers. Meetups allowed users and developers in the local community to attend events where presentations were given on results obtained from the SocIoTal project. This allowed prompt dissemination of the activities of the SocIoTal projected to those outside of academia, namely users and developers. For example, the CRS4 group collaborated with the *Need for Nerd* (needfornerd.com) group for a Meetup in Cagliari, Italy. In the third year of the project two meetings in Cagliari were hosted, plus a one-day workshop held in the Science and Technology Park of Sardinia, in Pula, during the activities related to a course about IoT platforms, targeted to future developers. The first two meetings engaged 30 people: 15 non developers and 15 developers. These events were organized in collaboration with Need for Nerd (needfornerd.com), a local community targeted to developers mentoring, which currently includes about 2800 members from Italy and counting. The two meetings included project dissemination activities and presentations, platform hands-on and discussions about the Internet of Things, and in particular its impact on society in terms of privacy and security and in terms of business opportunities enabled by IoT platforms, like SocIoTal. Another outcome was a valuable feedback concerning the User Environment and its user-friendliness, along with platform APIs exploration and feedback collection from developers. The one-day workshop, held during a course about IoT, social IoT and related existing platforms, engaged 20 people. It contributed to disseminate the project to students and future developers, allowing them to use the platform to build simple apps with connected devices and smartphones, showing them some security and privacy threats and comparing our approach to other existing platforms. Moreover, during the third year, an interview about the SocIoTal project was organized and broadcasted by a local TV station (TCS, https://youtu.be/wzWMWamqux8) and an additional outcome was an interview by a local journalist about the project; the article has been published on Sardinia Post1, a relevant local online newspaper.

In July, the SocIoTal platform has been used on a hands-on lesson in the context of the "Advanced Course of Web, Mobile and Internet of Things". The general course has been organized by CRS4, Sardegna Ricerche and the University of Cagliari [http://wma-iot.it].
The advanced course, an intensive one-week course, was focused on discovering and using some Web platforms for the IoT, taking into account privacy and security issues and user experience. Five platforms have been chosen and analyzed during the week: IFTTT, Paraimpu, Xively, Thingspeak and SocioTal. SocIoTal has been presented and used and experimented by 20 students, during the fourth day of the week. The students connected their smartphones, some Arduino-based sensors and Raspberry Pi to build some simple IoT trigger-based applications, they analyzed the Web User Environment platform as end users (filling the evaluation questionnaires) and, as developers, through the User Environment APIs. A comparative table of the platform has been created on the basis of the received students' feedback, and SocIoTal obtained a good score.

3.5 Hackathons

During the IoT Week in Belgrade, a Hackathon was co-organized with ICT research project RERUM, Almanac, ClouT, and industry partner Microsoft, enabling developers and citizens to make services on top of deployed beta instance of SocIoTal platform. The following activities were also a part of the Hackathon including: integration of devices/platforms with the SocIoTal such as Almanac and RERUM devices, Microsoft Azure, ClouT Gateway, etc. The Hackathon was announced 1-2 months ahead of the event, to involve developers and "non-developers" to participate in two categories with starting fund of 10k Euros. Finally there were 6 teams at

the event, with total of 20 participants. The valuable feedback was collected using prepared questionnaires as an evaluation methodology process.

The second venue was SenZations' summer school on IoT and its application that took place in Lochow Poland. As a part of the summer school the alpha version of SocIoTal platform available online was evaluated. On the first day of school SocIoTal tutorial was given to the students showing the platform tools, enabler and APIs. During these 5 days there were 6 teams working and developing on top of the platform. The winning teams split the fund of 800E and a trip to a startup competition in Dublin, Ireland.

3.6 Liaison with other projects

SocIoTal has collaborated with SMARTIE in the testing of some of the components developed and evaluation of possible synergies. Additionally, in the context of the IERC meeting and the IoT Week 2016 several exchange of experiences and ideas has been considered in special with RERUM with a proposal of a common workshop within the WF-IoT 2016 conference.

3.7 Summer school

SenZations Summer School was used as a wheel for the evaluation of the platform and user engagement as well as for interaction and integration with other projects. During the third year of project there was one Hackathon event organized as a part of the Summer School, engaging together more than 40 students, technicians and IoT enthusiasts.

The goal of the SocIoTal Hackathon was to provide participants technology developed during the project to enable them to deliver services and application on top of it. A motivation for the participants was 800 € and 6 tickets to a start-up competition held in Dublin.

In addition, LoRa network was deployed during the Hackathon and integrated with the SocIoTal Context Manager. Gateway was used for the aggregation of data and its forwarding to the Context Manager. All participants have successfully connected their devices to the LoRa.

The technology provided to the participants from the SocIoTal project was as follows:

- Mobile Environment (Android app – add device to workspace by QR code scanning)
- SocIoTal Web Environment (web platform – manage devices from user's workspace)
- F2F enabler Android application for the recognition of the social context based on distance between two persons;
- Gait recognition Android application for recognition of user that utilize device based on walk pattern;
- SocIoTal Idm Issuer
- SocIoTal Capability Manager
- SocIoTal Policy Decision Point
- SocIoTal Policy Administration Points
- SocIoTal Context Manager (pub/sub component with storage capability)

Before the start of the Hackathon tutorial was given on enablers and component to introduce the project, its architecture and APIs. There were two winning applications "IoT breath analysis" and "Farmer's Ubiquitous Network", both splitting the main rewards and the tickets for the start-up competition.

3.8 Fiware

One of the core components of the SocIoTal framework is the Context Manager. Part of the core functionalities of SocIoTal Integrated Platform first release relies on FIWARE enablers. The SocIoTal IdM and Communities Manager uses FIWARE KeyRock as User's Directory and Authentication Tokens/Community Tokens generator. The SocIoTal Context Manager relies on FIWARE Orion Context Broker as NGSI Resource Directory and Context Information store. This way, the entities, the context information and the users created and managed within SocIoTal will be perfectly integrated with FIWARE platform, so most of the SocIoTal technical novelties, such the Communities support, the Bubbles or the consumer's authentication based on credentials, can be easily adapted to expand the capabilities of this European FI Platform.

On the other hand, the licensing model of SocIoTal components and the way these are presented to potential users are also aligned with FIWARE dissemination activities. As a result of these convergences, the integration of SocIoTal within the FIWARE foundation is currently being pursued. With the SocIoTal Context Manager as part of FIWARE foundation will allow the project to have a further impact by leveraging the impact of FIWARE to increase the impact of SocIoTal.

