Smart Santander

Smart Santander Testbed

General description and architecture .................................................................3
Infrastructure..............................................................................................................4
Experimentation capabilities.....................................................................................8
Protocols and data formats.......................................................................................8
Security and access policies.......................................................................................9
Applications..............................................................................................................9

Smart Santander IoT platform

General description and architecture .................................................................12
Protocols and data formats.......................................................................................13
Control and management tools...............................................................................14
Security and access policies.......................................................................................15
Federation approach.................................................................................................15
Reusable components...............................................................................................16

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement 643275, and from the Japanese National Institute of Information and Communications Technology
Smart Santander Testbed

Smart Santander Testbed

General description and architecture ........................................................................................................3
Infrastructure ..................................................................................................................................................4
Experimentation capabilities ........................................................................................................................8
Protocols and data formats ........................................................................................................................8
Security and access policies ........................................................................................................................9
Applications ..................................................................................................................................................9
General description and architecture

The SmartSantander testbed is an experimental test facility for the research and experimentation of architectures, key enabling technologies, services and applications for the Internet of Things in the context of a city. Additionally, in order to manage the testbed, SmartSantander can work as a platform and is able to be increased in size with new heterogeneous sensors. Although SmartSantander project considered the creation of four testbed across Europe, the main SmartSantander testbed is located in the city of Santander, and all of the deployments has been made in the city context.

Figure 1 SmartSantander testbed

The SmartSantander follows a three tiered approach as depicted in Figure 1:
1. **IoT tier**: Responsible for sensing the corresponding parameter (temperature, CO, noise, light, car presence, soil temperature, soil humidity). The majority of them are integrated in the network devices named repeaters, whilst the others are stand alone and communicates wirelessly with the corresponding repeaters (it is the case for the parking sensor buried under the asphalt). For these devices, due to the impossibility of powering them with electricity, they must be fed with batteries. Repeaters are high-rise placed in street lights, public buildings, etc, in order to behave as forwarding nodes to transmit all the information associated to the different measured parameters. The communication between repeaters and IoT nodes performs through a proprietary protocol based on 802.15.4 called Digimesh. Additionally, an 802.15.4 native interface is available for experimentation purposes in the repeaters.

2. **Gateway tier**: Both IoT nodes and repeaters, are configured to send all the information (through Digimesh protocol) service provision and network management to the gateway. Once information is received by the gateway, it forwards the information to the SmartSantander upper layers, through the different interfaces provided by it (GPRS/UMTS or ethernet). Furthermore, most of the gateways contain enough intelligence to manage and control the network with different tools (OTAP, scan node, etc.).

3. **Platform tier**: Top layer in the SmartSantander architecture. This layer is the SmartSantander platform that provides access to all the devices deployed in Santander, as well as the rest of services injecting data into the platform. More information about this layer can be found in section Erreur ! Source du renvoi introuvable.

**Infrastructure**

The SmartSantander testbed is composed of around 3000 IEEE 802.15.4 devices, 200 GPRS modules and 2000 joint RFID tag/QR code labels deployed both at static locations (streetlights, facades, bus stops) as well as on-board of mobile vehicles (buses, taxis). Over the deployed testbed, several use cases have been implemented:

- **Environmental Monitoring**: around 2000 IoT devices installed (mainly at the city centre), at streetlights, facades provide measurements on different environmental parameters, such as temperature, CO, noise, light and car presence).

![Figure 2 Repeaters deployed within SmartSantander for environmental monitoring](image)

- **Outdoor parking**: almost 400 parking sensors (based on ferromagnetic technology), buried under the asphalt have been installed at the main parking areas of the city centre, in order to detect parking sites availability in these zones.
• **Mobile Environmental Monitoring**: in order to extend the aforementioned environmental monitoring use case, apart from measuring parameters at static points, devices located at vehicles retrieve environmental parameters associated to determined parts of the city. Sensors are installed in 150 public vehicles, including buses, taxis and police cars.

• **Traffic Intensity Monitoring**: around 60 devices located at the main entrances of the city of Santander have been deployed to measure main traffic parameters, such as traffic volumes, road occupancy and vehicle speed or queue length.
• **Guidance to free parking lots**: taking information retrieved by the deployed parking sensors, 10 panels located at the main streets’ intersections have been installed in order to guide drivers towards the available free parking lots.

