Deliverable D2.1

Use-cases definition and threat analysis

Editors:	Theodore Mouroutis, Athanasios Lioumpas (CYTA Hellas)
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	31 May 2014
Actual delivery date:	15 December 2014
Suggested readers:	End users, application developers, public administrations, service providers, hardware manufacturers, researchers
Version:	1.1 (Revised version)
Total number of pages:	157
Keywords:	RERUM, Internet of Things, smart cities, applications, use-cases, smart transportation, home energy management, environmental monitoring, comfort quality, threat analysis, security, privacy, confidentiality, integrity, availability, authentication, authorization, accounting

Abstract

This deliverable describes the RERUM smart city applications and identifies the possible threats and risks in terms of security and privacy. A brief review of the state of the art with respect to smart city use-cases is presented, aiming to analyse the research topics under investigation and the corresponding approaches that have been followed in the literature. Based on this analysis, the generic categories of the RERUM stakeholders and their expected benefits are analysed. Then, the RERUM use-cases are described in detail, analysing the key challenges, the objectives and KPIs, the system components involved, the main functionalities, as well as the stakeholders, their roles and benefits. For each use-case, a popularized example is given, showing clearly the impact of the use-case in the citizens' lives. The deliverable provides also a link between the user requirements (that stem from the cities' and citizens' needs), the RERUM technical requirements and the technical solution required in order to address the requirements. The use-case analysis also serves the second goal of this report that is to identify the possible risks and threats for the envisioned RERUM use-cases. To this end, the risk sources, the threats considering confidentiality, integrity and availability of data, as well as authentication, authorization and accounting for the RERUM use-cases is presented. Furthermore, privacy threats are identified as well, while examples for illustrating this analysis are given.

Disclaimer

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 609094

Impressum

Full project title	Reliable, resilient and secure IoT for smart city applications
Short project title	RERUM
Number and title of work-package	WP2 - The IoT Architectural Framework for Smart Cities
Number and title of task	T2.1 - Use-cases definition and vulnerability analysis
Document title	Use-cases definition and threat analysis
Editor: Name, company	Theodore Mouroutis, Athanasios Lioumpas, CYTA
Work-package leader: Name, company	Theodore Mouroutis, CYTA
Estimation of person months (PMs) spent on the Deliverable	

Executive summary

This report identifies the Use-Cases (UCs) that will be considered in the RERUM project and provides the threat analysis for them. These use-cases will be analysed in terms of vulnerabilities and threats and will be used as a basis to drive the design of the RERUM system. RERUM considers four UCs: (i) two outdoor UCs for smart transportation and environmental monitoring, and (ii) two indoor UCs, for home energy monitoring and comfort quality monitoring. In Section 1, the state-of-the-art is thoroughly reviewed, taking into account related European projects as well as other initiatives, analysing their goals, the key challenges and their results. As discussed in this section, the development of the security, privacy, and reliability mechanisms in previous or current projects is based on conventional security protocols and algorithms, without taking into account the special requirements of smart city applications. As a result, these solutions cannot always adapt to the specific needs, requirements and characteristics of each application. On the other hand, RERUM follows a different approach, aiming to ensure the trustworthy exchange of information between smart objects and the foreseen smart city applications, preserve privacy of data, secure the network to prevent attacks such as jamming, passive listening, data falsification, etc.; further, automatic secure configuration of smart objects will increase network reliability.

Section 2 gives a detailed description of the use-cases that are considered within RERUM. Each use-case is analysed in order to define: (i) the key challenges, (ii) the hardware components involved, (iii) the network interfaces, (iv) the data that will be sensed, (v) the actions that will be performed by the smart objects, and (vi) the stakeholders that are involved in smart city applications (e.g., citizens, vendors, public sector, etc.). Furthermore, the Key Performance Indicators (KPI)s for each use case were identified in order to provide ways to show the improvements that RERUM brings to those use cases. The main goal of the use-case analysis is to drive the threat analysis in Section 3 of this document, and to extract the system requirements of RERUM (presented in Deliverable D2.2).

In Section 3, the threat analysis for the smart city applications is presented, following a three-step methodology. The first step begins with an asset-centric approach, which includes Confidentiality, Integrity and Availability (C-I-A) analysis, and then follows an attacker-centric analysis by looking at specific threats against Authentication / Authorization / Accounting (AAA). The third step includes the analysis of the privacy threats that may exist in the use-case implementations. The identification of the IT assets is a critical aspect towards the threat analysis for each of the RERUM UCs, and, more importantly, the design of appropriate mechanisms for ensuring the system's security and privacy. These assets include the authentication credentials, user data (e.g., sensed and actuation data), command and control data, and all software running on RERUM devices and gateways. Besides the security threats, the design of the RERUM system will also take into consideration critical privacy issues. Such issues arise due to the need of smart city applications for automatically collecting, storing, using, and disclosing personal user information that can potentially reveal sensitive private data, which could be used to construct a profile of a user. Section 3 also presents examples about possible security and privacy threats for the RERUM use-cases.

In Section 4, the user requirements that stem from the cities', citizens' and stakeholders' (e.g., network operators, service providers, vendors, etc.) are analysed in order to identify the fundamental issues (security, privacy, reliability, etc.) that have to be resolved in order to satisfy those needs. These user requirements are related to the technical requirements of the RERUM system, which are detailed in the deliverable D2.2. The main goal is to provide a solid link between the user requirements, the key challenges, the technical requirements and finally the innovations that have to be developed within RERUM in order to realize the envisioned smart cities applications. Furthermore, exploitation plans and business models are provided for these innovations.

List of authors

Company/Organization	Author	Contribution
CYTA	Theodore Mouroutis (Editor)	State of the art, Home energy management use-case.
	Athanasios Lioumpas (Editor)	State of the art, Home energy management use-case. Contribution to URs and innovation tables;
ATOS	Dario Ruiz	Threat analysis: Environmental monitoring Contribution to innovation tables;
	M. Guadalupe Rodríguez	Threat analysis: Environmental monitoring
SAG	Jorge Cuellar	Threat methodology, privacy threats, attacker model, threat and privacy analysis, asset identification. Contribution to security UR and innovation table;
	Santiago Suppan	Privacy threats, attacker model, threat and privacy analysis (in particular for Smart Transportation) Contribution to innovation tables;
UNIVBRIS	George Oikonomou	Vulnerability Analysis: Overview and Comfort quality monitoring Contribution to innovation tables;
LiU	Vangelis Angelakis	State of the Art, Smart Transport Use-case Contribution to URs and innovation tables;
	David Gundlegård	Smart Transport Use-case
	Scott Fowler	State-of-the-art
UNI PASSAU	Henrich C. Pöhls	Threat analysis for security (in particular: Integrity and Authenticity and the Home Energy Monitoring Use-case,); Contribution to Methodology (in particular: Data-Flow based Asset identification, Differentiation of data assets extracted from Use-Cases); Contribution to security UR and innovation table;
	Joachim Posegga	Internal Reviewer of D2.1 with helpful comments on structure and content.
Zolertia	Antonio Jesús Liñán Colina	State-of-the-art and Comfort Quality Analysis Use-case Contribution to URs and innovation tables;
	Francisco José Paredes Vera	State-of-the-art and Environmental

		Monitoring Use-case
	Marc Fàbregas Bachs	State-of-the-art, Environmental Monitoring Use-case and Comfort Quality Analysis Use-case Contribution to innovation tables;
FORTH	Elias Tragos	Internal Reviewer, overall editing Contribution to URs and innovation tables;
	George Stamatakis	Comfort quality monitoring state of the art.
HER	Costis Mochianakis Manolis Fotakis	Use-cases scope and benefits, Comfort quality monitoring use-case contribution Contribution to URs and innovation tables;
AJTGNA	Xavier Reina Virgili	Use-cases scope and benefits Contribution to URs and innovation tables;
	Julio Español Jordan	Use-cases scope and benefits

Table of Contents

List of figures

List of tables

List of Contributions

Revision History

The following table describes the main changes done in the document after the review.

Revision	Date	Description
V1.0	31 May 2014	First version of the document submitted to the EC
V1.1	15 December 2014	Revisions in the new version: - Added KPIs for each one of the use cases at the Section 2. - Added Section 4 describing the links between the use cases, the user requirements, the technical requirements (described in D2.2) and the technical innovations of the project to be developed in WP3 and WP4. - Added related text in the introduction and in the conclusions - Added list of Contributions in the ToC

Abbreviations

3G	3rd Generation of mobile communications
6LoWPAN	IPv6 Over Low-power Wireless Personal Area Network
A-DATA	Actuation Data
AAA	Authentication / Authorization / Accounting
AC	Alternating Current
AES	Advanced Encryption Standard
BC	Black Carbon
BEMS	Building Energy Management Systems
C&C-DATA	Command and Control Data
CDR	Call Detail Record
C-I-A	Confidentiality, Integrity and Availability
CO	Carbon Monoxide
CO_2	Carbon Dioxide
CPU	Central Processing Unit
CI	Critical Infrastructure
DIY	Do It Yourself
DHCP	Dynamic Host Configuration Protocol
DOS	Denial of Service
DS	Directory Service
DSL	Digital Subscriber Line
DTLS	Datagram TLS
EC	European Commission
E-DATA	Environmental data
EDGE	Enhanced Data rates for GSM Evolution
EMF	Electro-Magnetic Field
EU	European Union
GC	Group Controller
GIS	Geographic Information System
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HCD	High-Consuming Device
HEMS	Home Energy Management Systems
ICN	Information Centric Networking
ICT	Information and Communication Technologies
IoT	Internet of Things
ITS	Intelligent Transportation Systems
KPI	Key Performance Indicator
LTE	Long Term Evolution
MAC	Medium Access Control
NET-DATA	Network data
NO_x	A composition of NO and NO_2
O_3	Ozone
OD	Origin-destination
OSH	Occupational Safety and Health
PAN	Personal Area Network
PM	Particulate Matter
POC	Proof of Concept
QoS	Quality of Service

RF	Radio Frequency
RH	Relative Humidity
RPL	Routing Protocol for Low-Power, Lossy Networks
SC	Smart City
SO_2	Sulphur Dioxide
QoS	Quality of Service
REST	Representational State Transfer
RH	Relative Humidity
S-DATA	Sensed Data
SaaS	Software as a Service
SIM	Subscriber Identity Module
SO	Smart Object
SSL	Secure Sockets Layers
SW	Software
TLS	Transport Layer Security
WIM	Weight In Motion
U-DATA	User Data
UC	Use-case
UR	User Requirement
UV	Ultra-Violet
UWB	Ultra-wideband
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VOC	Volatile Organic Compounds
WiFi	Wireless Fidelity alliance
WSN	Wireless Sensors Network

Definitions

Term	Definition	Source
Access network	The part of a telecommunications network that connects users to their service provider (e.g., mobile access networks (GSM, GPRS, UMTS, LTE, etc.), fixed access networks (xDSL, fiber, etc.))	
Acting element	An (embedded) device that has the capability to affect the condition of a Physical Entity, (like changing its state or moving it) by acting upon an electrical signal	RERUM/ IOT-A part of actuator [2]
Actuator	A smart device that includes one or several acting elements and receives (IT-based) information (command – CDATA) translating it to electrical signal for the acting elements. An actuator can also include a sensor so that there is knowledge on the Physical Entity it acts upon, in order to translate correctly the command into the electrical signal.	RERUM/IOT-A [2]
Application server	The point responsible for the end-user services (e.g., automation services, energy management, etc.)	RERUM/IOT-A [2]
Attack	An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.	RFC2828 [6]
Command and Control Data (C&C-DATA)	Data and metadata used to control, monitor and manage the system's overall state, in order to ensure correct functionality.	RERUM
Constrained networks	On the other hand, constrained networks provide relatively low transfer rates (e.g., smaller than 1 Mbps), as offered by, e.g., IEEE 802.15.4. These networks are also characterised by large latencies, due to the involved low-bitrate physical layer, or the power-saving policies (e.g., sleep-wake mechanisms for energy-efficiency reasons).	IoT-A [2]
Device	It can be a single or a combination of the following elements: • Sensors, which provide information about the Physical Entity • Tags, which are used to identify Physical Entities • Actuators, which can modify the physical state of a Physical Entity	IoT-A [2]
Entity	Something that exists by itself: something that is separate from other things. Could be physical, virtual, functional, etc.	Merriam-Webster dictionary [1]

Gateway	Network node equipped for interfacing with another network that uses different protocols.	Federal Standard 1037C [4]
High-level Application Data (H-DATA)	Data which result from the processing of the sensed data by an application server. These data are usually responses to end-users' queries and may include metadata about the user or necessary application parameters, such as the current location of the user or the destination of the current travel etc.	RERUM
IT-asset	A system resource that is (a) required to be protected by an information system's security policy, (b) intended to be protected by a countermeasure, or (c) required for a system's mission.	RFC4949 [5]
(IT) Threat	A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm. Here a security violation is an act or event that disobeys or otherwise breaches security policy	RFC2828 [6]
Network Data (NET-DATA)	All U-DATA, H-DATA and C&C-DATA while in transit.	RERUM
Network provider	A company that provides network connectivity either to an access network (e.g., cellular network provider, xDSL network), or/and within the constrained/unconstrained network.	RERUM
Physical entity (PE)	A discrete, identifiable part of the physical environment which is of interest to the user for the completion of his goal. Physical Entities can be almost any object or environment.	Merriam-Webster dictionary [1] / IOT-A [2]
RERUM Device (RD) or RERUM Smart Object	A RERUM Device (RD) is a piece of hardware and software (incl. the Operating System) that is equipped with intelligence. It has one or more Resources that the RERUM Device is able to either fill with interpreted and pre-processed sensory data or able to read and interpret the commands that are given. The RERUM Device has some Sensing, Tag or Acting elements directly attached to it.	RERUM
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.	RFC2828 [6]
Sensing element	An (embedded) device that perceives certain characteristics of the real-world environment (Physical Entities), translating a change into an electrical signal.	RERUM
Sensor	A smart device that includes one or several sensing elements and is able to translate the electrical signal of the sensing elements to some type of information (digital representation)	IoT-A [2]

	with specific value and semantic.	
Service provider	A company that provides IoT services (e.g., home energy management services).	RERUM
Smart Object	See RERUM Device	RERUM
Unconstrained networks	High-speed communication links (e.g., order of Mbps), where the link-level transfer latencies are small, which are the results of network-level congestion events, rather than physical layer limitations. Examples of such networks may include 802.11 based technology or wired technologies, such as Ethernet.	IoT-A [2]
User	A Human or a software that interacts with a system for transferring information.	Based on IoT-A [2] and ATIS telecom glossary [3]
User DATA (U-Data)	The user data that are further broken down into two categories: - Sensed Data (S-DATA). This can include for example location data or environmental data, which allow deducting information about the condition of a Physical Entity. - Actuation Data (A-DATA), e.g., the data that refer to actuators' state, requests, responses, etc.	RERUM

1 Introduction

1.1 The Smart City context

The development of Smart Cities is mainly driven by the fast growth of the urban population (more than 50 percent of people on the planet live in large cities [1]). This poses several challenges in providing infrastructure and public services (e.g., transportation, traffic congestion, etc.), raising the need for more eco-friendly management of natural resources and an improved quality of life for the citizens [1]. The concept of Smart Cities is based on advanced Information and Communication Technologies (ICT) which enable the interconnection of physical and virtual objects ("things") through a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols, seamlessly integrated into the information network. In this sense, this Internet of Things (IoT) interconnects people, data, things, and processes in order to work together towards the future smart cities and communities [7]. According to the definition provided in [8] *a city may be called 'smart' when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory government.*

The deployment of future Smart Cities is based on three major perspectives: the Future Internet research, the cities and urban development, and the user-driven innovation ecosystems [8]. While the research on Future Internet and IoT greatly contributes to understanding fundamental concepts and technologies, large-scale real-life projects are crucial towards the realization of Smart Cities. Such projects require both initiatives by the city's policy makers and the actual participation of the citizens. The actors, priorities, and policies for these perspectives are given in Table 1 [9]. As mentioned, the transformation of a conventional city to a Smart City mainly relies on the capability to interconnect people, data, things, and processes under a dynamic global infrastructure. The key enablers for this perquisite are:

- The existence of a high-capacity broadband network infrastructure supporting the interconnection of a huge number of objects and nodes.
- The deployment of a network of sensors, smart devices and actuators for real-time monitoring, management and processing of specific environmental parameters or any other type of information that presents interest.
- The development of the necessary applications and underlying software for exploiting the IoT to create user-friendly services.

The IoT is foreseen as the enabler of a wide range of services and applications [8], such as:

- IT and Networks
  - Public services
  - Enterprise services
- Security and public safety
  - Surveillance
  - Equipment monitoring
  - Tracking
  - Public infrastructure
  - Emergency services
- Transportation
  - Smart vehicles
  - Transportation systems

  - Parking services
  - Emission control
- Industrial
  - Resource automation
  - Distribution of resources
  - Industrial processes
- Healthcare & Life sciences
  - Home monitoring systems
- Smart environment
  - Energy efficiency
  - Resource management
  - Environmental protection
- Smart Living
  - Home quality of life
  - Individual health and safety
- Smart Governance
  - Citizen participation in decision making procedures

Table 1: The perspectives for the development of Smart Cities [9].

	Future Internet Research	**Cities and Urban Development**	**User-Driven Innovation Ecosystems**
Actors	- Researchers - ICT companies - National and EU actors	- City policy actors - Citizen platforms - Business associations	- Living Lab managers, citizens, governments, enterprises, researchers as co-creators
Priorities	- Future Internet technical challenges (e.g. routing, scaling, mobility)	- Urban development - Essential infrastructures - Business creation	- User-driven open innovation - Engagement of citizens
Resources	- Experimental facilities - Pilot environments - Technologies	- Urban policy framework - Organizational assets - Development plans	- Living lab facilities: methodologies & tools, physical infrastructures
Policies	- Creation of advanced testbed facilities - Federated cooperation - Experimental research	- City policies to stimulate innovation, business and urban development Innovative procurement	- User-driven innovation projects - Open, collaborative innovation

1.2 Deliverable structure and scope

The main scope of this report is to define the RERUM smart city applications and identify the possible threats and risk in terms of security and privacy issues. In this context, Section 1 includes a thorough review of the state of the art with respect to smart cities use-cases, aiming to analyse recent research topics and the corresponding approaches that have been followed. Based on the state of the art analysis and the expected benefits of the RERUM stakeholders, Section 2 defines the use-cases considered in this project in terms of the stakeholders, their roles, the scope and expected benefits in each use-case. The key challenges, the key components, the main functionalities and operations are analysed as well. This analysis serves the main scope of this report, which is to identify the possible risks and threats for the envisioned RERUM use-cases. To this end, Section 3 presents the methodology for extracting the risk sources and the threats by considering confidentiality, integrity and availability of data for the RERUM use-cases. Furthermore, privacy threats are identified and examples illustrating the presented analysis are given. Then, Section 4 provides a solid link between the needs of the smart cities stakeholders (cities, citizens, stakeholders, etc.), the user requirements, the technical requirements of the RERUM system and the innovations that have to be developed. In this context, several smart-cities use case situations are identified along with the respective user requirements and the key issues (security, privacy, reliability, etc.) that have to be resolved in order to realize the smart cities concept. Then, the innovations that resolve these issues and will be developed within RERUM are briefly described. Finally, the exploitation plans and business models for each of these innovations are provided. The structure of the deliverable and the relation between the separate sections is depicted in Figure 1.

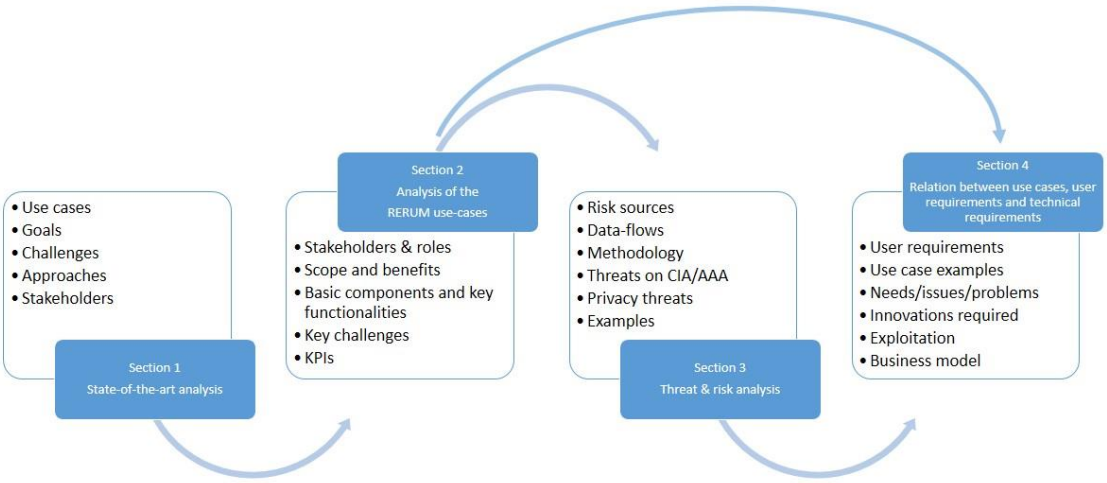

Figure 1: The structure of this report.

The main outputs of this deliverable (that reflects the work of RERUM Task2.1) will be used as input for defining the RERUM requirements and the smart object model, which will be detailed in the deliverable D2.2 (part of Task 2.2 and Task 2.3). These two deliverables will serve then as the basis for defining the system architecture in Task 2.4. Furthermore, D2.1 will provide Task 5.1 with the early definition of the use-cases in order to define the trial scenarios. These relationships are depicted in Figure 2.

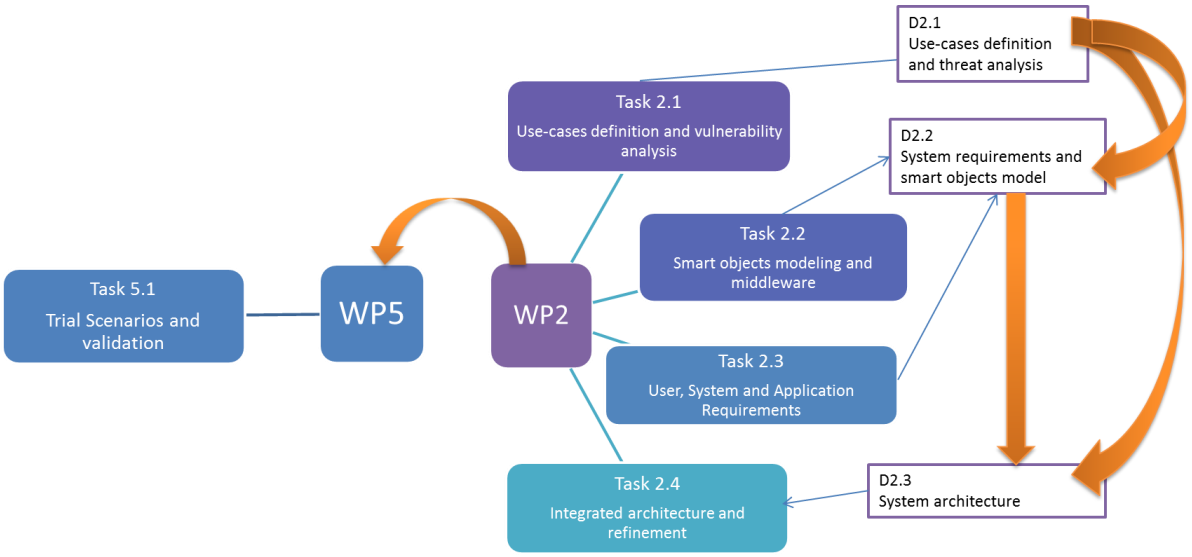

Figure 2: The relationship between D2.1 and other tasks/deliverables in RERUM.

1.3 State of the art and related work

The term Smart City goes back to the early '90s [11] when it was simply used to characterise the technological development of cities and their globalization. Nowadays, this term is associated with the IoT, where everyday things, people, data, and processes are readable, recognisable, locatable, and controllable via the Internet. The last three decades numerous research projects and other undertakings have been carried out towards developing and understanding the fundamental technologies and challenges for realising the concept of Smart Cities. As mentioned, the realization of the Smart City concept is tightly related to the IoT and hence the efforts are focusing on the latest advancements in wireless sensor networks, mobile and pervasive computing, middleware, and agent technologies. In what follows, the state of the art approaches for smart cities applications are reviewed and possible gaps with respect to the RERUM goals are identified.

1.3.1 Smart transportation (outdoor use-case, UC-O1)

Traditional road-fixed sensors are gradually combined or exchanged with cost efficient and flexible floating sensors, in the sense that vehicles are used as moving (floating) sensors that generate up-to-date information, known as "floating car data" [12]. The vehicles then can provide this information either to a service centre or to other vehicles using respectively V2I, V2V wireless networks, over 802.11p or cellular network infrastructures for example. Extensive use of such sensors is a challenge both in terms of connectivity and physical security, as well as in terms of traffic state estimation and prediction. Efficient and robust traffic state estimation relies on timely and accurate data, as well as on scalable traffic models and efficient data assimilation for temporal filtering and data fusion [10], [13], [14]. The literature reveals a variety of efforts to employ smart objects for traffic and environment monitoring. A comprehensive review of related issues and techniques is presented in [15].

A significant portion of research in this area has so far been using CDR (Call Detail Records) data intended for billing purposes in the operator's network (see for example [1] and the references therein). However, other kind of data from cellular subscribers are expected to become an important data source in the near future for extracting information such as travel time, traffic flow and the origin-destination (OD) matrix estimation [16]. Nevertheless, this gives rise to privacy issues due to the potential exposure of the users' usage of the cellular network.

Several European projects have dealt with smart transportation use-cases, following various approaches. Since the first trial to use cellular network data for road traffic estimation in the *CAPITAL* project [17], which could be considered as an early initiative for smart city applications, a lot of progress has been made. The *CAPITAL* project was not entirely successful due to inefficient location accuracy; however, since then, the available data volume with the advent of IoT has exploded and the methods to process them have dramatically been improved. Such available cellular networks related to road traffic estimation are described in detail for example in [19] and [18]. As of today, numerous projects have shown positive results and indicate a large potential for these data sources (see for example [20]).

CIVITAS [21] is an initiative for sustainable, clean, and energy efficient urban transport systems. The purpose was to approach the goal by implementing and evaluating certain couplings of technology and policies. To date, there have been three rounds of *CIVITAS* projects, I, II, and Plus. *CIVITAS I* (2002-6) having involved a total of 19 cities.

Among the broad set of European cooperative vehicular research activities, the FP7 *iTETRIS* project aimed at analysing the potential of cooperative vehicular technologies to improve road traffic management through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication and cooperative traffic management policies [22]. iTETRIS implemented an open-source simulation platform that integrates wireless communications and road traffic. *iTETRIS* is based on an architecture aligned with the communication architecture defined by ETSI for Intelligent Transport Systems (ITS). The project's central output was an open and flexible simulation platform, based on the open source SUMO and ns-3 simulators that enable large-scale traffic scenarios using the city of Bologna as a test- bed.

CARBOTRAF [23] aims to create an ITS handbook for improved, real-time urban traffic management, involving sensors to measure CO_2 emissions and guidelines on how to handle traffic to reduce them. The test sites at Glasgow and Gratz were equipped with a sufficient number of traffic sensors, such as loop counters at intersections and additional traffic counters on the main arterials. Additional "smart eye" sensors, i.e. a bio-inspired optical input based counting sensor, are expected to be installed mainly to collect data on the vehicle fleet composition. Within the project, the effects of distributing traffic amongst a set of alternative routes is expected to have a significant impact. A key question is the magnitude of the achievable effect of "soft" actions such as information provision in combination with "hard" actions such as managing traffic lights.

STREETLIFE [24] will develop an urban Mobility Information System (MIS) to provide mobile information services to end users for sustainable transport alternatives. It also aims at addressing ICT solutions to control the mobility resources and policies for traffic managers and city administrations. A variety of information sources will be integrated in the *STREETLIFE* Mobility Information System for this purpose: large amount of real-time data will be taken from transport planning, traffic management, and connected cars (crowdsourcing). Therefore, intelligent data processing and fusion methods will be employed. The MIS goal is to provide citizens with up-to-date information regarding the best available travel route and combinations of transport means. The MIS will be implemented in three pilot sites, Berlin (Germany), Tampere (Finland), and the town of Rovereto (Italy). The significantly different sizes and cultural characteristics of each site from the rest are expected to reflect in the trial outcomes.

MYWAY [25] will similarly develop a platform, called the "European Smart Mobility Resource Manager", which will facilitate a holistic view of sustainable mobility. The aim is to combine available transport services and their usage by travellers into a seamless point-to-point mobility service. *MYWAY* further targets to provide travel suggestions optimized to the users' preferences. *MYWAY* will be tested in three 'living labs' in Barcelona, Berlin, and Trikala. *MYWAY* is expected to boost the travellers' usage of greener mobility services by stimulating users to switch to more sustainable mobility choices and behaviours.

MOVESMART also aims at time-dependent route planning and personal mobility services using a set of crowdsourcing tools for collecting real-time information by a wide range of travellers. The core of *MOVESMART* is a hierarchical urban-traffic infrastructure that is hosted on a cloud architecture. *MOVESMART* is based on an urban traffic knowledge base (UTKB), enabled by live-traffic logging and the centralized generation of time-dependent city traffic metadata. This data is kept and used to enable fast rapid route planning. The traffic reports are securely and anonymously gathered directly by the travellers via simple portable navigation devices and/or smartphone application interfaces. The traffic-reporting is conducted via a crowd-sourcing service, which allows the live (in-route / emergency) reports as well as post-route assessments of travellers for the recommended route plans.

Besides the European initiatives, *Mobile Millennium* [26] was a research project that included a pilot traffic-monitoring system using GPS receivers on cellular phones to gather traffic information, process, and distribute traffic information results back to the cell phones in real time. A public-private research partnership between UC Berkeley, the Nokia Research Centre, and *NAVTEQ*, with sponsorship from the California Department of Transportation— launched a pilot program on 2008 for 12 months. During that time more than 5,000 users downloaded the *Mobile Millennium* traffic software onto their phones.

The *Mobile Millennium* traffic-monitoring system is still operational at UC Berkeley and integrates numerous feeds into traffic models, which broadcast highway and arterial traffic information in real-time. The feeds include data obtained from GPS-enabled mobile phones, and all of San Francisco's taxis (through GPS), plus radar, loop detectors, and historical databases.

The team integrated a high level of privacy that separated position data from information about individual phone users. These included collecting the data using "virtual trip lines" —data collection points that yield only traffic information and do not detect a user's personal information— and transmitting the data using strong encryption.

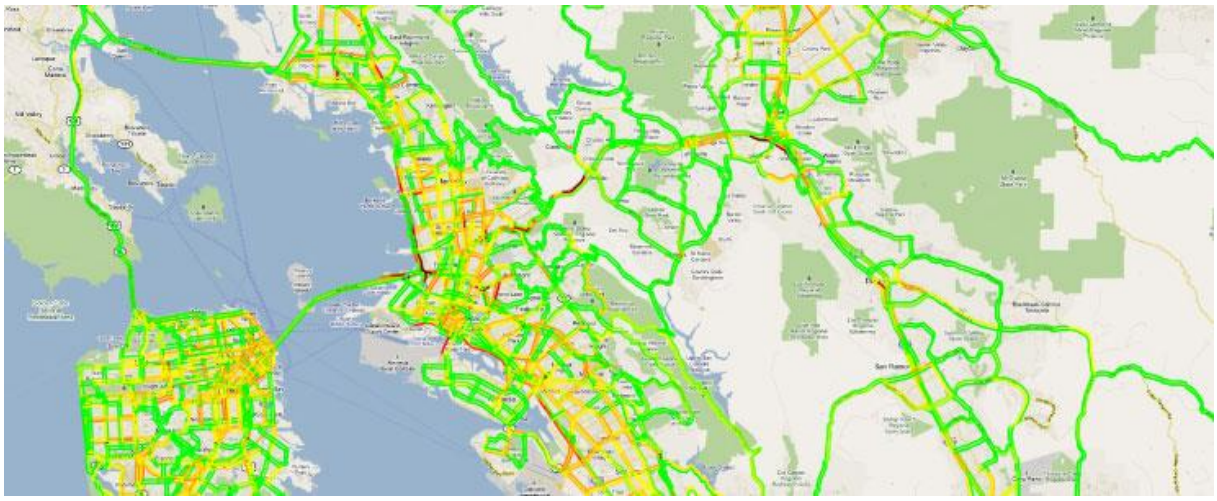

Figure 3: Snapshot of *Mobile Millennium* Traffic in San Francisco and the Bay Area [25].

The *Mobile Millennium* Stockholm project [27] was initiated by the Swedish Transport Administration to leverage on the Mobile Millennium project for a timely traffic information system in Sweden. The purpose of the project was to build upon the previous knowledge and develop new methods for data fusion. The data fusion methods utilize each data source available to improve estimations and predictions of the traffic state. The project was a collaboration between the Swedish organizations Linköping University, the Royal Institute of Technology, Sweco Infrastructure, and UC Berkeley in the United States.

The RERUM approach: Security and reliability in existing traffic management systems is mostly based on conventional security algorithms, with a strong focus on anonymisation of collected data, which are usually collected and retained over prolonged periods of time. Existing systems allow also long term data collection of individual traffic users. In RERUM, a different approach is required to support the concept of security and privacy by design. The idea is to obtain and retain data only when needed based on the real requirements of each application. Furthermore, RERUM aims to ensure the reliable operation of the system, the trustworthy exchange of information between the smart objects and the foreseen smart city applications. RERUM also aims to preserve the privacy and non-disclosure of the traveller trip data and patterns (i.e. a pattern trips may expose the habits or health issues a user may have), and avoid attacks, such as passive listening, data falsification, etc. Finally, RERUM will utilize opportunistic networking to enable the timely collection of data.

1.3.2 Environmental monitoring (outdoor use-case, UC-O2)

The industrialization of first world countries resulted in severe environmental issues that are more evident in big cities, where the population is denser and the industrial activities are more intense.

In the last decades, the relationship between the climate change and the pollution problems in cities highlighted the need for stricter environmental policies and more efficient environmental monitoring, as well as for better resource management towards facing these problems. In this context, the cities of the future must use the technology and their resources to enforce environmental protection policies. To this end, different initiatives, both private and under EU-funded projects, aim to utilize existing technologies for environmental monitoring and control in the cities.