3.9 Open platform

CEA has developed an open IoT platform, namely sensiNact. The origin of the platform comes from the European BUTLER project. Other EU projects such as ClouT, FESTIVAL, OrganiCity and SocIoTal have taken over the development of the platform after the end of the BUTLER. SocIoTal project contributed in particular to the sensiNct Studio, which is a tool to create, deploy and manage IoT applications using data connected to the sensiNact platform. Thanks to the SocIoTal project we could have developed a connection towards the SocIoTal Context Broker by building a northbound bridge for the NGSI protocol. We also could integrate security work achieved in the SocIoTal project.

sensiNact platform is part of the European open platforms landscape, which is described in the white paper from the AIOTI alliance. It is also part of the open platforms initiative of the European IoT-EPI (http://iot-epi.eu/). More information about the platform can be found at the link: http://open-platforms.eu/library/sensinact-aka-butler-smart-gateway/#description

3.10 Eclipse

During the second year of the project we were approached by a representative of Eclipse at IoT week, Lisbon. After watching the demonstration of the technology that we provided, he recommended that we look into applying to have the project incorporated into Eclipse as an Eclipse project.

The aim was to incorporate the SocIoTal project into the Eclipse Foundation as a project. However, we ran into the issue of licensing which means that this was not possible. The issue related to third party tools that we used in the SocIoTal project. The licence of these tools is incompatible with the EPL. Some of the tools used are licenced with GPL or AGPL. For example, the main database for storing information is based on the Fiware Orion Context Broker, which includes a MongoDB instance. This is licensed with GPL and AGPL and these are incompatible with the EPL, therefore they cannot be used in an Eclipse project.

We had many discussions with Eclipse concerning incorporation of the SocIoTal project into the Eclipse Foundation as a project. However, it wasn't until a later stage that the issue of

licencing arose. It was when we were discussing the third party tools that we used in the construction of the SocIoTal framework that Ian Skerrett (VP Marketing, Eclipse Foundation) began flagging it as an issue and asked us to report back on the licences of the third-party tools that were being used. It was then that we were informed that they were incompatible with the EPL and it would not be possible to use them in an Eclipse project.
Ian Skerrett has stated that other projects have run into this issue. Some projects have taken the time to replace the GPL and AGPL components, while the Eclipse Foundation have had to turn down others due to the conflict in licencing. He stated that "The intent is that anyone should be able to use an Eclipse project in a commercial product." He also stated that AGPL (and GPL) is not considered business friendly.

Despite our best efforts to promote the SocIoTal project in a widely-used platform, our efforts were in vain due to licensing issues that were down to our earlier choice of using Fiware components. We learnt a valuable lesson on licensing during the project, one that we will use to ensure that this does not happen again in future projects.

3.11 Support of the SocIoTal Framework

The SocIoTal consortium will provide support and bug fixes for the component of the SocIoTal framework for 1 year after the project ends. Support and access to the components of the project will be provided via GitHub.

The SocIoTal framework is available for download from GitHub, details of which can be found in Section 4.2. In addition, a public instance of SocIoTal is available. This is a pre-installed and full operational instance of the framework that the public can access and use.

Support for the SocIoTal framework will be provided for one year starting from September 2016. Support is managed through the GitHub issues tab. Here users can report issues they are having with a particular component. The consortium member responsible for the component will respond to the raised issue in order to solve the problem of the user or developer.

In addition, SocIoTal have created a wiki which contains documentation and tutorials on the SocIoTal framework. This can also be found on GitHub as detailed in Section 4.2. The wiki aims to describe in detail the operation of the framework and its API. In addition, there are tutorials on how to perform common actions.

3.12 Stakeholder toolkit

One of the main results of the SocIoTal project was the examination of the technological and socio-economic barriers to citizen participation in IoT. It as shown that there are three barriers to citizen participation in the project. These are;

- Lack of third party trust providers
- Lack of oversight for SME's in the technological landscape and success stories
- Lack of rich scenarios

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. They are described in the yearly WP6 reports (D6.1,

D6.3, and D6.4 and D6.5). The issues identified are strongly aligned while every City has its own areas of focus.
The stakeholder toolkit is a real commercial offering and is being updated continuously. It is available online. http://www.theinternetofthings.eu/smartcityworkshop

3.13 mijn buurtje platform

SocIoTal has organised three workshops with mijnbuurtje.nl. We co-hosted the first workshop in the CAPS program, July 8/9, BXL with the brief to propose a smart manner to connect devices and make sense of the information collected, so think of what could be the ideal features of a platform connecting objects with a collective purpose.
Especially on the box 'Sensory Data' in the mijnbuurtje Architecture slide below

SocIoTal can show how the mijnbuurtje platform can develop, integrate and build #IoT sensors as community assets. It already works on implementing the service sharing of tools like power drills.

They are matching their needs in such a way that the demand is coming from the neighborhood platform, not pushed by companies or councils:

- How to strengthen the neigborhood community by maximizing the usage of #IoT?
- Which #IoT services can become assets of the neighborhood?

The second workshop5 took place March 11th, in Santander with the aim to establish a common knowledge base and understanding about the level of technology and processes available (from SocIoTal side) and understanding of the possibilities and options that mijnbuurje offers and may be used to achieve the closest possible level of interaction between SocIoTal and mijnbuurje. The key question from Eric Hendriks: Is it possible to add #IoT like apps and services to a socially cohesion driven neighborhood web platform? was answered positively. According to him SocIoTal has set up good cases in Santander and Novi Sad. What is missing is its becoming really a seamless part of everyday life in real neighborhoods.

The third meeting will be held in September 28 in Nijmegen with the purpose of exploring IoT applications and SocIoTal tools in the mijnbuurtje architecture: to prepare a small experiment to show how you can bring an IoT service through the SocIoTal dev kit into the mijn buurtje community platform (target group: IT developers from Munity Services/mijn buurtje), organise a meeting around the theme How do you connect the IoT with everyday life? (targetgroup smart city, city council, developers), organise a meeting on the theme How do you develop an IoT solution for your village or neighbourhood? (targetgroup: technically skilled volunteers). Activities on the longer term include developing the Munity platform in order for local developers to integrate new IoT services in an easy way.

The report from this workshop as well as the Meetup of September 23 with local hackers at Ghent Whitespace that will provide insight into the robustness of the tools, will be available in the online smart city workshop environment. It will be part of the tutorial.