• **Parks and gardens irrigation**: around 50 devices have been deployed in two green zones of the city, to monitor irrigation-related parameters, such as moisture temperature and humidity, pluviometer, anemometer, in order to make irrigation as efficient as possible.
- **NFC/QR tags**: more than 2000 tags have been deployed and distributed to different strategic places in the city centre of Santander. These tags are mainly in the transportation points (bus stops, taxis, etc...), points of interest (monuments, etc...) and shops. All the information provided is online and can be updated at any time.
Experimentation capabilities

SmartSantander testbed provides several experimentation tools. For service experimentation offers data access through the software component called IOT API and the FIWARE Generic Enablers. Additionally, reprogramming tools and a specific IDE with developed functions can be used to create experiments and flash them in the deployed infrastructure. There are two types of experimentation possibilities depending on its nature:

- **Service experimentation**: It uses the data received from the sensors to create new experiments or services (e.g. noise data to generate noise maps, etc).
- **Node Experimentation**: flash deployed nodes to load new experiments and make use of the 802.15.4 interface to communicate within them in urban scenarios (e.g. opportunistic protocol communication buses and repeaters, etc).

Protocols and data formats

SmartSantander testbed uses the protocols and data formats described in section 0. However, the communication performed in the two lower layers, corresponding to the gateways and the IoT nodes, uses a different protocol, specifically defined for the communication in the SmartSantander testbed. The protocol was defined to deliver the sensor data frames from the IoT nodes to the gateways as well as supporting the primitives defined to modify the behavior of the nodes in real time as well as updating the firmware of the nodes.

<table>
<thead>
<tr>
<th>Table 1 SmartSantander Service Frame example</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Frame example" /></td>
</tr>
</tbody>
</table>

Table 1 shows an example of a service frame using the protocol developed within SmartSantander for the communication among nodes and gateways. As it is shown, the protocol is divided in two main parts, the headers including the client id, which is used to differentiate between applications managing nodes; the payload ID to specify the type of the primitive; the options and the frame type are reserved for future use; the node ID identifies the node; the sequence number is a byte that is increased every time a frame is sent;
the node type specifies the type of the node; the length specifies the payload length; and, finally, the payload is composed of the measurements from the sensors integrated in the repeater, following a TLV approach.

**Security and access policies**

The access policies and the security applied to this layers is the same as explained in section 0 as the methods to access the data relies in the SmartSantander platform.

**Applications**

SmartSantander implements two mobile applications to make the citizens participants of the testbeds and provide a gateway to access the SmartSantander data. Additionally, one new application is being developed under the framework of ClouT.

- **Participatory Sensing service**, see application appearance in aims at exploiting the use of citizens’ smartphones to make people become active in observations and data contribution. In this scenario citizens, Santander City Council and the local newspaper “El Diario Montañés” are connected into a common platform where they can report, share and be notified of events happening in the city. As an example, a user walking in the city centre who finds a hole in the pavement can take a picture, write a text and finally share this incidence with other users of the application. The Santander City Council will therefore be notified of the occurrence of the event and proceed accordingly by sending an employee to the location in order to fix this problem.

  ![Figure 10 SmartSantander Augmented Reality application](image)

- **The AR service** (developed within the SmartSantander project) includes information about more than 2700 places in the city of Santander, classified in different categories: beaches, parks and gardens, monuments, buildings, tourist information offices, shops, art galleries, libraries, bus stops, taxi ranks, bicycle hire points, parking lots and sports centres, as shown in Figure 69. Furthermore, it allows real-time access to traffic and beach cameras, weather reports and forecasts, public bus information and bike hire service, generating a unique ecosystem for end users when moving around the city.
Additionally to the mobile applications, the SmartSantander testbeds include several application services that are being used by the municipality and citizens:

- **Parking information panels**: use of the deployed panels to inform the citizens about the state of the free parking spots in the city center.
- **Traffic status in motorway panels**: motorway panels are being feed with the information about the traffic density in the city, so the drivers can take decisions to choose the best route before entering in the city center.
- **Irrigation**: the information about the humidity and temperature in the parks and gardens of the city is being sent to the corresponding parks and gardens managers to decide whether they need to irrigate or not.
SmartSantander IoT platform

General description and architecture ................................................................. 12
Protocols and data formats ................................................................................. 13
Control and management tools ............................................................................. 14
Security and access policies .................................................................................. 15
Federation approach ............................................................................................... 15
Reusable components ............................................................................................ 16
General description and architecture

SmartSantander platform is the upper layer from the SmartSantander testbed. It is in charge of managing and control deployed resources in the city of Santander as well as external services that might use the platform to store and retrieve data later.