The *CITIZENSENSE* project [28] is an ERC project which intends to engage citizens on using wireless sensors to monitor environmental parameters using different practices and devices, such as mobile phones and networked devices. This project aims to “democratise” the environmental monitoring use-case, giving an important role to the citizen, which is traditionally handled by the city’s municipalities. Three use-cases are considered: “wild sensing” (i.e., tracking of flora and fauna), “pollution sensing” (i.e., monitoring air and water contamination), and “urban sensing” (i.e., noise monitoring for more sustainable and efficient cities). The project, besides the benefits from involving the citizens into new environmental policies, also engages politicians to take part and use this information to improve the quality of life in cities.

The *TWISNet* project [29] aimed to support and secure the integration of sensor networks into large-scale industrial environments, such as defense, public security, energy management, traffic control, and health care. A number of use-cases, from nuclear plant facilities to energy supply and management, were identified and supported. In those use-cases, user's privacy, node authentication or data reliability appear to be the most important security requirements. This project resulted in the creation of a platform for commanding and controlling sensor networks in a secure and trusted way. By integrating commercial off-the-shelf or pre-standard devices, that platform served as a mediation layer between the sensor network and industrial applications. Empowered with security architecture to address the major security requirements (e.g. user's privacy, data confidentiality, reliability), that platform was validated based on the identified use-cases. Finally, the scientific and technical outcome of TWISNet was its contribution to standards, such as IETF 6lowpan.

EVERYAWARE [30] intended to conceptualize a new approach regarding the environmental monitoring that directly involved citizens through the social networks. The project aimed to integrate all crucial phases (environmental monitoring, awareness enhancement, and behavioral change) in the management of the environment into a unified framework (Figure 4). A new platform was created relying on Internet-connected smart phones, combining sensing technologies, networking applications and data-processing tools. The scalability of the platform was tested, involving as many citizens as possible, leveraging on the low cost and high usability of the sensing devices. The

integration of participatory sensing with the monitoring of subjective opinions was also novel and crucial, exposing the mechanisms by which the local perception of an environmental issue, corroborated by quantitative data, evolves into socially-shared opinions, eventually driving behavioral changes.

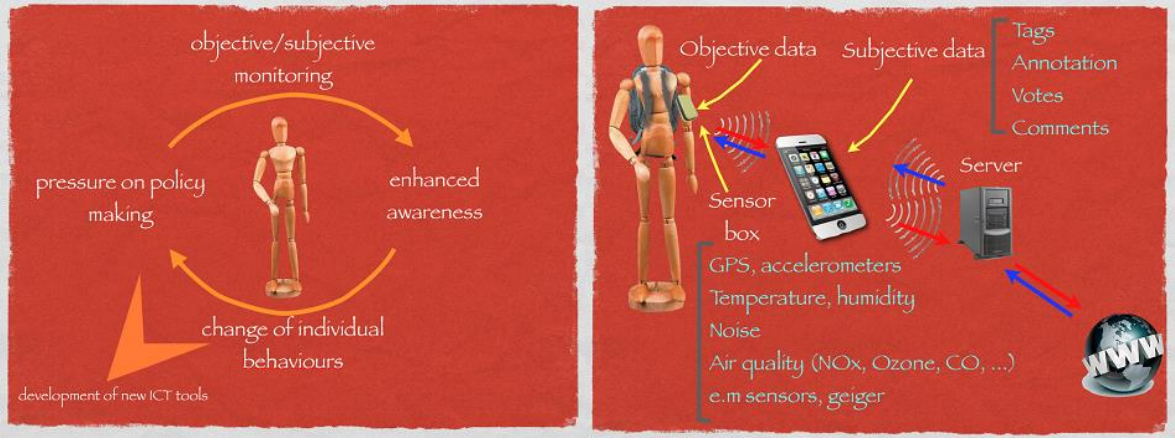

Figure 4: EVERYAWARE concept and platform.

SAFECITY [31] dealt with smart public safety and security in cities. The main objective was to enhance the role of Future of Internet in ensuring people feel safe in their surroundings at time that their surroundings are protected. Most of the use-cases were focused on security on the streets but the use-cases deployed in Athens included also a road accident involving burning of chemicals.

The goal of *ENVIRONMENTOR* project [32] is the development of a network of experts and consultants towards assisting companies and authorities with the *Integrated Pollution Prevention and Control Directive (IPPC)* directive. IPPC provides rules about the emissions of large industries in the EU. *ENVIRONMENTOR* focuses on large emission sources within the plastic and chemical industries deploying Environmental Management Systems (EMS) and Emission Trading Scheme (ETS). It offers a web-based environmental consultancy toolkit (utilizing artificial intelligence techniques) to the participating end-user SMEs in order to help them in their daily activities.

The project *DIADEM* [33] focused on the environmental management in industrial scenarios, namely creating a seamless and efficient platform to integrate: (i) robust and efficient gas monitoring systems, and (ii) advanced decision support/planning systems, facilitating a rapid high-quality and information based decision making. The goal is to contribute to: (i) safer and healthier environment in industrialized areas, contemplating the mitigation of consequences of catastrophic chemical incidents, through quick and reliable gas detection, monitoring and decision-making processes, (ii) the prevention of catastrophic chemical incidents and reduction of chemical pollution, through planning based on collaboration of many experts and efficient use of advanced tools, and (iii) the prevention of chemical air pollution in industrial areas.

The *SEMSORGRID4ENV* [34] project intended to be another step towards the future of the environmental monitoring, using sensor networks to get real data and support them with tools to make decisions. The project addressed two major challenges: (i) the development of an integrated information network where new sensor networks can be easily discovered and integrated, and (ii) the rapid development of flexible and user-centric environmental decision support systems using data from multiple, autonomous, independently deployed sensor networks and other applications. This was achieved by enabling: (i), a semantically-consistent view of several heterogeneous sensor networks as a global data-resource Grid, (ii) a rapid development of Grid services that combine real-world real-time data, coming from autonomous, heterogeneous sensors networks, with legacy historical data, and (iii) a rapid development of open, flexible, contextual knowledge-based thin applications (e.g., mash-ups) for environmental management. Two environmental monitoring and management use-cases were used to test and demonstrate project's results.

Besides the initiatives from collaborative research projects, there are also some privately funded projects targeting the environmental monitoring; however, none of them addresses the issues related to security, privacy, reliability, etc. Actually, professional noise meters or air quality analysers already exist in the environmental monitoring market and are used for that purpose. However, they are very expensive and high energy consuming. This is more or less the same situation with current weather stations.

Different DIY (Do It Yourself) projects like *AirQuality* Egg [35] and *Pollux'NZ* [36] arose recently to make this kind of measurement something more "democratic" but the minimum quality of such measures is not guaranteed.

MyAirBase [37] project also adds a social perspective to that kind of measures, allowing the user to connect with other users and share data, alarms and historic data through social networks; but the data are not analyzed, correlated or corroborated, which might create false alarms when the information is shared and spread on the social platform. On the other side, *RERUM* raw data will have better accuracy than those of *MyAirBase*. They will be securely transported and will never be delivered to third parties or the citizens without pre-processing and corroboration by the city council.

There is also another area of solutions built upon cellular mobile phones using already embedded sensors (such as microphones or acceleration sensing elements) or adding external sensors to them. Mobile applications gather the information and send it into the cloud using 3G cellular data. In this area we can find the *NoiseTube* project [38] in London, *Air Casting* [39] which has also a DIY part on the sensors side, and the *SensPod* from Sensaris [40].

Finally, there are other types of projects that are not as private as the previous ones but are driven by city councils as self-funded internal projects. This is the case, for instance, of the project *OPENSENSE* that focuses on controlling and reducing the pollution in the downtown of London and Zurich [41]. This is an interesting project since it intends to be an open platform to analyse this type of data that are collected by sensors installed on a public transportation network covering large areas with a minimum investment.

The *RERUM* approach: Despite the fact that several projects have been or are currently addressing the environmental monitoring problem, *RERUM* is the only project with a key focus on the security, privacy, reliability, and robustness of the communications on the sensor networks' side. The past projects focused mainly on the application layer (*ENVIRONMENTOR*, *DIADEM*, *SAFECITY*), the citizen involvement (*CITIZENSENSE,* EVERYAWARE), and the data and decision taking platform. Even *SEMSORGRID4ENV* and *TWISNet* that share similar goals with *RERUM* in terms of data privacy, confidentiality and reliability, intend to realize them on the application platform, instead of following a device-driven approach. Furthermore, *RERUM* follows an IoT based approach for implementing an environmental monitoring use-case. The RERUM project will also try to combine low-cost and low-power solutions, while trying to maintain high measurement accuracy and enable security into the communication stack of the wireless SO.

1.3.3 Home energy management (indoor use-case, UC-I1)

Home Energy Management Systems (HEMS) or Building Energy Management Systems (BEMS) are two of the most frequent cases considered in Smart Cities deployments. The European Union (EU) is particularly interested in HEMS and BEMS, as a part of the wider fight against climate change and the objective of reducing the energy consumption by 20%, which is one of the five targets of the Europe 2020 strategy for smart, sustainable and inclusive growth [42]. To this end, several projects have been funded by the EU, focusing on the deployment of ICT architectures for HEMS and BEMS and the corresponding software, middleware and hardware, as well as on security aspects.

The EU project *3eHouses* [43] deals with the integration of the most established ICT technologies in social housing in order to provide services for energy efficiency, real time monitoring of the energy consumption, integration of renewable energies and lower the energy consumption. The 3eHouses project investigates the spatial and temporal dependency of the instantaneous energy solution which highlights the need for a dense local network of sensors and actuators connected to a global communication network of remote and distributed data sources. The underlying ICT infrastructure and the HEMS architecture is depicted in Figure 5 [43].

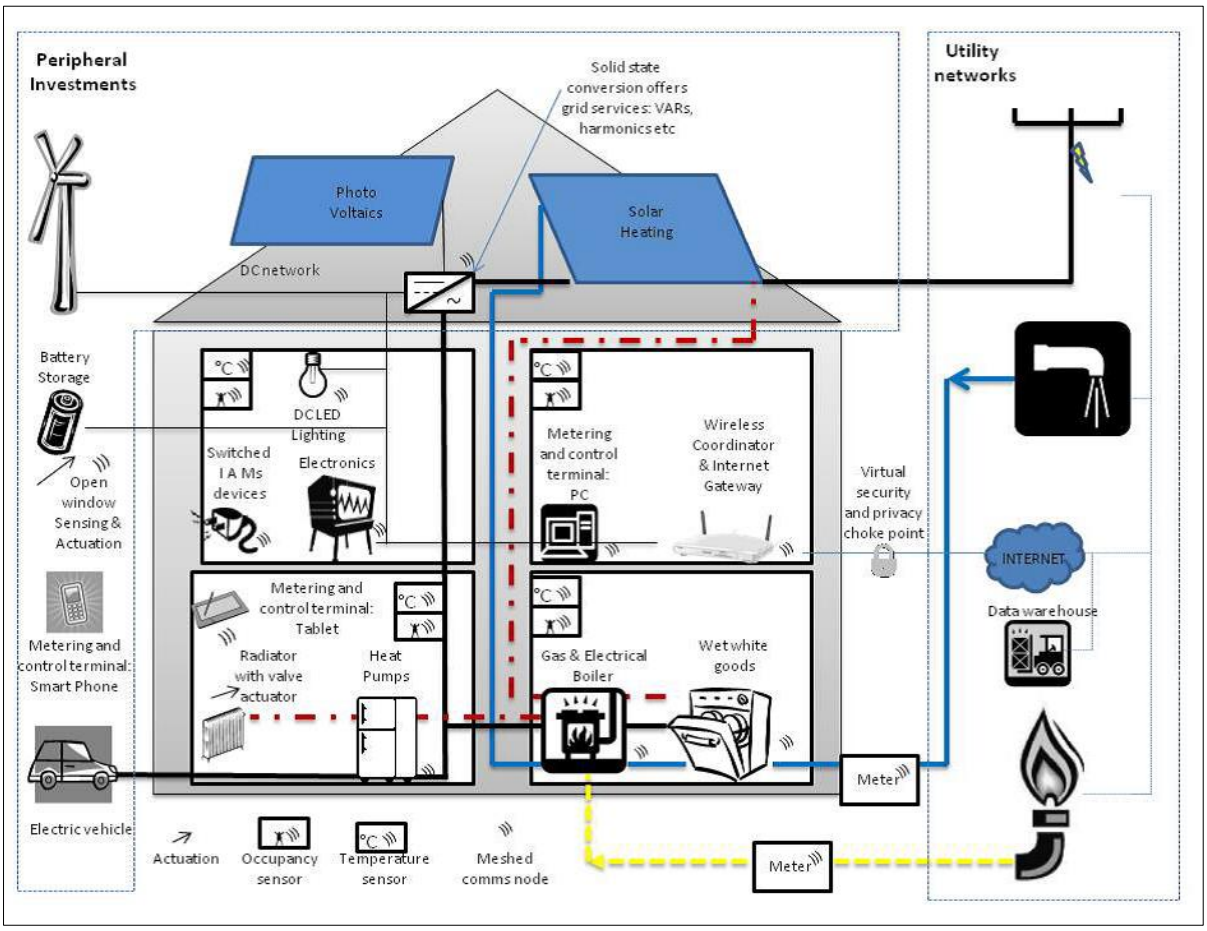

Figure 5: The architecture for the HEMS use-case proposed by [43].

The *Digital Environmental Home Energy Management System (DEHEMS)* project investigated how ICT can be used to improve domestic energy efficiency and hence reduce CO_2 emissions. Furthermore, this project proposed solutions for households to reduce their energy usage through better management and analysis of their energy consumption [44]. A model for measuring and analysing energy consumption was developed in order to classify data into utilization patterns which can be further exploited for the energy reduction. Furthermore, DEHEMS focuses on creating new policies in carbon allowances and supporting the increased localised generation and distribution of energy.

The *Active Distribution networks with full integration of Demand and distributed energy RESourceS* (*ADDRESS*) project [45] aims to convert the "passive" consumers into "active demands" consumers by installing the so-called *ADDRESS* Energy Box (EB) in homes. The goal is to manage the main home loads, such as the air conditioner or other appliances, based on the optimal combination of user preferences and reward-based requests to modify energy consumption and optimally fulfil the consumer requirements (comfort, load scheduling and money savings) as well as the electricity

market requirements (Figure 6). These EBs were installed in 400 homes for contacting trials and tests, with each EB being connected with 5-10 existing loads of different types through smart sensors, which convert a conventional appliance to a smart one. Similar approaches for balancing the energy generation-consumption demands through smart sensors on home appliances were followed by the EU projects *PEBBLE* [46] and *SmartCoDe* [47].

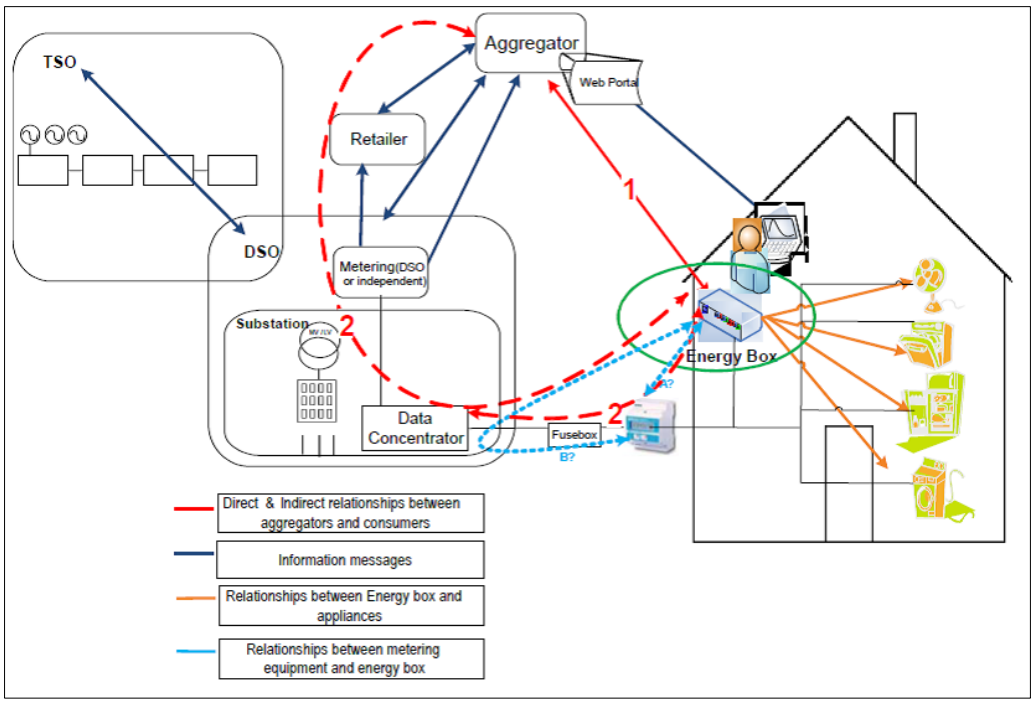

Figure 6: Relation between the ADDRESS EBs and the home equipment [45].

The security and the reliability of the HEMS/BEMS is a crucial aspect that has to be taken into consideration. Besides the conventional security methods such as Secure Sockets Layers (SSL) and IPsec, in [48] an Information Centric Networking (ICN) approach was followed, where the core idea is to allow applications to ask for data in a content-centric manner regardless of the data's physical location. In this sense, the security of data relies on the data itself which upon creation is signed (for integrity and authenticity) and encrypted (for confidentiality). The architecture for this ICN-based concept involves the home devices (e.g., power sensors and thermostats), a Directory Service (DS) and a Group Controller (GC) (Figure 7). In short, a device can publicise its own data and can discover the data to which it wants to subscribe via the DS, which creates a database of data based on names. The GC controls data by only issuing group keys to authorised devices for data encryption/decryption according to the security policy. The DS and GC may run in a dedicated server or simply in one of the devices accessible on the network [48].

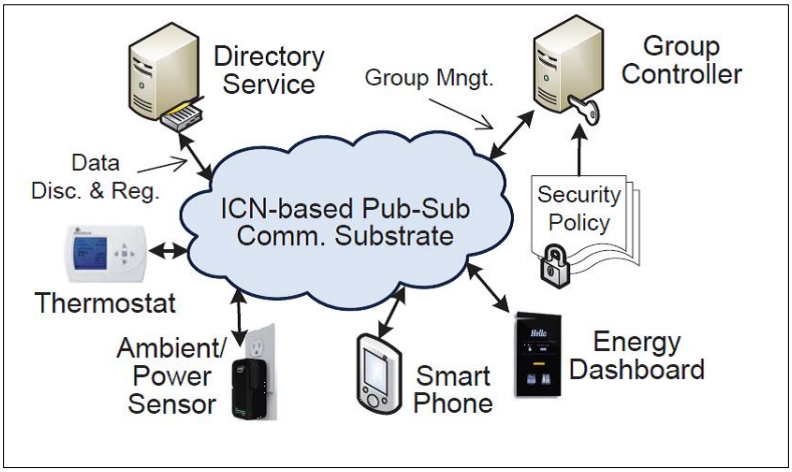

Figure 7: The ICN-based security architecture for HEMS [48].

In [49] a Privacy enabled Home Energy Management System (PeHEMS) was introduced, which is a home energy management system, prototype, and load balancing algorithm in order to protect electrical metering privacy. Two crucial security issues related to service provision are discussed in [50], i.e. the establishment of a secure communication procedure among the electric utility, consumers, and service providers and the privacy-preserving yet accountable authentication framework among the smart grid entities without relying on any trusted third party. The proposed approach for facing these issues is based on the Boneh's group signature scheme (Figure 8) and involves three kinds of entities: electric utility, service providers, and consumers organised in groups.

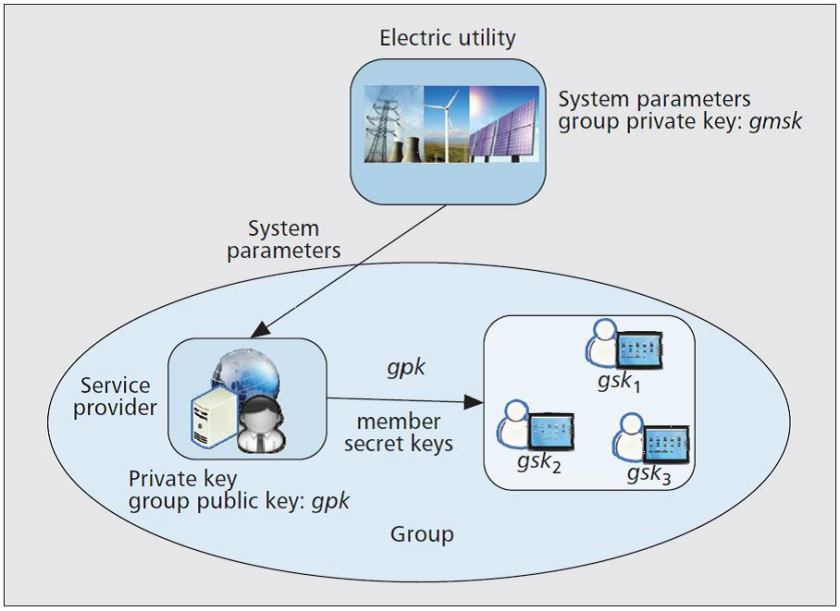

Figure 8: The BONEH's group signature scheme [50].

The RERUM approach: The security and reliability of existing energy management systems is based on conventional security protocols and algorithms i.e. standard encryption. This approach entails several limitations since the existing security schemes cannot always adapt to the specific needs, requirements, and characteristics of each application. For example, some data encryption algorithms may be too computationally intensive for low-complexity low-power consumption sensors or they may produce too many overhead bits with respect to the actual information. In this sense, a different

approach is required, which will develop lightweight algorithms by design, based on the real requirements of each application and use-case. RERUM primarily aims to ensure the reliable operation of the system and the trustworthy exchange of information between the smart objects, and the foreseen smart city applications. Furthermore, this project will develop those mechanisms for preserving the privacy and non-disclosure of the end-user data and patterns (i.e. a pattern in lights could show the hours that a user is absent, which may be used by burglars), supporting the "always connected" nature of the indoor smart objects. Another important goal is to secure the network and avoid attacks, such as jamming, passive listening, data falsification, etc. and enable the automatic secure configuration of smart objects and avoid network failures.

1.3.4 Comfort quality analysis (indoor use-case, UC-I2)

Although indoor comfort quality is something important for most people, there are few projects or products targeting this in a concrete way, apart from the relationship between the in-home comfort and the home energy management use-case discussed in the previous chapter.

The *Integrated Air Quality Sensor for Energy Efficient Environment Control* (*INTASENSE*) project [52] aims to improve quality of life and productivity of EU citizens by providing a comprehensive indoor air monitoring system. The main focus of the project is the development of a novel detector that will be able to detect key indoor pollutants such as, carbon monoxide, carbon dioxide, nitrogen dioxide, ozone, benzene, formaldehyde, and particulates (PM_{10} and $PM_{2.5}$). *INTASENSE* utilizes a wireless sensor network for the transmission of measurements to the building's climate control centre.

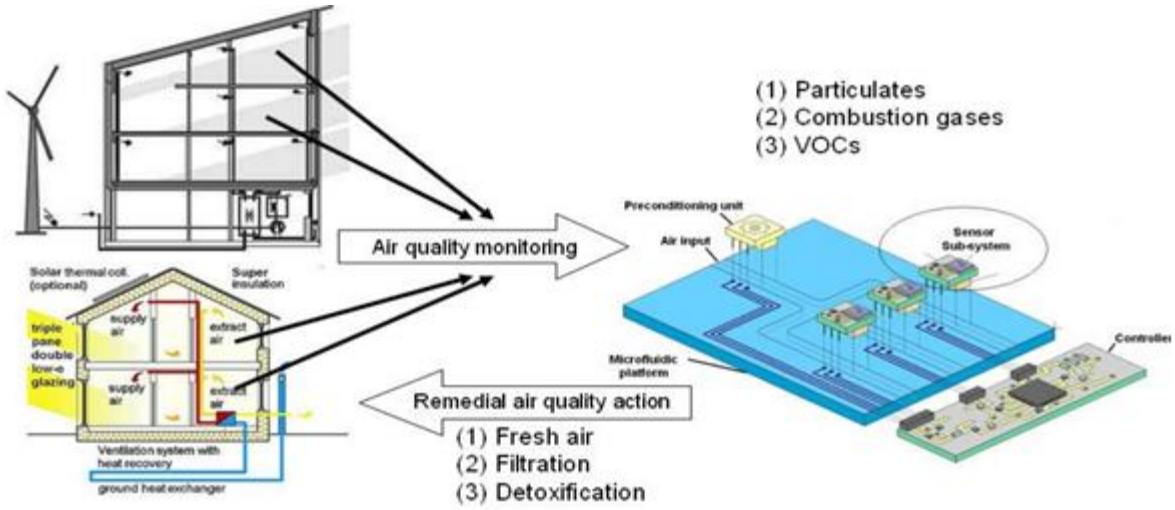

Figure 9: INTASENSE indoor air quality monitoring architecture.

The *Cost-Effective Tools for Better Indoor Environment in Retrofitted Energy Efficient Building* (CETIEB) project [53] aims to develop monitoring and control systems, as well as simulation models for indoor environments. The main motivation for the project is the indoor environment deterioration when retrofitting existing buildings. The retrofitting process usually leads to more airtight buildings and thus significantly affects the indoor air quality and environment. Within CETIEB the collaboration of cost-effective wireless or wired sensor systems that are able to detect a variety of indoor environmental factors, with active ventilation systems is of crucial importance. Furthermore, bio-filters and nano-functional materials for the recycling of indoor air and the removal of pollutants and pathogenic microorganisms will be used along with simulation models that assess the thermal and health conditions of buildings. Figure 10 and Figure 11 present a *CETIEB* use-case and the system's architecture respectively.

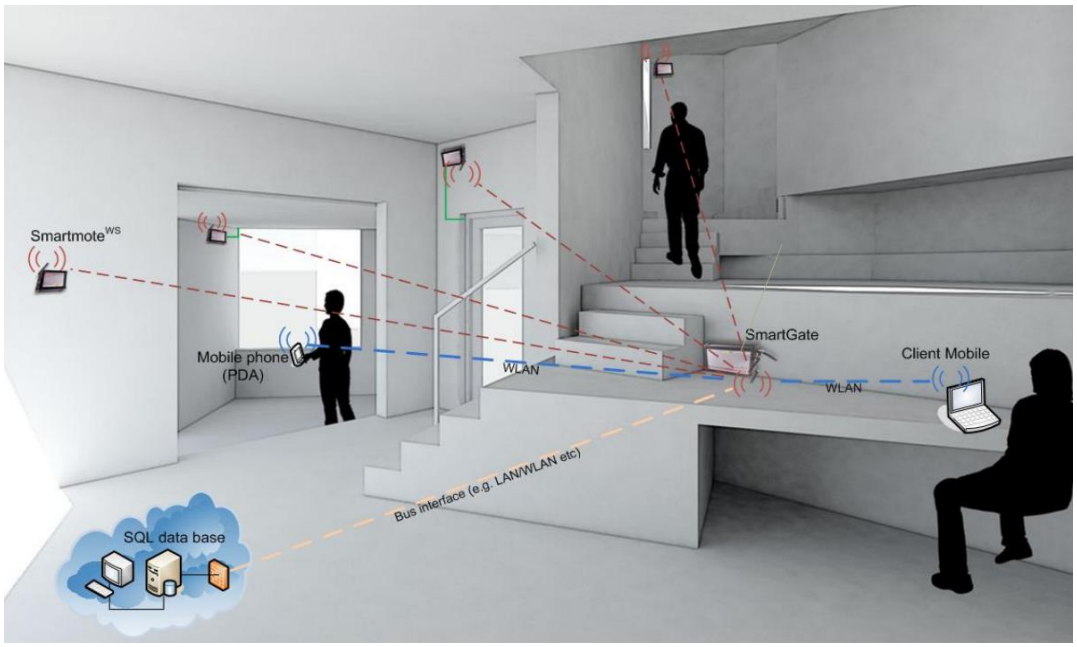

Figure 10: CETIEB wireless sensor network use-case.

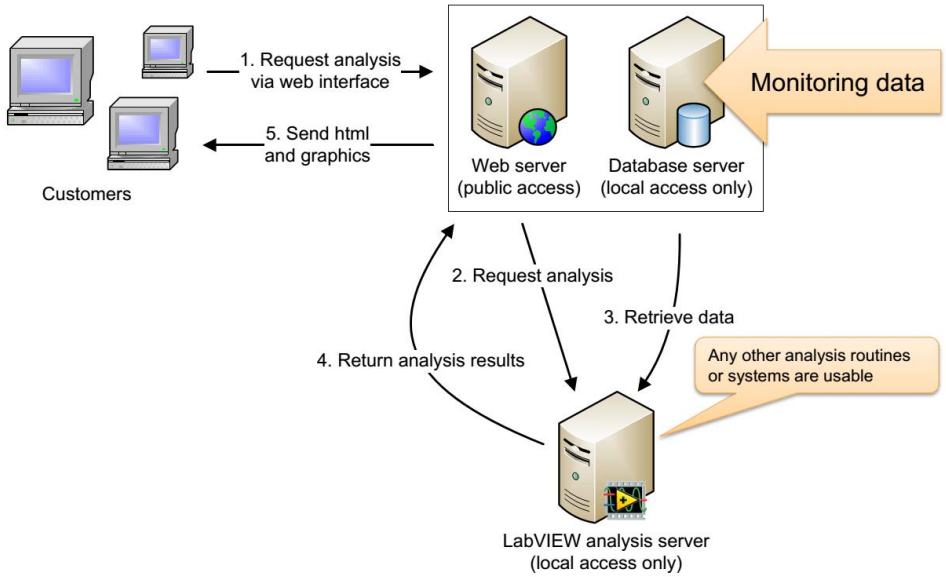

Figure 11: CETIEB architecture.

The purpose of the *Smart Monitoring of Historic Structures* (*SMooHS*) project [54] was to monitor important factors related to historic building deterioration such as temperature, humidity, air velocity, strain and crack opening, acoustic emissions, vibration, ambient or UV light levels and chemical attacks and provide recommendations for actions based on smart data processing and material deterioration models. Within *SMooHS* a smart monitoring system was developed using wireless networks of robust sensors for minimally invasive installation at historic buildings. The architecture of the wireless network is the same with the architecture presented in Figure 11 for project *CETIEB*. Furthermore, *SMooHS* placed great emphasis on the sensitivity, reliability, robustness and integration of wireless sensor motes and the development of user-friendly, modular and open source software to address specific problems and steer various combinations of sensors. Figure 12 presents the indoor placement of nodes at the Museum Island in Berlin.

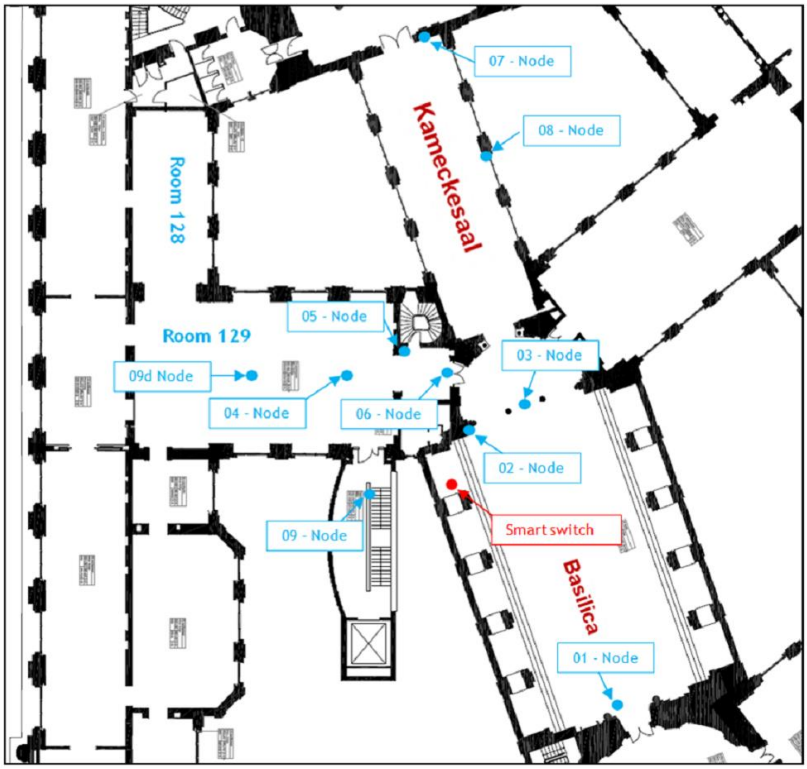

Figure 12: SMooHS Indoor placement of wireless sensors at the Museum Island in Berlin.

TIBUCON project [54] aimed to develop a self-powered wireless sensor network to monitor buildings' thermal conditions. Although the project's main objective is to improve, energy-wise, the use of building's heating, ventilation and air conditioning systems, temperature monitoring is directly related to indoor comfort quality monitoring and thus related to RERUM's comfort quality monitoring use-case. The project proposed the use of Self Powered Multi Magnitude Wireless Sensor Networks that completely avoid use of cables and removable batteries by combining energy efficient wireless communication technology, ultra-low power electronics and power harvesting. The strict requirements related to energy efficiency and autonomy of the power harvesting wireless sensors lead to the development of a custom MAC layer, based on LL-MAC protocol, on top of 802.15.4 in order to address the deficiencies in existing protocols such ZigBee, Wibree and Wireless Hart.

Another project relative to the indoor comfort quality use-case, as considered within RERUM, is the European project *Ambient Assisted Living initiative* (*AAL*) [51]. Nevertheless, this project focuses on the assistance for elder people and comfort is only considered as the automation of specific processes or the remote control of devices.

Domotics (a neologism to define home automation systems) have had a big hype of expectations at the beginning of this millennium, but unfortunately not a big success in the market, so far. Most of the applications of domotics could be related to indoor comfort and, so, included as SOTA although they are mostly unused nowadays and is currently rather difficult to find houses with this kind of technology installed. Indeed, nowadays domotics are mainly found in hotels, office buildings, luxury vehicles like private planes, etc.

Recently, several products have been released for wireless sensing for comfort quality in a kind of IoT approach, such as the *Nest* [56], recently acquired by Google Inc., *Netatmo* [57], *Sensorist* [58]. Nest is a smart thermostat that learns the patterns of its users and is able to control the heating/cooling of the house according to the schedule of the users. *Netatmo* is a system that can be controlled by a mobile phone and includes a thermostat and a weather station, measuring various parameters of indoor comfort quality. *Sensorist* is a system that uses smart sensors custom designed and user friendly for sensing the comfort quality at homes. The sensors send measurements for temperature

and humidity every 15 minutes to a gateway, which then passes the measurements to an external server, which provides the measurements to the end user.

In contrast to the commercial products, several DIY (Do It Yourself) projects can be found in the web letting the citizens build their own home automation applications, including sensors and devices targeting the comfort at home. Some examples can be found in [59].