The third workshop with mijnbuurtje.nl has led to a joint application with SIDN to apply for funds to integrate the SocIoTal enablers into the mijn buurtje platform, build a developer community and assist local developers with co-creation sessions with local SME and shops as well as citizens.

Section 4 - Information on the project

4.1 SocIoTal on the internet

4.1.1 SocIoTal website

On the SocIoTal website http://sociotal.eu/ there are tutorials.

The SocIoTal website also provides access to the public implementation that is detailed in the documentation on GitHub.

4.2 SocIoTal on GitHub

The SocIoTal GitHub, https://github.com/sociotal , provides the platform.

The SocIoTal wiki is provided here, https://github.com/sociotal/SOCIOTAL/wiki .

Available components.

Component	Github link
SocIoTal Authorization Manager	https://github.com/sociotal/AuthorizationManager
Web User Environment	https://github.com/sociotal/web-user-environment
Identity Manager	https://github.com/sociotal/IdentityManager
Group Manager	https://github.com/sociotal/GroupManager
Mobile User Environment	https://github.com/sociotal/mobile-environment
Communities Manager	https://github.com/sociotal/CommunitiesManager
Gait recognition	https://github.com/sociotal/gait-recognition
Context Manager	https://github.com/sociotal/Context-Manager
Localisation-based trust and reputation	https://github.com/sociotal/Localisation-Based-Trust-and-Reputation
Face-to-face enabler	https://github.com/sociotal/f2fenabler

4.3 SocIoTal on Twitter

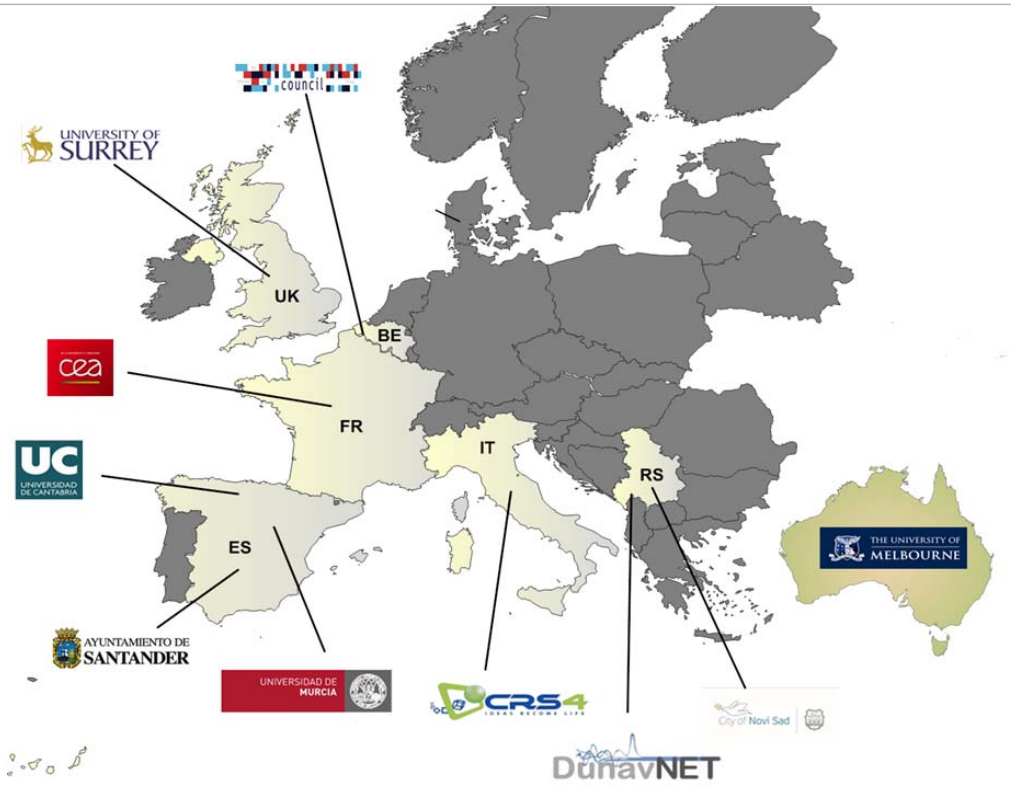
Our twitter account: https://twitter.com/sociotal

4.4 SocIoTal toolkit

The SociTal toolkit is available online.

http://www.theinternetofthings.eu/smartcityworkshop

4.5 The SocIoTal Consortium



University of Surrey, United Kingdom
http://www.surrey.ac.uk/

DunavNET, Serbia
http://www.dunavnet.eu/

Resonance Design, Netherlands
http://www.theinternetofthings.eu/

Santander Council, Spain
http://santander.es/

University of Melbourne, Australia
http://www.unimelb.edu.au/

University of Murcia, Spain
http://www.um.es/

University of Cantabria, Spain
http://web.unican.es/

City of Novi Sad, Serbia
http://www.novisad.rs/

Commissariat a l'Energie Atomique, France
http://www.cea.fr/

CRS4, Italy
http://www.crs4.it/

Section 5 - Use and Dissemination of Foreground

5.1 Publications

No.	Publication type	DOI code	Publication title	Date of Publication	Publication journal	Publication event	Source issue	Author name	Author Affiliation Name
1	Paper	10.1002/ett.2771	User-Centric Smart Buildings for Energy Sustainable Smart Cities	January 2014	Transactions on Emerging Telecommunications Technologies		http://onlinelibrary.wiley.com/doi/10.1002/ett.2771/abstract	Moreno, María V and Zamora, Miguel A and Skarmeta, Antonio F	University of Murcia
2	Paper		A Holistic IoT-based Management Platform for Smart Environments	To appear		IEEE ICC 2014 - Selected Areas in Communications Symposium ('ICC'14 SAC')	http://icc2014.ieee-icc.org/index.html	María V. Moreno, José Santa, Miguel A. Zamora and Antonio F. Skarmeta	University of Murcia
3	Paper	http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6803136	User Role in IoT-based Systems	6-8 March 2014		IEEE World Forum on Internet of Things WF-IoT 2014.	http://sites.ieee.org/wf-iot/	M. Victoria Moreno, José Luis Hernández Ramos and Antonio F. Skarmeta	University of Murcia
4	Paper	DOI 10.1109/WAINA.2014.161	A Framework for Citizen Participation in the Internet of Things	2014		International Workshop on Pervasive Internet of Things and Smart Cities (PITSaC 2014).	http://www.aina-conference.org/2014/	M. Victoria Moreno, José L. Hernández, Antonio F. Skarmeta, Michele Nati, Nick Palaghias, Alexander Gluhak and Rob van Kranenburg	University of Murcia, Centre for Communication Systems Research
5	Paper	DOI 10.1109/WAINA.2014.160	A New Location-Aware Authorization Mechanism for Indoor Environment	2014		International Workshop on Pervasive Internet of Things and Smart Cities (PITSaC 2014).	http://www.aina-conference.org/2014/	M. Victoria Moreno, J. Luis Hernández and Antonio F. Skarmeta	University of Murcia