Figure 12 SmartSantander platform tier

As it is shown in Figure 12 the SmartSantander platform tier has two main access points. The bottom access point allows to inject data into the platform, to be stored and retrieved later. This is managed by the IoT API.
component which provides a REST interface to inject data and register new devices. The upper access is also managed by the IoT API and is part of the Fed4Fire federation. This access allows external experimenters and service providers to access the data injected into the SmartSantander platform.

The platform also provides the components to manage both, the new sensors and services registered in the platform, through the resource directory and resource register manager components; and the data injected from the services and sensors, which is stored in the internal repository based on a mongo database.

Finally, the platform also provides the integration with FIWARE, allowing to inject directly the sensor data received into the corresponding instances: ORION for the context manager of IoT devices managed by the FIWARE resource configurator component, and COSMOS for the historical storage of IoT sensors, managed by the FIWARE storer component.

### Protocols and data formats

The SmartSantander platform internal communications are made using the ZMQ communication framework. The zeroMQ communication framework offers several possibilities of communication using TCP sockets and provides several communication mechanisms: PUB/SUB, REQ/REP and PUSH/PULL. Additionally, the platform uses REST-based http requests for the IoT API interfaces.

All the internal messages use the JSON format. The content of the JSON depends whether it describes sensor data or a resource. In the case of the sensor data the JSON is divided in several fields representing the urn, which is the unique identifier for every resource injecting data in SmartSantander; the observations array, which contains the timestamp (when the measurement was taken), the location (where it was taken), and the measurements array, where the measurements are set using a triplet of type, value and unit. The described JSON is also used when accessing to the data using the IoT API in the upper layer, while using FIWARE the format is JSON as well but follows a different structure.

#### Table 2 JSON example of SmartSantander sensor data

```
{
    "urn":"urn:x-iot:smartsantander:24xsu0:los_castros",
    "observations":[
        {
            "timestamp":"2014-04-30T11:41:01.123+02:00",
            "location":{
                "coordinates":[
                    -3.8643275,
                    43.4664959
                ],
                "type":"Point"
            }
        }
    ]
}
```

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement 643275, and from the Japanese National Institute of Information and Communications Technology.
"measurements": [
  {
    "type": "trafficDensity",
    "value": 2,
    "unit": "unitless"
  }
]

Every resource in SmartSantander has a URN that identifies the resource uniquely within the SmartSantander platform. The URN format is based on the RFCs RFC2141 and RFC3406 and has a maximum length of 255 characters, divided in groups as follows:

- **URN prefix**: is the first field of the resource name and it is always the same: “urn:x-iot:”.
- **Domain name**: this part represent to what domain (proyect, external testbed / service) the node belongs.
- **Provider Id**: This is a unique id for each service provider (who is generating and injecting measurements into the platform).
- **Local Id**: specific identifier that can be defined by the service provider.

### Table 3 URN example for SmartSantander

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Domain</th>
<th>Provider Id</th>
<th>Local ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:x-iot:</td>
<td>festival:</td>
<td>Zxc123:</td>
<td>santander123</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>urn:x-iot:festival:Zxc123:santander123</td>
</tr>
</tbody>
</table>

**Control and management tools**

SmartSantander has several control system tools to manage the infrastructure deployed. For accessing the nodes and reprogramming, a set of tools programmed in Java have been developed. These tools allow to reprogram and perform different requests (e.g. delete a program, get node characteristics, change service cadence, etc.). These tools are mainly two: the testbed runtime implementation for SmartSantander that is being migrated to the specific tools to meet the FED4FIRE requirements, and the digi-smart-tool application, ready to maintain and load new programs into the nodes from the gateways deployed in the city.

Furthermore, the SmartSantander platform has also several internal tools to manage the registered devices in the platform. Currently, there is a software component in charge of keeping track of the
deployed devices as well as those sensors or external services that inject data into the platform. This component is also being migrated to a second version, which will use JSON as the standard for the resource description and will act as an authorization server for incoming data injected in the platform. Moreover, the FED4FIRE API takes advantage of the resource directory to explore and discover the resources available in the testbed through the IOT API.

Finally, there is also another component within the Smartsantander platform to provide the current health state of the platform monitoring the sensor data. The component called NodeManager monitors the frequency of the measurements and data injected into the platform to infer if the device or the source is not available, and then it gets deactivated in the resource manager.