Finally, there are some technological research entities, such as SICS [60], Fraunhofer [61], Smart-Homes Technological Center [62] that are also working on internal research projects about indoor comfort quality monitoring and analysis. So, likely, in the future we could see some of this research transferred to the industry as new products for indoor comfort analysis.

The RERUM approach: Considering the comfort quality use-cases as it seen from the RERUM point of view, the private initiatives are still in a very early stage. Most of the existing use-case implementations or products are utilizing external servers to store the data. Almost none takes into consideration the potential security and privacy issues or only conventional cryptography and/or proprietary protocols are utilized, which may not be the right approach for an IoT oriented use-case. RERUM aims to go much deeper into limiting the type of data that are being sent to external servers so that they could not be linked to users' private information. Furthermore, the project will ensure the reliability of the data that the sensors are gathering, minimizing the possibility of false alarms or for misdetections of potentially hazardous situations.

2 Use-cases

This section discusses the details of the Use-Case (UC) scenarios for the realization of the Smart City applications, which will serve as the basis for the RERUM system development. The definition of the use-cases includes the actors, stakeholders, the key challenges, the physical entities and smart objects, the data that will be sensed, and the actions that will be performed by the objects. The RERUM UCs involve two outdoor UCs for smart transportation (UC-O1) and environmental monitoring (UC-O2), as well as two indoor UCs for home energy management (UC-I1) and comfort quality monitoring (UC-I2). The selection of the use-cases was based on the analysis of the existing smart city use-cases and the expected benefits of the key stakeholders involved in the RERUM project with respect to those applications. The stakeholders are grouped into three main categories: (i) the public stakeholders, i.e., national and municipal agencies and organizations, and in general all public interest groups, (ii) the commercial stakeholders, i.e., companies that have direct interest in smart cities business, and (iii) the private stakeholders, i.e., citizens and commercial stakeholders' clients. More details about the players that are involved in each category can be found in Table 2.

Table 2: Smart cities applications stakeholders.

Public stakeholders	Public sector organizations and service providers, e.g., schools, universities, libraries, municipalities, public transportation, hospitals and health care providers. These public interest groups may be the key facilitators of smart city applications and they can either give incentives to commercial groups to develop applications or set regulations for better controlling the deployment of applications and the handling of user data gathered by the applications.
Commercial stakeholders	- Vendors: manufactures and suppliers of devices (e.g. sensing elements, smart objects, gateways); companies for installation of equipment, maintenance and support. - Network (telecom) providers: they provide the backbone network for the interconnection between devices, applications and users. In some use-cases, gateways send collected data to a centralized data sink. Depending on the technology adopted for this communication, the network provider can be either a (i) home broadband provider (DSL, cable, metro-ethernet, fibre optic broadband), (ii) a mobile broadband provider (3G, 4G, etc.), or (iii) a fixed network operator providing connectivity to the devices that are deployed within the city area. - Service and solution providers: companies that aim to provide smart cities services (e.g., smart home, smart traffic, smart waste management). - Software companies and developers: The developers of the software running on smart objects and gateways, as well as the developers of the applications that will utilize the RERUM system. This category includes developers implementing an application that takes advantage of RERUM's security- and privacy-enhancing mechanisms and the developers of the underlying operating system for SOs. - Utility companies: public or private companies that generate or distribute energy.
Private stakeholders	- Citizens and commercial stakeholders' clients. They are the end users of the smart city applications, including the users that are the owners of the premises where the installations are deployed. For indoor use-cases, ownership of the premises does not necessarily imply ownership of the installation, which may be offered as a managed service by a third party. For outdoor use-cases, end-users are citizens but also local authorities and public bodies including their staff. Lastly, for the traffic monitoring use-case, vehicle owners are also considered end-users.

The smart cities concept creates endless opportunities for new business, with important benefits for the stakeholders. The expected benefits for the stakeholders involved in the RERUM project use-case are summarized in Table 3 for the outdoor use-cases and in Table 4 for the indoor ones. These benefits are mostly related to (i) new business opportunities as seen by the commercial stakeholders' point of view, (ii) better resource management and offered public services for public sector stakeholders and (iii) improved quality of life and enhanced service experience for citizens and private clients.

Table 3: The expected benefits for the stakeholders involved in RERUM (outdoor use-cases).

	Outdoor use-cases	
Use-case / **Stake-holder**	Smart transportation (UC-O1)	Environmental monitoring (UC-O2)
ATOS (Service and solution providers)	-Evaluate new technics to improve decision making rules. -Improve available tools with new technics to infer new or modified rules on decision making functionality.	
SIEMENS (Service and solution providers)	- Define and develop new privacy-enhancing technologies that will enable the roll out of solutions to the smart transportation in cities.	- -
ZOLERTIA (Vendor / Software companies and developers)	- Get new knowledge on a market we have not entered so far. - Study the use-case with the intent to find a new killer app for this key use case that appears to be full of opportunities.	- Improve the measurement accuracy of solutions we have already implemented for this type of scenarios. - Introduce new (for our company) sensing elements to our portfolio for this type of scenarios. - Update the hardware technology we have been using for this type of scenarios.
CYTA Hellas (Telecom provider)	- Entry to new markets. - Network provider for new type of customers (e.g., transportation companies) - New services to customers and new products.	- Entry to new market. Network provider for new type of customers (e.g., municipalities that need network connectivity for environmental monitoring services)
TARRAGONA (Municipality)	- Improve available tools for strategic analysis: evaluate how sensor data may be used as feedback for Tarragona's Sustainable Urban Mobility Plan. - Evaluate how tactical decisions (traffic lights , …) affect urban mobility	- Availability of a richer environmental diagnostics of Tarragona by combining data from formerly isolated sensing systems - Study how to improve decision-making processes according their impact on the environment.

	- Geolocalized data exploitation. (bus stops, …) - Availability of a richer environmental diagnostics of Tarragona by combining data from formerly isolated sensing systems	- Evaluate the use of noise sensors to detect emissions over the permitted - Collect updated information on sensing systems operated both by Governmental bodies and other entities. Study possibilities for inter-operation and integrated management of such systems -"Real-time" environmental information. (focused on tourism and public health issues)
HERAKLION (Municipality)	- Improve the transportation system of Heraklion - Provide a near real-time traffic information system for the citizens - Exploit historical data for better city road planning - Improve the bus stop system	- Provide a visualized platform to inform the citizens about weather conditions in the city, as well as for information regarding health hazards - Exploit the environmental monitoring information to identify pollutant factors - Improve the quality of life of the citizens by better handling the environmental information and using it for influencing the decision making processes regarding construction works within the city

Table 4: The expected benefits for the stakeholders involved in RERUM (indoor use-cases).

	Indoor use-cases	
Use-case / **Stake-holder**	Home energy management (UC-I1)	Comfort quality (UC-I2)
ATOS (Service and solution providers)	-Study how new policies for privacy may affect real time scenarios. -Improve available tools to evaluate the use and feedback of sensors.	
SIEMENS (Service and solution providers)	- Define and develop new privacy-enhancing technologies that will enable the roll out of solutions to the smart home.	- Define and develop new privacy-enhancing technologies that will enable the roll out of solutions to the smart home.
ZOLERTIA (Vendor / Software companies and	- Utilize the use-case as a starting point for the creation of a new product targeting energy management at home. As a company we have already devoted some effort on this market and consider it to be	- Extend to an indoor scenario the knowledge we have on outdoor environmental monitoring, opening thus a new market for us. - Develop a new hardware platform

developers)	extremely interesting.	to implement such kind of applications.
CYTA Hellas (Telecom provider)	- New services to customers and new products (e.g., smart home services) - Added value to existing services - Entry to new market. Network provider for new type of customers (e.g., smart grid service providers)	- New services to customers and new products - Added value to existing services - Entry to new market. Network provider for new type of customers.
TARRAGONA (Municipality)	- Define indicators to be used in subsequent analyses of town council's facilities - Improve energy management. - Improve energy saving and efficiency (smart home/office services). - Detection of anomalies.	- Define indicators to be used in subsequent analyses of town council's facilities - Use indicators to manage appliances (air conditioning, heating systems, etc.). - Detection of anomalies.
HERAKLION (Municipality)	- Use the system for monitoring the energy consumption of public buildings and identifying the buildings and appliances that consume excessive energy. - Use the previous information to develop solutions for minimizing the energy consumption of those devices and decrease public spending - Promote the concept of energy efficiency to the citizens by giving direct access to the benefits of the system for public buildings and showing how much money the citizens can save using an intelligent energy management system	- Use the system for monitoring the comfort quality of public buildings/offices - Identify buildings/offices that may be hazardous for the health of public servants - Use the results to improve the working conditions of public servants - Combine this system with the home energy management to develop a building automation system that can improve the air quality of offices, while concurrently it saves energy

2.1 Smart transportation (outdoor use-case, UC-O1)

2.1.1 Introduction

There are currently over 400 Key Performance Indicators (KPI)s [63] on the urban transportation system, ranging from measurable ones, like availability and travel time, to intangible ones like community impact and passenger comfort. With the steep increase in vehicle numbers over the recent years, there is an increasing need for efficient Smart City traffic management, to avoid traffic jams and to optimize traffic flow. Traffic jams have significant impacts on fuel consumption due to the frequent starts and stops, as well as increased carbon emissions, while traffic control at intersections, is crucial to limit the risk of accidents. In this context, adaptive traffic management schemes, dependent on traffic conditions, are becoming a smart city necessity. To enable these, a means to estimate the traffic conditions on the city streets is required. Towards this end, this use-case is focused on secure and mainly privacy-preserving methods for collecting traffic data that can be utilized to perform traffic estimation on and an approximately real time (in a minute-long scale) for an intelligent transportation system.

Monitoring of the civic transport infrastructures, be they roads, parking spaces, and natural congestion points (e.g. bridges), or accident-prone points (e.g. intersections), provides awareness that enables a more efficient use of resources, enabled by the collected data. Intelligent and real-time monitoring eliminates the need for regular scheduled inspections by personnel, reducing costs, while it allows for accurate traffic flow forecasting. Thus, systems of sensors, deployed for traffic monitoring, collect data that are necessary for the implementation of Intelligent Transportation Systems (ITS).

For ITS to be realized, efficient methods to monitor traffic are required. Accurate methods of sensing vehicles traditionally involve induction loop detectors which are buried in roads [62]. Such loop detectors can be used to detect the presence of metals hence when a vehicle approaches, the loop's resonant frequency increases, and this measurement is interpreted as a vehicle. This change in frequency varies by car length or height, which allows estimating the kind of vehicle sensed. This information can then be further used to estimate vehicle speed or other parameters, which can be useful for traffic management.

More sophisticated, and at the same time less intrusive, methods involve for example cameras and Bluetooth detectors [62]. These approaches are more attractive mainly because they can be easily installed on fixed points (traffic lights, street corners, etc.) and their required installation and maintenance costs are typically low, compared to the previous approaches. Furthermore, in instances where surveillance cameras are already installed, these can be used for intelligent transportation applications.

As of lately, new methods to estimate the traffic state have emerged, bringing the end user closer to the system, as they are enabled by devices with a GPS receiver such as a smartphone or navigation device that are carried by citizens. Input data can be directly applied to provide the bearer's location and from there extract the traffic conditions, utilizing traffic flow. Mounting such devices to vehicles (e.g. on a portion of the local taxi/busses fleet, etc.) is a well-investigated method in traffic management schemes [62]. Still, it remains of high relevance to investigate how such data may can be combined with the data from other, alternative sources, to improve overall quality and cost-effectiveness.

In general, there is a need to assess the potential of new data sources in a short, medium, and long-term perspective of traffic data monitoring, bearing in mind many new challenges related to estimation robustness and integrity. Therefore, for this use-case, data sources of interest are Smart Objects that can be equipped with GPS, accelerometer, and the wireless interfaces.

2.1.2 Scope and benefit

The use-case is focused on secure methods for collecting traffic data, over heterogeneous networks of various sensors and smart objects, which can then be utilized to perform real time traffic estimation for intelligent transportation systems in Smart Cities. To achieve this goal, sensors (including the users' mobile phones and other smart objects that are defined below) will be placed in vehicles (i.e. buses, taxis or private cars). In this case the participation of citizens is encouraged and can be very beneficial, since the results of the use-case depend heavily on the penetration it has in the population. If the application gets a large number of measurements from many devices, then it can compute much more accurate estimations for the traffic. Citizens will be able to use their mobile phones (with the RERUM mobile application installed) for contributing to the crowdsourcing sensing framework.

This use-case enables benefits at three levels:

1. Operational – real time: Successful real time traffic estimation from intelligent urban traffic monitoring can be leveraged to unlock a host of applications, ranging from user travel planning for travel time / cost reduction, information systems for parking availability and driver alert systems for upcoming congestion or hazards.

2. Tactical – non real time: With traffic information acquired in longer time spans than minutes, trends and habits can be unveiled leading to more efficient traffic management decision support. For example, adjusting green light durations for heavy loaded traffic lights or re-locating traffic assistance resources could help reduce traffic in the city.

3. Strategic planning: With long-term acquired traffic information trends and habits can be unveiled leading to efficient transport planning (rescheduling or even re-routing of busses, increasing the number of taxi licenses) up to infrastructure planning for ease of use of the city transport system (forecast for more parking spaces) or even security (identification of hazardous intersections, or crossings).

2.1.3 Key challenges

The major challenges in traffic monitoring revolves around the reliability of the system in (i) the data sensing, and (ii) the data transfer both within the network of sensors but also to the external network (e.g., a traffic forecasting and management office). Here, the notion of reliability entails the availability and accuracy of sensors and their communication, the data security, the user privacy and system robustness, especially against the potentially adverse outdoors conditions. Furthermore, the age of collected/transmitted information is of high relevance, since in a real-time traffic estimation system the value of obtaining a measurement with a long delay is very small. Specifically:

- **Sensing of the traffic primitives**. Such primitives, depending on the implementation and requirements of the traffic estimation server, can range from (i) the user speed, acceleration, and position in a crowdsourcing-based system, to (ii) the number of vehicles passing a traffic light at a given time, to (iii) the trip duration for a vehicle between two fixed points in the traffic network, and so forth. This challenge refers to the uninterruptable operation of the sensing SOs and the correctness of the measured information. Energy efficient sensing is of high priority for battery-dependent SOs such as smartphones used in crowdsourcing. The outdoor deployment of fixed (wired/wireless) or mobile SOs leads to additional challenges, since they are susceptible to not only the adverse environment conditions which may hamper measurements (e.g. in the case of cameras), but also to physical, DoS and falsification or forgery attacks (for example in Bluetooth-based car measurement systems), which may hinder their operation. The potentially large number of deployed sensors/SOs, along with the computational burden of sensing and data storage also leads to cooperation issues amongst the SOs for distributed sensing.

- **Information Exchange**. The internetworking of SOs and other dedicated sensing devices relies primarily on wireless technologies (discussed in 2.1.4), hence measures have to be taken for ensuring the availability of communication resources and the robustness, security, and trustworthiness of the communication process. Cognitive Radio-inspired techniques can be utilized for sensing the available spectrum to enable dynamic spectrum access techniques. Dynamic access to the traffic estimation and management providers should be subject to successful authentication based on trust monitoring between the SO's and pre-established trusts between the SO's and the service providers. Mutual trust between the communicating SOs as well as between SOs and the traffic estimation/management servers is another key challenge for intelligent transportation systems. This is because malicious or misbehaving SOs sending false data can have severe impact on the ITS performance.
- **Information age:** in this use-case the age of information plays a very important role on the accurate estimation of traffic, because the use-case has very strict delay requirements. Imagine a scenario when the traffic estimation application produces estimations according to measurements it gets every i.e. 2 minutes. If (due to i.e. congestion in the wireless networks, loss of coverage, etc.) the measurements from the sensors arrive with 10 minutes delay, then the estimation application will compute inaccurate results about the traffic at the streets. In this case, the SOs should be able to know the application requirements and when they identify that due to some reasons their measurements are not sent at a specific time duration, then they should refrain from transmitting them. This will both help to avoid affecting the estimation application and save energy on the SOs due to not transmitting unnecessary information.

2.1.4 High level overview and network components

In this subsection the high-level view of the smart transportation use-case is presented. This high-level overview will serve as the basis for defining the RERUM architecture. In this context, this subsection aims to identify:

- The key components for realizing this use-case
- The logical relation between the components and the basic functionalities
- The stakeholders and their role in this use-case.

In this UC, the main goal is to collect data and provide them to a traffic estimation server (i.e., application server) in order to obtain the traffic conditions on city roads. This will be achieved via a combined use of the motion-based sensors of the smart objects along with complementary data from the radio access networks, or by direct user input, i.e. the user may be involved by being prompted to provide inputs (in case of uncertainty or simply to validate inferred itineraries/modes of transport). Actually, the information regarding the mode of transport plays a significant role in the traffic monitoring applications (but this is out of the scope of RERUM). Different modes of transport play different roles in the traffic scenario. For example in a city without dedicated bus lanes a traffic estimator can straightforwardly infer that the delay of a bus on a stop can very fast result in traffic queues behind it. Therefore the mode of transport along with the position and time of travel need to be transmitted.

The Physical Entities (using the terminology of IoT-A [2]) involved in this UC include:

- **The vehicles**, with measured attributes being the speed, the acceleration, the orientation and the location. These measurements are obtained via the smart objects that can be mounted on some of the vehicles or carried by passengers (in the case of crowdsourcing via android mobile phones) and their embedded sensors as described in Table 6.

- **The road** (or the road segments depending on the implementation of the application) which is considered as a larger physical entity monitored by several heterogeneous SOs in cars, buses, etc. The main attribute of the road, i.e., its traffic conditions (in terms of travel times, or congestion) is the main scope of this UC.

The key components for realizing UC-O1 are summarized in Table 5, while the high level overview of the UC is depicted in Figure 13 and Figure 14.

Table 5: UC-O1 main components.

Component	Description
Sensors	Sensing elements of the type described in Table 6.
Smart Objects	• Smart phones are devices that have several sensors and actuators on board, together with software that embeds intelligence for managing those sensors and their communication with other devices. Smart phones are ideal smart objects for this use-case, because they are widely used by users in vehicles and can provide accurate measurements regarding traffic. • General purpose computing devices with sensors e.g. Zolertia Z1 devices. Sensor platforms are also a type of smart objects considered in this use-case. They can be mounted on cars (especially buses) and transmit speed information using accelerometers (most platforms have them on board without the need for connecting external sensors) providing
Actuators	In this use-case there are mainly no actuators involved. In some use-case implementations we can assume that the traffic monitoring system can be connected with the traffic lights management system of the police to control the traffic lights. Furthermore, device to device communication with actuators on traffic lights can also be considered for the emergency vehicles (ambulances, police cars, fire fighter vehicles, etc.). Both these cases are outside of the scope of the RERUM project.
Network gateway and intermediate data aggregation points (i.e. cluster heads)	These are intermediate devices that play the role of aggregation and forwarding points. They can opportunistically forward traffic from SOs over 3G/4G/Wireline networks to the application servers. They serve as opportunistic access and aggregation points in order to send the measured/sensed data to a service provider (e.g. a Traffic Estimator as in Figure 13 via an external network. They may be also used as points for running complex mechanisms that can't be run on the sensing and measuring devices (e.g., data encryption). The functionalities of the gateway are particularly important for the case of heterogeneous sensing and measuring devices, where the interoperability of different access technologies must be guaranteed. Finally, the gateway and the cluster heads are responsible for critical security functionalities, as well as providing an interface to external traffic data providers. Typical gateway installations for this case can be on lamp-posts where it can be expected that the coverage of 3G/4G will be poor, and can run with 802.11(a/b/g/p) to offer vehicle-to-infrastructure opportunistic offloading.

Application server	This is the traffic estimator, namely a web server presenting the traffic state of the road network (see Figure 3: Snapshot of *Mobile Millennium* Traffic in San Francisco and the Bay Area [25]. Application servers are responsible for the transport services (e.g., traffic estimation, visualization of real-time traffic state, traffic management). They can be owned by the city, outsourced, or they can be completely private for the city to make a commercial profit out of the traffic data it owns. Each application server shall be securely accessible via the internet, by the non-crowdsourcing users of the system and also by city officials for traffic management and planning.

Table 6: Sensor types for UC-O1.

Sensor	Description	Common Uses	RERUM use
ACCELEROMETER	Measures the acceleration force in m/s^2 that is applied to a device on all three physical axes (x, y, and z), including the force of gravity.	Motion detection (shake, tilt, etc.).	Movement detection, traffic queue detection and historic hazardous zone detection
GYROSCOPE	Measures a device's rate of rotation in rad/s around each of the three physical axes (x, y, and z).	Rotation detection (spin, turn, etc.).	Movement detection and location estimation
MAGNETIC_FIELD	Measures the ambient geomagnetic field for all three physical axes (x, y, z) in μT.	Orientation estimation.	Location estimation
GPS_RECEIVER	Measures the location in the WGS84 reference system as well as point speed, orientation and time.	Location, speed and orientation estimation.	Location, speed and orientation estimation.
WIFI_MODULE	Captures the MAC address and RSS of current and nearby WiFi access points.	Energy efficient location estimation, in comparison to GPS.	Energy efficient location estimation. Movement detection.
CELLULAR_MODULE	Measures the Cell Id and RSS of current and nearby cellular base stations.	Energy efficient location estimation.	Energy efficient location estimation. Movement detection

Smartphones are continuously getting more powerful in terms of resources, thus they are becoming a key enabling technology for crowdsourcing and this has been thoroughly investigated in the literature [66], [67]. For instance, when users regularly update their location status on social networks like Twitter and Facebook, it is possible to aggregate and use these data for estimating the speed of movement. Furthermore, by using sensor data on a smartphone, it is possible to determine a person's mobility state (i.e., whether the user is stationary or not). These data can be collaboratively used in dedicated applications to obtain information regarding the transportation network traffic state.

During the last couple of years a number of crowdsourcing applications have been developed and the number of users is steadily increasing. For the purpose of crowdsourcing, Android phones will be considered in RERUM. The Android platform is open source and in general supports three broad categories of sensors: *Motion, Position, and Environmental*[1] *sensors.* One can access sensors available on the device and acquire raw sensor data by using the Android sensor framework.[2] The sensor framework provides several classes and interfaces that help the developer perform a wide variety of sensor-related tasks. For the Smart Transportation the sensors of Table 6 are relevant[3]. The sensors in this table are hardware sensors; however, the Android framework also includes software sensors which combines data from multiple hardware sensors. An example of a software sensor is the orientation sensor, which is a combination of the magnetometer, the accelerometers and when available also the gyroscope.

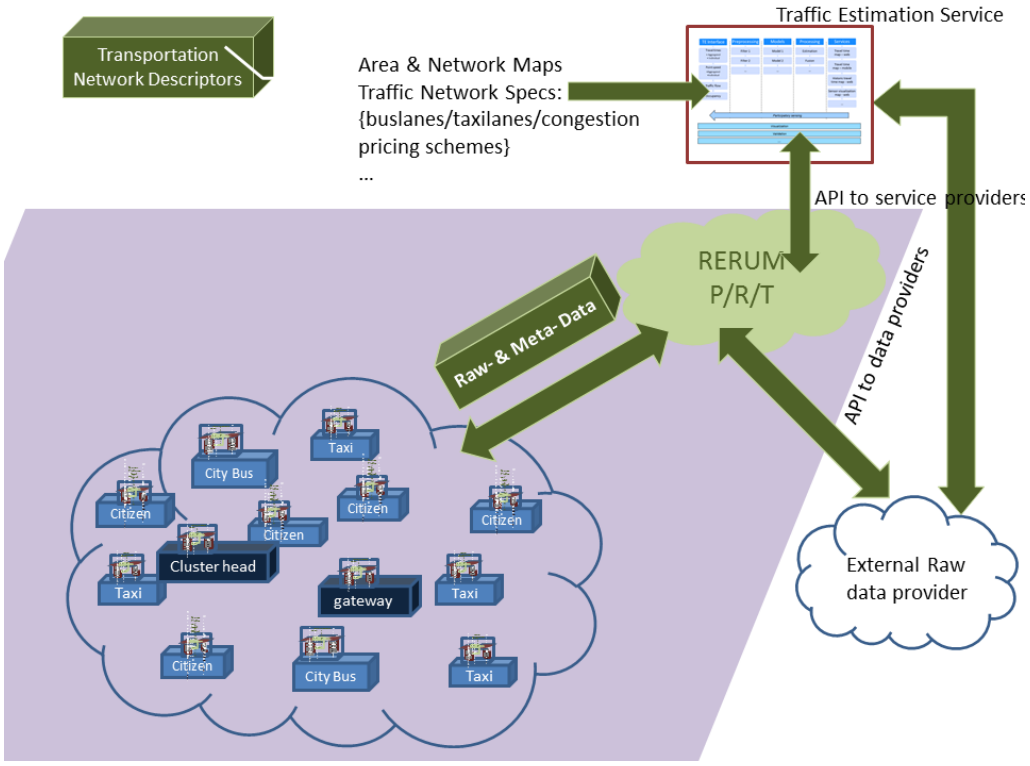

Figure 13: The complete outlook of the Smart Traffic UC.

[1] For our purpose of this RERUM use-case the environmental sensors are of no use, they are presented here for completeness.

[2] The Sensors Hardware Abstraction Layer (HAL) API, available online at: http://source.android.com/devices/sensors/index.html

[3] For an exhaustive list and more detailed information the reader is directed to the *Android Developers Sensors Overview web page*.

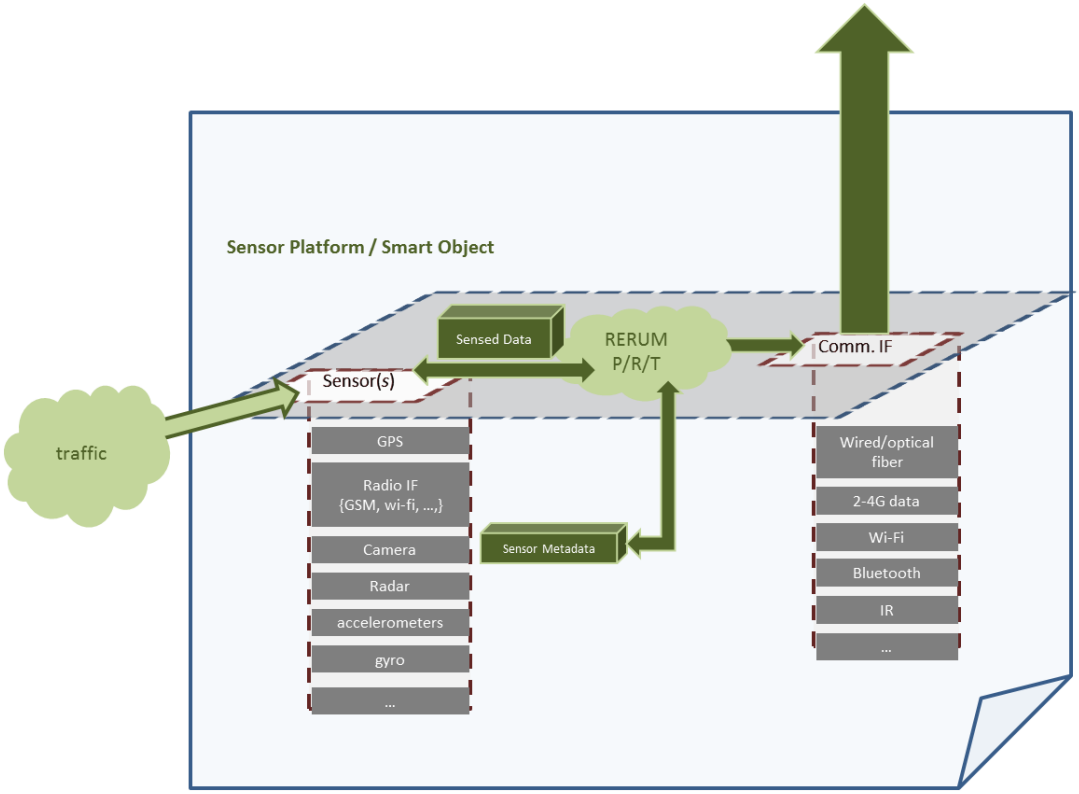

Figure 14: Schematic of the Sensor/SO within the UC of Smart transportation.

The Sensor and SOs can be either mobile or static (Figure 14). Mobile mounting options can be

- **Civic vehicles, e.g. city busses or garbage trucks**: These vehicles operate with well-known schedules and methods so data extracted regarding e.g. their location, travel times, duration of stops, etc., at various times of the day can provide significant input for both the real-time and the non-real time case as, they are moving continuously, so they can provide traffic measurements in long periods in a day and in many areas around the city.
- **Taxis**: Taxis are a large fleet of vehicles that are “patrolling” the city in a different pattern than that of the fixed-route civic vehicles, but likewise tend to drive greater distances every day compared to private cars. For both busses and taxis, one must be aware that, in the case where there are dedicated lanes, the extraction of traffic information from the data is not straightforward using the travel times to estimate congestion.
- **Crowdsourcing volunteers**: This is a case where the citizens utilize their cell phones to obtain data from the on-board phone sensors described above. Each type of data has to be carefully considered by the mode of transportation the user choses when he enables the recording of traffic data. The travel patterns derived can be wildly different if a user is on foot, on bicycle, in a private car, or on a bus. Therefore the user in such cases, should interact with the application and give input on her transportation mode. This can be done with the application automatically prompting the user to notify the mobility mode, when the application detects a significant location change during the first few minutes of a travel.

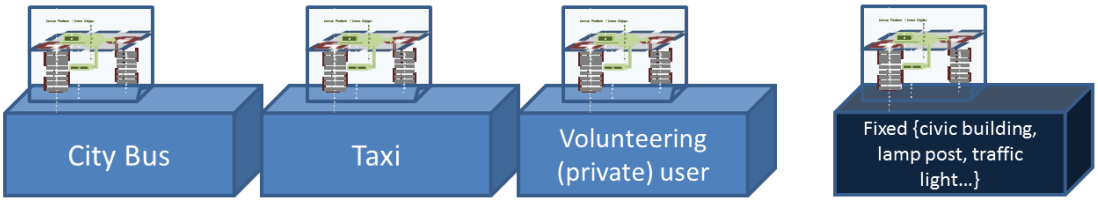

Figure 15: Mounting options of the sensing platform/ SO on mobile and fixed locations.

Considering the data types in UC-O1, they exist on three planes:

1. On the device that collects them
2. Traversing the SO network before reaching the gateway (applicable in scenarios where M2M communication over 4G or ad-hoc networking will be employed).
3. On the intermediate nodes that can be the gateway, the fusion points, the cluster heads, etc.

Furthermore, on each one of those planes there are also metadata describing:

1. Sensor properties: e.g. sensory data type, range of values, error range, timestamp of measurements, frequency of sensing.
2. Mounting properties: e.g. mobility, means of transport (pedestrian, bicycle, car, etc.), route type (fixed/random).
3. Network interfaces availability.

The data types come primarily from the sensor types described above which can be semantic information from cameras, cellphone UDID (Universal Device ID number) or interface MAC, timestamps of measurements, GPS locations, and derived mode of transport for the crowdsourcing case.

The wireless air interfaces that will be employed play a critical role, since it determines several parameters, such as energy efficiency, security of data transmissions, privacy, scalability, transmission range, etc.

The wireless technologies that could be used in the traffic management use-case include:

- **3G and LTE**. In terms of existing wireless communication infrastructures, 3G and LTE, have worldwide available infrastructures. LTE, in particular, has been a main enabler of high performance M2M applications, due to coverage, high throughput and low latency. Their services are provided by telecommunications operators and the data plan cost is still considerable in some cases. Although they are ubiquitously available on smartphones, one needs to keep in mind that these devices operate on a rechargeable battery, yielding significant end-user issues of device lifetime. Furthermore, the 3GPP standards are not optimized for dedicated use in sensor networks (low power). Hence, for enabling these technologies to be adopted for dedicated sensing, the power consumption has to be considered.
- **ZigBee**. As sensor nodes are typically designed to be low-power devices, the communication standard needs to take that into account because the communication process consumes most of the energy. Low-power standards such as IEEE 802.15.4 have limited range and a non-negligible number of repeaters would be needed in a city for full coverage. Furthermore, the developed mechanisms would have to support a very large number of devices. 6LoWPAN defines mechanisms which allow transmission of IPv6 packets over IEEE 802.15.4 based networks. Although this certainly presents

itself as a solution to the power consumption issue, the network coverage is quite limited in the order of tens of meters.

- **Dash7**. It is a promising open source RFID-standard for long distance, low power wireless sensor networking applications [64]. Its protocol stack is small and its communication range is typically below one kilometer. It operates at the 433 MHz ISM band, which allows better penetration than 2.4 GHz, especially for indoor networks. For wide area networks (WANs), Dash7 is also appealing because of the long range coverage. It offers AES 128-bit shared key encryption support, and data transfer of up to 200 kbit/s. Dash7 has received considerable attention for military applications, including substantial investments. Nevertheless, to the best of our knowledge, there is no significant active academically-driven research focused on Dash7. Dash7 is being developed for "smart" billboards and kiosks, likewise "smart" posters that can be read from many meters (or even kilometers) away, creating new opportunities for both tracking the effectiveness of advertising spend but also creating new e-commerce opportunities. DASH7's potential to automate check-ins and check-outs provides essential infrastructure to location-based advertising and promotions.
- **RFID and NFC**. For short range communication, there are two key technologies in the smart cities context. Radio Frequency Identification (RFID) consists of an “RFID tag”, where information is stored, and an RFID reader, which induces an electromagnetic field when in near proximity to passive tags providing power to the devices (longer ranges for active tags), enabling it to read data from the tag's memory. RFID enables a range of applications for smart cities ITS, such as localization and tracking of objects and smart parking. Near Field Communication (NFC) is used in mobile and similar devices, for a very short bi-directional communication range (in contrast with RFID which is unidirectional). These ranges are usually in the order of centimeter. The recent integration of NFC into smartphones has enabled a wide range of smart applications.
- **Bluetooth**. It is, well-known from hands-free devices. Bluetooth allows the matching of consecutive captures of the device MAC address and the estimation of travel times between two sensor locations. For example, a vehicle equipped with an active Bluetooth device is driving along a road and is logged and time stamped by a sensor at location *A* at time t_1. After driving a certain distance the vehicle is logged again by a sensor at location *B* at time t_2. As with all type of data collected by re-identification, the collected data has to be pre-processed and outliers have to be removed. This is primarily enabled by the short communication range of the Bluetooth radio, resulting in good accuracy in the measurements.
- **802.11p**. For Wireless Access in Vehicular Environments (WAVE), IEEE 802.11p amendment defines data exchange through links without the need to establish a basic service set (BSS), and thus, without the need to wait for the association and authentication procedures to complete before exchanging data. For that purpose, IEEE 802.11p enabled stations use the wildcard BSSID (a value of all 1s) in the header of the frames they exchange, and may start sending and receiving data frames as soon as they arrive on the communication channel.