6	Paper		SocIoTal: Creating a Citizen-Centric Internet of Things	2014		4th International Conference on Information Society and Technology (ICIST 2014)	http://www.yuinfo.org/icist2014/icist_registration.html	Nenad Gligoric, Srdjan Krco, Ignacio Elicegui, Carmen López, Luis Sánchez, Michele Nati, Rob van Kranenburg, M. Victoria Moreno, Davide Carboni	DunavNET, University of Cantabria, Centre for Communication Systems Research, University of Liepaja, University of Murcia, CRS4
7	Paper	10.1007/s00500-014-1278-9	A soft computing based location-aware access control for smart buildings	13 April 2014	Soft Computing		http://link.springer.com/article/10.1007/s00500-014-1278-9	José Luis Hernández Ramos, M. Victoria Moreno, Antonio J. Jara and Antonio F. Skarmeta	University of Murcia
8	Paper		An IoT Based Framework for User Centric Smart Building Services	To appear	International Journal of Web and Grid Services		http://www.inderscience.com/jhome.php?jcode=ijwgs	Moreno, María V and Zamora, Miguel A and Skarmeta, Antonio F	University of Murcia
9	Paper	10.1080/00207160.2014.915316	DCapBAC: Embedding Authorization logic into Smart Things through ECC optimizations	22-may-14	International Journal of Computer Mathematics		http://www.tandfonline.com/toc/gcom20/current	José L. Hernández-Ramos, Antonio J. Jara, Leandro Marín and Antonio F. Skarmeta	University of Murcia
10	Paper	10.1007/978-3-319-06811-410	Internet of Things Security, Privacy and Trust Considerations	2014		10th VLDB Secure Data Management Workshop (SDM 2013)	http://www.hitech-projects.com/sdm-workshop/sdm13.html	Antonio F. Skarmeta and M. Victoria Moreno	University of Murcia
11	Paper	10.1007/978-3-319-06608-0_48	Privacy-Preserving Collaborative Anomaly Detection for Participatory Sensing	2014		18th Pacific-Asia Conference on Knowledge Discovery and Data Mining	http://pakdd2014.pakdd.org/	Sarah M. Erfani, Yee Wei Law, Shanika Karunasekera, Christopher A. Leckie, and Marimuthu Palaniswami	The University of Melbourne
12	Paper		Towards Privacy-preserving Data Sharing in Smart Environments	2014		3rd International Workshop on Extending Seamlessly to the Internet of Things (esIoT-2014)	www.esiot.com	José Luis Hernández-Ramos, Jorge Bernal Bernabé and Antonio F. Skarmeta	University of Murcia

13	Paper	10.3390/s140609582	How can We Tackle Energy Efficiency in IoT Based Smart Buildings?	2014	Sensors Journal		http://www.mdpi.com/1424-8220/14/6/9582	M. Victoria Moreno, Benito Úbeda, Antonio F. Skarmeta and Miguel A. Zamora	University of Murcia
14	Paper		CARD: Context-Aware Resource Discovery for mobile Internet of Things scenarios	2014		IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks	N/A	Riccardo Pozza, Michele Nati, Stylianos Georgoulas, Alexander Gluhak, Klaus Moessner, Srdjan Krco	University of Surrey, DNET
15	Paper		Privacy-Preserving Security Framework for a Social-aware IoT	2014		8th International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2014) & 6th International Work-conference on Ambient Assisted Living (IWAAL 2014)	http://link.springer.com/chapter/10.1007/978-3-319-13102-3_67	Jorge Bernal Bernabe, J. Luis Hernández, M. Victoria Moreno and Antonio F. Skarmeta	University of Murcia
16	Paper		Co-creation as the Key to a Public, Thriving, Inclusive and Meaningful EU IoT	2014		8th International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2014) & 6th International Work-conference on Ambient Assisted Living (IWAAL 2014)	http://link.springer.com/chapter/10.1007/978-3-319-13102-3_65	Rob van Kranenburg, Nathalie Stembert, M. Victoria Moreno, Antonio F. Skarmeta, Carmen López, Ignacio Elicegui and Luis Sánchez	University of Cantabria, University of Murcia
17	Paper	DOI 10.1109 JIOT.2014.2359538	Security Protocols and Privacy Issues inot 6LoWPAN stack: A synthesis	2014	Journal of IoT			Christine Hennebert and Jessye Dos Santos	CEA Grenoble
18	Paper	10.1109/ISSNIP.2014.6827606	Profiling spatial and temporal behaviour in sensor networks: A case study in energy monitoring	2014		IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information	http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6827606&tag=1	Rashidi, L.; Rajasegarar, S.; Leckie, C.; Nati, M.; Gluhak, A; Imran, M.A; Palaniswami, M.	University of Melbourne, University of Surrey

						Processing (IEEE ISSNIP)			
19	Paper	10.1109/ICC.2014.6884036	Spatio-temporal estimation with Bayesian maximum entropy and compressive sensing in communication constrained networks	2014		IEEE International Conference on , Communications (IEEE ICC)	http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6884036	Rajasegarar, S.; Leckie, C.; Palaniswami, M.	University of Melbourne
20	Article	10.1109/MTS.2014.2345203	Participatory Sensing, Privacy, and Trust Management for Interactive Local Government	2014	Technology and Society Magazine, IEEE		http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6901335	Marusic, S.; Gubbi, J.; Sullivan, H.; Law, Y.; Palaniswami, M.	University of Melbourne
21	Paper	10.1016/j.jcss.2014.12.021	SAFIR: Secure Access Framework for IoT-enabled Services on Smart Buildings	2014	Journal of Computer and System Sciences		http://dx.doi.org/10.1016/j.jcss.2014.12.021	José L. Hernández-Ramos, M. Victoria Moreno, Jorge Bernal Bernabé, Dan García Carrillo and Antonio F. Skarmeta	University of Murcia
22	Paper		An Indoor Localization System Based on 3D Magnetic Fingerprints for Smart Buildings	2014		2015 IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for the Future (RIVF)	http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7049897&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7049897	M. Victoria Moreno and Antonio F. Skarmeta	University of Murcia
23	Article	10.1007/978-3-319-09177-8_14	Future Human-Centric Smart Environments	2014			http://link.springer.com/chapter/10.1007/978-3-319-09177-8_14	María V. Moreno-Cano, José Santa, Miguel A. Zamora-Izquierdo, and Antonio F. Skarmeta	University of Murcia

