INFSO-ICT-257992 SmartSantander

D5.3

SMART SANTANDER Regulations for use of experimental facility

Contractual Date of Delivery: 31.8.2011.

Actual Date of Delivery: 1.09.2011

Editor(s): EYU

Author(s): See authors list

Participant(s): EYU, UC, CTI

Workpackage: WP5

Estimated person months (per partner): EYU 1.2, UC 1, CTI 0.8

Security: Public

Version: 1.0

Abstract: This deliverable provides acceptable use policy and terms and conditions for using the SmartSantander testbed.

Keyword list: *Acceptable Use Policy, Terms and Conditions*

Disclaimer: This document reflects the contribution of the participants of the research project SmartSantander. The European Union and its agencies are not liable or otherwise responsible for the contents of this document; its content reflects the view of its authors only. This document is provided without any warranty and does not constitute any commitment by any participant as to its content, and specifically excludes any warranty of correctness or fitness for a particular purpose. The user will use this document at the user's sole risk.

Authors

Partner	Name	E-mail
EYU	Srdjan Krco	srdjan.krco@ericsson.com
UC	Luis Munoz	luis@tlmat.unican.es
CTI	Evangelos Theodoridis	theodori@cti.gr

Table of Contents

Acronyms and Abbreviations

AUP	Acceptable Use Policy
IoT	Internet of Things
S3C	SmartSantander Steering Committee
WSN	Wireless Sensor Network

EXECUTIVE SUMMARY

The nature of generally acceptable experiments is provided together with appropriate network etiquette as well as an indication of non-acceptable activities and usage rules. A short description of complaints handling procedures is also provided.

Due to the living nature of the SmartSantander platform and continuous updates and addition of new IoT nodes and functionality, this document will be updated after each deployment phase to ensure that all relevant policies are included.

INTRODUCTION

The main goal of the project is the creation of a European experimental test facility for the research and experimentation of architectures, key enabling technologies, services and applications for the Internet of Things (IoT) in the context of the smart city. This deliverable provides acceptable use policy and terms and conditions for using the testbed deployed in SmartSantander, by the researchers, service developers and end-users.

SmartSantander is a consortium established to create and manage a both service provision and experimentation platform in the context of a city. The facility is deployed in the outdoors environment, designed to enable IoT related experiments run by the researchers, service developers and end users. The complete testbed consists of several sites: Santander (the main site), Lübeck, Guildford and Belgrade. All uses of the testbed should be consistent with this high-level goal.

SmartSantander Consortium is supervised by a Steering Committee (S3C – SmartSantander Steering Committee) consisting of “Steering Committee Members”.

SmartSantander testbed consists of a set of interconnected components (IoT devices) and applicable network devices and communication links that enable deployment and running of the experiments as well as collection of the results.

The SmartSantander system has a special value as a research tool because it is open to the public Internet, facilitating cutting-edge IoT research in the context of real-life, on a city scale, but through federation of the sites on the global scale as well. Due to the open nature of the system and since it is embedded in the city environment it is necessary to prevent malicious users, disruption of normal city services and citizens’ activities as well as fair usage to all interested parties. For this reason, SmartSantander has a system of safeguards in place to ensure rapid resolution of any incidents that might arise.

ACCEPTABLE USE POLICY (AUP)

Article 1: The nature of the SmartSantander testbed

As an overlay, SmartSantander is not a "testbed" in the usual sense of a controlled environment for experiments. It consists of IoT devices placed in public and private infrastructures of Santander and other cities and providing support to both experimentation and end-user services in the context of the smart city. In this first call, the experimenters will have access to a three level architecture made of the under-the-asphalt buried sensors, repeaters and gateways. The latter are the elements connected to the backbone hence providing access to the whole infrastructure with previous authentication and experiment configuration. It also provides access to other testbeds that are interconnected with SmartSantander in a world-wide federation and allows for the deployment of experimental services that are accessible to all users of the Internet. Therefore, running an experiment on SmartSantander is fundamentally different from running it in a LAN-based lab or on an isolated wide-area testbed.

Article 2: General guidance on the acceptability of experiments

When designing an experiment it is important to bear in mind that the SmartSantander platform is concurrently supporting experimentation and city context service provision. This means that besides the traditional bandwidth constraints the experimenters have to carefully consider the implications in terms of concurrent service provision to avoid disruption of ongoing services used by the city government and citizens in general. It is their responsibility to ensure that the use of SmartSantander falls within these constraints. This means that experimenters have to debug own code in a controlled environment first, to be confident about the behaviour of the code.

Further to this, it is not allowed to use the testbed to harm or in any other way provide false information to general public (for example using public displays that are part of the testbed).

The rules applicable to standard network experiments, like performing systematic port scans, using more than assigned share of bandwidth as well as the number and type of IoT devices are applicable as well.