2.1.5 Stakeholders

The key players that are involved in the use-case fall in three broad categories: Public, Private and Commercial. The main benefits of the use-case in relation to the different players are described in Table 7.

Table 7: UC-O1 stakeholders and expected benefits.

Smart transportation stakeholders	Expected benefits
Public stakeholders. Public transportation, city traffic planners	The **city** itself can significantly benefit from the deployment of an improved citizen-participatory ITS system. Once the concern for privacy is covered, which is one of the primary targets of RERUM, this UC provides the users the feeling of giving back to the city. The **public sector stakeholders** involved in the UC can utilize their civic vehicles (busses, garbage trucks, and police vehicles) for installing sensors or SOs in order to provide traffic data. Each of these types of vehicles allows for different inference from the collected data. Busses for example, when not running on dedicated lanes, can actually be the cause of congestion at a stop. Another class of public stakeholders is **city traffic planners** who upon a visual representation of the acquired data can utilize them for decision support for strategic planning solutions.
Commercial stakeholders. Vendors, software companies, service providers.	The realization of Smart Cities requires by definition the deployment of smart devices, which may range from simple sensors and measuring devices to smart appliances. Considering that Smart Cities will involve millions of sensors and smart devices, the opportunities that are offered to devices **manufacturers** and **vendors** become obvious. Also dedicated planning **service providers** can be enabled to develop new services based on the efficient processing of the traffic data.
Private stakeholders. Citizens, Commercial stakeholders' clients	**Individual users** fall in two categories: (a) the ones participating in the crowdsourcing, providing their city travel data and (b) the ones that consume the output of the ITS by using applications based on the traffic estimation from the use-case implementation. For the first category all privacy/confidentiality and security aspects of their data have to be respected in order for the system to have a rich participatory crowd. For both categories, there is a large potential in gaining benefits in terms of both reduced travel times and environmental impact.

The roles of the smart transportation stakeholders are highlighted in Table 8. It is noted that information can be communicated to the Service Provider directly or indirectly via the gateway.

Table 8: The roles of the stakeholders in UC-O1.

		Operation	
		Real-time Traffic Estimation	**Historic Traffic Estimation for Strategic Planning**
Stakeholder		**Stakeholder's role**	
Gateway administrator (actors with gateways)	Users permissions	- Full access to gateway configuration - Installation of new gateways	- Full access to gateway configuration - Installation of new gateways
Private user		- SO settings - Traffic information	- Not available
Service provider		- Access to location/speed data from SOs	- Access to location/speed data from SOs - Only aggregated traffic information stored for private users - Location/speed data stored for bus/taxis
Public user (Traffic Management Centre, Bus/Taxi Company)		- Real-time Traffic information - Access to location/speed data where applicable (only bus/taxi, not private users)	- Historic traffic information - Access to historic location/speed data where applicable (only bus/taxi, not private users)

2.1.6 Popularized example

In the following, a daily life example is presented, demonstrating the use-case's main characteristics and usages.

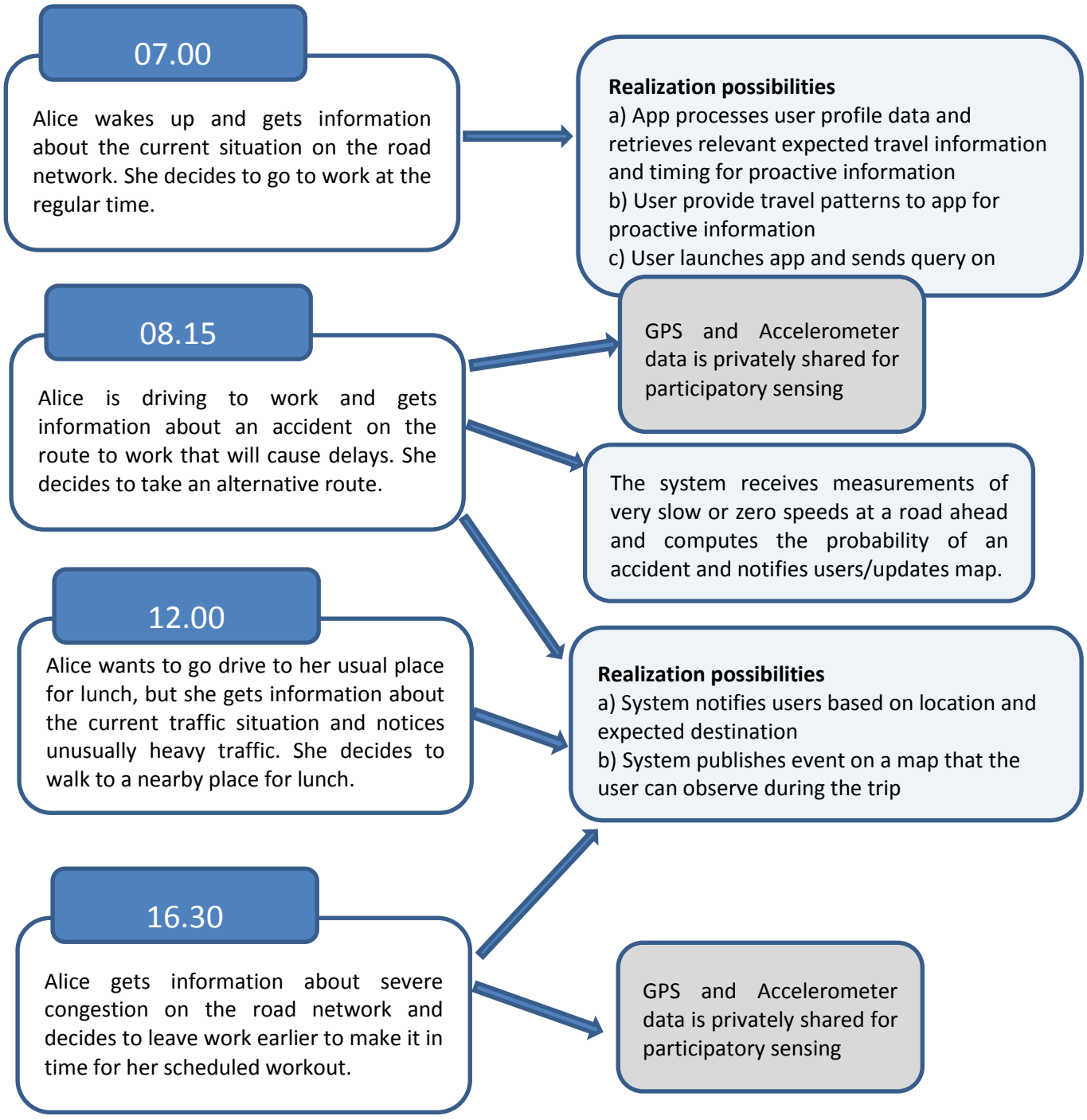

Figure 16: A popularized example for the smart transportation use-case.

2.1.7 Use case KPIs

The evaluation of the performance levels of the use case and the alignment with the objectives will be performed against the Key Performance Indicators (KPI)s that are shown in Table 9. This preliminary table will be refined in the deliverable D5.1, which aims at defining the methodology for evaluating the use cases at laboratory experiments and real world trials.

Table 9: KPIs and performance metrics UC-O1.

KPI Nr.	Title	Performance metric
UCO1-KPI_1	Participatory Sensing	% of citizens participating in traffic sensing via their smartphones
UCO1-KPI_2	Scalability	Area of performed traffic estimation, # of vehicles, # of smartphones sending data
UCO1-KPI_3	Sensing Multimodality	Number of different source types of traffic sensing; increase of the complementarity and accuracy in estimation
UCO1-KPI_4	Transport mode flexibility	Number of different modes of transport taken into account (difference of vehicles, private, public, including pedestrians)
UCO1-KPI_5	Connectivity & Reliability	% of time the devices are connected to the application server and send data
UCO1-KPI_6	Sensing Accuracy / Trusted measurements	% of dropped measurements (outliers) & false positives or true negatives
UCO1-KPI_7	Sensed Information Timeliness	Age of information from measurement timestamp to arrival at server
UCO1-KPI_8	Traffic estimation quality	Mean square error (MSE) in travel times, traffic loads, average speed in links
UCO1-KPI_9	Accident prevention	Reduction % of traffic accidents by utilizing a traffic estimation module
UCO1-KPI_{10}	Privacy protection	Possibility to identify the name and id of the persons that participate in the traffic sensing at a specific time
UCO1-KPI_{11}	User acceptance	Percentage of users acknowledging the usefulness of the application
UCO1-KPI_{12}	Data availability	% of lost data due to network failures (congestion, collisions, interference) or attacks (DoS, manipulation) or device failures
UCO1-KPI_{13}	Service QoS	Improvement in the QoS of the provided services by the system
UCO1-KPI_{14}	Energy efficiency	Maximum runtime of a smartphone running the application and sending data before the battery depletes.

2.2 Environmental monitoring (outdoor use-case, UC-O2)

2.2.1 Introduction

The development of the modern cities and their continuous growth has raised several problems related to environmental issues and pollution in the last decades. The uncontrolled increase of public and private vehicles, the activities of the heavy industry and the increasing demands on electrical energy consumption are the main reasons behind the hazards for the environment. The main effects of this stress in the short term are the decline of the quality of the air we breathe in the cities, as well as the presence of other kind of pollution such as the noise and the EMF radiation [68]. In the long term, this is definitely related to the climate change [69]. The Environmental Monitoring UC intends to provide a system based on wireless sensors to measure and monitor the quality of the environment in cities.

2.2.2 Scope and benefit

The main goals and expected benefits of an environmental monitoring system for the cities are the following:

- Get indicative measurements of the air quality of the city at different spots.
- Study the effects on the air quality when different decisions are taken from the city council in terms of mobility in the streets (traffic light periods and synchronization, street direction, etc.).
- Monitor and control the pollution generated by construction works, shops, business, etc., on the streets.
- Know the amount of particulate matter in suspension and which part of it is related to vehicular traffic or to other things.
- Prevent and forecast episodes of halted contamination due to low atmospheric pressure weather conditions.
- Correlate all measures made with the existing weather on each part of the city the system is deployed.

2.2.3 Key challenges

The main goal for this use-case is to gather environmental information from various areas around a city and provide them to the interested parties. Deploying a city-wide infrastructure only for environmental monitoring is not cost-efficient, so the deployed nodes may be also utilized simultaneously by other smart city applications. This requirement for interoperability induces several communications, energy consumption and security/access control challenges. Therefore, the network deployment should be designed with specific security, privacy, and reliability mechanisms in order to ensure its reliable operation, the trustworthy exchange of information, and the optimum network performance.

The smart objects utilized by this use-case are connected to an application server where the sensed information is stored and used by the municipalities for providing various services to the citizens, e.g., opening it to citizens, showing the data in maps, for Geographical Information Systems (GIS) or similar interfaces, and for developing a supervision system to create alarms when an indicator is out of the expected bounds.

In this way, the use-cases development and deployment has a strong focus on the SOs, the network and the gateways, while the application server could be provided by third parties, or could be adapted to something existing and already deployed by the cities; the only requirement in those cases will be that the interface with the application server must be IoT based, such us the Representational State Transfer (REST) one.

Cost and power consumption constraints are also applied to the sensors and the wireless nodes since the idea behind this use-case is to implement it using simple, low-cost and low-power sensors and environment-friendly systems. The accuracy of measurements is always considered when deciding which sensors will be used to measure the environmental metrics.

2.2.4 High level overview and network components

In this subsection a high-level view of the environmental monitoring use-case is presented. This high-level overview will serve as the basis for defining RERUM's architecture. In this context, this subsection aims to identify:

- The key components for realizing this use-case
- The logical relation between the components and the basic functionalities
- The stakeholders and their role in this use-case.

In this UC, the main goal is to measure the quality of the environmental conditions in cities. The physical entities involved in this UC includes:

- The outdoor environment, which can be any specific area of interest within the city (a street, a park, a city square, etc.). The SOs in the environmental monitoring use-case are monitoring he outdoor environment through the following attributes:
    - **The air**, with its measured attributes being the SO_2 and the NO_X related to the fuel combustion, O_3, which is a toxic gas for humans, created in low altitudes when NO_X is summited to UV radiation from sunlight, VOC, organic compounds, related to smells and PM_{10} (or additionally and if it is feasible $PM_{2.5}$), which particulates in suspension, most harmful compound for human health [70], [71].
    - **The noise**, i.e., the L_{Aeq}, equivalent continuous sound level, A-weighted, the most used parameter to measure noise, also related to EC environmental directives [72][74]; the integration period is to be decided with city council's environmental representatives. Other related parameters (like L_{SPL}, L_{AT}, L_{Apeak}, etc.) [75], ideally always keeping the A-weighting, that the municipalities involved in the project consider interesting.
    - **EMF radiation**, as wide-band as possible but, if not, preferably measuring the microwaves band; self-radiation (radiation self-added to the system while wirelessly transmitting the data to network) measurement will be avoided [77].
    - The **weather conditions**, getting measurements for:
        - *Temperature and Relative Humidity* (RH), usually both metrics measured with a single sensor, as key indicators of climate status,
        - *Atmospheric pressure*, to detect potential situations of high pressure which could increase the pollution concentration,
        - *Rain*, to detect abnormal measures of noise or air compounds due the air cleaning it causes,
        - *Wind speed* (average and gusts) *and direction*, could help to understand why there is abnormally high noise or abnormally clean air situations.

A high level overview of UC-O2 is depicted in Figure 17, while the key network components are summarized in Table: 10:

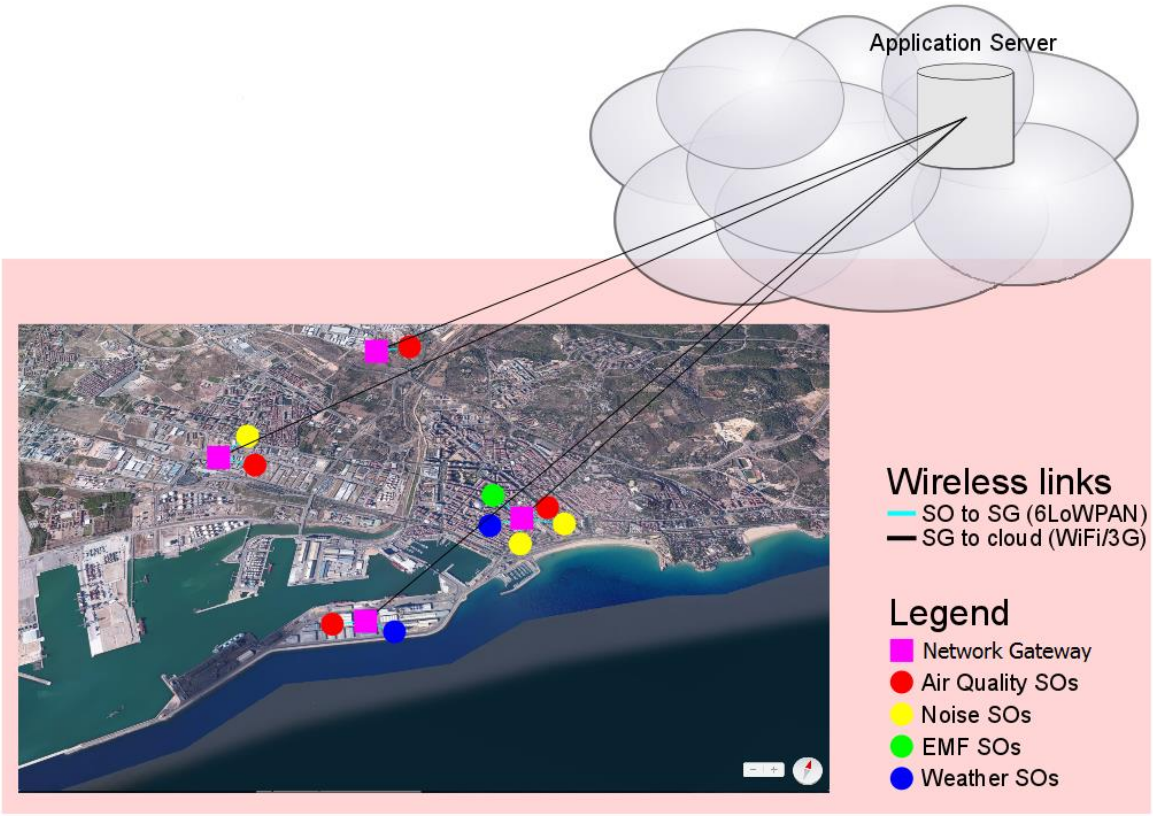

Figure 17: The overview of the environmental monitoring use-case.

Table: 10 UC-O2 main components

Component	**Description**
Sensors	Convert physical parameters into electric ones in order to be able to measure those using electronic based systems. The measurements will be digitalized and transmitted through digital communications systems. See Table 11 for further details on sensors used in UC-O2.
Smart Objects (SOs)	The SOs are different nodes of a network connected through a star, tree, or mesh topology. They are installed on the streets or on city square gathering information from sensors. Mounting supports for the SOs are used to attach the devices on different placements on the city's streets. The support is also used as a base for the power supply of these devices. For example, partial power supply (e.g., the streetlights one, only available during the night) could be applied for charging the batteries of those devices, in order to ensure their operation during the day. Solar cells could also be used to power nodes with low power requirements. On the other hand, in the case of more energy-greedy devices, such as gateways, a 24/7 power supply might be required. SOs communicate wirelessly, using 6LoWPAN over 802.15.4 (on the specified frequency bands). SOs are composed of: • A RF 802.15.4 interface. • A CPU (a micro-controller) managing the 6LoWPAN communication stack and getting measures from the sensors. • One or more sensors connected to the CPU, through analog or digital

	interface, depending on the sensors. • A power supply, optionally with batteries when power is not always constantly available. The use of more than one sensor per SO is useful for correlated types of measurements, for example when different type of gases are measured in one spot, or when it is required to relate different measurements with each other, e.g., the concentration of specific materials in the air with the amount of rain or the relative humidity. In this way, the next measurements are available on a single node: • Measure of all gases suggested in the same node, since they are related to fuel combustion and its chemical combinations with the air and the sunlight. • PM_{10} and RH, because in high humidity situations (e.g., due to fog), a possibly wrong figure will be shown because it will act as an interference to the optical sensors usually used for such kind of measurements. Spectrometric measure could avoid that situation but its cost keeps it out of the scope of many such installations[4]. • Noise and rain: according also to the EC directives [65], the noise could not be measured while it is raining due the impact of the drops on the structure or the microphone and due the amplification of the vehicular noise when the asphalt is wet.
Actuators	No direct actuators are used in this UC
Network Gateway or cluster heads (intermediate nodes)	Due to the limited communication range and bandwidth restrictions of the SOs' wireless communication technology, it is necessary to add gateways or cluster heads close to SOs to communicate/fuse the gathered data to the application server over the internet. Thus, a gateway will be equipped with an 802.15.4 interface for communication with the SOs and appropriate interfaces to connect to the Internet over a wired or wireless link, e.g. a wifi interface could be used in case a suitable 802.11 based mesh infrastructure already exists in the city. All intermediate nodes should ensure security, privacy and reliability when forwarding the information to the application server.
Application server	The application server, equipped with an appropriate software application, will provide end-users with a graphical interface giving access to raw data, graphs, queries, threshold configuration, alarm setting and transmission, etc. The server will be owned by the city authorities and can be either outsourced or kept private. In certain cases city authorities could even exploit the data for their own profit. In any case, it must have at least an IoT based interface, i.e. support web-services over REST interface to gather the data from the sensor devices.

[4] Rain also changes the particulate matter in suspension on the air, making it fall down and improving the air quality but in this case is not affecting the measurement directly but due the high RH. After the rain, the particle sensor will work again initially showing a great air quality but, unfortunately and soon, when the asphalt dries and the traffic increase, all deposited particles will be back in suspension on the air.

Table 11: Sensor types for UC-O2.

Sensor	Sensing elements	Connectivity	Description	Common Uses
Air Quality	SO_2 NO_X O_3 VOC PM_{10}	Wireless	Measures the key air compounds (mainly those related to traffic and fuel combustion)	Determine an air quality index, control the PM to keep it into the normative and detect the traffic congestion effects
Noise	Microphone	Wireless	Measures the noise level with A-weighting, peak, average and daily distribution	Control the noise levels in order to keep under the maximums regulated by the European normative
EMF	EMF sensor element	Wireless	Measures the electromagnetic radiation	Detect abnormal EM radiation
Weather	Temperature RH Atmospheric pressure Rain Average wind speed Burst wind speed Wind direction Lux meter	Wireless	Measures the weather conditions	Implement a weather station and use that information to interpret the air quality and noise information

2.2.5 Stakeholders

The key players that are involved in the use-case fall in three broad categories: Public, Private and Commercial. The main benefits of the use-case in relation to the different players are described in Table 12.

Table 12: UC-O2 stakeholders and expected benefits.

Environmental monitoring stakeholders	Expected benefits
Public stakeholders	Municipalities. The city (public administration) and the citizens are the end-users. The UC will provide them with the infrastructure to gather the information necessary to know the environmental status of the city and to make decisions, take actions and apply policies to improve it. Citizens will be at the end the beneficiaries of these

	actions and policies but, if they have also access to the information, they could make their own decisions to improve the environmental quality through small and simple actions, such as using the public transportation. The public administration can utilize the environmental pollution information to try to identify measures to address this issue. Furthermore, the city may be able to better schedule the time of constructions and avoid them in specific weather conditions that may result in an intolerable atmosphere in the city.
Commercial stakeholders	Vendors and suppliers. Specialized companies that develop sensors, sensor platforms and sensing elements related to environmental monitoring. Specifically, hardware for measuring air quality in outdoors with good accuracy is quite expensive and there is a huge market opportunity for addressing the challenge of developing cheap and accurate sensing devices for monitoring the environmental pollution. Equipment installers and maintainers. Usually both roles are taken over by a single company. They are key players in city-wide deployments and they also handle the maintenance of the equipment. These efforts are most of the time directly carried out by the municipality, while in some cases they are subcontracted to external private companies. Network providers. They provide the communication between the gateways and the application server (or the internet in general). This kind of service is mandatory for the environmental use-case. Software companies. The IoT-based software platform (where the system sends all the gathered data, and where and the users access the information) could be provided by an external company or a department from the municipality that set-up and take care of that. Application developers and providers. Depending on the way the cities want to use all the data generated, there can be opportunities for private companies or departments from the municipality to create software applications to work with the data. They can, digest it, and create a business intelligence, implement a human interface, as visual as possible and communicate the data to end users creating reports, alarms, messages, etc.
Private stakeholders	Citizens. They will benefit from the services that the municipalities provide through the environmental monitoring system, since the goal is the reduction of the contamination in cities and the improvement of the citizens' quality of life. The citizens are able to monitor the weather and the pollution around the city. The elderly can also identify possible areas that may be hazardous for their health.

The roles of the stakeholders of UC-O2 are highlighted in Table 13. SOs can send information (pre-processed data and maintenance information) to the application server and other SOs via the gateway. The end users could view, trace and interpret that information directly on the application server via Internet access. The application server is also responsible for triggering the communication with the end user in case of alarms.

Table 13: The roles of the stakeholders in UC-O2.

		Operation	
		Environmental contamination monitoring	**Weather station**
Stakeholder		**Stakeholder's role**	
Administrator	Users permissions	Full access to gateway and SOs configuration Creation/deletion of platform user accounts with specific permissions and information access Admission of new SOs	
End-user		View, trace, interpret and process information on the platform. Also configure and get alarm triggers through the platform	View and trace information on the platform. Also configure and get alarm triggers through the platform
Maintainers		View and trace maintenance information on the platform. Also configure and get alarm triggers through the platform	
Public user (i.e. citizens)		View pre-processed information on the platform	View and trace raw information on the platform
Service provider		In case that a service provider hosts the application server platform, instead of the municipality, it may have access to the volume of stored data for maintenance purposes but not to the data itself	
Network provider		The network provider is able to control the transmission bandwidth and transport the information from the gateway to the **Access Network** towards the application server.	

2.2.6 Popularized example

These are some short descriptions of different situations this use-case could cover:

- Example 1: Pollution in the downtown
  - Citizens living in the downtown area of the city are complaining about bad air quality and noise in their neighborhood.
  - The city council decides to install in that area, usually with a lot of vehicular traffic, (the main reason for pollution in cities), some of the devices to get accurate information about the air quality, the noise in the streets, and the EMF contamination as well.
  - The smart objects measuring air quality monitoring, noise, and EMF measurement, and weather conditions are placed at some strategic points of the downtown, some close to the traffic, others close to the citizens' houses in a close area with connectivity to a gateway which will forward the data to an application server.
  - Engineers specialized in environmental analysis and specialized technicians of the city council get access to the data through the application server, interpret the data, including the weather conditions and create reports that get published on the city's webpage and sent to the citizens who are complaining about that.

- Example 2: Constructions in the commercial harbor
  - New construction works have started at the city's harbor.
  - City council decides to install a network of smart objects on the streets to measure noise and air quality, especially the particles in suspension (both are parameters under EU regulations [65][72]) at the place where the construction takes place, e.g. SOs are placed in nearby houses. A gateway is also placed close by to create sub-networks of devices.
  - Data (only indicative when measured with the low-cost sensors) are monitored by technicians of the city council and can also be shared with the company responsible for the construction, so that they may reschedule their work in order to avoid the violation of noise and pollution regulations.
  - Alarms are programmed on the application server to be automatically sent by email and SMS to the city council's representatives in charge and to the construction company. City's council could appoint a technician with an approved meter to perform an homologated measure and fine the construction's company; however, the company could also avoid fines by being aware of the situation and take measures to reduce noise and particles (for instance, reducing trucks displacements or heavy machinery works, like jackhammers).
- Example 3: Industrial contamination
  - The city is surrounded by some industrial areas with potential contamination on of the air (foundries, chemical, etc.) or EMF radiation.
  - The city council decides to install one or more clusters of smart objects incorporating environmental sensors close to the potential contaminating industries and/or next to the closest households, measuring the air compounds and the EMF radiation; furthermore, the weather is monitored, especially the atmospheric pressure, to detect potential risk of high contamination without natural air renovation.
  - The gateway of each cluster sends the data to an application server where the city council can preview or detect with automated alarms those situations and react very fast.

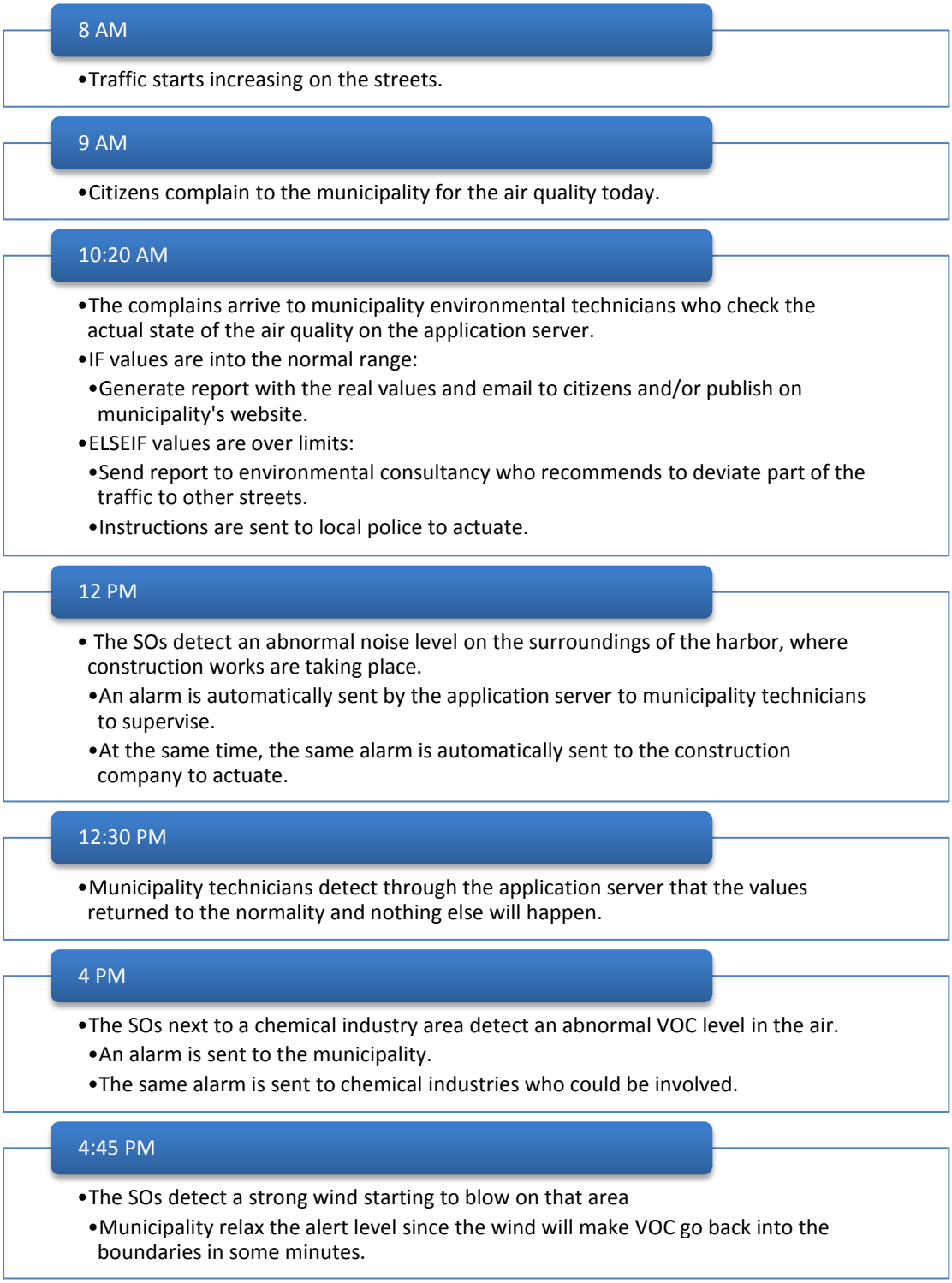

Figure 18: A popularized example for the environmental monitoring use-case.

2.2.7 Use case KPIs

The evaluation of the performance levels of the use case and the alignment with the objectives will be performed against the Key Performance Indicators (KPI)s that are shown in Table 14. This preliminary table will be refined in the deliverable D5.1, which aims at defining the methodology for evaluating the use cases at laboratory experiments and real world trials.

Table 14: KPIs and performance metrics UC-O2.

KPI Nr.	Title	Performance metric
UCO2-KPI$_1$	Reliability of the geo-located data	Improvement (%) of the accuracy of the readings per deployment area compared to the more generic ones provided by weather stations or weather casts in the area
UCO2-KPI$_2$	Predictability of weather related events	Comparison with conventional methods. Readiness and likelihood of events based on estimation and correlation of variables, such as temperature, humidity and atmospheric pressure to forecast rain
UCO2-KPI$_3$	Flexibility to measure and federate different parameters	Number of monitored variables and events
UCO2-KPI$_4$	Distributed and ubiquitous sensing / scalability	Number of deployed sensors per square kilometer compared to the current information sources available in the same geographical area
UCO2-KPI$_5$	Distributed sensing overall savings	Deployment cost compared to conventional methods, i.e., having an environmental agency with monitoring devices, typically sampling at single location for fixed amounts of time
UCO2-KPI$_6$	Energy efficiency	Decrease in energy consumption by using the RERUM mechanisms for data gathering, transmission and energy efficiency
UCO2-KPI$_7$	Trustworthiness of data	Improvement in the accuracy of the system measurements by avoiding false data or malicious users affecting the measurements
UCO2-KPI$_8$	Alarm detection	Improvement in the ability of the system to identify false alarms and to minimize miss-detections regarding events.
UCO2-KPI$_9$	User acceptance	Percentage of users acknowledging the usefulness of the system for being informed about the weather or hazardous events
UCO2-KPI$_{10}$	Data availability	% of lost data due to network failures (congestion, collisions, interference) or malicious user actions
UCO2-KPI$_{11}$	Privacy protection	Possibility to identify the name and id of the persons that participate in the environmental sensing at a specific time, either via their smartphones or via their home-installed devices.
UCO2-KPI$_{12}$	Connectivity & Reliability	% of time the devices are connected to the application server and send data

2.3 Home energy management (indoor use-case, UC-I1)

2.3.1 Introduction

The home energy management use-case aims to monitor the energy consumption of high-consuming devices within users' homes, businesses and government buildings. The efficient monitoring of energy consumption of devices can also enable the optimal management of devices' operation, which may result into minimization of the total energy consumption. In this use-case smart objects are attached to high consuming appliances and monitor their energy consumption. The SOs transmit their data directly and wirelessly to a central gateway, which, in turn, forwards the data to the application server that visualizes the energy consumption of the devices. The energy consumption monitoring can be combined with additional sensing systems (e.g., sensing of environmental factors, such as temperature and lighting), or other type of sensors (e.g., sensing of opened windows or doors) for further energy savings. Furthermore, aggregations and averages of the monitored data could also be delivered to the utility provider, in order to exploit them for performing consumption forecasts.

In the case of businesses, office buildings and storage areas are of high interest for energy management. For example the energy expenses for refrigeration of sensitive goods such as fresh fruit or frozen goods are very important for businesses in the food sector. Local (or central) governments have also an interest in managing energy consumption vis-à-vis the requirements for specific environmental conditions in public administration buildings, schools, hospitals, museums, public meeting buildings, and retirement homes.

2.3.2 Scope and benefit

The energy management use-case primarily aims at creating an intelligent system for managing the energy consumption at home or municipal/governmental buildings. The motivation comes from the European Commission proposal for directive [42], which sets the target to reduce the energy consumption by 20% for smart, sustainable and inclusive growth. The benefits that stem from smart energy management systems are as follows:

- **Energy savings** via efficient monitoring of the energy consumption of appliances, as well as monitoring of environmental factors (e.g., indicate that a window is open, while air-condition or heating devices are operating, automatically turnoff devices or lighting when not in use, etc.).

- **Remote monitoring and control** of devices/appliances (e.g., via smartphones), allowing daily activities and routines to be programmed and scheduled (e.g., heat water remotely, turn on heating devices before getting at home). Smartphones, laptops and tablets allow this remote monitoring and control.

- **More efficient operation and management of the electrical grid**. The information that is gathered by the monitoring of the energy consumption can be exploited towards a more efficient energy management. Costly events, such as blackouts can be prevented, given that the energy generation/consumption relation is known in real time.