24	Paper		Managing Context Information for Adaptive Security in IoT Environments	2015		International Workshop on Pervasive Internet of Things and Smart Cities (PITSaC 2015).	http://voyager.ce.fit.ac.jp/conf/aina/2015/	José L. Hernández-Ramos, Jorge Bernal Bernabe, Antonio F. Skarmeta	University of Murcia
25	Paper	10.1109/JSAC.2015.2393436	Toward a Lightweight Authentication and Authorization Framework for Smart Objects	2015	IEEE Journal on Selected Areas in Communications		http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7012039&tag=1	José L. Hernández-Ramos, Marcin. P. Pawlowski, Antonio J. Jara, Antonio F. Skarmeta, Latif Ladid	University of Murcia
26	Paper	10.1007/s00500-015-1705-6	TACIoT: multidimensional trust-aware access control system for the Internet of Things	2015	Soft Computing		http://dx.doi.org/10.1007/s00500-015-1705-6	Jorge Bernal Bernabe, Jose Luis Hernandez Ramos, Antonio F. Skarmeta Gomez	University of Murcia
27	Paper	doi:10.3390/s150715611	Preserving Smart Objects Privacy through Anonymous and Accountable Access Control for a M2M-Enabled Internet of Things	2015	Sensors Journal		http://www.mdpi.com/1424-8220/15/7/15611	José L. Hernández-Ramos, Jorge Bernal Bernabé, M. Victoria Moreno and Antonio F. Skarmeta	University of Murcia
28	Paper	10.1109/IMIS.2015.49	Certificateless and Privacy-enhancing Group Sharing Mechanism f or the Future Internet	2015	4th International Workshop on Extending Seamlessly to the Internet of Things (esIoT-2015)	www.esiot.com		José L. Hernández-Ramos, Jorge Bernal Bernabe, Salvador Perez Franco, Antonio F. Skarmeta	University of Murcia
29	Conference Paper	10.1109/VTCSpring.2015.7145918	Location-Based Pseudonyms for Identity Reinforcement in Wireless ad hoc Networks	2015	IEEE Vehicular Technology Conference-Spring 2015 (IEEE VTC-Spring'15)		http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7145918&tag=1	Iulia Tunaru, Benoît Denis, Bernard Uguen	Commissariat a l'Energie Atomique
30	Conference Paper		Privacy Issues in 6LoWPAN wireless sensor network	2015	Connected security Word, eSmart 2015		http://www.smartcontactlessworld.com/	Christine Hennebert, Jessye Dos Santos and Cédric lauradoux	Commissariat à l'Energie Atomique

31	Conference Paper		Preserving privacy in secured ZigBee Wireless Sensor Network	2015	IEEE World Forum IoT		http://www.ieee-wf-iot.org/	Christine Hennebert, Jessye Dos Santos and Cédric lauradoux	Commissariat à l'Energie Atomique
32	Conference Paper	10.1109/ICUWB.2015.7324430	Cooperative Group Key Generation Using IR-UWB Multipath Channels	2015	IEEE International Conference on Ubiquitous Wireless Broadband (IEEE ICUWB'15)		http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7324430&tag=1	Iulia Tunaru, Benoît Denis, Régis Perrier, Bernard Uguen	Commissariat à l'Energie Atomique
33	Conference Paper	ISBN:978-86-85525-16-2	Smart City Services for Citizen-Centric Internet of Things	2015	5th International Conference on Information Society and Technology Proceedings		5th International Conference on Information Society and Technology	Nenad Gligoric, Srdjan Krco, Dejan Drajic, Ignacio Elicegui, Carmen López, Luis Sánchez, Michele Nati, Jorge Bernal Bernabé, José L. Hernández-Ramos, Davide Carboni, Alberto Serra	
34	Paper	doi: 10.5220/0005475704980503	Humanizing the Internet of Things - Toward a Human-centered Internet-and-web of Things	2015	WEBIST 2015 - 11th International Conference on Web Information Systems and Technologies		http://www.scitepress.org/Portal/PublicationsDetail.aspx?ID=KWME3sdYT6w=&t=1	Antonio Pintus, Davide Carboni, Alberto Serra, Andrea Manchinu	CRS4
35	Conference Paper	http://dx.doi.org/10.1109/ICC.2015.7248384	Accurate detection of real-world social interactions with smartphones	2015		IEEE International Conference in Communications		Palaghias N, Hoseinitabatabaei, S.A. ; Nati, M. ; Gluhak, A. ; Moessner, K.	University of Surrey
36	Conference Paper	10.1109/WF-IoT.2015.7389153	Dynamic security credentials PANA-based provisioning for IoT smart objects	2015	IEEE 2nd World Forum on Internet of Things (WF-IoT)	IEEE 2nd World Forum on Internet of Things (WF-IoT)		José L. Hernandez-Ramos, Dan García Carrillo, Rafael Marín-López, Antonio F. Skarmeta	University of Murcia
37	Journal	10.3390/s150717168	MagicFinger: 3D Magnetic Fingerprints for Indoor Location	2015	Sensors Journal		7	Daniel Carrillo, Victoria Moreno, Benito Úbeda and Antonio F. Skarmeta	University of Murcia