**Security and access policies**

The access to the SmartSantander platform resources can be granted by contacting the University of Cantabria by using its internal methods (IoT API). However, data generated from the testbed is available for anyone in the ORION and COSMOS component in FIWARE. The access to this platform can be done following the tutorials uploaded in the SmartSantander webpage.

The access to the testbed resources using IoT API can be done using RESTful webservice and being authenticated in two ways. On the one hand, external experimenters working with the SmartSantander data will be able to access the data using a unique API key that will be sent under request. On the other hand, experimenters will be able to access the API by using CA certificates based on the X.509 v3 standard. Additionally, all the communications made to inject and retrieve data are end-to-end encrypted.

**Federation approach**

At the time being, SmartSantander supports two types of federation: using available FIWARE components and following FED4FIRE directives.

**FIWARE**

FIWARE is a new infrastructure for the creation and development of services and applications on the Future Internet. Cloud-based it aims at being a new open alternative for entrepreneurs and users of the services on the Future Internet. The main objective of FIWARE is to provide the basic elements with which to build new services and applications in such diverse areas as smart cities, the Internet of things, e-health, e-education, advanced manufacturing, multimedia applications, etc.

FIWARE is divided in several components, the so-called Generic Enablers, which provide different functionalities out-of-the-box. As commented above, SmartSantander uses two GE from FIWARE to store and manage the sensor data generated in the testbed: ORION and COSMOS.

**FED4FIRE**

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement 643275, and from the Japanese National Institute of Information and Communications Technology.
SmartSantander is federated within the FED4FIRE project. It aims at provide a unified access to heterogeneous testbeds to perform experimentation on available resources. The project takes into account three types of testbeds for federation: Associated testbeds, Light federation and advance federation.

SmartSantander is being federated following the second model at the time being. Future works foreseen federation under the advanced federation. The federation carried out in SmartSantander is being done through the IOT API component, what implements the required APIs to be part of FED4FIRE. Additionally, the certificates implemented in SmartSantander are also compatible with FED4FIRE.

FED4FIRE foreseen the federation with external testbeds that are not included in the initial project, following one of the previous types of federations. The requirements within Fed4fire depends on the testbed type being federated and the approach followed (light, advanced or associated). Whilst associated testbed does not require more than available documentation, light and advanced testbeds require technical integration. Common requirements are described at following:

- Documented REST API for testbed access.
- Support of Fed4Fire credentials in a client-based SSL API

Advanced testbed federation requires in addition the implementation of a component called Federation Aggregate Manager. This component implements XML-RCP over SSL connections to expose an API that follows specific Fed4Fire guidelines. Implemented AM needs to support:

- SFA for resource discovery using RSpec for the resources description format.
- Sensor data use OML format.
- Optionally, in order to control the experiments, a FRCP implementation using OMF format.

**Reusable components**

SmartSantander platform can be reused completely, using the APIs provided to register new external devices and inject data into the platform. These data will be then made accessible using different methods: FED4FIRE APIs developed within the platform and the FIWARE components ORION and COSMOS. The formats descriptions used in SmartSantander (JSON description for observations as well as the URN to name the resources) are also available to be ported to other platforms.

Finally, several components initially developed for the SmartSantander platform might be available to be deployed in other platforms to extend its capabilities:

<table>
<thead>
<tr>
<th>Software module name:</th>
<th>Digi-smart-tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Binary to reprogram and perform requests on top of the SmartSantander nodes.</td>
</tr>
</tbody>
</table>
Is it portable and/or reusable (license): It is belongs to the UC. It can be used but the reprogramming protocol must be implemented in the nodes to be reprogrammed.

Software module name: NodeManager
Description: Scan for active nodes by checking the frequency of measurements. The nodes that are not sending measurements and cannot be accessed are deactivated in the Resource Directory.

Is it portable and/or reusable (license): It belongs to the UC. It can be used but the nodes need to implement the protocol.

Software module name: Resource Directory
Description: Java application which stores all the resource information within the SmartSantander platform in a database. New data can be inserted through a REST interface. Nowadays being migrated within the SmartSantander platform.

Is it portable and/or reusable (license): SmartSantander component that can be deployed anywhere (no dependencies).

Software module name: Yes (Nowadays being migrated to Fed4Fire): Testbed Runtime.
Description: Wisebed implementation for managing and control the resources for experimentation. It also allows resource reservation and reprogramming.

Is it portable and/or reusable (license): Yes, can be implemented in the testbeds by following the instructions in the webpage. Nowadays is discontinued as the project ended in 2012.