2.3.3 Key challenges

The major challenge for energy management systems is the reliable transfer of the sensed or measured data both in the internal home network and in the external network (e.g., the utility company's network). Reliability incorporates the issues of security, privacy, availability, robustness, and flexibility to changing environmental conditions. As the intelligence of the SOs increases, they

become autonomous, active and seamlessly integrated in the everyday life of smart cities, new problems and new security issues arise. The primary challenges include:

- The reliable sensing and measurement of the environmental factors, which refers to both the uninterruptable operation of the sensing devices and the correctness of the measured information. Energy efficiency is particularly important for battery dependent SOs. Since the SOs that measure energy consumption are consuming themselves some amount of energy, it is important to keep that amount as low as possible. That way, the total energy consumption of the home will not increase significantly due to the SOs. The deployment of wireless SOs leads to additional challenges, since they are susceptible to wireless attacks, which may hinder their operation. Assuring the correctness of the sensed information is very critical in the case where the SOs serve as actuators, which determine specific actions (e.g., turning off high-consuming devices and preventing devices from overheating).
- The secure exchange of information within the network. False measurements can lead to erroneous decisions or estimations, when considering either the energy measurements (e.g., make wrong estimations of the electrical consumption), or the actuation part of the applications (e.g., shut down the wrong devices, or windows). The inter-networking of SOs and devices usually relies on wireless technologies, and considerable attention is required for encountering intruders and malicious attacks. Dynamic access to the service providers should be subject to successful authentication based on properly pre-established trust between consumers and service providers. Trust between devices (e.g., SOs, gateways) and the application server is another key challenge for energy management systems. Malicious or misbehaving SOs sending false data/commands can have severe effects on the system performance, which decrease the credibility of the applications.
- The maintenance of privacy and confidentiality for keeping secret or private information from being disclosed to unauthorized parties is particularly important since meter data and device information may expose customer habits and behaviour. Such patterns (e.g., indicating the absence of residents) could be exploited for criminal activities.

2.3.4 High level overview and network components

In this subsection the high-level view of the energy management use-case is presented. In this context, this subsection aims to identify:

- The key components for realizing this use-case
- The logical relation between the components and the basic functionalities
- The stakeholders and their role in this use-case.

The energy management use-case includes two main sub use-cases: (i) a home energy management system and (ii) an energy management system for municipal/governmental building. The physical entities in this UC are the following:

- **Appliances** that consume energy (i.e., heating devices, washing machines, etc.). Their measured attributes include the electrical current and voltage.
- **Rooms**. The measured attributes include the temperature, humidity and ambient light. These attributes can be in a combination in order to help the SOs to make decisions about the operation of the appliances and the actuators in general.
- **Windows and doors**. Their attributes include their state, i.e., open close. This information can be used towards energy savings decisions, e.g., a window could

cooperate with an operating air-condition device and decide whether to turn-off the air-condition or close the window in case that a window is open.

- **People:** The existence of a person in a room could be considered as an attribute of the room as well. In any case, this information can be used towards energy savings decisions, e.g., turn off the lights in the cases that no persons exist in a room. However, customized energy management for different persons requires knowing exactly who is in the room, so the People can be considered as a different PE. For example, one kid may like a low light in the room, while the father that does not see very well may want a very bright light. Thus, the HEM should monitor who is in the room, to get his preferences and then change the operation of the appliances according to pre-defined policies (that also affects the energy consumption of the appliances).

The key network components are described in Table 15, while the Sensors that are used are described in Table 16.

Table 15: UC-I1 main components.

Component	Description
Sensors	The sensors measure a physical condition of the physical environment surrounding the location of the sensor, such as electrical voltage and current, water flow and pressure, temperature, sources of light, motion, etc. Details about the sensors are given in Table 16.
Smart objects	The SOs are able to provide information of the physical environment surrounding (*environmental data*) to other SOs or act on the environment according to incoming *commands*. Furthermore they have the capability to send the sensed information (via wires or wirelessly) to other network nodes (e.g., SOs or gateways) for further processing. In UC-I1, SOs include smart home electrical appliances, smart objects related to energy consumption (e.g., windows, doors, water),
Actuators	They are able to perform specific actions (e.g., turn-on/off or dim lights, close windows, trigger alarms, turn on heating devices, etc.) based on the sensed data and policies defined by the end-user.
Gateway	It serves as an access or aggregation point in order to send the measured/sensed data to an external network (e.g., the internet, the utility company network etc.). The gateway may be also used for transferring the complexity from the sensing and measuring devices to it (e.g., data encryption). The functionalities of the gateway are particularly important for the case of heterogeneous sensing and measuring devices, where the interoperability of different access technologies must be guaranteed. Finally, the gateway is responsible for critical security functionalities and for the home network management.
Application server	It is responsible for the end-user services (e.g., automation services, energy management, etc.). Depending on the implementation options, it may be accessed through an external network (e.g., xDSL network).

Table 16: Sensor types for UC-I1.

Sensor	Connectivity	Description	Common Uses
Temperature	Wireless/Wired	Measures the temperature of the air or the surface temperature of an object (e.g., electrical device)	Automatic air-conditioning, alarms (e.g., overheating prevention)
Humidity	Wireless/Wired	Measures the relative humidity in the air.	Automatic air-conditioning, alarms (e.g., for devices requiring specific humidity values for operating properly)
Electrical current/voltage	Wireless/Wired	Measures the operating electrical current/voltage of devices.	Energy consumption monitoring and control
Ambient light	Wireless/Wired	Measures the ambient light in a room.	Lighting automation, energy consumption control
Water pressure/flow	Wireless/wired	Measures the water flow pressure.	Water consumption monitoring and control, alarms (e.g., flooding)
Motion	Wireless/wired	Detects motion	Alarms (e.g., open windows, doors, etc.)

Table 17: Actuator types for UC-I1.

Actuator	Connectivity	Description	Common Uses
Circuit switch	Wireless/wired	Allows to turn on and off or dim electrical devices	Turn off high energy consuming devices if not needed. Dim or switch off lights.
A/C Control	Wireless/wired	Allows to control the A/C	Reduces the home energy consumption by decreasing or increasing the temperature in the room depending on the environmental conditions and the persons in the room (if any).
Hot water boiler Control	Wireless/wired	Allows to control the heat of water in a building or for certain sinks	Allows to pre-heat lots amounts of water only if all members of the family

			need to take a shower at the same time. Allows turning off the hot water boiler in the kitchen if no one is the washing dishes by hand
Heating control	Wireless/wired	Allows to control the radiators within the house.	Controls the temperature in the room in the winter time depending on the environmental conditions and the preferences of the residents.

UC-I1 is divided into two sub use-cases:

(a) UC-I1 sub use-case 1: Private houses/apartments

Considering this use-case, the main scope is to enable three main functionalities: (i) home automation in terms of SOs cooperation without the human intervention for achieving energy savings, (ii) the monitoring of electrical consumption and specific environmental factors (e.g., temperature, etc.) and (iii) the control of specific actuators for e.g., turning off/on devices or controlling their operation. The sensors expected to be utilized in this use-case are detailed in Table 16, while the actuators are presented in Table 17. SOs share information directly to each other or indirectly via the gateway. They can also send activity information to the gateway (e.g., for logging purposes), while the gateway may send activity information to the end-user[5] if it is allowed (Figure 19). The data are processed at the application server, which is responsible to provide the service to the end-user.

The application server can reside either:

(i) at a specific device within the home network or
(ii) at a device external to the home network which can be located at a trusted third party.

The former case considers that information gathered by SOs and sent to the gateway can be transmitted to third parties. For example, aggregated and average consumption data may be sent to the energy (electricity and/or gas) provider or the public administration to enable them to monitor the total energy consumption in the city. Utility providers could receive these data as well and use it for forecasting and controlling energy consuming devices; this is one of the many features discussed in the so-called Smart Grid. The sharing of such data gives rise to privacy attacks. Hence, prior to the transmission of these data to the third parties, it must be ensured that all privacy policies to which the end-user consented are met. In general, policies for privacy must be specifically adjusted to each end-user and each use-case individually.

In the latter case, the application server is residing logically within the home network. Then the HEMS is a closed-loop control system and no external entities are accessing these data; only the data owner has access, e.g. the citizens living in the apartment. The SOs and the gateway are performing actions based on a configured automation policy that could reside inside the SOs or the gateway (or

[5] The end-user may be a local user or a remote user that establishes a secure connection to the gateway (e.g., via VPN). Thus, all actions may be performed either locally or remotely (e.g., via a web browser).

somewhere else internal and trusted). Keeping the sensed data within the closed system raises fewer privacy concerns. However, to maintain privacy, the system must not be vulnerable to confidentiality breaches. Hence, confidentiality needs to be protected even in this case in order to enforce the system's property of being "closed".

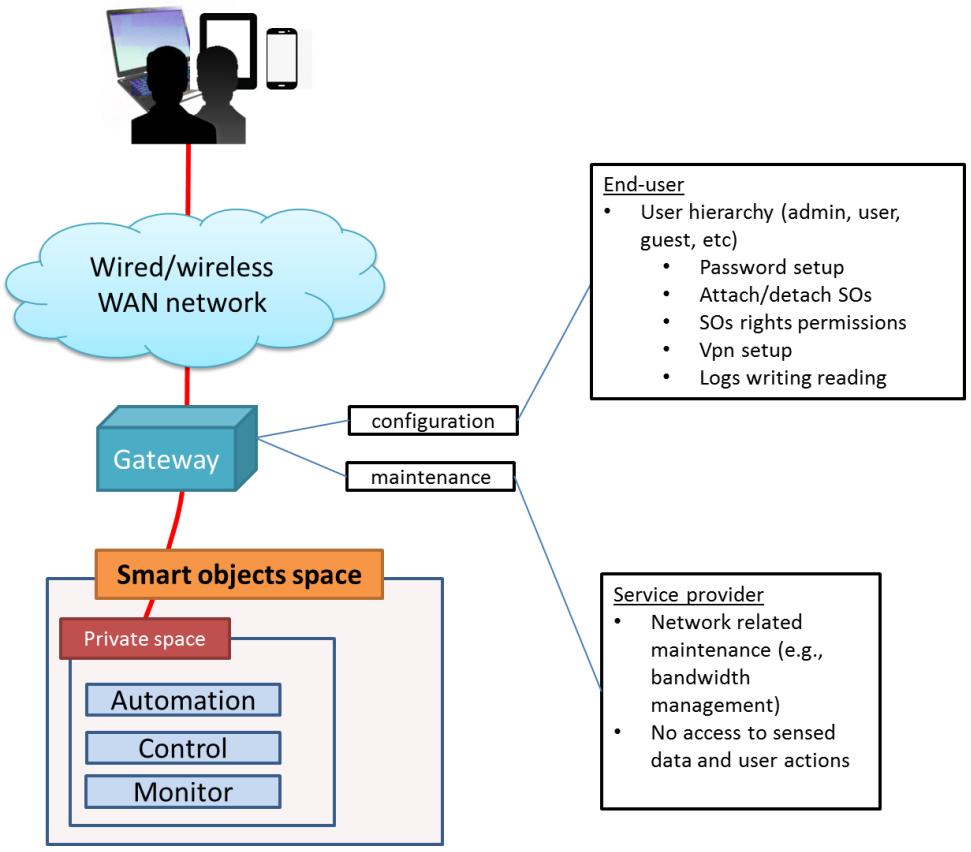

Figure 19: The home energy management use-case UC-I1.

(b) UC-I1 sub use-case 2: Public buildings and private houses/apartments with shared spaces

This special case considers the energy management of apartment buildings that also have some spaces that are shared within the residents of the different apartments. In this case, the monitoring and management of the shared spaces must be very carefully designed, since the monitoring data can be used for extracting presence/location information for the residents. For example, if at one apartment building the lights on the 3rd floor are on every Tuesday afternoon at 17.00 this means that one resident of that floor is coming back from work at that time. Thus, the energy monitoring data must be considered as privacy sensitive. As a result, to preserve the privacy of the residents, for the shared spaces (e.g., laundry room) only automation services for energy savings purposes can be envisioned. For these cases the activity information of the SOs installed at the shared spaces should be private and not accessible by anyone, except from an administrator of the building. A similar case regards the public buildings have private spaces (e.g., offices), where the end-user may be able to set up automation services for energy management, monitor the environment and take specific actions. For shared spaces in public buildings the use-case under consideration envisions only automation services for energy savings purposes. For these cases the activity information of the SOs installed at the shared spaces should be private and not accessible and it should be possible to link them with specific persons or actions (Figure 20).

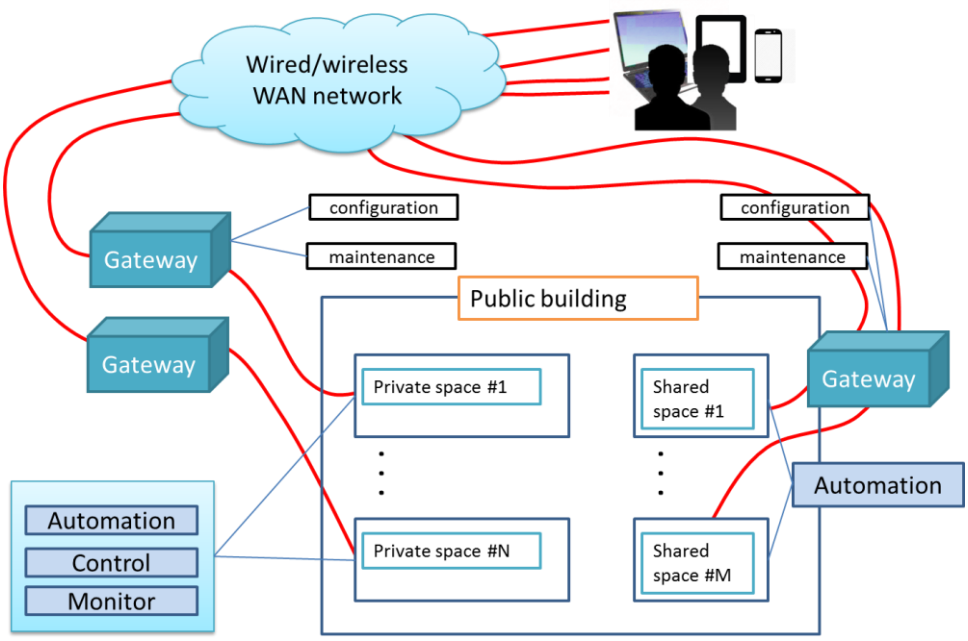

Figure 20: The energy management use-case UC-I1 for public buildings or houses/apartments with shared spaces.

The wireless air interfaces that will be employed plays a critical role, since they determines several parameters, such as energy efficiency, security of data transmissions, privacy, scalability, transmission range, etc. The wireless technologies that could be used in the energy management use-case include:

- IEEE 802.11 (WiFi). WiFi is one of the most popular and widely used technologies for wireless air interfaces, offering high-speed data transmission and relatively strong security. Nevertheless, the required power consumption is not suitable for battery-powered sensor devices, where the data transmission speed is not of a great importance. WiFi implements two main security mechanisms: (i) the Wi-Fi Protected Access (WPA) and (ii) the Wi-Fi Protected Access II (WPA2), which are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

- IEEE 802.15.4 (ZigBee) [73]. ZigBee is a low-power, short distance wireless communication standard designed by ZigBee Alliance based on IEEE 802.15.4 Low-Rate Wireless Personal Area Network. It uses the license-free ISM bands either 2.4GHz or 868/915 MHz. It allows unicast, broadcast, and groupcast messaging in ad-hoc self-organized networks. Security in ZigBee networks includes a hand-shake protocol to confirm the correct delivery of packets. But furthermore, ZigBee standard includes security aspects in each layer, at network layer for network command frames and also at application layer for Application Support Sublayer frames. It also describes two security modes:

    - Standard Mode. Based on two network keys, application security via network key and the ability to switch these keys. Optional use of Application Link Keys for pairs of communicating devices at the application layer.

    - High Security Mode. Implemented only in ZigBee Pro devices, it is composed by two network keys, separate Link Keys for pairs of communicating devices at application layer. Master Keys with the Trust Centre for key transport and key establishment,

and also the ability to switch network keys. It provides mechanism for entity authentication between all pairs of communicating devices within the network.

2.3.5 Stakeholders

The key players that are involved in the use-case fall in three broad categories: Public, Private and Commercial. The main benefits of the use-case in relation to the different players are described in Table 18.

Table 18: UC-I1 stakeholders and expected benefits.

Smart transportation stakeholders	Expected benefits
Public stakeholders.	Municipalities/Governments. Energy management of public buildings would radically increase their energy efficiency and hence would reduce public expenses. Citizens are also expected to benefit from these energy savings with lower city taxes.
Commercial stakeholders.	Utility companies. The utility companies can greatly benefit by the deployment of energy management systems in buildings, since it gives them the ability to optimally manage the power generation-consumption trade-off, which is directly related to the operational costs. Moreover, they can provide services with higher quality, e.g., predict massive peak demands and avoid black-outs Telecom operators. The ICT that is required for realizing the Smart Cities concept and the energy management systems offers many opportunities to telecom operators, stemming from the need for specialized communication techniques between devices and systems for better, reliable, and secure power delivery and improved customer satisfaction. The interconnection of a large number of smart objects and their access to the internet creates new demands and new opportunities. Several utility companies have already made agreements with telecom operators in order to replace their private networks with those provided by the operators in order to improve their reliability and reduce the maintenance costs. Moreover, TP could be involved in the cases where i) devices are contacting the user for alarms via mobile calls/SMS, which may cause network congestion (ii) QoS is essential for emergency calls via the IP network. Smart device vendors. The realization of Smart Cities requires by definition the existence of smart devices, which may range from simple smart sensors and measuring devices to smart appliances. Different types of SOs vendors can exist. For example, standalone SO manufacturers could provide end-users with those devices to turn any physical object that consumes energy into a SO. Another example would be home appliance manufacturers that embed that type of SOs on energy consuming devices for enabling smart energy management. Hardware installers and maintainers. The installation of the RERUM system in public buildings and houses, as well as their maintenance is expected to benefit

	this category of stakeholders. Service providers**.** The energy management systems pave the path for new services, such as energy savings services that are based on the efficient processing of the measured data.
Private stakeholders.	End users**.** The benefits offered by the smart energy management systems, such as energy and money savings, remote monitoring and security make them attractive to individual customers.

Table 19: The roles of the stakeholders in UC-O1, sub use-case 1.

		Operation		
		Automation for energy management	**Monitoring**	**Actuators controlling**
Stakeholder		**Stakeholder's role**		
Client (Administrator)	Users permissions	- Full access to gateway and SOs configuration - Creation/deletion of user accounts with specific permissions - Installation of new SOs - Reading SOs information and log files - Creating/modifying/deleting automation policies	The same as in the automation application plus: - Modifying users permissions about allowed monitoring activities	The same as in the monitoring application plus: - Modifying users permissions about allowed **actuator** controlling activities
Client (Limited user)		No permissions	-Reading monitored data from allowed SOs.	- Programming and controlling specific actuators
Service provider		In case that the application server is hosted by a SP: - The SP has access to the volume of stored data for maintenance purposes.	The same as in the automation.	The same as in the automation.
Telecom provider		The TP is able to control the transmission bandwidth and other transmission parameters from the gateway to the access network, in the case that the application may cause abnormal network operation.	The same as in the automation.	The same as in the automation.

2.3.6 Popularized example

A typical winter day for a family living in a house with energy management is summarized in Figure 21. The HEM use-case involves two main categories of actions that serve the optimum energy management: (i) the cooperation of SOs, which exchange information in order to make decisions about the operation of the devices and the status of physical objects and (ii) the intervention of humans who can program, control and affect the decision making of the SOs. Considering an example in the first category, a smart window which is in status “open” could cooperate with an operating air-condition device and decide whether to turn-off the air-condition or close the window. These types of interactions serve the ultimate goal, which is the optimum energy management. Furthermore, the operation of the SOs is adapted to the end-users’ habits and activity patterns. For example, the smart water heating device can learn (e.g., with the help of other motion-detection SOs) that it should start heating water at a specific time, since the user is expected to use the water soon.

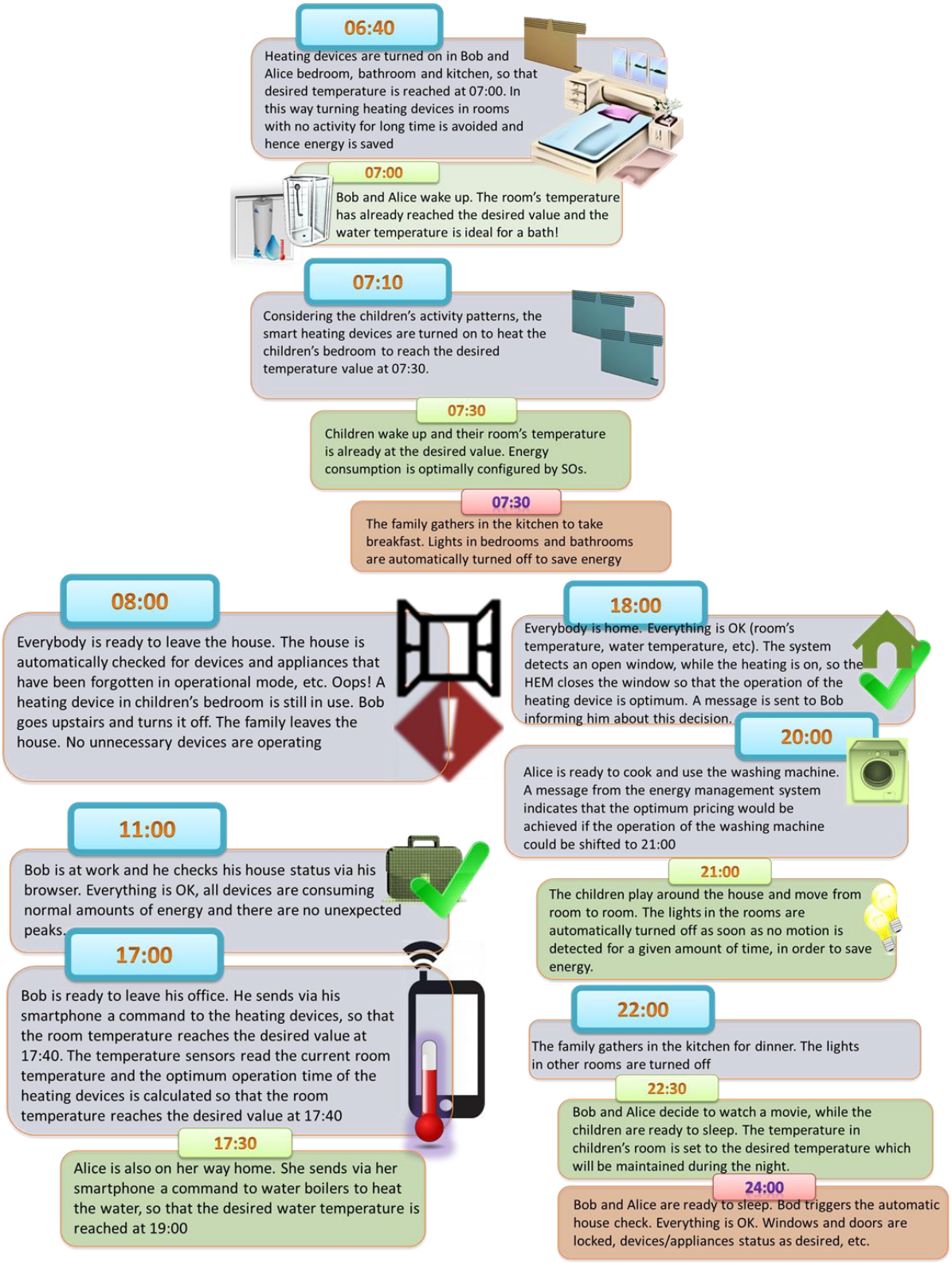

Figure 21: A popularized example for the home energy management use-case.

2.3.7 Use case KPIs

The evaluation of the performance levels of the use case and the alignment with the objectives will be performed against the Key Performance Indicators (KPI)s that are shown in Table 20. This preliminary table will be refined in the deliverable D5.1, which aims at defining the methodology for evaluating the use cases at laboratory experiments and real world trials.

Table 20: KPIs and performance metrics UC-I1.

KPI Nr.	Title	Performance metric
UCI1-KPI_1	Energy savings for high energy consuming devices	% of previous energy consumption for same operation scenario
UCI1-KPI_2	Total energy savings of the household – reduction of the energy related expenditures	% of previous energy consumption for same operation scenario
UCI1-KPI_3	Total energy savings due to habit awareness (understanding people routines and habits, detecting malpractices and optimizing saving policies, etc.)	Cost reduction (%) for the same operation scenario
UCI1-KPI_4	Flexibility in measuring different related factors (e.g., electrical energy consumption, temperature, etc.)	Number of different monitored/sensed factors
UCI1-KPI_5	Network reliability and failures	Connectivity outage probability for devices/sensors
UCI1-KPI_6	Always on	% of system downtime
UCI1-KPI_7	Reliability of alarming	Probability for false alarm (negative false and positive false)
UCI1-KPI_8	Privacy protection	Possibility to extract inhabitants patterns of usage of appliances, possibility to identify if an inhabitant is at home at a specific time
UCI1-KPI_9	User acceptance	Percentage of users acknowledging the usefulness of the application
UCI1-KPI_{10}	Data availability	% of lost data due to network failures (congestion, collisions, interference) or attacks (DoS, manipulation) or device failures
UCI1-KPI_{11}	Service QoS	Improvement in the QoS of the provided services by the system
UCI1-KPI_{12}	Network connectivity	% of time the devices are connected to the system and send data
UCI1-KPI_{13}	Scalability	Number of devices connected to the household system without degrading its performance

2.4 Comfort quality monitoring (indoor use-case, UC-I2)

2.4.1 Introduction

The purpose of this UC is to provide measures for the quality of life in indoor environments (the home comfort). Despite the fact that the comfort may seem to be an abstract term, different studies corroborate it's relation to our quality of life [75] and try to indicate subjective parameters in order to be able to measure and evaluate it. To this end, comfort quality will be associated mainly with the indoor ambient temperature and relative humidity, noise, light and air quality, especially during rest time.

This UC aims to provide tools to improve the quality of life of the citizens, getting real-time data about these parameters, programming alarms when these are out of certain bounds and creating graphs for historic data and trends. The Comfort Quality Monitoring indoor UC could be deployed in houses, offices, gyms, supermarkets, restaurants, etc., and in general in any place people spend their time.

2.4.2 Scope and benefit

The indoor comfort quality monitoring use-case aims to let end users perform the following actions:

- Get indicative measurements of air quality in their homes.
- Study the effect on air quality when they take actions to improve it, like airing out the rooms in the morning for a few minutes.
- Detect isolation problems in their houses and become aware of any kind of outdoor pollutant infiltrating their homes degrading thus their quality of life.
- Manage the indoor comfort actuators, such as air conditioning systems, in a smarter way after assessing the exact comfort situation on different parts of the house through monitoring.
- Monitor the comfort (the air quality and the temperature/humidity) in museums, art galleries and other areas with specific requirements for environmental conditions.

2.4.3 Key challenges

The goal of this use-case is to provide environmental information related to indoor air and comfort quality to the interested parties. The use-case includes mainly the design and development of a wireless network of SOs that will be deployed in indoor places. The network has to be provided with security, privacy, and reliability by design mechanisms, ensuring reliable operation, trustworthy exchange of information, and optimum network operation.

The SOs will connect to an application server (either within the indoor environment or in an external trusted third party) where the information gathered by the sensors (e.g., air quality, noise, EMF radiation, ambient, and security) will be stored and used by the citizens to check the status and the historical trends for all the indicators measured. In case of actuators, the platform will be also the tool for the citizens to manually control them.

The end-users will have access to the collected data through the direct connection with the application server, without the need for contacting directly the SOs. The server should have access control mechanisms that would define for each user the information that can extract in order to ensure security and privacy. The server should also provide the users those mechanisms to remotely control and, ideally, program the behaviour of the actuators in the UC (e.g. switch on the air conditioning system when there is in the house certain average temperature, or sound an alarm when there is a security issue).

Cost and power consumption constraints are also major challenges, since comfort quality systems should involve simple, low-cost and minimum power consumption sensors. The accuracy of the

measurements is of high importance in order to identify potential hazardous situations and for raising alarms and contacting the end users if needed.

2.4.4 High level overview and network components

In this subsection the high-level view of the comfort quality use-case is presented. In this context, this subsection aims to identify:

- The key components for realizing this use-case
- The logical relation between the components and the basic functionalities
- The stakeholders and their role in this use-case.

In this UC, the main goal is to measure the comfort quality in indoor environments and this relies on monitoring the following physical entities:

- **The rooms of the indoor environment (or the apartment/building as a larger entity)**, the quality of which is defined by the following attributes:
  - the concentration of CO in the air, related to gas combustion and fires, and the concentration of CO_2 in the air, related to the refresh of the indoor atmosphere,
  - the concentration of Particulate Matter in suspension (PM_{10}, $PM_{2.5}$) and VOC, i.e., organic compounds related to smells,
  - the EMF radiation, as wide-band as possible but, if not, preferably measuring the microwaves band; self-radiation measurement will be avoided **[77**]
  - the noise, i.e., L_{Aeq}, equivalent continuous sound level, A-weighted, the most used parameter to measure noise, also related to EC environmental directives, intending to detect the acoustic isolation from the outdoor noise; the integration period is to be decided in the future. Other additional related parameters (like L_{SPL}, L_{AT}, L_{Apeak}, etc.) [75], ideally always keeping the A-weighting.
  - ambient, which provides information for the temperature and RH, usually both things measured with a single sensor, as key indicators of indoor air conditioning performance, and the light, to be measured (especially) during resting time.
  - Smoke and fire; maybe in the case of fire we could use a combination of CO, temperature and RH, but we will use also a particle sensor to detect smoke. These attributes are related to security and safety.
- **Objects** within the rooms, i.e. home appliances, doors and windows are also Physical Entities and the SOs are attached to them or monitoring them for serving several user applications, i.e. one SO may monitor the status of the window, so that when the temperature in the room is very high it will open the window to let the breeze cool the room.
- **People:** Similar to the Home Energy Management use-case, the existence of a person in a room could also be considered as an attribute of the room. In any case, this information can be used for decisions related to improving the comfort quality. However, different people have different needs in terms of air and comfort quality, so the system should be able to identify who is in a room at a specific point in order to act according to his needs. For example, an elderly person or someone with respiratory problems has specific requirements about the air quality, while this may not be the same for a person that needs higher humidity in the room.

Furthermore, it will be possible to add actuators, mainly related to the parameters that are being measured, like air conditioners control, thermostats, alarms, blinds, lights, and domotics in general. A high level overview of UC-I2 is depicted in Figure 22, while the key network components are summarized in Table 21.

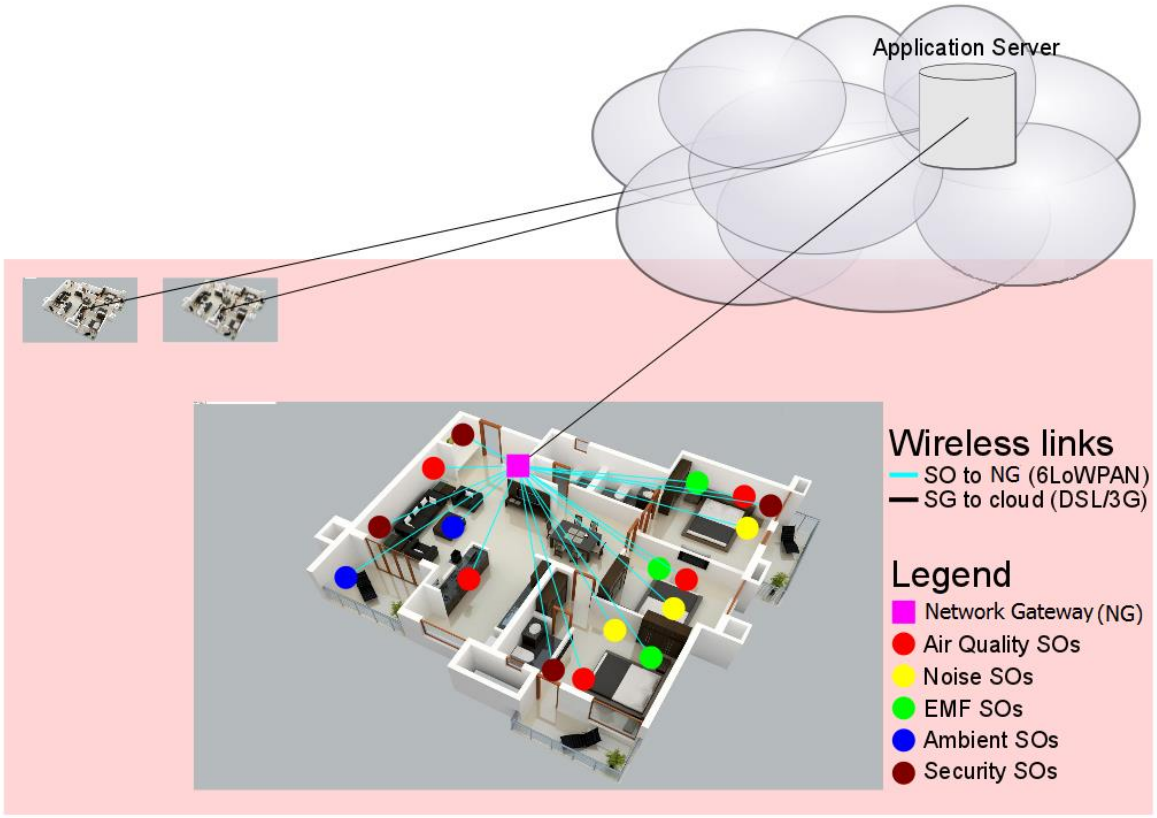

Figure 22: The overview of the comfort quality use-case.

The key network components are summarized in Table 21.

Table 21: UC-I2 main components.

Component	**Description**
Sensors	Converts physical parameters into electric ones in order to be able to measure them using electronic based systems. The measurements will be digitalized to send them through digital communications systems and protocols. See Table 22 for further details on sensors used in UC-I2.
Smart Objects (SOs)	Different nodes communicating in a star, tree, or mesh networks will be installed into buildings to gather information from the sensing elements they have on board. SOs communicate mostly wirelessly, using 6LoWPAN over 802.15.4 or wires through Ethernet connectivity. Most of the SOs are powered directly by plugging them on into power supply net wall sockets and, in those cases where this is not feasible, they are powered by batteries, ideally rechargeable ones, requiring a regular maintenance, replacing or recharging once they start to be empty. The same plugs used to power the SOs are also used as supports for the devices.