38	Book	0302-9743	MagicFinger: A New Approach to Indoor Localization	2015		9th International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2015)	10	Daniel Carrillo, Victoria Moreno and Antonio F. Skarmeta	University of Murcia
39	Conference Paper	10.1109/Kaleidoscope.2015.7383648	A required security and privacy framework for smart objects	2015		ITU Kaleidoscope: Trust in the Information Society (2015)		Antonio Skarmeta, José L. Hernández-Ramos, Jorge Bernal Bernabe	University of murcia
40	Book	10.1201/b19516-12	A User-centric Decentralised Governance Framework for Privacy and Trust in IoT	2016	Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations			Jorge Bernal Bernabé, José Luis Hernández, Moreno, V., Antonio F. Skarmeta, Niklas Palaghias, Michele Nati and Klaus Moessner	University of Murcia Centre for Communication Systems Research
41	Conference Paper	ISBN: 978-1-4799-6664-6	Opportunistic Smart Object Aggregation based on Clustering and Event Processing	2016		IEEE International Conference on Communications (ICC-2016)		Fernando Terroso-Saenz, José Luis Hernandez Ramos, Jorge Bernal Bernabé, Antonio Fernando Skarmeta Gomez	University of Murcia
42	Book	ISBN: 978-87-93379-81-7	Trusted IoT in the Complex Landscape of Governance, Security, Privacy, Availability and Safety	2016	Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds			Elias Z. Tragos, Jorge Bernal Bernabe, Ralf C. Staudemeyer, Jose Luis Hernandez Ramos, Alexandros Fragkiadakis, Antonio Skarmeta, Michele Nati and Alex Gluhak	University of murcia

43	Journal Article	Accepted, in press	ARMY: Architecture for a Secure and Privacy-aware Lifecycle of Smart Objects in the Internet of My Things	2016	IEEE Comunications Magazine			José L. Hernández-Ramos, Jorge Bernal Bernabe, Antonio Skarmeta	University of Murcia
44	Conference Paper	Accepted	Ephemeral : Lightweight Pseudonyms for 6LowPan MAC addresses	2016	PIMRC	PIMRC		Jessye Dos Santos, Christine Hennebert, Cédric Lauradoux, Jean-Christophe Fonbonne	CEA-LETI
	Journal Article	https://doi.org/10.1007/s10922-016-9395-7	Priority Service Provisioning and Max–Min Fairness: A Utility-Based Flow Control Approach	2016	Journal of Network and Systems Management			J. Jin, M. Palaniswami, D. Yuan, Y.-N. Dong, and K. Moessner	University of Melbourne
	Journal Article	https://doi.org/10.1109/tfuzz.2014.2322385	Evolving fuzzy rules for anomaly detection in data streams	2015	IEEE Transactions on Fuzzy Systems			M. Moshtaghi, J. C. Bezdek, C. Leckie, S. Karunasekera, and M. Palaniswami,	University of Melbourne
	Conference Paper	https://doi.org/10.1109/riot.2015.7104904	DP1SVM: A dynamic planar one-class support vector machine for Internet of Things environment	2015		Recent Advances in Internet of Things (RIoT), 2015 International Conference on, 2015		A. Shilton, S. Rajasegarar, C. Leckie, and M. Palaniswam	University of Melbourne
	Journal Article	https://doi.org/10.1145/2736697	Geospatial Estimation-Based Auto Drift Correction in Wireless Sensor Networks	2015	ACM Transactions on Sensor Networks (TOSN)			D. Kumar, S. Rajasegarar, and M. Palaniswami	University of Melbourne

	Journal Article	https://doi.org/10.1007/s00371-015-1192-x	A visual-numeric approach to clustering and anomaly detection for trajectory data	2015	The Visual Computer			D. Kumar, J. C. Bezdek, S. Rajasegarar, C. Leckie, and M. Palaniswam	University of Melbourne
	Journal Article	https://doi.org/10.1109/jiot.2013.2296516	"An information framework for creating a smart city through internet of things	2014	IEEE Internet of Things Journal			J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami	University of Melbourne
	Conference Paper	https://doi.org/10.1109/issnip.2014.6827606	Profiling spatial and temporal behaviour in sensor networks: A case study in energy monitoring	2014		Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on		"Profiling spatial and temporal behaviour in sensor networks: A case study in energy monitoring	University of Melbourne
	Journal Article	https://doi.org/10.1016/j.patcog.2014.04.006	Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks	2014	Pattern Recognition			S. Rajasegarar, A. Gluhak, M. A. Imran, M. Nati, M. Moshtaghi, C. Leckie	University of Melbourne
	Conference Paper	https://doi.org/10.1109/percomw.2016.7457159	An improved scheme for privacy-preserving collaborative anomaly detection	2016		2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshop		L. Lyu, Y. W. Law, S. M. Erfani, C. Leckie, and M. Palaniswami	University of Melbourne

5.2 Dissemination Events and Activities

No.	Type of Activity	Main leader	Title	Date/Period	Place	Type of Audience	Size of Audience	Countries Addressed
1	Workshop	Srdjan Krco (DNET), Svjetlana Krco (DNET)	Workshop #1-#9: Meeting with Local Communities, Tenants Councils and Public Companies, September-October 2013	September-October 2013	Novi Sad			
2	Workshop	Rob van Kranenber, Srdjan Krco, Nathalie Stambert	Workshop#10: Co-creation Workshop with Research Teams	28th February 2014	Novi Sad	Research teams from DunavNET, City of Novi Sad, Centar za Promociju Nauke Beograd, Javno Preduzece Informatika		
3	Workshop	Rob van Kranenber, Srdjan Krco, Nathalie Stambert	Workshop#11: Rob van Kranenber and Srdjan Krco, Nathalie Stambert, Co-creation Workshop with Local Communities/Tenants Councils	29th February 2014	Novi Sad	Representatives of Tenants Councils and Local Communities		
4	Workshop	Rob van Kranenber, Srdjan Krco, Nathalie Stambert	Workshop#12: Co-creation Workshop with Computer Users (not programmers)	29th February 2014	Novi Sad	Computer Users (but not programmers)		
5	Workshop	Rob van Kranenber, Srdjan Krco, Nathalie Stambert	Workshop#12: Co-creation Workshop with programmers	29th February 2014	Novi Sad	Progremmers/ developers		
6	Panel	Srdjan Krco (DNET)	Living bits and things 2013: "Sociotal: Project overview and use cases"	13th November 2013	Bled, Slovenia			
7	Meetup	Srdjan Krco (DNET), Rob van Kranenburg (RD)	Iot Meetup#1: "Internet of Things in Novi Sad: Technology, the City, Society and Citizens "	27th February 2014	Faculty of Philosophy, Novi Sad			
8	TV show	Srdjan Krco (DNET)	TV Show "Naukovati" - Internet of things	24th May 2014	Radio Televizija Novi Sad			
9	Meetup	Srdjan Krco (DNET), Rob van Kranenburg (RD)	IoT Meeup#2: "Second IoT Meetup"	24th April 2014	Faculty of Philosophy, Novi Sad			
10	Meetup	Srdjan Krco (DNET), Rob van Kranenburg (RD)	IoT Meetup#3: "Danube IT conference"	29th May 2014	Danube IT, Ribarsko ostrvo, Novi Sad			
11	Panel	Srdjan Krco (DNET), Nenad Gligoric (DNET)	Living bits and things 2014: "Fostering End-user involvement into the Citizen-centric Internet of Things"	4th June 2014	Bled, Slovenia			