Article 3: Responsibility of sites with regard to their users

SmartSantander is designed to support a broad community of users (researchers, service developers and providers, citizens and city officials). As a consequence, it could indirectly support users that have not officially registered with SmartSantander, and may even be unknown to you (the resource provider). It is your responsibility as a site administrator and user (as experimenter) to ensure that your users do not cause your service to violate the terms of this Acceptable Use Policy. In particular, site administrators should ensure that their users are not able to hijack the service and use it to attack or spam other nodes or network users.

Article 4: Standards of network etiquette

SmartSantander is designed to support IoT experiments that can purposely probe the communication links, measurements done by the sensors or actions to be executed by the actuators. However, we expect all users to adhere to widely-accepted standards of network etiquette in an effort to minimize complaints from network administrators. Activities that have been interpreted as worm and denial-of-service attacks in the past (and should be avoided) include sending SYN packets to port 80 on random machines, probing random IP addresses, repeatedly pinging routers, overloading bottleneck links with measurement traffic, and probing a single target machine from many SmartSantander nodes.

It is likely that individual SmartSantander sites will have their own Acceptable Use Policies. Users should not knowingly violate such local Acceptable Use Policies. Conflicts between site Acceptable Use Policies and SmartSantander's stated goal of supporting research into IoT should be brought to the attention of the SmartSantander administrators.

Article 5: Handling of complaints

While the central SmartSantander authority is often the first point of contact for complaints about misbehaving services, it is our policy to put the complainant in direct contact with the researcher who is responsible for the service.

To report a suspected violation of this policy, contact SmartSantander Support: **support@smartsantander.eu**.

Article 6: No guarantees

a) No guarantees

SmartSantander provides absolutely no privacy guarantees with regard to packets sent to/from IoT nodes. In fact, the users should assume that packets will be monitored and logged, for example, to allow other users to investigate abuse (see previous paragraph).

SmartSantander also does not provide any guarantees with respect to the reliability of individual nodes, which may be rebooted or reinstalled at any time previous administrator authorization. Reinstalling a node implies that the disk is erased, meaning that users should not treat the local disk as a persistent form of storage.

ANY GOODS, SERVICES, AND WRITTEN MATERIALS PROVIDED BY SMARTSANTANDER OR ITS AGENTS OR ANY MEMBER IN ANY FORM, WHETHER FURNISHED IN DRAFT OF FINAL FORM ARE PROVIDED "AS-IS WITH ALL DEFECTS" AND WITHOUT ANY WARRANTY OF ANY KIND. SMARTSANTANDER DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

b) Liability limited

IN NO EVENT SHALL SMARTSANTANDER OR ANY OTHER MEMBER BE LIABLE TO ANY OTHER MEMBER OF SMARTSANTANDER FOR ANY CONSEQUENTIAL, INCIDENTAL, PUNITIVE, OR LOST PROFIT DAMAGES, OR FOR ANY DAMAGES ARISING OUT OF LOSS OF USE OR LOSS OF DATA, TO THE EXTENT THAT SUCH DAMAGES ARISE OUT OF THE ACTIVITIES OF SMARTSANTANDER OR THIS AGREEMENT OR ANY BREACH THEREOF EVEN IF MEMBER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Nothing contained in this Agreement shall be deemed as creating any rights or liabilities in or for third parties who are not Members of SmartSantander.

Article 7: Rules of use

a) Overall rules

- SmartSantander should not be used for any illegal enacted by any law or regulation.
- SmartSantander may be used for industrial innovation activities as well as for research and educational purposes.
- Access rights granted to SmartSantander exclude any rights to sublicense, including to affiliates, unless expressly stated otherwise.
- Access rights granted to SmartSantander don’t give the rights to accede to any other SmartSantander platform that is not federated with SmartSantander.
- While SmartSantander is federated with other testbeds, access rights to those testbeds may be restricted by those testbeds or by agreements between SmartSantander and those testbeds.

b) IoT node usage rules

- Use existing security mechanisms.
- Do not circumvent accounting and auditing mechanisms. This means you must associate your identity with the SmartSantander account in which your service runs, and you must not do anything to obfuscate the audit trail.

- No hacking attempts of the SmartSantander nodes. This includes "red team" (hacker test) experiments. All access is non-root.
- Causing physical damage or tampering with the nodes (including casing, power supply, etc.) is not allowed.
- Avoid spin-wait for extended periods of time. If possible, do not spin-wait at all.

c) Network usage rules

- Do not use your SmartSantander account to gain access to any hosting site resources that you did not already have.
- Do not use one or more SmartSantander nodes to flood a site with so much traffic as to interfere with its normal operation. Use congestion-controlled flows for large transfers.
- Do not do systematic or random port or address block scans. Do not spoof or sniff traffic.

d) Consequences

Violation of this Section “Acceptable Use Policy” may result in any of the following:

- disabling the account;
- removing the Site from SmartSantander ;
- informing the organisation's administration.

To report a suspected violation of this policy, contact SmartSantander Support: **support@smartsantander.eu**

In case of any breach with this acceptable use S3C shall terminate this Membership Agreement at any time and without written notice as provided with the Section Terms and Conditions of Membership, Article 1.

REFERENCES

[Onelab2-D2.6]	FP7 Onelab2, Deliverable D 2.6