	Smart Objects are composed of: • An RF 802.15.4 interface. • A CPU (a micro-controller) managing the 6LoWPAN communication stack and getting measurement data from the sensors. • One or more sensors/actuators connected to the CPU, though analog or digital interface, depending on the sensors. • A power supply, sometimes directly from the $220V_{AC}$ plug, sometimes with removable or rechargeable batteries. The use of more than one sensor or **actuator** per node could only be justified to reduce the number of devices connected in the user's home.
Actuators	The SOs could also actuate to the different systems already present in the building to control the comfort, namely: • Doors, windows, blinds and curtains. • Alarm bells. • Lights and net plugs. • Fire alarm and sprinkler. • Door locks. • Air conditioning/heating systems
Network Gateway	A single gateway per home is used to send the gathered information on the 802.15.4 network to the application server, which could be placed either within the house or at a trusted third party (accessed through the internet). The gateways have an 802.15.4 interface to connect with the SOs and, on the other side they will connect with the application server using Ethernet or WiFi. When the application server is located outside the home network, the gateway may use application server the building Internet connection, likely a DSL router to connect to the server. The gateway is mainly responsible for maintaining the security, privacy, and reliability when forwarding the data to the application server.
Application server	A software will run on an application server providing end-user with a graphical interface giving access to raw data, graphs, queries, setting-up of thresholds and transmission of alarms, etc. The application server can be located either within the home/building network and owned by the user or it could be located at a server of an outside trusted company. In the latter case, the connection between the gateway and the application server should be performed over a Virtual Private Network (VPN) to ensure the privacy and non-disclosure of data.

Table 22: Sensor types for UC-I2.

Sensor	Sensing elements	Connectivity	Description	Common Uses
Air Quality	CO CO_2	Wireless	Measures the indoor key air compounds (mainly related	Determinate an air quality index and detect abnormal odor

	VOC		to combustion and odor)	
Noise	Microphone	Wireless	Measures the noise level with A-weighting, peak, average and daily distribution	Control the noise levels in order to keep under the comfort standards
EMF	EMF sensor element	Wireless	Measures the electromagnetic radiation	Detect abnormal EM radiation
Ambient	Temperature RH Lux meter	Wireless	Measures the ambient conditions	Detect abnormal indoor temperature (also for a potential fire) and excess of light indoor during the rest time
Safety and Security	PM_{10} Infrared	Wireless	Detect smoke (as a potential fire indicator) and presence (heat in movement)	Detect a potential fire and unexpected presence of people in the house

2.4.5 Stakeholders

The key players that are involved in the use-case fall in three broad categories: Public, Private and Commercial. The main benefits of the use-case in relation to the different players are described in Table 23.

Table 23: UC-I2 stakeholders and expected benefits

Smart transportation stakeholders	Expected benefits
Commercial stakeholders.	Vendors and suppliers. Specialized companies, capable to develop hardware sensors for the measurement of indicators related with air and comfort quality. Network providers. To communicate between gateways and an external application server is necessary to use an external network provider. In cases that it is not possible to install the application server within the house, the need for a communication service provider, mainly wired DSL company is evident. In case DSL is not possible, cellular communications are also a choice, so respective companies can also be a stakeholder. Software platform application developers. The software platform to which the SOs will send all the gathered information and on which the users will connect to get visualized results and alarms. Hardware installers and maintainers. The installation of the RERUM

	system in public buildings and houses, as well as their maintenance is expected to benefit this category of stakeholders.
Private stakeholders.	End users. The citizens living in the house where the use-case is deployed. They will actually be the direct and mostly benefitting stakeholders. They will get a system to measure the comfort of their home. With this, they could take actions (for instance, ventilate the room during certain times per day, reduce temperature on heaters in winter and increase air conditioning in summer without losing performance; these can be combined also with home energy management use-case) to improve that comfort and measure the results of each action in real time; examples such actions are: ventilate the room during certain times per day, reduce temperature on heaters in winter and increase air conditioning in summer without losing performance; these can be combined also with home energy management use-case.

The roles of the indoor comfort analysis stakeholders are highlighted in Table 24. SOs send information (pre-processed data and maintenance information) to the application server via the gateway. The end users could view, trace and interpret that information directly on the server via Internet access. The server is also responsible of triggering the communication with the end users in case of alarms.

Table 24: The roles of the stakeholders in UC-I2.

		Operation	
		Environmental contamination monitoring	**Weather station**
Stakeholder		**Stakeholder's role**	
Client (Administrator)	Users permissions	- Full access to gateway and SOs configuration - Creation/deletion of platform user accounts with specific permissions and information access - Admission of new SOs	
Client (Normal user)		View, trace, interpret and process information on the application server platform. Also configure and get alarm triggers through the platform	
Client (Limited user)		View pre-processed information on the platform	No access available
Service provider (SP)		In case that a SP hosts the application server, instead of running it locally on a server into the house, it may have access to the volume of stored data for maintenance purposes but absolutely not to the data itself, which will be all private.	
Telecom provider (TP)		In case the data is going to be sent to a SP, the TP will be able to control the transmission bandwidth and transport the information	

	from the gateway to the **Access Network** towards the application server, but must not have access to it. The purpose is to avoid any improper operation of the access network (e.g., network congestions).

2.4.6 Popularized example

These are some short descriptions of different situations this use-case could cover:

- Pollution at home:
  - Pollution is not only a problem in the streets of highly populated cities but also in the houses and flats of those cities.
  - In the specific case of a person who suffers from a respiratory disease, like asthma is very important to keep under control the air quality within their houses, monitoring it and acting whenever necessary to improve the environmental conditions.
  - Some devices including sensor elements for air pollution measurement are installed in the homes; this will keep the people informed (through the Internet) about the status and trends of some air quality indicators. The UC will also give users access to data history.
  - The indoor measurements combined with outdoor ones will also be very useful for the part of the population who suffers from respiratory problems.
- Rest time quality:
  - Something as simple as the rest during the night has a lot of effects on human health, including effects on energy, intellectual skills, etc.
  - The basis of a restorative rest is a quiet and dark environment.
  - With a network of devices measuring noise and ambient light, users could track, and therefore take measures, to improve their own rest quality.
  - Again, correlating outdoors noise measurements with indoor ones, could help users to detect a bad noise isolation problem on their house construction.
  - In spite the fact that the effects of EMF radiation on the health have not been scientifically demonstrated (even though various research groups are studying that), the EMF radiation during the rest can also be measured.
- Set the right temperature/humidity on the house/buildings:
  - Setting a wrong temperature at home, apart from the obvious consequences of energy consumption, also targeted on UC-I1, could have effects on human health like colds, low blood pressure, etc.
  - SO that will measure temperature and relative humidity to know (also remotely) in depth the climate at home and all its rooms.
  - With this, the users could improve the climate control. If necessary, some SO will be used to control also the climate actuators (heaters, air conditioners, etc.) to allow a totally remote system.
  - High temperature and humidity can have severe effects on artefacts in Museums, art galleries, as well as on PCs in server rooms, so the environmental conditions in such closed areas should be very carefully monitored and managed.
- Improvement, in a very basic way, of the safety in buildings:
  - Some basic sensors related to safety, such as fire sensors and presence sensors, can be installed within buildings and remotely monitored and controlled.
  - Using the application server, alarms could be arisen whenever a potential fire situation could exist.
  - Also, some presence sensors could let users know if there is someone in the house. The user could notify the application server when they are going in or out from home

and the application server could automatically generate an alarm if there is someone at home when all members had notified they are out. Please note that in this specific case privacy is a critical issue.

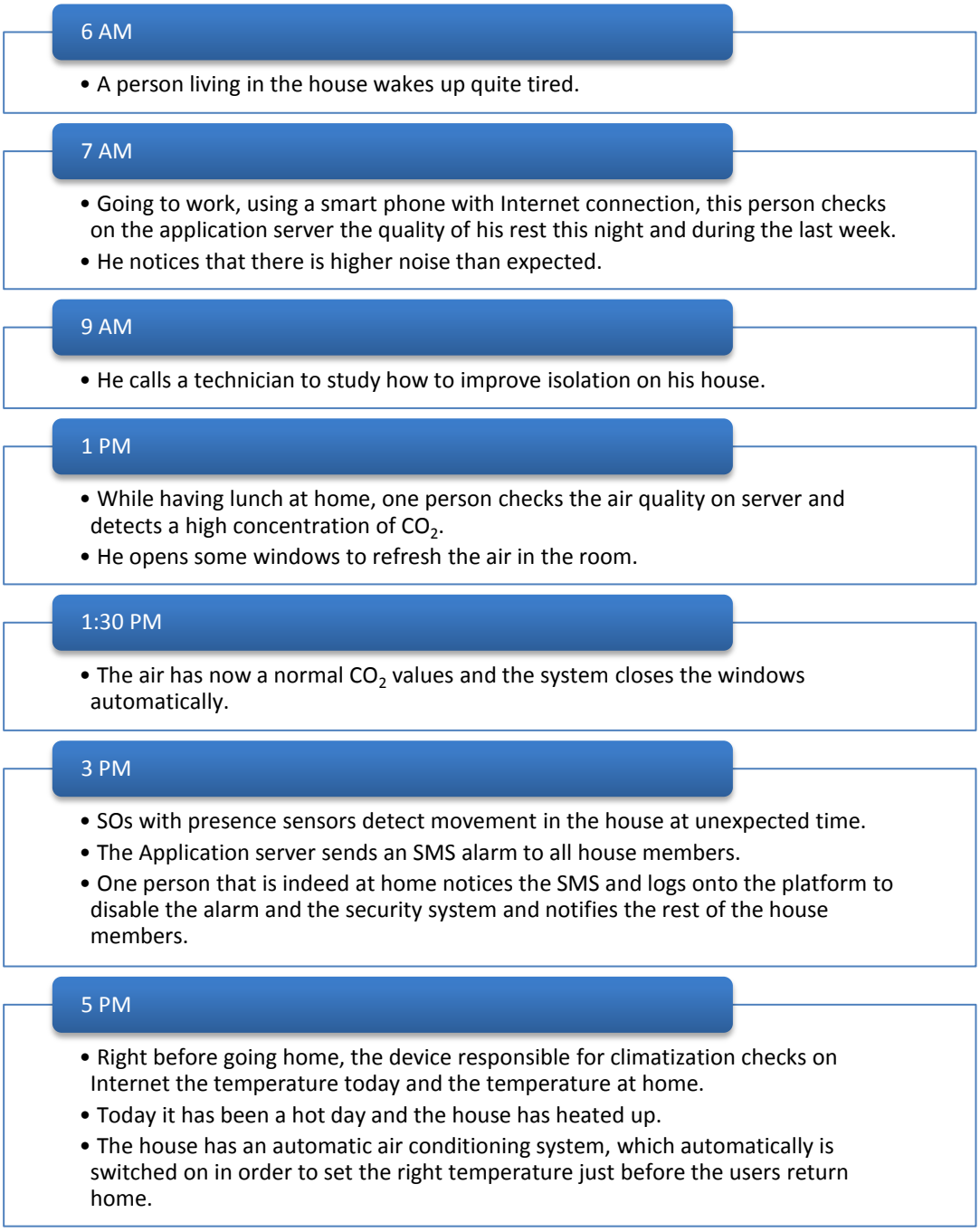

Figure 23: A popularized example for the comfort quality use-case

2.4.7 Use case KPIs

The evaluation of the performance levels of the use case and the alignment with the objectives will be performed against the Key Performance Indicators (KPI)s that are shown in Table 25. This preliminary table will be refined in the deliverable D5.1, which aims at defining the methodology for evaluating the use cases at laboratory experiments and real world trials.

Table 25: KPIs and performance metrics UC-I2.

KPI Nr.	Title	Performance metric
UCI2-KPI$_1$	Total energy savings due to habit awareness (understanding people routines and habits, detecting malpractices and optimizing saving policies, etc.)	Cost reduction (%) for the same operation scenario
UCI2-KPI$_2$	Citizen approval rating	People endorsement and approval rating compared to the current, evaluation on public places, evaluation of the information provided
UCI2-KPI$_3$	Flexibility to measure and federate different parameters	Number of monitored variables and events
UCI2-KPI$_4$	Reliability of the data	Accuracy of the readings per indoor deployment compared to conventional ones provided by weather stations or weather casts in the area, likely centralized or general
UCI2-KPI$_5$	Health improvement	Analysis of pollutants measured with respect to not having sensing at all, for example noise and CO/CO2 levels, humidity and temperature conditions vs. potential flu outbreaks
UCI2-KPI$_6$	Home security improvement	Improvement in the possibility to identify physical intrusions in the house
UCI2-KPI$_7$	System usability	Evaluation of the easiness to use the system by the citizens either as simple users or for setting up their own advanced services
UCI2-KPI$_8$	Comfort quality	Improvement in the comfort of the inhabitants by automating the procedures of the system
UCI2-KPI$_9$	Privacy protection	Possibility to identify if a home owner is at home at a specific moment by assessing the traffic patterns of the system
UCI2-KPI$_{10}$	User acceptance	Percentage of users acknowledging the usefulness of the application
UCI2-KPI$_{11}$	Data availability	% of lost data due to network failures (congestion, collisions, interference) or attacks (DoS, manipulation) or device failures
UCI2-KPI$_{12}$	Service QoS	Improvement in the QoS of the provided services by the system
UCI2-KPI$_{13}$	Energy consumption	% of increased energy consumption of the household due to the consumption of the devices
UCI2-KPI$_{14}$	Network connectivity	% of time the devices are connected to the system and send data

3 Threat analysis

In this section we conduct a threat analysis for the four use-cases discussed in Section 2. The goal is to analyse a system that is currently under design, rather than an operational deployment. This poses limitations in terms of the scope of this analysis, as well as in terms of the choice of methodology. The idea behind this threat analysis is to identify: (i) what are the basic security and privacy issues in the IoT deployments for these four use-cases, (ii) which are the assets that need to be protected and (iii) what type of attacks can be realised in such deployments. This threat analysis will be the key foundation for extracting the requirements for the RERUM system architecture, in order to reflect the concepts of security, privacy and reliability by design.

Generally speaking, there are at least three approaches to systematically understand and categorize threats: (i) attacker-centric, (ii) software-centric, and (iii) asset-centric.

The ***software-centric approach*** can be used when there is software (SW) to perform penetration testing, static analysis, dynamic analysis (i.e. differential debugging), etc. Since the RERUM software has not been defined yet, a software-centric approach is considered out of this deliverable's scope.

Asset-centric threat modelling starts by making an inventory of the IT-assets of a system which could be hardware (HW), software, processes, and data. In business applications this covers business relevant information about users, clients, production plans, strategy, organization, and others. In communication systems this includes routing tables, performance monitoring processes, infrastructure data and processes. In IoT applications, all data that are relevant for the provisioning of the services and in particular the sensitive personal information of users can be considered as "assets".

The ***attacker-centric analysis*** investigates the possible threats posed by an attacker and his actions.

We will be restricting ourselves to discuss the threats to **IT-assets than can be tackled by IT means**. This means, in particular, that the physical protection of hardware assets is not within our scope. In general it is difficult to provide IT-security mechanisms to help to protect HW as such. This may be the case when a piece of HW has embedded a device that can be located if stolen. If an attacker breaks physically into some HW to steal some cryptographic keys or administration information, then the asset to be secured is not the HW itself, but the keys or data the attacker wants to compromise. The information may be sometimes secured using combinations of physical security and IT security, like a trusted computing module, or data encryption and storage of the encryption key in a tamper-resistant device.

Our threat analysis follows a **three-step approach**. We begin by an **asset-centric approach**, whereby we conduct Confidentiality, Integrity and Availability (C-I-A) analysis on identified assets. Subsequently, we conduct an **attacker-centric analysis** by looking at specific threats against Authentication / Authorization / Accounting (AAA). Lastly, we look at **privacy-related threats**. Due to the fact that we are conducting threat analysis of a system under design, it is very difficult to evaluate the likelihood and severity of individual risks and as such we refrain from conducting a full-fledged risk assessment.

In this section, we begin by narrowing down the scope of this threat analysis, in Section 3.1. Subsequently, we document an attacker model in Section 3.2, followed by a description of our methodology in Section 3.3. IT asset identification is driven by the use-case descriptions in the previous section and is documented in Section 3.4, followed by an analysis of data flows in Section 3.5. The three following sections focus on C-I-A threats (Section 3.6), AAA threats (Section 3.7) and Privacy threats (Section 3.8). Lastly, examples of the threat analysis are given for RERUM's use in Section 3.9.

3.1 Scope and Context

In this section we narrow down the scope of this threat analysis in terms of the types of risk sources under consideration. We also set some terminology around the types of network data flows which will be considered in this study. These notions will be used subsequently for the identification of IT assets.

3.1.1 Risk Sources

As discussed above, this study focuses on IT assets and more specifically on threats which can be tackled through IT means. We identify the following risk source categories:

- **Human** risk sources, such as theft, loss, accidents, user errors, and attacks initiated by malicious users. Among those risk sources, this threat analysis only aims to identify intentional malicious attacks. All other human risk sources are out of scope.
- **Non-human** risk sources can be due to natural phenomena, such as flood or fire, or device failures. Non-human risk sources are also out of scope.

Even though some risk sources are out of scope as identified above, it is possible that some IT protective mechanisms will also be able to mitigate the impact of some of those risks. For instance, secure storage of cryptographic keys and user data at rest will also mitigate the negative impact of device theft, which is not explicitly within our scope.

3.1.2 Data Flows

For the use-cases described in this deliverable, we can identify the following classes of network traffic, subsequently referred to as “Data Flows”:

3.1.2.1 Control Plane Data Exchanges

These are data flows used to monitor and control the use-case deployment’s behaviour. This can include network management functionality (in a traditional ISO FCAPS [78] context), routing control messages, neighbour discovery messages, link-layer associations, TCP session establishment handshakes, network management requests and responses (e.g. "Enter sleep mode for a specific duration" or "Switch to RF channel 11"). Control plane data flows are normally invisible to end users and of little interest to them. We will onwards use the term “control traffic” as an alternative name for data flows of this category.

3.1.2.2 Data Plane Data Exchanges

These involve application layer network traffic, which is visible and of interest to end users, even in cases where they are not necessarily user-initiated. We will onwards use the terms “application traffic” or “user traffic” to refer to this class of traffic, with the two terms being equivalent. Some examples include: Temperature readings transmitted from sensor nodes; actuator state queries sent by a user to a node and the corresponding responses; actuator state change requests, followed by a response if applicable.

Throughout this document, we make a distinction between *data in transit* and *data at rest*. The term “data in transit” is used to describe data being transmitted over the network, while the term “data at rest” describes data stored at a device. In the case of data in transit over a network, RERUM will provide security- and privacy-enhancing mechanisms for end-to-end communication, for example between an SO to an application server. Part of this communication takes place over network infrastructures outside RERUM’s influence, such as the Internet or an ISP’s infrastructure. Furthermore, the exact technologies used to deploy such infrastructures are unknown. For these reasons, we do not attempt to discuss threats against the external network infrastructures in this section.

3.2 Attacker Model

RERUM will expose several assets to a wide variety of devices and entities, which may introduce many different types of errors or threats into the system. IT security is concerned with the protection against malicious entities, not against users or systems that inadvertently and involuntarily compromise the integrity of data or processes, and not against errors due to channel noise, introduced during transmission from the source to a receiver. For those areas there are particular methods that help not only to detect such situations, but also to prevent or correct such problems.

We call *attackers* those malicious entities that try to read confidential data or try to modify data relevant for the correct service delivery. There are many types of attackers that can be differentiated by their respective capabilities to retrieve information, their position regarding the system (e.g., outside or within a certain network), their motivation, as well as the layer(s) of network protocols to which they have access, which are exploited and used as an entry point by the attacker.

In order to simplify the analysis and obtain a useful model of the attacker, a restricted worst-case situation is chosen:

- **"Worst-case"** refers to an attacker that is highly motivated, has access to all non-encrypted data flowing in the network and to well-known or public information and that has physical access to all communication channels between different nodes, at all layers of the network. The rationale for this choice of a strong attacker is twofold: on the one hand, such an attacker is not totally unreasonable, or at least any weaker attacker is probably too restrictive. On the other hand it subsumes all other attackers in the network. This attacker is known as the Dolev-Yao attacker [79].
- On the other hand, we need some restrictions for the attacker: If the attacker is able to break the cryptography of the system, then there is absolutely no protection against him. He would be able to retrieve the secrets of users and entities and therefore to circumvent the authentication mechanisms. This will allow him to masquerade users and modify data in transit in any way he chooses. Therefore, it is customary to assume that the cryptography used is secure and that the implementation is correct. Similarly, and particularly at this stage of the design, it is customary to assume that the security mechanisms planned will be securely implemented. This is particularly true because at this stage there are no mechanisms implemented that one could test to evaluate their efficiency.

In more detail, following the proposal of Pfitzmann & Federrath [80], we make an additional assumption besides the attacker's capabilities and motivation: the attacker's strength toward security and privacy mechanisms, and assumptions about the mechanisms themselves, respectively.

1. A flawless implementation of security mechanisms. This assumption is many times unrealistic: security implementations usually *may* contain flaws. But the implementations can be tested for security functionality and for the presence of so-called "common vulnerabilities", which are the ones that attackers can detect without an enormous effort. The assumption can be formulated in the following weaker way: The attacker is not able to find implementation flaws of security mechanisms that offer access to assets protected by them.
2. The attacker is not able to guess or break cryptographic protocols, which are considered secure by standardization organizations.

3. Cryptographic protocols are considered public and thus accessible to any attacker targeting a protected asset. This implies that assets won't be protected by secret, proprietary cryptographic solutions.
4. Signature schemes are considered cryptographic protocols; they are flawlessly implemented and publicly known.
5. The attacker is not able to penetrate physical security mechanisms.

The attacker is considered to be either an *external to the system* or a *legal member of the system*. He is able to *actively initiate* or to *passively listen to* communications and data flows in the use-cases. Moreover we assume that he is aware of the existence of assets and entities in the system. He is able to collect information from the system and use it to synthesise any message built upon this information. The information from the system that he can collect is: (i) public information, (ii) the information that he is authorized to obtain if he is a member of the system, (iii) the messages that he can overhear or intercept over the network, and (iv) the responses to queries or requests he is able to formulate. He is, as we mentioned above limited by the constraints of the cryptographic or security mechanism used.

Thus, the attackers we consider are end users or external persons that have access to the premises of the installation or the communication channels. This includes citizens and also, to a certain extent, local authorities, public bodies and their employees or other staff working for them. Of course, the city authorities could misuse the data provided by RERUM to their applications, but this will be outside of the scope of this project.

Other stakeholders are – from a RERUM point of view – considered to be trusted, including in particular:

- **Sensor Developers and Suppliers**, including the developers of the software running on smart objects and gateways,
- **Integrators / Solution Providers**
- **Equipment Installers and Maintainers**
- **Network Providers**
- **Application Developers** and **Third Party Solution Providers**

Those parties, in principle, could insert at different places backdoors or other malicious mechanisms to abuse of the data or functionality of RERUM. Although there are methods to cope with this type of attacks or minimize their probability or impact, we consider this type of attack to be outside of our scope. In other words, all suppliers, vendors and providers are assumed to be trusted and extra mechanisms outside of our scope will be necessary to manage the corresponding risks.

Our generic attacker can be either *active* or *passive*. An active attacker is able to initiate any data flow described in Section 3.5. Thus he is able to modify data packages, block transmissions, resend messages from himself and other participants, and, as a valid member, exploit those cryptographic secrets that are available to him. In his passive role, the attacker is able to listen to and record every communication flow described in Section 3.5. Thus, he is able to capture any transmitted information and subsequently analyse it offline, but he is not considered to actively use that information in his passive role.

The attacker is considered to have *high computational capabilities and high availability of time*, but not enough to break the cryptography or guess the credentials or secrets of the system or entities. The attacker is additionally considered to have *middle to high financial resources*. He is considered to afford special devices if needed, but not enough to masquerade a GSM base station or compromise the standard 3G or 4G security.

3.3 Methodology

In this threat analysis we start with an *asset-centric approach* and identification of a list of IT assets that need to be protected. Once the IT-assets have been determined, they are evaluated regarding the possible threats to their Confidentiality, Integrity, and Availability. Strangely enough, some data may be subject to strong integrity requirements, without being subject to strong confidentiality requirements, or vice versa. Some assets must remain confidential, while perhaps other assets should be available all the time or the moment they are required and/or should only be modified by authorised entities according to the established procedures in the correct conditions and environment. Trying to have all assets to be protected both against confidentiality and integrity threats may render the system to be useless, or at least quite inflexible. A security expert may understand this if he considers, for instance, that a system complying both with a Biba [81] and Bell-LaPadula [82] model may not have different interacting security levels. Notice that changing a small amount of personal data (i.e. the location of some users) or management data may be a nuisance, but the system could have the ability to recover from those problems, while overwriting a very large amount of the same type of data can be difficult to recover from.

After the asset-centric approach, we proceed with an *attacker-centric analysis*. In this second step, possible attackers, their motivation and expertise, the methods they could use and the consequences of their attacks are analysed. The attacker centric approach looks first at the possible goals of an attacker, the actions that could lead him to achieve those goals, and the consequences of those actions. To be specific, in the second phase, we focus on possible threats to Authentication, Authorization, and Accounting.

Note, that by now we have six security properties that we are looking at: Confidentiality, Integrity, Availability, Authentication, Authorization, and Accounting. These six closely correspond to the six properties in the STRIDE methodology of Microsoft [83]. STRIDE stands for “Spoofing, Tampering (integrity threat), Repudiation, Information disclosure (confidentiality threat), Denial of Service (DoS, availability threat), Elevation of privilege”. We give a mapping between STRIDE and C-I-A/AAA later in this section.

Third, we consider *privacy threats*. On first sight privacy threats are mostly related to confidentiality. In some cases, depending on the use of the data, there are also important integrity issues. If an attacker manipulates the personal data of a user, this could have very negative consequences for the data subject, that is, the person to whom the data relate. The confidentiality requirement applies not only to large amounts of data (stealing the personal information of hundreds of users) but also to attacks against single users.

Privacy is a complicated topic, and this is true in particular in settings like the IoT, because the combination of different pieces of information related to an individual may drastically increase what attackers might know about those individuals. In many cases, data thought to be perfectly anonymous might be correlated to other data, say public information, and the result is very sensitive personal information. Examples of this will be given below.

Lastly, we have to state that we do not calculate explicit probabilities or estimate the real costs of possible attacks. We focus on eliciting those vulnerabilities that, if no counter-measures are in place, either have a rather large probability of happening, or would cause a big damage and have a non-negligible probability of happening.

3.3.1 First Phase: Asset Identification and C-I-A Threat Analysis

The first phase is carried out in two steps:

- Step 1: Identify assets that need protection (Section 3.4) and analyse data flows (Section 3.5)
- Step 2: List Threats to C-I-A for these assets

We identify IT assets, such as information and user data, giving also the classification scheme used for RERUM to categorize the data. Later, we also provide a data flow analysis, where we use the classification of the types of data to identify how they are exchanged between the components in each use-case (the components are described in detail in Section 2).

This view allows us to identify for all UCs the relevance of protecting a given type of data and also highlight where each data type will become relevant.

For each identified asset we evaluate what could happen if it is disclosed improperly, if it is modified without authorization, or if it is made unavailable to normal users of the system. Thus, a threat is one of these three types:

1. (C-) **Information disclosure / Loss of confidentiality:** Asset gets disclosed to an unauthorized entity: - What is the worst case? Who should not know this?
2. (I-) **Tampering / Loss of integrity:** Asset gets manipulated (modified) by an unauthorized entity: - What is the worst case? What could happen if this modification is not detected?
3. (A-) **Denial of Service / Loss of Availability:** Asset is not available to entities that need to access it - What consequences can this have?

Looking at the costs of such threats we want to answer the question: Which threats have to be avoided in any case?

To do so, possible attacks are evaluated on the level of the described use cases taking into account possible implementation details. This gives a rather clear indication of the impact of an attack, if no particular counter-measures are met. Intuitively, the risks related to attacks with a high impact and relatively high probability (say, the probability of at least one attack in a period of a few years is not negligible) have to be treated. A treatment of a risk is, in our context, the identification of a security countermeasure (mitigation) for the issue.

3.3.2 Second Phase: Attacker-Centric AAA Threat Analysis

The second phase is the attacker-centric analysis, which lists AAA threats to the previously identified assets. We differentiate these threats from the C-I-A ones, as they also require discussing which roles an entity could possibly have within the UC. Here, we consider what would happen if the UC would not be able to properly enforce needed AAA (Authentication/Authorization/Accounting) functionality.

It is possible to penetrate many systems and to break the security of the basic AAA (Authentication/Authorization/Accounting) functionality. An attacker could manipulate parts of an infrastructure or abuse management information in the system in order to perform one of the following attacks:

1. **(A-) Spoofing an identity, a role, or a member of a group / Breach of Authentication:** Spoofing can take place against any type of identity, for example an attacker may impersonate a different person, a different device, or traffic flow.
2. **(A-) Elevation of privilege / Theft of Authorization:** This can be encountered in systems that define different permissions to different users or device classes. Attackers are malicious users and attempt to gain access to the system with rights higher than those assigned to their class.
3. **(A-) Repudiation / Accountability breach:** Hereby a user takes an action on the system and subsequently wrongfully claims not to have taken said action, with the system unable to prove the contrary.

Again, a treatment of one of the above risks is, in our context, the identification of a security countermeasure (mitigation) for the issue. There are several possible approaches to this, for instance:

- We may require stronger AAA mechanisms. For instance, we may use PKI, which is considered to be stronger than normal passwords, or we use two-factor authentication mechanisms.
- We may require security in depth, that is, redundant security measures, also known as a second-line of defence.
- We may reduce (somehow) the attack surface, for instance by constraining the interfaces.
- We introduce intrusion detection techniques, that allow us to react to critical situation in real-time and avoid damage.

For now, we are only interested in finding out what an attacker could do if he could break any AAA security mechanisms.

To analyse those threats, an attacker approach is used: what can an attacker do to spoof an identity, repudiate an action, or perform an action for which he is not authorized?

3.3.3 Third Phase: Privacy Threat Analysis

In the final phase of this threat analysis we focus on threats against user privacy, which may arise as a result of an attacker's ability to collect, store, use and disclose user personal information. This information can subsequently be used to construct a profile of a user, his habits, tastes, interests, etc. Extensive work has been done to find a concept for proper privacy protection, such as [84] or [85]. There are four fundamental reasons for privacy issues:

- Data can be collected without the user knowledge or consent or in moments or circumstances where he is not expecting his data to be collected or he is not aware of that
- Data can be used for secondary purposes not initially considered
- Data (both during the communication and at rest) can be accessed improperly or without authorization
- There may be errors in storing or accessing of personal information.

For privacy threat elicitation, we refer to the privacy terminology by Pfitzmann et al. [86]. Similar to the previous two phases of this threat analysis, our privacy analysis methodology corresponds to the LINDDUN method proposed by Deng et al. [87], which was designed as the privacy related equivalent of STRIDE.

3.3.4 Risk Assessment

At this stage we are not conducting a threat analysis of a deployed system, but rather of a system under design. Consequently, it is very difficult to evaluate the likelihood and severity of individual risks and as such we refrain from conducting a full-fledged risk assessment. The categories and examples of threats (see Section 3.9) should give a rough idea of the probability and impact of the threats without trying to quantify them more precisely.

3.4 IT Asset Identification

Since RERUM's design is not complete, some crucial infrastructure related IT-assets, meta-data, management, or administrative data have not been defined yet. This includes data and processes related to the infrastructure or security mechanisms we want to implement. This information may include, depending on the design, indexes, routing tables, channel state information, cryptographic keys, configuration tables, management data, semantic models, etc. Manipulating or reading this information leads to serious threats that could create a large damage.

Even though the exact types and nature of meta-data do not appear in the use-cases explicitly and are often independent of the use-case, they are part of our infrastructure. In some cases we know that we are going to require some type of data or information, and we may already anticipate roughly the related threats and some protection requirements.

Also note that dumb hardware, such as sensing elements, is not in our scope. There is a clear distinction between a sensing element and a sensor platform, as discussed in the definitions section at the beginning of this deliverable. The sensing element (which is the hardware that takes the sensing information, i.e. the thermometer) is not an IT-asset, but the sensor platform (the node including the software running on it) is an IT-asset that should be subject to the threat analysis. In the same context, there is a distinction between a "sensing element" and a "sensor reading". As discussed previously, physical protection of non-IT assets, such as protection of sensing elements from physical damage or tampering, is outside our scope. However, physical attacks on hardware could have an adverse influence on sensor readings (data), which are considered IT assets and therefore subject to this analysis. Thus, as an example, incorrect sensor readings are a data integrity breach that can be tackled by IT means and the protection of the system against these false readings is considered within our scope.

From the use-case descriptions, we can identify some IT assets common to all four of them and in a broader sense, common to all IoT applications. Additionally, some IT Assets are not immediately visible in the use-case description, but are likely to form a part of RERUM's protective mechanisms in order to achieve the project's objectives. An indicative list of assets in this category would include RERUM's configuration data and the cryptographic keys used by authentication mechanisms. The exact number, nature, and technologies used to generate and store keys and credentials will be identified during RERUM's later stages.

In the following subsections we describe the IT assets identified from the use-case analysis.

3.4.1 Authentication CREDENTIALS

Authentication credentials are data used for identifying participating entities, e.g., secret keys that allow the differentiation between an administrative or a limited user, or a key used to sign data. Authentication credentials are part of control plane data exchanges.

3.4.2 User Data (U-DATA)

User data can be further broken down into the following categories:

- Sensed Data (S-DATA)
- Actuation Data (A-DATA)
- High-level Application Data (H-DATA)

All user data are part of data plane exchanges, as discussed in an earlier section (3.1.2). The subcategories listed above include the transmission of actual data readings, as well as user queries that may have triggered them. For example, the transmission of an ambient temperature reading is considered U-DATA. The user request that triggered this reading's transmission is also considered U-DATA.

3.4.2.1 Sensed Data (S-DATA)

Even though there are some overlaps across use-cases, the types of S-DATA are largely related to each individual use-case. Examples of S-DATA include:

- Energy consumption measurements both at rest as well as in transit (i.e. electrical energy, water, gas)
- Room, building and important environmental measurements (at rest as well as in transit)

- Safety-related measurements, such as smoke and surface temperatures (at rest as well as in transit), fire and intrusion logs (at rest) and alerts (in transit).
- Air quality measurements (at rest as well as in transit)
- Noise measurements (at rest as well as in transit)
- EMF radiation measurements (at rest as well as in transit)
- Weather related measurements (at rest as well as in transit)
- Ambient measurements, such as temperature and light level (at rest as well as in transit)
- Other indicators, for example those related to industrial activity close to the cities where the pilots will be installed (at rest as well as in transit), could be added upon request of the local authorities
- User requests to get access to sensed data are also considered S-DATA (in transit).