12	Conference sponsored	DNET, UMU	PITSaC, International Workshop Pervasive Internet of Things and Smart Cities (PITSaC 2013)	14-15 May, 2014	Alberta,Canada	Scientific Community,		Worldwide
13	Thesis (PhD)	M. Victoria (UMU)	An IoT-based Information Management System for Energy Efficiency in Smart Buildings	31st October 2014		Scientific Community, Industry, Other		Worldwide
14	Panel	M. Victoria Moreno (UMU)	IoT Week 2014. Best Practices for involving communities in European IoT projects	19th June 2014	London (UK)	Scientific Community, Industry		Worldwide
15	Panel	Antonio F. Skarmeta (UMU) Srdjan Krco (DNET)	IoT Week 2014. Semantic Interoperability; Security, Privacy, Trust & the ARM	18th June 2014	London (UK)	Scientific Community, Industry		Worldwide
16	Conference sponsored	UMU	8th International Conference on Ubiquitous Computing and Ambient Intelligence (UCAmI 2014)	2nd-5th Dec 2014	Belfast (UK)	Scientific Community		Worldwide
17		Srdjan Krco (DNET), Rob van Kranenburg (RD)	IoT Meeup#4: "IoT Museum"	18th Septembar 2014	Faculty of Philosophy, Novi Sad			
18	Meetup	UC	1st IoT Santander Meetup	21th February 2014	Santander (Spain)	Citizens	19	Spain
19	Meetup	UC	2nd IoT Santander Meetup	30th May 2014	Santander (Spain)	Citizens	25	Spain
20	Workshop	Nathalie Stembert, Rob van Kranenburg, UC	Co-creation Workshop with Research Teams		Santander (Spain)	Research Team from SocIoTal and other IoT projects	8	Spain
21	Meetup	UC	3rd IoT Santander Meetup	21st October 2014	Santander (Spain)	Citizens	25	Spain
22	Meetup	UC	4th IoT Santander Meetup - Workshop to create IoT devices (I)	22nd May 2015	Santander (Spain)	Citizens	21	Spain
23	Summer School	DNET	SenZations' 14 - 9th Summer School on IoT Applications	31th August - 06th September 2014	Biograd na Moru (Croatia)	Students, PhD students, developers		
24	Panel	Nenad Gligoric (DNET), Srdjan Krco (DNET)	SocIoTal – Creating Citizen Centric Internet of Things, ICT Forum 2014	14th-16th October 2014	Nis (Serbia)	Scientific and business clusters		
25	Panel	Nenad Gligoric (DNET)	Smart City Services for Citizen-Centric Internet of Things	8th-11th March 2015	Kopaonik (Serbia)	Scientific community		Worldwide
26	Panel	Nenad Gligoric (DNET)	Panel session for involving dorms in SOCIOTAL	17th April 2015	Borsko jezero (Serbia)	Non scientific community (dorms presidents)		
27	Meetup	Srdjan Krco (DNET), Boris Pokric (DNET)	SocIoTal presentation and call for participation as end users/developers	21st April 2015	Belgrade (Serbia)	Business clusters and government agencies		Serbia

28	Meetup	Nenad Gligoric (DNET)	MeetUP: SocIoTal presentation and API evaluation	1st July 2015	Novi Sad (Serbia)	Developers		Serbia
29	Meetup	Dejan Drajic (DNET)	SocIoTal presentation for local community	13th July 2015	Novi Sad (Serbia)	citizens		Serbia
30	Conference sponsored	UMU	International Workshop Pervasive Internet of Things and Smart Cities (PITSaC 2015)	24th-27th 2015	Gwangju (South Korea)	Scientific community		Worldwide
31	Conference sponsored	UMU	International Workshop on Extending Seamlessly to the Internet of Things (esIoT 2015)	8th-10th July 2015	Blumenau (Brazil)	Scientific community		Worldwide
32	Meetup	UC	5th IoT Santander Meetup - Workshop to create IoT devices (II) and Web User Environment	9th October 2015	Santander (Spain)	Citizens and developers	20	Spain
33	Session with developers	UC	SocIoTal session with developers (platform presentation)	27th October 2015	Santander (Spain)	Developers	6	Spain
34	Conference sponsored	UMU	IEEE World Forum on Internet of Things (WF-IoT) 2015	14-16 December 2015	Milan (Italy)	Scientific community, Industry		Worldwide
35	Meetup	DNET	MeetUP: Services from Smart Cities. SocIoTal platform presentation and Hackathon announcement	23rd December 2015	Belgrade, Chamber of commerce (Serbia)	Citizens, Students, Developers	54	Serbia
36	Meetup	DNET	MeetUp: IoT Week announcement and SocIoTal tools presentation	8tj March 2016	Belgrade, Chamber of commerce (Serbia)	Citizens, Students, Developers	65	Serbia
37	Meetup	UC	6th IoT Santander Meetup - Workshop SocIoTal platform	29th April 2016	Santander (Spain)	Citizens, developers	17	Spain
38	Workshop	UMU	IoT Week Belgrade	May 31th-June 2nd 2016	Belgrade (Serbia)	Panel Session on IoT Security and Privacy	50	European
39	Session with students	UC	Visit of students from Higher Level Training Course in Electronic Maintenance	9th June 2016	Santander (Spain)	Students	20	Spain
40	Hackathon	DNET	IoT Week Belgrade - Hackathon	May 31th-June 2nd 2016	Crown Plaza Hotel, Belgrade, Serbia	Students, developers, citizens	25	European
41	Workshop	UMU	IERC Meeting	June 24th	Valencia (Spain)	AC3 meeting	75	European
42	Workshop	UMU	AIOTI GA	30th May	Berlin (Germany)	GA		European
43	Conference Panel	UMU	EIP SCC Meeting	April 28th	Webinar	'Addressing Privacy in Smart Cities' Webinar	35	European
44	Summer School	DNET	SenZations' 16 - 11th Summer School on IoT Applications	27th August – 02nd	Lochow (Poland)	Students, PhD students, developers	60	Worldwide

				September 2016				
45	Meeting	CRS4	SocIoTal Events & NeedforNerd	8th june 2016	Cagliari	Citizens, Students	15	Sardinia
46	Meeting	CRS4	Sociotal Events & NeedforNerd	9th June 2016	Cagliari	Developers, Students	15	Sardinia
47	TV/Press release	CRS4	TCS TV station interview about SocIoTal project	17th May 2016	Pula	Citizens		Sardinia, Italy
48	Workshop/course	CRS4	Advanced course in Web plaforms for the IoT	July, 2016	Pula	Students	20	Sardinia
49	Press release	CRS4	Article about SocIoTal on SardiniaPost online newspaper	14th July 2016	Cagliari			Sardinia, Italy
50	App Presentation	UC + SDR	Presentatin of DisApp application (I)	13th July 2016	Santander (Spain)	Citizens	13	Spain
51	Meetup	UC	7th IoT Santander Meetup – Web User Environment with Communities functionalities	15th July 2016	Santander (Spain)	Citizens, developers	12	Spain
52	Press release	SDR	Press release about DisApp application http://www.eldiariomontanes.es/agencias/cantabria/201607/17/personas-discapacidad-prueban-aplicacion-729338.html	17th July 2016	Spain			Spain
53	App Presentation	UC + SDR	Presentation of DisApp application (II)	2nd August 2016	Santander (Spain)	Citizens	23	Spain
54	Workshop	DNET	IoT Convivio	19 Sep 2016	Milan (Italy)	Industry, public administration	40	Italy

5.3 Exploitable Foreground

Type of Exploitable Foreground	Description	Confidential Yes/No	Foreseen embargo date	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner & Other Beneficiary(s) involved
General advancement of knowledge	Face-to-face enabler - This is an algorithm which performs context recognition. Using the sensors and bluetooth signal on a smartphone it is able to determine social interactions between users of the application.	No	None	Algorithm	Internet of Things		None	UniS
General advancement of knowledge	Gait recognition enabler - This performs user authentication using a novel biometric. The algorithm uses the accelerometer in a smartphone to model a user's walk.	No	None	Novel biometric	Internet of Things		None	UniS
Smart City expertise	The SocIoTal Stakeholder Coordination toolkit, a solution to the identified barriers, is made available as a commercial offering by Council in the form of a smart city workshop.	No	None	Workshop and potential follow up offerings on further enabler ecosystem	Internet of Things/ Smart Cities	Continuously updated	None	Council
General advancement of knowledge	Web User Environment and related APIs: A user-friendly web dashboard to manage connected devices/services, targeted di end users	No	None	Platform design	Internet of Things		None	CRS4, DNET
Exploitation of results through (social) innovation	Smiling kiosk, a solution for promotion of smart city (and other) services	No	None	Integrated solution	Smart cities, marketing	Included in the commercial offering	None	DNET
Commercial exploitation of R&D results	SocIoTal platform instance to be used as the basis for smart city offering.	No	None	Platform	Smart cities	Being integrated with other smart city solutions	None	DNET

SocIoTal Commuities Concept and Information sharing groups	SocIoTal Communities Manager component- combining SocIoTal IdM and SocIoTal Context Manager, it allows the creation and management of closed groups of users and related information sources	No	None	Platform component	Smart cities, IoT development, Business Models	Integrated with other IoT Platform	None	UC
Secure Context Information Management	SocIoTal Context Manager component - provides other IoT Context broker with additional security layers, offered by the SocIoTal Security Framework, protecting the Context Information Sources	No	None	Platform Component	Smart cities, IoT development, Business Models	Integrated with other IoT Platform	Current version is linked to FIWARE Orion Context Broker	UC, UMU
Commercial exploitation of R&D results	Authorization Manager component of SocIoTal security Framework, that is based on Capability Based access Control (DCapBAC)	No	None	Platform Component	IoT, Smart Cities	Exploted in OdinS	None	UMU
Commercial exploitation of R&D results	Secure Group data Sharing component, based on CP-ABE cryptographic scheme	No	none	Platform Component	IoT, Smart Cities	Exploted in OdinS	None	UMU
General advancement of knowledge	Identity Management for IoT, based on private ABC credentials (Idemix) and Fi-ware IdM (Keyrock)	No	none	Platform Component	IoT, Smart Cities		None	UMU
Exploitation of results through (social) innovation	Smiling kiosk, a solution for promotion of smart city (and other) services	No	None	Integrated solution (DNET)	Smart Cities, marketing	Included in the commercial	None	NS as beneficiary
Commercial exploitation of R&D results	SocIoTal platform instance to be used as the basis for smart city offering.	No	None	Platform	Smart Cities	Being integrated with other smart city solutions	None	NS as beneficiary
First PoC of geo-localization including end-to-end security & confidentiality	This platform can be used to manage the energy, in particular the heating for intelligent building according to the movement and the habits of the occupants	No	None	Platform & Integrated solution	Smart Buildings	2017	None	CEA (owner)

Technological brick to hide the MAC addresses during the routing in a WSN	For example, for the scada applications, it is crucial to hide the MAC addressed at low layers over the air to protect against industrial spying. The eavesdropping of the metadata provides information about the local network, its topology and its capabilities.	Yes	End of 2017	Integrated solution Embedded lightweight technique to manage pseudonyms of the source & destination MAC addresses	Scada & all Smart domains	2018	Patent in process for deposit	CEA (owner)
Commercial exploitation of R&D results	An IoT service development and management tool	No	None	sensiNact Studio	Smart city, smart healthcare, smart industry, smart agriculture, etc	2017	EPL license & proprietary code	CEA (owner)
-General advancement of knowledge -Commercial exploitation of R&D results	Technique enabling channel-based secret key generation for small ad hoc groups of mobile wireless devices, exploiting all available physical links in a full mesh Topology and reducing over-the-air traffic in comparison with conventional cooperative approaches.	No	None	Ad hoc method enabling the joint generation and distribution of group secret keys for wireless devices.	Wireless telecommunications activities, All smart domains	2017/2018	Patent application n° EN 15 57728, Aug. 2015	CEA (owner)

END OF REPORT