3.4.2.2 Actuation Data (A-DATA)

Data related to the operation of actuators:

- Actuator state (A-DATA at rest)
- Actuator request and response logs (A-DATA at rest)
- Actuation requests (A-DATA in transit) sent by the end user in order to control a high energy consuming device, e.g. turn lights on and off, adjust heating of unused rooms, or to control a home comfort parameter, such as to change a thermostat control.
- Actuation requests (A-DATA in transit) sent either from end users, or initiated automatically, based on user configuration (named 'automation'). For the latter case, the user configuration can include S-DATA as triggers.
- Actuation requests (A-DATA in transit) sent automatically by an application server (see below), based on user configuration. These can be based on triggers or on a fixed time schedule.

Some examples of time-scheduled or sensor-triggered automation scenarios:

- Turn off the light if no motion in the room.
- Turn on air condition if temperature exceeds 26^{o}C
- Set thermostat to 23^{o}C at 6pm

Depending on implementation details, all aforementioned actuation requests with A-DATA in transit may be followed by a response, such as a success or failure indication.

3.4.2.3 High-level Application Data (H-DATA)

Besides the aforementioned data categories, there might be data in some cases, which result from the processing of the sensed data by a system node (which could be the device itself, the gateway or an intermediate node). These data are usually in response to end-user queries and may include metadata about the user, or necessary application parameters, such as the current location of the user, the destination of the current travel, aggregated/average sensed data or alarms after computing some sensed data. These high-level application data (H-DATA) might be more sensitive than S-DATA or A-DATA in specific cases, since they include high-level information. This requires mechanisms for ensuring their privacy and the secure delivery.

3.4.3 Command and Control Data (C&C-DATA)

C&C-DATA are data and metadata used to control, monitor, and manage the system's overall state, in order to ensure correct operation. Based on the RERUM scope identified at the beginning of this threat analysis as well as the use-case definition, we identify the following C&C-DATA:

- EUI-64 identifiers [88] for network interfaces (e.g. IEEE 802.15.4-compliant RF transceivers) on sensor nodes and the gateway.

- 6LoWPAN prefix information used for the communication within a 6LoWPAN mesh
- IPv6 routing tables
- Spectrum/channel usage information/history
- Neighbour Discovery caches
- Application configuration data
- Application version updates

When in transit, these data are part of control plane data exchanges.

3.4.4 Software (S/W)

All software that we consider is running either on SOs or on gateways. The analysis focuses on software components in operation on smart objects themselves, but it excludes network service provider software infrastructure. It also excludes software at the application server. Some examples of software that needs to be protected:

- Software implementing RERUM's security- and privacy-enhancing mechanisms. This may include APIs, interfaces, network protocols, device drivers and other components. These will be specified in detail during subsequent stages of the project.
- Operating Systems: For low-end Smart Objects (e.g. wireless sensor nodes), software implementation can be bespoke, whereby all software components are developed from scratch specifically for the use-case in question. Alternatively, the implementation may take advantage of an embedded operating system, such as the Contiki OS / TinyOS / FreeRTOS. For higher end devices, such as smartphones, the presence of an operating system is guaranteed. For gateways, the operating system could be embedded Linux or a full-blown version of a –nix operating system, depending on hardware capability.
- Software implementation of the network stack. For low-end SOs, this can be TCP/IP-based or a bespoke stack, but in both cases it will feature implementations for protocols of all network layers, including application layer networking components, APIs and interfaces (e.g. RESTful). For higher end devices, such as smartphones, the network stack is normally implemented in the operating system's kernel space and is difficult or outright impossible to modify. In the case of gateways, the network stack is also implemented at kernel space. However, in the case of open-source operating systems (e.g. Linux), modifications are possible.
- Data generation and reporting software: Software used to collect data from sensing elements and report them to the gateway.
- Actuation software: Software used to receive, verify authenticity and validity, and execute actuations.

3.5 Data Flow Analysis

Based on the use-case definitions that were presented in Section 2, this subsection will describe the data flows between the system components for each use-case. The system components are presented in detail in Section 2 for each use-case.

3.5.1 Smart Transportation Data Flows

According to the use-case description, the SOs in the Smart Transportation use-case will mostly use a cellular network Internet connection. If the connection goes down, the system will opportunistically choose available (lamp post) gateways operating with Wi-Fi under an SSID predetermined at deployment. These gateways will have an Internet connection via the network provider and they offer some form of connectivity to a 3rd party service provider.

Following the UC, the foreseen data is focusing primarily on (i) user location and (ii) speed properties which will be handled by the application (traffic estimation) server to produce an estimation of the traffic state. Within this use-case we foresee the following data flows:

3.5.1.1 U-DATA Flows

For estimating the state on the road network, the SOs need to sense and report measurements that can be related to the traffic state at the location of the sensor. The users' mobile phone sensors report the location and speed of individual vehicles they are currently riding. Furthermore, these sensors can also play the role of fusion centres (or cluster heads) receiving measurement from the neighbour vehicles using i.e. Bluetooth and forwarding these measurements to the gateway.

S-DATA Flow: SO to Application server

Some sensors will be providing a unidirectional flow of information, since they will only report S-data to the application server. S-data will be sampled and transmitted to the application server for processing and estimating the network traffic state. S-data will be sent to the application server after any security- and privacy-enhancing modifications that will be carried out locally in the SO. The rate of position, acceleration, speed, samples and their transmission interval will be determined locally by the SO.

H-DATA Flow: SO to application server (bi-directional)

Another case can be considered when other SOs may also request to know the traffic state in the road segments ahead, so they are involved in participatory sensing, both providing S-data to and requesting/receiving H-data from the application server. In this respect, the SOs are sending the S-DATA to the application server, which estimates traffic state and sends back the traffic load or travel times on network links to the participatory sensing users. Thus, these flows are bidirectional. The traffic state data will be requested by the SOs and the request can, depending on implementation, potentially include S-DATA or user input data to filter the traffic state data: For example the SO location can be included in the request to filter traffic state data relevant for the user area. If the request does not contain any user-specific data, thus it is a request of the traffic state e.g. for the whole city, the response from the application server will not contain any user specific data either. However, if the request includes user specific data, also the response may contain user specific data that should be considered in terms of integrity.

3.5.1.2 C&C-DATA Flows

The only C&C data required in this use-case has to do basically with network connectivity. Specifically if the sensing SOs do not have connectivity they expect C&C data (WiFi IEEE 802.11 SSID broadcast beacons) from the lamp-post gateway. When some SOs play the role of fusion centres/cluster heads, other C&C-DATA could be considered to enable the communication between the cluster head and the transmitting SOs, as well as the identities of the SOs requesting to send measurements to the cluster head.

3.5.2 Home Energy Management Data Flows

According to the use-case description, the SOs and the gateway will either form a 6LoWPAN mesh network over IEEE 802.15.4 radio or use IEEE 802.11 (WiFi). The gateway will have an Internet connection via the network provider and will offer some form of connectivity to a 3rd party service provider.

Following this description the foreseen data's content is either good for monitoring the energy consumption directly, but also to check if there are good reasons for the utilization of the power-consuming device (e.g., do we need the lights turned on in the room if nobody is in the room?), or for control (e.g., turn lights off). For example an actuator that controls electrical light is getting the C&C-

DATA to be switched off, or a smart object with a light-sensing element sends the current luminosity representing the brightness of the light (natural and artificial) in the sensor's physical environment.

From the use-case we foresee the following data flows:

3.5.2.1 U-DATA Flows

The U-DATA flows are reflecting the exchange of U-DATA between the components of the UC. Loss of availability of S-DATA will result in a situation where an accurate reading of the environment from a SO is not received at the communication partner. This means that instead of reporting that a window is closed, the gateway or application server would receive no data regarding the window's state. This absence of sensed data might be detected by timestamps or other liveness checks. Nevertheless, the loss of availability of sensed data disables the application server's or gateway's or user's decision process, e.g. not knowing the state of a window makes it impossible for the user to have correct knowledge of the status of his house and thus the user does not know whether "Everything is OK" or not. Hence, the application for monitoring and all applications build on top of it (automation, energy saving) will not function/behave as expected. The same holds true for attacks on the integrity of U-DATA.

Confidentiality loss of U-DATA will result in privacy breaches whenever private data is transported. Also, the loss of confidentiality will result in an actuator or SO commands being disclosed to unauthorized 3rd parties. Knowledge of the actuation commands can disclose information about the environment, e.g. if a motion detection sensor instructs the lights to turn on, then we know that something moved inside the environment, i.e., infer the information that the environment monitored is currently occupied. In a home use-case environment this information means that someone is in the house and is clearly private data. In a building or office use-case environment, access to this data must be correctly controlled as defined per application's privacy policy, because any uncontrolled access might result in the attacker being able to link sensed data with specific persons or actions.

S-DATA Flow: SO to SO; SO to Gateway (bi-directional):

The SO will generate and send S-DATA due to

- a continuous monitoring loop as a periodic message, or to
- the reception of a control message instructing the sensor to wake-up, or to
- an internal application with an associated policy triggering the sending due to pre-defined and sensor internally generated event (generated by the internal application and the policy). For example the motion sensor could trigger sending a "motion started" message whenever it detects motion if it previously detected no motion.

The SO may need to send S-DATA intended for another SO via the gateway, which acts as an intermediate node that processes and re-packages messages in order to relay S-DATA between heterogeneous SOs. A SO may receive S-DATA when a SO's internal application is doing some form of storing or processing of S-DATA locally according to an internal policy. The SO may receive S-DATA not only from another SO but also from the gateway.

A-DATA Flow: SO to SO, SO to Gateway (bi-directional):

A SO can send A-DATA in order to instruct actuating components according to some internal policy, based on readings received from sensing elements. For example the lights in a room are switched off or on by the motion sensor in the room, without the need for other components to be involved in this closed sensor-actuator control loop. If the SO is an actuator it may receive A-DATA when the gateway's internal application is doing some form of storing or processing of S-DATA locally according to an internal policy. The actuator may receive A-DATA from another SO via the gateway.

U-DATA Flow: SO or Gateway to Application server (bi-directional)

If the application server is logically outside RERUM's scope (and this is often also behind the gateway) then the server receives the data that RERUM allowed to be forwarded directly according to security and privacy policies. If the data are not allowed to be forwarded, then they are either dropped or subject to some further processing on the gateway, to comply with the RERUM security and privacy policies. For controlling the actuators, the gateway will receive the commands from the application server and forward them to the SO in a specific format that the SO understands, allowing the application server to overcome the heterogeneity of the SOs. This also involves that all required authentication credentials are either checked and the result of this check is secured and trusted, or that the required authentication credentials are forwarded to the SO to make the access control decision locally.

The sensed data (S-DATA) or the commands to act (A-DATA) can be processed according to some policies on the gateway. This allows the gateway to execute functions that will protect against threats related to authentication and authorization as well as privacy.

If the application server is behind the gateway, the application server needs to always send all communications, e.g., A-DATA or requests for S-DATA, through the gateway in order to reach an SO, and all the answers to his request, e.g. S-DATA, is also sent back via the gateway in order to serve the application it is running.

3.5.2.2 C&C-DATA Flows

For this use-case C&C Data Flows are depending on the network technology used to communicate between the SOs and the gateway to ensure the correct operation of the network. Based on the use-case description, a Home Energy Management deployment will rely either on IEEE 802.11 (WLAN) or 802.15.4 at the link layer. Even though not explicitly stated in the use-case, in the former case we anticipate a standard TCP/IP stack for the network and transport layers. In the latter case, the deployment will use IPv6 / 6LoWPAN and related specifications at the network layer, and standard TCP/UDP at the transport layer. Hence, those protocol's control messages are all C&C-DATA. Depending on the source and destination of C&C-DATA exchanges, we identify the following flows:

C&C-DATA Flow: From SO to SO or Gateway (bi-directional)

- Host and network configuration message exchanges, e.g. for the Dynamic Host Configuration Protocol (DHCP) [112] or DHCPv6 [113].
- Routing control datagrams: (i) In the case of a WiFi network, we do not anticipate routing control messages. Even though a routing protocol can be used, in residential WiFi networks devices typically use static routes, which are configured automatically through DHCP when a device joins the network and refreshed periodically afterwards. (ii) In the case of a 6LoWPAN over IEEE 802.15.4 deployment, routing messages (e.g. RPL control messages packets) will be exchanged for the formation of the 6LoWPAN mesh
- Address Resolution Protocol (ARP) [111] exchanges for the maintenance of ARP caches on SOs and the gateway (WiFi / IPv4 networks only).
- IPv6 Neighbour Discovery (ND) or 6LoWPAN-ND [110] messages for the maintenance of ND caches at SOs and at the gateway (IEEE 802.15.4 / 6LoWPAN networks only).
- TCP session establishment and tear-down
- Configuration management read or modify requests and responses

C&C-DATA Flow: From SO or Gateway to Application server (bi-directional)

- TCP session establishment and tear-down
- Configuration management read or modify requests and responses

C&C-DATA Flow: Application server to gateway to SO:

In order to check the health of an installed system, e.g., check that all SOs are still working, the application server might instruct the installed system to report. The C&C-DATA serve the following purposes:

- To carry out network maintenance checks, e.g., check system‘s health
- To receive and update to the SO gateway’s internal application or the internal policy

The application server will not be able to communicate directly with the SOs, but only through the gateway. Thus, if the C&C-DATA was not intended for the gateway, the gateway might need to send C&C-DATA to the corresponding SO.

3.5.3 Environmental Monitoring and Comfort Quality Monitoring Data Flows

According to the use-case descriptions, SOs and the gateway used for the deployment will form a 6LoWPAN mesh network over IEEE 802.15.4 radio. The gateway will have an Internet connection to an application server. With this in mind, this section lists the following data flows:

3.5.3.1 U-DATA Flows

From the network layer perspective of the TCP/IP stack, data flows are of a multi-hop nature. Within the deployment’s premises, U-DATA flows will traverse multiple SOs, with each one acting as an intermediate router in a 6LoWPAN mesh. If the flow involves the application server either as the source or the destination of the flow, then the gateway will also act as a router while U-DATA travel between the gateway and the application server over a public network. While in transit through the Internet, U-DATA are exposed to various well-known, Internet-related security threats. This threat analysis has a use-case specific focus. Even though RERUM will protect data in transit between the gateway and the application server, which may take place partially over the Internet or an ISP network, threat analysis of those networks is out of scope of this section.

As specified by the UC description, U-DATA flows among SOs, and between an SO and the gateway (from a link layer perspective) take place over IEEE 802.15.4 wireless links at the monitored location.

S-DATA Flow: SO to SO; SO to Gateway; Gateway to Application server

Link layer and network layer aspects of S-DATA flows were discussed in a previous subsection. From an application layer perspective, sensory measurements will have one of two final destinations: (i) the application server or (ii) the gateway. In both cases, U-DATA may undergo RERUM-specific security- and privacy-enhancing modifications at intermediate SOs.

When U-DATA are sent to the application server, from an application layer perspective the transmission can be:

- Either directly from the SO to the application server,
- or to the application server via the gateway. In this case, the gateway may apply further RERUM-specific security- and privacy-enhancing modifications to the S-DATA, such as aggregation, anonymisation, or pseudonymisation.

A-DATA Flow: Application server to SO (bi-directional); Gateway to SO (bi-directional)

Link layer and network layer aspects of A-DATA flows were discussed in a previous subsection. From an application layer perspective, A-DATA data flows will either originate at the gateway or at the application server. In the former case, A-DATA are confined within the monitored location. In the latter case, the data flow can take place:

- Either directly from the application server to one or more SOs,

- or from the application server to SOs via the gateway. In this case, the gateway may undertake further RERUM-specific protective functions, such as functions related to authentication and authorization.

3.5.3.2 C&C-DATA Flows

These data flows relate to the correct operation of the networking protocols and algorithms in place for this use-case. Based on the use-case description, a Comfort Quality Monitoring deployment will rely on the following: IEEE 802.15.4 at the link layer; IPv6, RPL, Neighbour Discovery (ND) and 6LoWPAN at the network layer; TCP / UDP at layer 4. All control messages exchanged by those protocols constitute a C&C-DATA flow. Depending on the source and destination of C&C-DATA exchanges, we identify the following flows:

C&C-DATA Flow: From SO to SO or Gateway (bi-directional)

- Routing control datagrams for the formation of the 6LoWPAN mesh
- IPv6 Neighbour Discovery (ND) or 6LoWPAN-ND [110] messages for the maintenance of ND caches at SOs and at the gateway.
- TCP session establishment and tear-down
- Configuration management read or modify requests and responses

C&C-DATA: From SO or Gateway to application server (bi-directional)

- TCP session establishment and tear-down
- Configuration management read or modify requests and responses

3.6 Threats on Confidentiality, Integrity and Availability (C-I-A)

This section documents the first phase of the threat analysis, by listing threats against asset Confidentiality, Integrity and Availability.

3.6.1 Loss of Confidentiality of Authentication CREDENTIALS (Threat#01)

An attacker can gain access to CREDENTIALS either while they are at rest or in transit.

- **At Rest**: If an unauthorized entity manages to read CREDENTIALS at rest by executing malicious code on an SO or gateway, or by gaining remote access to one through successful identity spoofing.
- **In Transit**: Through an eavesdropping or man in the middle attack.

CREDENTIAL confidentiality breach can be used to launch subsequent impersonation attacks, leading to eventual U-DATA confidentiality loss (Threat#02)

3.6.2 Loss of U-DATA Confidentiality (Threat#02)

An attacker can gain access to U-DATA either while they are at rest or in transit.

- **At Rest**: If an unauthorized user manages to read U-DATA at rest by executing malicious code on an SO or gateway, or by gaining remote access to one through successful identity spoofing.
- **In Transit**: For example through an eavesdropping attack or man in the middle attack.

Depending on the use-case, U-DATA may be private data and therefore their disclosure may constitute a privacy breach.

3.6.3 Loss of C&C-DATA Confidentiality (Threat#03)

Loss of C&C-DATA confidentiality can occur while data are at rest or in transit.

- **At Rest**: May occur if an unauthorized user manages to read C&C-DATA at rest by executing malicious code on an SO or gateway, or by gaining remote access to one through successful identity spoofing.
- **In Transit**: This can be the result of eavesdropping on control plane traffic.

C&C-DATA confidentiality loss will reveal information about a deployment's network topology. A malicious user can subsequently use this information in order to launch targeted attacks on U-DATA against specific SOs.

3.6.4 Loss of S/W Confidentiality (Threat#04)

Loss of S/W confidentiality may occur while S/W is at rest or in transit:

- **At Rest**: May occur if an unauthorized user manages to read S/W at rest by executing malicious code on an SO or gateway, or by gaining remote access to one through successful identity spoofing. It may also be the result of a successful attack against U-DATA integrity or C&C-DATA integrity. In the former case, malformed data plane traffic can give an attacker remote access to a node. In the latter case, malformed control plane traffic can result in a new system configuration, one that would allow an attacker to gain access to the system.
- **In Transit**: This can be the result of eavesdropping on control plane traffic. S/W confidentiality may be breached during an over-the-air application update.

S/W confidentiality loss may have a negative impact on the stakeholder that developed it. For instance, it may reveal their trade secrets. Additionally, the S/W becomes exposed to reverse engineering efforts. If successful, reverse engineered software can reveal important information about security mechanisms in place, it may reveal security vulnerabilities and it may ultimately facilitate the launch of further attacks against the deployment.

3.6.5 Loss of U-DATA Integrity (Threat#05)

An attacker can modify U-DATA while at rest or in transit.

- **At Rest**: If a user manages to modify U-DATA by executing malicious code on an SO or gateway, or by gaining remote access to one.
- **In Transit**: Through attacks on the network infrastructure. This can be the result of a man in the middle attack, by exploiting routing protocol, or neighbour discovery vulnerabilities.

If an attack is successful, the application will start providing incorrect S-DATA values. Of a more severe nature is the case of integrity loss of A-DATA, whereby a malicious user can trigger undesirable, potentially even privacy-breaching actuations, such as opening a window or turning on audio recording equipment.

This attack may be used as a facilitator to launch subsequent attacks against software confidentiality, integrity as well as availability, and it is thus considered of very high severity.

3.6.6 Loss of C&C-DATA Integrity (Threat#06)

Loss of C&C-DATA integrity can occur while data are at rest or in transit. In particular, the manipulation of routing information can lead to performance or service degradation, or it can lead to fragmentation or unavailability of the network by restricting the number of routers with which communication can be maintained. Another, less severe attack is routing information exposure to an attacker. That is, the attacker learns routing information, the network topology, or information about

the configuration and connectivity of the network. He learns in this way about the key nodes or links to be targeted in further attacks. In a similar approach, an attacker can modify spectrum sensing information exchanged between nodes in cooperative sensing and manipulate the results in order to exploit the available spectrum holes fir his benefit (this is known as a Spectrum Sensing Data Falsification - SSDF - attack in cognitive radio networks).

- **At Rest**: This can be for example alterations of routing tables or spectrum sensing information, which can take place if a user manages to execute malicious code on an SO or gateway, or by gaining remote access to one. Alteration of data at rest can also occur as a result of malformed control plane messages, e.g. malicious routing protocol advertisements or neighbour advertisements, TCP session hijacking, ICMP redirect attacks, etc.
- **In Transit**: Loss of C&C-DATA integrity while in transit can occur by man-in-the-middle attacks, whereas a malicious user modifies control plane messages. A successful attack of this nature is also likely to cause modifications of C&C-DATA at rest.

Loss of C&C-DATA integrity is very likely to have an impact on U-DATA confidentiality and availability. It may also have an adverse impact against S/W confidentiality, integrity as well as availability. This threat may therefore be used as a facilitator to stage subsequent attacks and is considered of very high severity. For example, an SSDF attack may result to the case that SOs select a very congested frequency, resulting to unavailability of getting access to the wireless medium, thus becoming incapable of transmitting data. Thus, a result of SSDF can be the loss of availability of U-DATA (see Threat#08).

3.6.7 Loss of S/W Integrity (Threat#07)

Loss of S/W integrity may occur while S/W is at rest or in transit:

- **At Rest**: This can occur if an unauthorized user manages to delete or to modify S/W at rest by executing malicious code on an SO or gateway, or by gaining remote access to one through successful identity spoofing.
- **In Transit**: This can be the result of a man-in-the-middle attack against control plane traffic. A successful attack of this nature may result in S/W integrity breach during a software update.

Breach of S/W integrity will have a negative impact on its performance or may render the S/W entirely non-functional. This may be used to stage subsequent attacks of a different category against the system. S/W integrity breach could further result in negative impacts on the software's value in terms of reputation, bad reviews, reduced number of users, shrinking install base.

3.6.8 Loss of U-DATA Availability (Threat#08)

Loss of U-DATA availability can occur while data are at rest or in transit.

- **At Rest**: This can be the result of intentional deletion by a malicious user, which may materialize if a user manages to execute malicious code on an SO or gateway, or by gaining remote access to one.
- **In Transit**: Indicatively, loss of availability in transit could be the result of a radio jamming, SSDF attacks, attacks on network protocols at the control plane (e.g. routing or neighbour discovery), or sinkhole attacks.

Depending on the attack, this threat may occur simultaneously with loss of confidentiality, in which case there is a likelihood of a privacy breach and therefore the threat's severity increases. For example, a vampire attack aims to drain the energy source of a battery-powered device. If an SO becomes the target of a successful vampire attack, its batteries will become depleted and the SO will become unresponsive. This constitutes a successful attack against U-DATA availability, but U-DATA

confidentiality does not get compromised. Conversely, selective forwarding or sinkhole attacks compromise network forwarding capability. They constitute an availability breach, but the same attacks can also compromise confidentiality.

3.6.9 Loss of C&C-DATA Availability (Threat#09)

Loss of C&C-DATA availability can occur while data are at rest or in transit.

- **At Rest**: This can be the result of intentional deletion by a malicious user. For example, a malicious user can gain remote access to an SO or gateway and subsequently remove entries from routing tables. Alternatively, a malicious user can perform the same attack by installing malicious software on the SO or gateway.
- **In Transit**: Indicatively, loss of availability in transit could be the result of a radio jamming attack, attacks on network protocols at the control plane (e.g. routing or neighbour discovery), or sinkhole attacks.

Loss of C&C-DATA availability is very likely to result in some SOs getting disconnected from a deployed network and will therefore have an adverse impact on U-DATA availability.

3.6.10 Loss of S/W Availability (Threat#10)

Loss of software availability occurs when the firmware installed on an SO or gateway fails to execute. It will normally manifest itself as software crashes, non-responsive devices or device resets and can be the result of unauthorized manipulation. It may occur if an unauthorized user manages to delete or modify S/W at rest by executing malicious code on an SO or gateway, or by gaining remote access to one through successful identity spoofing. Lastly, it may occur as a result of battery depletion, which may be the result of a vampire attack.

Loss of S/W availability will seldom be encountered in isolation, but it will normally be the result of a breach against S/W integrity, or U-DATA integrity, or C&C-DATA integrity. Malformed data plane or control plane traffic can result in a device crash. Malformed data plane traffic can also give an attacker remote access to a node. Additionally, malformed control plane traffic can result in a new system configuration, one which would allow an attacker to gain access to the system and perform an attack against the software.

Loss of S/W availability can also be the result of faulty design or implementation, but these are out of this threat analysis' scope, since they are not the result of intentional malicious actions.

3.7 Threats on Authentication, Authorization and Accounting (AAA)

This section discusses threats against Authentication, Authorization and Accounting. As discussed in each individual sub-section, these threats will often allow to carry out a second stage of attacks that will result in breaches against confidentiality, availability and integrity of IT assets.

3.7.1 U-DATA Repudiation (Threat#11)

This threat occurs when the origin of U-DATA later claims that the U-DATA originated elsewhere. In the case of S-DATA, the origin is an SO and it should be possible to hold SOs accountable for S-DATA generation. A-DATA commands can either be triggered by a user directly, or they can be triggered automatically based on a schedule or on events specified by the user. In both cases, the system must be capable of holding the user accountable for manual triggers as well as for specifying a schedule or events.

3.7.2 C&C-DATA Repudiation (Threat#12)

This threat occurs when an attacker is able to convince another entity later that the attacker was not the origin of C&C-DATA or even is able to convince another entity that the data originated elsewhere. C&C-DATA are generated by SOs or the gateway, in which case the system should be capable of holding specific devices accountable for the generation of C&C-DATA. Since this would require a method of uniquely identifying devices, non-repudiation mechanisms could have privacy implications.

3.7.3 Identity Spoofing of a User with Higher Privileges (Threat#13)

This threat occurs when malicious users send commands to the system under the pretence that they are a system administrator. In doing so, they may be able to read or modify the system's configuration, eventually leading to asset confidentiality, integrity or availability loss.

3.7.4 Device Identity Spoofing (Threat#14)

This threat occurs when a device joins a network by pretending to be a different device (or node). If an attacker can join the infrastructure network without authenticating or if the attacker can falsify his identity or take over another node identity, then he may be able to take over the role of a legitimate node (or for that matter, of several ones) previously existing or not in the network. The intruder may be able to report false readings or provide inappropriate control messages. The attacker could then also re-direct traffic to itself in order to mount further attacks. If he continuously adds fake nodes, the infrastructure resources (say, the available space or computational power to manage large identity and routing tables) become scarce, leading to system unavailability. This can lead to a breach of confidentiality, integrity or availability of U-DATA, as well as of C&C-DATA when in transit.

3.7.5 User Privilege Elevation (Threat#15)

This threat occurs when a user gains access to the system with higher privileges than normally available to him. As a result, the malicious user can then read U-DATA or send A-DATA to the system without having the permission to do so. This can lead to a breach of confidentiality, integrity or availability of U-DATA, as well as of C&C-DATA when in transit.

3.7.6 Device Privilege Elevation (Threat#16)

This threat occurs when a device assumes the role of a different device with higher privileges. For instance, this can occur if a SO assumes the role of a gateway. In all cases, a successful attack of this category can be a breach of confidentiality, integrity or availability of U-DATA, as well as of C&C-DATA when in transit.

3.8 Privacy Threats

In Section 3.3 we proposed a security threat methodology comparable to the threat elicitation in Microsoft's STRIDE security lifecycle. For privacy threats we refer to the privacy terminology by Pfitzmann et al. [86], as it is the most recognized terminology in the privacy research community. As per the methodology proposed in Section 3.3, our privacy elicitation method presents several threats, and the resulting methodology corresponds to the LINDDUN method proposed by Deng et al. [87], which was designed as the privacy related equivalent of STRIDE[6].

The LINDDUN methodology – which we hereby use in a simplified manner due to the fact that we have not a complete software-intensive system, but a system under design – will help us elicit privacy

[6] The equivalence is referenced several times in the LINDDUN proposal paper.

requirements and select privacy enhancing technologies accordingly. Each letter of "LINDDUN", as seen in "STRIDE", stands for a privacy threat, as per the following sub-sections.

3.8.1 Linkability (Threat#17)

Linkability is the ability to sufficiently specify the difference of two or more Items Of Interest ("IOIs", such as subjects, messages, actions). As an example, think of the smart transportation use-case. The traffic data gathered by GPS-enabled vehicles may be completely anonymous. However, if the request for these data (the requests are C&C-DATA) from a server to the vehicle can be linked every time to a certain vehicle, then the traffic data can be deanonymized as well.

3.8.2 Identifiability (Threat#18)

Identifiability refers to a set of subjects or IOIs. This ability means that the attacker can sufficiently identify the subject within this set. This may occur when U-DATA are not sufficiently aggregated, and certain U-DATA sets can be sufficiently identified as subject to a certain user.

3.8.3 Non-repudiation (Threat#19)

Non-repudiation describes the inability to successfully challenge the validity of a statement. It is needed for security, but it competes as a threat for privacy. Deng et al. in [87] describe non-repudiation as the ability of an "attacker to gather evidence to counter the claims of the repudiating party and to prove that a user knows, has done or has said something". This could occur again in the case of smart transportation, when a user is reporting anonymously data about a location X, which in his personal life or context is problematic, and an attacker can prove that the data must have been gathered by that person in that location at a certain point in time. The user won't be able to repudiate his role as the source of the respective H-DATA.

3.8.4 Detectability (Threat#20)

Is the ability of an attacker to sufficiently distinguish whether a subject or an IOI exists or not. Deng et al. in [87] exemplify messages as IOIs: If messages are "detectable", then they can be sufficiently distinguished from, e.g., random noise. This could be the case in the home energy management use-case: C&C-DATA is sent every time a user is away from home and is checking on his home's status. An attacker might take advantage from the knowledge that a user is not at home. This again could be circumvented by random C&C-DATA messages from the user at random intervals. If the attacker can still distinguish the random messages from the real ones, then the attacker exploited detectability.

3.8.5 Information Disclosure (Threat#21)

Information Disclosure is very close to the security goal of confidentiality, as this threat describes the disclosure of personal information to individuals who are not allowed to have access to it. Confidentiality, as a security goal, categorizes IOIs in a binary manner as readable or non-readable for a certain party. Besides the allowed parties, information disclosure additionally defines in what context the disclosure may take place. Disclosure of U-DATA may happen in every use-case, if appropriate security mechanisms are not applied. Additionally, the enforcement of privacy policies is necessary: U-DATA may be allowed to be accessed by a certain party in a certain time horizon, but it may be prohibited thereafter.

3.8.6 Content Unawareness (Threat#22)

This threat describes the threat of a data subject's unawareness of the information disclosed to the system. The data subject is either unaware of how much information he/she is disclosing, which allows an attacker to retrieve the subject's or an IOI's identity or how inaccurate information can cause wrong decisions or actions. This could be the case in the comfort quality monitoring use-case. Which data has to be really considered U-DATA by a person in a monitored space? Is the CO_2

measurement a hint to the user's current activities, or is the noise measurement capable of detecting speech and disclosing every word that was said?

3.8.7 Policy and consent Noncompliance (Threat#23)

This threat defines a system's noncompliance to its advertised policies and/or its commitment to data subjects consent. With no guarantees of the system, a subject's U-/H-/S-/C&C-DATA may still be processed or disclosed against his consent, even if agreements or policies were defined differently.

As in STRIDE, LINDDUN proposes to elicit assets and data flows, and their mapping to the LINDDUN privacy threats above. In a similar and coherent approach, we map each asset and data flow of each use-case with every privacy requirement, and reason about what kind of threats may occur, as proposed in the security methodology section.

3.9 Threat Scenarios

In this section we give more concrete examples for each threat that we have listed for C-I-A (Section 3.6), AAA (Section 3.7), and Privacy (Section 3.8). These examples will show why it is important for RERUM to cater for the respective threat, because they highlight what would happen in a specific use-case if this threat was not counteracted. They will build upon our deep investigation of the vulnerabilities for each use-case and the data flow analysis carried out in Section 3.5.

3.9.1 C-I-A Threats in the Smart Transportation Use-Case

Due to the large amount of peers providing traffic data for smart transportation applications, *availability* seems not much of a problem. However, if an attacker is able to impersonate an administrator of the RERUM IoT-services, he can cause large service degradation, in terms of data collection denials, as well as full-blown Denial of Service (DoS) attacks for all traffic estimation and regulation services.

Integrity has a high impact directly on the service quality and on the cyber-physical consequences of the smart transportation use-case. As shown in [89], false data injection attacks by fake or compromised devices can cause service malfunctioning, which may remain undetected over a longer period of time. The data quality and the overall correctness of data will determine on traffic forecasts and decision making.

The smart transportation use-case will heavily process U-DATA, which could identify the subjects providing the data. In this use-case *confidentiality* threats are mostly subsumed into privacy threats, see below.

3.9.2 AAA Threats in the Smart Transportation Use-Case

There are many types of attacks that can be mounted via *node impersonation*. An attacker can pretend to be the gateway or the service provider and send false information to vehicles in order to divert the traffic to other routes different than the ones he is planning to use, or worse, in order to direct a particular car into side streets in order to ambush the passengers.

3.9.3 Privacy Threats in the Smart Transportation Use-Case

The possible attacks on the privacy of citizens are innumerable and range in impact from relatively mild to very serious. In the following we will demonstrate the threats in a hypothetical scenario.

Imagine a small city of "The Den" with Alice, her boyfriend Bob and an acquaintance of Bob's called Constantin. The Den is a small town, which has suffered previously from heavy traffic. Using smart transportation applications, the city has been able to tackle the usual traffic congestions. Constantin is an acquaintance of Bob; he works at the local service provider in charge for the traffic estimation, and has access to smart transportation location data. Bob has been jealous for some time, and he

wants to track Alice; he wants to know which places she visits regularly and if she does what she has told him. The location information, if only pseudonomised, will disclose many details about Alice by *correlating movements* of the different hours or days. Just by the information of certain routes, Bob can add additional personal information which is available to him and identify the pseudonym that was given to Alice, but similar information maybe also available from public sources like social networks. This correlation will show very detailed information, that she leaves her house at "NW-Boulevard 15" at 7:00 a.m., arrives at works at the "Pacific Mall" at 7:30 a.m., that she goes in her spare time regularly to the hospital "Merciful Brothers", even that she is under treatment in the hospital's section 3. In the smart transportation use-case, much of the functionality depends on the analysis of the location information of end users. This includes not only the location of users using androids, but also for taxi drivers, or persons using public transportation.

Individuals in our use-case are mobile objects that can be subject to several types of threats:

- They can be traced continuously in space & time, perhaps without their knowledge or consent.
- They can be intercepted on their movements along a street or path, for a physical attack for instance.
- They can be redirected to new, sub-optimal trajectories.
- Their data can be archived in long-term surveillance databases
- Data of individual users can be linked with data of other individuals, organizations, or companies. For instance, location data can reveal the fact that an individual visited a certain meeting of a political party, or a competitor, etc.
- Individuals can be linked to activities of leisure or work. For instance, location data can reveal the fact that an individual visited a particular medical clinic during a certain time or a particular meeting of a political party.
- Family members, co-workers, or even unrelated people might use location information of their victims for stalking, coercion, and violence. In an extreme case, a person can track the location of a family member, an employee, a friend, a victim, a suspect over time and exert coercive pressure on him, forcing him to visit certain places, or to avoid them, or to perform or withdraw from certain activities. Some researchers see here the imminent danger that location-based systems introduce the opportunity for real-time control, which may go far beyond other forms of privacy issues, see in particular in [78].

The privacy risks and the different degrees of privacy concerns regarding location-based services also depend on some technical issues and the way that the user has to interact with the system. Services in which the mobile device is sending location information without the direct participation of the user (say, triggered by some event, like entering a certain area or attaining a certain velocity), are in general more problematic than services where the user is actively sending his location information at his discretion. In any case, the user must be aware of what caused the transmission of location information. Location-tracking systems (as part of the transport Use-case) are, by definition, more problematic than location-aware services, since the former ones offer information to entities other than the user, while location-aware services are meant to supply only the user with information related to his current location.

There are several proposals for providing location privacy in general location-based systems. One simple method for obfuscating the location information is spatial and temporal cloaking [90]-[93], where the exact location and time is not sent to the server but rather only approximate values. Nevertheless, doing this naively is not too useful, as there are still several rather simple attacks on these mechanisms [94], [96].

Another alternative is to create regions in space or time where the client (user) does not send location information to the server. Those mix regions, in different variants, are known under the names mix zones, silent zones, or silent times [97], [98]. In most proposals, before leaving the mix

region, the device identifier (a pseudonym) is changed. In this way, an observer may not correlate who is entering and who is leaving such a mixing region. This, however, may compromise the functionality of the system.

Other, more secure, methods (like the one presented in [99]) employ a coordinate transformation that depends on a secret, which is applied to the location data sent to the server. If a friend of the user shares the secrets he can reverse the transformation. These types of solutions are not usable in our setting, because the velocities of the different users in the same place have to be compared and aggregated in the server.

Further privacy-enhancing technologies for location privacy are for instance Silent Periods [100], [101], SLOW [102], Mix Zones, Pro-Mix [103]. All these concepts aim to provide a secure, unlinkable pseudonym switchover via radio silence or encryption.

3.9.4 C-I-A Threats in the Home Energy Management Use-Case

Losses of U-DATA *confidentiality* will most of the time result in a breach of privacy. In general, the loss of confidentiality will result in unauthorized entities gaining access to data sent over the network. This is a very natural assumption for all networks; especially wireless communication is prone to attacks likes eavesdropping. For UC-I1 it can be easily seen that network data would contain sensed data of the environment, e.g. the current energy consumption of the washing machine, or commands like switch lights off.

The loss of confidentiality of U-DATA is easily recognized as having negative effects. However, in some cases the loss of confidentiality of C&C-DATA (i.e. data needed for routing packets) can also create problems. For this example we will consider just a loss of confidentiality for C&C-DATA that is required to achieve the networking functionality. The loss of confidentiality of such data will result in the networking infrastructure's flow of messages becoming observable for an attacker. Hence, attacks like traffic analysis are possible. This is will then lead to a privacy threat, which is described in section 3.9.6.

The loss of *integrity* will result in **actuators** or SOs receiving a modified command that was originally correctly sent by the communication partner. We assume that a loss of integrity means, that such a change is not detected. The attacker can change a correctly computed command into an incorrect one, either after or before it is emitted from the component, and his attack is not detected. Hence, an attacker can influence the physical environment by sending malicious commands. Depending on the instalment this can result from minor disturbances to more drastic consequences leading to health impacts or financial losses. For example, instead of telling the heating to turn on the heating in the morning, it could be turned down, or instead of issuing a command to close a window a burglar could open it and turn off the alarm.

The loss of U-DATA *availability* for UC-I1 results in either loss of relevant information about the environment or in the inability to carry out the actions on the environment. Again, depending on the length of the interruption, the consequences of not being able to manage the energy consumption could have negative consequences or at least be a nuisance decreasing user acceptance of the IoT system.

3.9.5 AAA Threats in the Home Energy Management Use-Case

The use-case clearly communicates that data gathered are correct and unchanged (e.g. detecting overheating devices) and that false/commands should not be issued to actuators. In order to clearly distinguish malicious SOs from genuine ones, we need to have *authenticated* SOs and we must be able to build authorization decisions on this. The use-case explicitly mentions that it requires separating two roles (i.e., administrators and limited users) as they are authorized to carry out different tasks.

The use-case describes that sensed data gathered by one application use-case might also be used for other applications. One example from the Smart Grid applications is to use the control of high consuming energy devices in Demand Side Management (DSM). In this case, for accounting or transparency reasons the consumer could need to prove later that a washing machine was switched on at a specific time. Hence, some applications might require some form of *accounting*, e.g. the possibility of logging and later proving that certain sensed data were sent from an authenticated source (e.g. the smart meter) or that the command "turn washing machine on" was sent from an authorized entity (e.g. your DSM). This calls for a verifiable authentication of origin that can be used to build accounting, when it would be required. This had been captured in Threat#11 U-DATA *Repudiation*.

In order to take decisions based on received sensed data into question, a component that sent sensed data should be held accountable for having created that data. Otherwise, the component or entity takes the full risk and responsibility for all the decisions of that component/entity when the decision is based (fully or in part) on repudiable information. This had been captured in RERUM-Threat#12: C&C-DATA *Repudiation*. This requires a form of verifiable data origin authentication. Otherwise, decisions will have to be based on information coming from potentially unreliable or unknown sources. When sources are verifiable and recognizable, trust and reputation calculations can guide a decision process.

The importance of the *Identity* of Administrative Users or Nodes is captured in Threat#13 and Threat#14: In order to gain unauthorized access, malicious entities might try to impersonate legitimate ones. For example an entity, which is in the group of limited users, might try to pretend being in the group of administrators. If the threat is not dealt with, this can lead to loss of confidentiality of any data or credentials to which the authorized entity had access. Even if it might not give them access to data or credential, it might allow them to influence the system in a malicious manner. For example, an attacker could see sensed data even though it originally was not authorized to do so. E.g. the attacker could see timing and the energy consumption of the shared washing machine in the laundry room.

For UC-I1 *authorization* is important. If "user privilege elevations" or "identify spoofing of a user with higher privileges" are not countered, then a limited user would be able to gain more privileges and eventually become as powerful as an administrative user. In order to gain unauthorized access limited users might try to pose as administrators. This will then lead to loss of confidentiality of any data or credentials to which the authorised entity had access. Even if it might not give them access to data or credentials, it might allow them to influence the system in a malicious manner. For example, an attacker could send control messages even though it originally was not authorized to do so. E.g. the attacker could switch on the heating.

3.9.6 Privacy Threats for the Home Energy Management Use-case

Loss of confidentiality of messages that contain data about the environment is a threat to privacy, because they allow inferring at least the usage pattern of the High Consuming Device (HCD). Another way for an attacker to obtain information that might allow him to obtain the usage pattern is that the attacker gets access to just the flow of messages. The latter attack is called traffic analysis.

Traffic analysis, following RFC6973 [108] allows the inference of information from the observation of traffic flows (presence, absence, amount, direction, timing, packet size, packet composition, and/or frequency), even if the data inside the flows are encrypted. Here, the attacker only knows that a message was sent from one specific SO to some specific SO; the attacker could be able to guess that one SO is the gateway and the other SO is a specific HCD, e.g. the washing machine, or the TV.

Consider the following example: Assume the that the motion sensor instructs the light switch due to two rules: (i) if motion is detected we immediately send a command to turn the light on, and (ii) if no motion happens for two time periods of 1 minute each, send command to turn light off. Even if the

C&C-DATA from the motion detector to the light switch is encrypted, the fact that the motion detector sends a control packet to the light switch lets an attacker do traffic analysis to defer that the observed space is now occupied (case 1) or was recently occupied (case 2).

Hence, not addressing these threats would result in privacy breaches in the Home Energy Management use-cases.

3.9.7 Threats in the Comfort Quality Monitoring Use-Case

As per the use-case description, we examine a comfort quality monitoring installation with multiple SOs collecting environmental data and executing actions. The deployment is controlled by a gateway, which also communicates with an external application server whereby U-DATA are collected. As per the use-case description, SOs and the gateway form an IEEE 802.15.4 network and communicate over 6LoWPAN. The deployment uses RPL [106] for routing.

For this particular use-case, attacks against U-DATA confidentiality can reveal end-user habits and they can also reveal whether they are physically present in the premises or not, situations which constitute privacy violations. For example, an attacker may be able to gain access to motion sensor readings, readings regarding the ambient light level, or to determine that the heating or gas boiler is on. A high ambient light level during night-time, combined with motion and the knowledge that the gas boiler is on, are strong indications that someone is present at the premises. A different attacker may be a competitor of the company that has developed the firmware running on SOs. This attacker may attempt to obtain a copy of the firmware in order to harm its competitor's reputation or in order to reverse engineer it and use parts of it for his/her own software, as part of an industrial espionage attempt.

We examine some example scenarios, each one with different security mechanisms in place.

3.9.7.1 Naïve Deployment

In this first scenario we assume a very naïve deployment with no protective mechanisms in place:

- Traffic at the IEEE 802.15.4 link-layer is unencrypted
- Traffic at the network layer is unencrypted
- Traffic at the application layer is not protected: SSL/TLS/Datagram TLS (DTLS) [114] are not in use.

Thus, C&C-DATA as well as U-DATA are all transmitted in clear. Additionally:

- Routing control plane traffic (RPL traffic) is unauthenticated

An imaginary attack scenario could be as follows. A malicious user positions a node nearby but outside the user's premises. This node passively energy-scans IEEE 802.15.4 RF channels for traffic. Once the deployment's channel has been identified, the node switches to this channel permanently and starts listening for control and data plane traffic. This constitutes a C-I-A breach in U-DATA and C&C-DATA confidentiality (Threat#02 and Threat#03 respectively).

Once a sufficient amount of traffic has been collected, the attackers can reverse engineer the protocol used at the application layer and figure out details about the format of data-plane packets.

Once this goal is achieved, the malicious node simply captures all U-DATA (Loss of U-DATA Confidentiality) and transmits them to an Internet host or stores them locally. Aggregation, data anonymisation and other privacy-enhancing methods are therefore bypassed, and the attacker has full access to all U-DATA.

3.9.7.2 Encrypted U-DATA traffic

In this second scenario we make the same assumptions as earlier, but assume that U-DATA are encrypted at the application layer. This can be, for example, by using DTLS between SOs and the gateway.

The attack starts in the same fashion as earlier, with the attacker eavesdropping on the RF channel used by the deployment. In this case, U-DATA cannot be interpreted, the attacker therefore cannot reverse engineer the application layer protocol.

However, the attacker can understand that this is a 6LoWPAN deployment that uses RPL for routing. The attacker then performs an attack against RPL itself. Because control traffic is not authenticated, the attacker introduces malicious traffic impersonating a node which offers a better network path between SOs and the gateway (AAA Threat: Device Identity Spoofing). Once such attack is successful, all traffic goes through the malicious host (U-DATA Confidentiality Loss), allowing attackers to simply drop all traffic (U-DATA Availability Loss), therefore rendering the deployment non-functional. This constitutes an availability breach.

Let us now assume that the attacker chooses to not attack availability. Instead, he listens passively and waits for a software update to take place. In doing so, he is being very stealthy, and will likely remain undetected unless someone inspects the network's topology at layer 3. As per the assumptions in this scenario, the software update will be unauthenticated and will be transmitted unencrypted. The attacker can reverse engineer the protocol used for software updates. The attacker can thus capture the new version of the software while it's being transmitted. This constitutes a Loss of S/W Confidentiality. An attacker can subsequently transmit his own software "update" to nodes forming the deployment. This constitutes a Loss of S/W Integrity and can be used to allow the attacker to gain remote access to nodes. This situation can then open the deployment to various AAA threats, allowing Device Privilege Elevation or User Privilege Elevation (for example the attacker could impersonate the gateway), facilitating Privacy attacks such as Non-repudiation and compromising U-DATA Confidentiality before the application of higher layer protective mechanisms.

3.9.7.3 Traffic Encrypted at the Link-Layer, with Authenticated Routing

For this scenario, we assume traffic is encrypted at the application layer (end-to-end) as well as at the link-layer. We also assume that the deployment uses RPL in "Authenticated" security mode [106]. Therefore, RPL control plane traffic is protected in terms of confidentiality, integrity as well as authenticity.

Let us assume that encryption at the link layer uses AES in CCM mode (Counter with CBC-MAC) for authentication and confidentiality. Broadly speaking, there are two methods to establish encryption keys: i) preinstalled key pools or ii) dynamic key establishment [115]. If dynamic key establishment is not in place, then the attackers simply have to repeat the previous attack and eavesdrop for long enough until they can expose a subset of the encryption keys through brute force attacks. Let's assume that encryption at layer two uses some form of dynamic key establishment, by employing for example Elliptic Curve Diffie-Hellman (ECDH). This may be susceptible to man-in-the-middle attacks, which can be employed by attackers to gain access to link layer traffic. Routing traffic is still authenticated though, and RPL's crypto keys have not been exposed yet, so the attackers cannot compromise the routing infrastructure. However, since the attackers now have access at the link-layer, they can attempt an attack against IPv6 neighbour discovery. This will allow them to capture traffic as well as decrypt the link layer payload. Application layer traffic is still protected against confidentiality attacks, but the deployment's availability is now exposed (Loss of U-DATA and C&C-DATA Availability).

As per the previous scenario, application layer and routing traffic is encrypted, but software updates are not. This means that, once the link layer payload can be deciphered, the confidentiality of software updates is no longer protected. Attackers are thus able to reverse engineer the software

update process as per the previous scenario. They can then transmit their own malicious software and *compromise* some of the deployment's nodes. This can potentially expose keys used for encryption at higher layers and use this information to attack the routing infrastructure, or even to decrypt application layer U-DATA.

3.9.8 Threats to C&C-DATA Integrity in the Environmental Monitoring Use-Case

As per the use-case description, we examine an environmental monitoring installation with multiple SOs collecting environmental data and executing actions. The deployment is equivalent to that of the Comfort Quality Monitoring use-case, with one exception: Every SO is installed on the street on a mounting support. The fact that SOs are mounted on streets implies that both the installation and execution environments are much less secure than the comfort monitoring one. Hence all threat examples of the Comfort use-case are applicable to this one and are not going to be repeated. Instead, in this section we will focus only on those cases that are not also applicable to the comfort quality monitoring scenario.

In this scenario we assume a deployment where:

- At least part of the C&C Data for each SO are retrieved from external sources, let it be a single or several servers hosting them. For the purpose of this example we will call these hosts providing these C&C data 'configuration servers' and
- The SW running in the SO object itself is subject to be downloaded from external hosts, whose definition and location is part of the C&C data retrieved as well.

In this scenario, we consider the time period during which SOs are being installed physically on the mounting platforms. As part of the installation, each SO will need to obtain its first C&C Data from the configuration server/s, and this will be a particularly good moment to try a 'man in the middle attack', for instance during the negotiation phase of the keys in the establishment of the connection between the installed SO and the configuration server. Should an attacker got to impersonate a valid configuration server during this phase, It could *compromise* the SO and possible even its measures.

The scenario could be something like this:

1. A municipality worker physically connects the new SO to the power and network and switches it on
2. As part of the aforementioned initialisation process, the SO tries to connect to the configuration servers to obtain external C&C data, including valid keys for future connections
3. During the negotiation phase of the establishment of the connection, an attacker intercepts the communications and presents itself as the addressed configuration server, forwarding all communications to the real configuration server. If the attacker got to do this interception during the negotiation phase, it would get access to the communication keys, being able to tamper all the transmissions and sending its own configuration to the SO, including rewriting the location of the hosts providing the SW for the SO for making them to be malicious hosts
4. Malicious hosts get their own SW to replace the one from the SO
5. Once the SO is working with a configuration sent by an attacker and running the SW from the pirate hosts, it is subject to any kind of malicious attack, either by installing new malicious components or sending its information to a fake server.

Once an attacker got to provide his own configuration data, it would lead all the threats explained in this document except *Device Privilege Elevation* in the following way:

Loss of Confidentiality of Authentication CREDENTIALS: If the SO got its credentials during the negotiation phase, an attacker would get them as well during the disclosure of the negotiation phase

Loss of U-DATA Confidentiality: The attacker could send the address of a new fake server to receive the measured data as part of the C&C data faked

Loss of C&C-DATA Confidentiality: Once the SO is running pirate SW, it can gain access to any C&C-DATA, with the possible exception of the previous configuration servers, which were overwritten in the first moment of the attack.

Loss of S/W Confidentiality: Once the SO is running pirate SW, it could make a whole inventory of the previously existing SW and even forward it to a pirate server.

Loss of U-DATA Integrity: The attacker could make use of the credentials of the SO stolen during the initial negotiation phase to impersonate it and send completely faked data

Loss of C&C-DATA Integrity: The attacker could completely rewrite the whole set C&C Data with his own SW downloaded

Loss of S/W Integrity: The attacker could completely rewrite the whole SW installed in the SO with his own SW downloaded

Loss of U-DATA Availability: The attacker may simply send the U-Data to a different host, making it unavailable for the legitimate one or it could even rewrite the collecting SW for making sure that the data is never collected

Loss of C&C-DATA Availability: The attacker could completely delete the whole set C&C Data with his own SW downloaded

Loss of S/W Availability: The attacker could completely delete the whole SW with his own SW downloaded

U-DATA Repudiation: The attacker could completely modify, delete or alter the saving process of the by replacing the SW responsible for producing or saving the logs

C&C-DATA Repudiation: Same as U-Data Repudiation

Identity Spoofing of a User with Higher Privileges: The attacker could add his own authorization SW to invoke the previous one and see the result of each request in the system to infer the privileges of each user trying to access the system

Device Identity Spoofing: The attacker could install his own SW to retrieve any identity files stored in the system. Nevertheless, should these files would be protected against disclosure, spoofing them would not be trivial and could require a complex process of reverse engineering of the previously installed SW to break it, depending on the protection type.

User Privilege Elevation: The attacker could completely replace the whole SW responsible for authorizing requests with his own one, letting only requests coming from a pirate user to pass. This would be true even for requests authorized externally to the SO, because the attacker could modify the configuration of the service to be exposed by a different (malicious) application server that surpass the original authorization process

A key measure to prevent this kind attack is to ensure that the establishment of the connection between the SO and its associated configuration servers is protected against disclosure even during the phase of key negotiation. A common way to achieve this is to work using a predefined set of keys that are not negotiated during the establishment of the connection but have been stated out of the transmission instead. For instance, the SO might be using a smart card with a key previously stored that also knows the key from the configuration server, and the same for the configuration server itself. This way, the transmissions could travel encrypted by these keys without the need to negotiate them during the establishment of the connection itself.

3.9.9 Threats to U-DATA Integrity in the Environmental Monitoring Use-Case

In this second scenario we do not make any additional assumption to the use-case and study a kind of attack that is very specific of an outdoor scenario. In an indoor scenario, either it is not easy for an attacker to physically access the measured environment or is not likely that the people with that

physical access are interested to perform an attack (in the case of the comfort monitoring it would not have much sense for the owner of the house to tamper U-Data).

But in the case of the environmental scenario an attacker could indeed be motivated to *tamper* U-DATA. Environmental measures may be used as a political weapon, either to blame the administration for poor management producing bad measures or to deceive the people stating that the pollution levels are much better than the real ones.

The attacking scenario could be like this:

1. The system is correctly set up and running
2. It is 3:30 a.m. There is nobody in the streets and an attacker hired by a political rival wants to produce heavy CO_2 levels to blame current municipality administration for high pollution levels. The attacker stands below the SO and burns a paper there. The paper produces smoke with pure CO_2, which is dissolved on the surrounding air, producing the measures taken some meters above in the sensor to indicate CO_2 levels much higher than usual.
3. The sensor properly reads this altered U-data, that results in faked U-Data reported (the false high levels of pollution measured)

As it can be seen, this is an extremely straightforward attack that can be executed with no technical knowledge at all. In this case, it is the data measured what has been compromised, that is, but the system remains intact. For this reason, any protection mechanism against this type of attack but be based on an analysis of the measured data themselves aiming to locate weird values and discarding or at least putting them on quarantine.

4 Relation between Use Cases, User requirements and RERUM technical contributions

4.1 Discussion

This Section describes the technical contributions of RERUM in the context of security, privacy and reliability requirements for IoT in Smart Cities, providing an overall vision, relating the various scientific and technological achievements with the use-cases and the exploitation strategy.

As a summary on the broad scope of IoT challenges, let us state that

- The IoT will have a huge amount of security, privacy and reliability problems, including the ones of the current Internet.
- There is a tension between functionality and privacy, particularly in the IoT. Largely, the dream of IoT is the use (and re-use) of data, openly and without barriers and obstacles, to enrich the data with other related information and to compose new services. This, in general contradicts the principles of privacy, based on the idea that IoT data should be treated as private data and the collection and processing purposes must be defined beforehand.
- Will people in the Internet age ever earnestly try to regain their privacy? There is a large controversy and a societal debate about whether this is possible and reasonable.

With those challenges in mind, let us state that

- The amount of effort to secure the IoT as a whole is beyond the scope of this project.
- RERUM will not try to work on Internet security problems (like the security of PKI in general or TLS) nor plans to tackle the Human factor in IT security – which is often the weakest link: employees and even administrators do not comply with existing security policies, users are not well-educated in security issues and rely blindly on the technological infrastructure, etc.).
- RERUM's focus is to enable the development of secure, resilient and reliable solutions for a city environment incorporating Privacy Enhancing Technologies (PETs) and 'privacy by design' (PbD) into the development process and providing building blocks adequate to the new constrained environments of the IoT.
- The RERUM approach is based on the principles of multilateral security, where each principal has minimal assumptions about others. Each party has his own protection goals, can formulate them in policies; can have assurance about the enforcement of its protection goals (given some necessary assumptions on trusted parties). In particular, RERUM offers the possibility to End Users to describe their own privacy policies, independently of the security goals of the infrastructure, the application or the service owners. In a similar way, the other stakeholders are able to express and enforce their policies.

The Internet of Things offers a much larger attack surface compared to the conventional Internet. This is due to the large number of devices and therefore the amount of single interfaces that require protection, and to the new interaction possibilities between devices and between users and devices, creating new ways of exploiting vulnerabilities and threats. On the other hand, the constrained devices will restrict the possibilities of security measures; the IoT will require efficient lightweight cryptographic primitives, authentication, and authorization procedures and primitives suitable for low resource consumption (energy, time, space). Moreover, due to the ubiquitous and embedded characteristics of smart devices in IoT, which pervade everyday life, the privacy dangers due to unobtrusive data collection methods are more critical than in traditional office or home situations. The devices and the system must cope with changes in connectivity, routes, or environmental context due to mobility of some of the devices, or errors, power failures, etc. The IoT integrated with

the rest of the Internet must co-exist with the standard Internet security protocols and mechanisms (like IKEv2/IPsec, TLS, PANA/EAP, SAML, and XACML) or bridge to them. The IoT requires new intrusion detection systems and survivability mechanisms to detect problems and has to be able to react to changes in such environments. Trust management will have a major importance, due to the large amount of devices and users of many different environments to establish trust relationships between users and devices, which might be complete strangers to each other. Authentication of new devices and key management in this context is still an open issue. It is necessary to define Security/privacy policy languages and mechanisms to enforce them to control how the data are created, accessed, and protected. The resulting policies and security levels must have a high usability value: the security for IoT-based applications must be understandable and manageable by end-users. The software maintenance process is prone to security issues in a larger extent than what is already the case in more conventional systems, due to the large number of devices, the constrained interfaces, and the heterogeneous administration. Who will be responsible for updating the security mechanisms or providing "patches" for devices in a world with many different device manufacturers, service providers, device owners, administrators, etc.? (And how will the different solutions work together?) “Things” belong to people and collect information about actions of them, but the devices and interfaces should not leak personal information about the location, activities, and preferences of users in an uncontrolled manner. It is necessary to avoid that a communication partner (or an administrator, or a service partner) is able to collect large amounts of information, and draw inferences about behaviour of the citizens. Current algorithms do not prevent this type of attacks.

Besides all this, the vulnerabilities of the existing Internet and Computer Systems endanger the security of the IoT. If hackers can enter into the servers that provide the interfaces to users to manage their IoT devices or configurations, or if Trojans or malware can compromise the computers of the city or of the users, the security of the IoT is also in trouble.

Already the table of contents of standard handbooks of security practice (see [116], [117], [118]) show the vast amount of topics that are necessary to cope with to secure current IT systems. All these are also necessary for the IoT and in many cases they require more effort than for non IoT environments, due to the constraints in the solution space and to the larger attack surface.

In order to secure the IoT, it will be necessary to secure the Internet itself (servers, services, clouds, etc.), but the current security problems have been clearly demonstrated by the devastating attacks against cornerstones of the Internet security such as PKI, TLS, passwords, Hardware, etc. (see [119], [120], [121], [122], [123]).

[124] claims that “our privacy died when we grew obsessed with free”. Indeed, the current model of the new Internet economy is to obtain information from users to provide “targeted advertisement”; in this way providers may offer their service in a way which is perceived as “for free” by the user. If this trend becomes the de-facto model for the IoT, then indeed “IoT will kill our privacy”, see [125]. What is the economic model that RERUM proposes? What are the services? What are the addressed problems? Who gets the value? Who would be prepared to pay for them (and why)? This is not a trivial question, and the debate goes on whether users will like to pay more for transparency and control of their private data. Regulation will play an important role in this discussion, but the society requires technical innovations that make PETs and PbD a viable alternative. Privacy, security and reliability will not come to the IoT for free. To be more specific: What new services will offer RERUM? RERUM will not offer, as much of the current research on IoT does, new visions on how to provide more intelligence,, increased efficiency, smoother interoperability, improved business processes, reduced costs, sensor-driven decision analytics (see for instance Section 3.1 “Internet of Things Vision” of the IoT-IERC Cluster Book [126]). On the contrary, the PbD methodology (and in particular the fundamental principles of purpose and consent (see [127]) or transparency and control (see [128]) will limit and inhibit the free data sharing of IoT data, which should be considered as private data, as the Data Protection and Privacy Commissioners have concluded Oct 2014 in their Mauritius Declaration on the Internet of Things [129].

We do not want to and we can't secure the IoT as a whole: this is surely beyond the scope of any project.

The project's main objective is to develop a framework, that offers proactive and reactive security and privacy-enhancing mechanisms which enable the secure establishment of networks of smart objects, as well as their secure and reliable communication. RERUM should provide some technical options to cities to protect the personal data of their citizens and enable them to provide end users control over the usage of their data in smart environments. Such options rarely exist in current environments (see [130]).

Perhaps the society will end giving up privacy. Google's Chief Internet Evangelist Vint Cerf for instance doesn't think we ever really had that privacy to begin with. He thinks that privacy is, perhaps, an "anomaly", and that "it will be increasingly difficult for us to achieve privacy" [131]. In any case, the privacy/security/reliance front will need technical solutions to be able to fight the battle. The RERUM consortium believes that the society will recognize the need to regain their privacy and will be willing – or forced, by regulation – to pay a price for this. This faith, or hope, is the basis of our business model in the project. As the Data Protection and Privacy Commissioners conclude in their recent Declaration [129]: "Privacy by design and default should no longer be regarded as something peculiar; They should become a key selling point of innovative technologies."

Beside the security and privacy issues that have to be encountered in IoT applications, there are also other critical challenges related to networking, connectivity and energy efficiency issues. More specifically, a vast number of interconnected devices is expected in IoT applications, raising the need for improved resource utilization and scalability, especially for applications involving wireless connectivity. Furthermore, exactly due to the large number of devices that are expected to be interconnected in IoT applications, the needs for energy efficient communications and for reliable connectivity have to be addressed at the design of a new system. RERUM has identified the key challenges of IoT with regards to efficiently interconnecting devices that provide various services that may have quite different QoS requirements and aims to provide efficient networking mechanisms to increase the reliability of the networking of the devices. Furthermore, in the IoT world most devices either run on batteries or have limited power sources, which raises the issue of low energy consumption in order to extend the lifetime of the devices. This is of outmost importance basically from a technology point of view because devices with dead batteries can't send data and can't contribute to the system. When these are "leaf" devices, only their own data are lost, but when these are intermediate devices playing the roles of forwarders and cluster heads the system's performance can degrade significantly. From a non-technological view, however, the increased lifetime of devices means a not frequent requirement of manual intervention to exchange batteries, decreasing the manual overhead and decreasing the expenditures of the service providers/cities. It is reasonable to assume that the more mechanisms are running on the devices, the higher energy consumption they have; however, within RERUM we have identified this issue, and for this reason we aim to make lightweight mechanisms for consuming very low system resources and to develop specific techniques that aim to reduce the energy consumption of unused devices. Additionally, reliability, availability and energy efficiency can be also enhanced through the employment of opportunistic and cognitive communications, which enable the utilization of unused wireless resources in a more efficient way than traditional wireless technologies.

4.2 RERUM technical contributions

In the following, we present a detailed overview of the contribution of RERUM to the cities and the citizens. The tables to follow summarize the following questions, see Figure 24:

- What are the particular **situations** in the **Use Cases** that require, from the point of view of security, privacy or reliability, a special attention?
- What **Security or Privacy Issues,** or **Reliability/Availability/ Scalability/Efficiency Issues** that

an end user – normally a citizen, but in some cases a city officer, an administrator, a network/service provider or an authority – may encounter in those particular situations? Why does conventional technology do not solve this problems in this situation?

- What are the **User Requirements** that emerge from this issue? What does the user want, in terms of privacy, security, reliability or efficiency? For the sake of readability and to offer the reader a better overview, we have clustered the User Requirements in 28 logical groups and numbered them as UR1, UR2, etc. A summary of the User Requirements is found later at the end of the Section in Table 26.
- How are those User Requirements implemented as **Technical Requirements**? The technical requirements correspond to the ones discussed in Deliverable D2.2.
- Besides the technical requirements, that RERUM wants to tackle, what side-**constraints** must be met, what conditions should be true, or what other requirement that is **out of our scope** must be fulfilled, so that the issue is solved?
- How will the requirement be implemented? What will be the **contribution** of RERUM to the end user or to the city? Why will the End User like to user RERUM?
- What is the **Status of the Innovation**? Will the contribution be fully specified, simulated, implemented, or even demonstrated in the RERUM trials?
- What is the **Exploitation / Service on Market** strategy? What services are planned and what marketing opportunities are foreseen?
- What are the **Business models & go to market approach**? How will the RERUM partners capitalize on the investment?
- What is the **Priority of the contribution?** How important will this be in a smart city deployment?

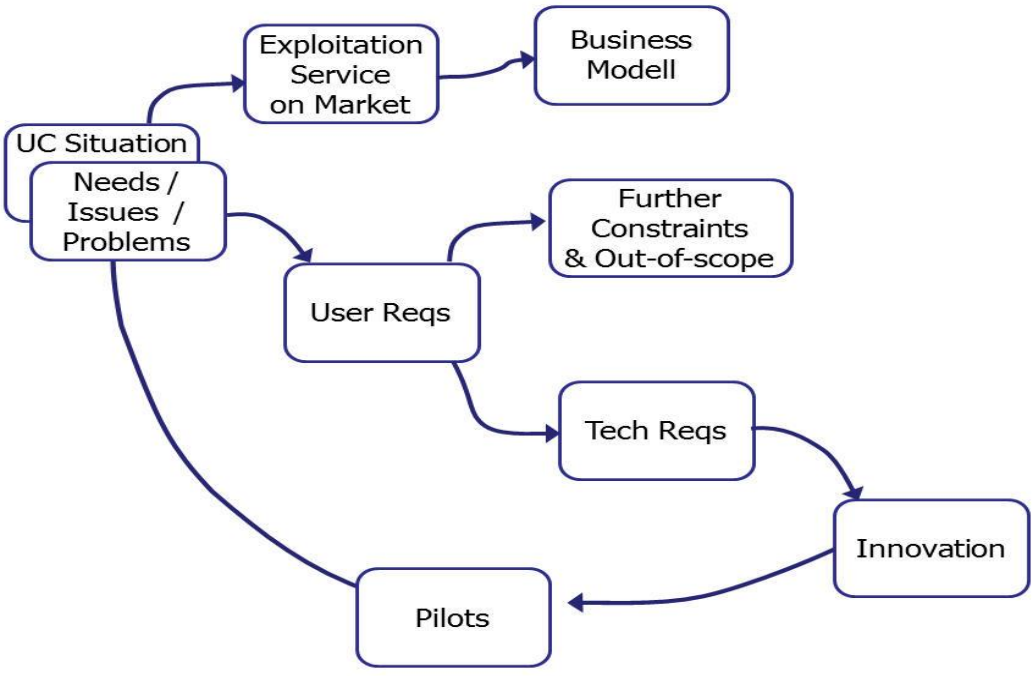

Figure 24: Links presented in the table

The next set of tables describe the technical innovations / contributions of the RERUM project, which will be defined in detail, and evaluated in the deliverables of the pure technical work packages of the project, namely WP3 and WP4. At the title of each innovation we state exactly the WP that each innovation belongs, so that the reader can refer to the respective future deliverables for more information.

Title	Secure Credential Bootstrapping (WP3)
Priority	Medium-High: In a real-life deployment of RERUM, it will be necessary to endow commercially available devices with the proper credentials to interact with the network in a secure manner. In closed environments the requirements for security on the bootstrapping protocol level are less than in open environments.
Use Case Situation	(All UCs) The end user has bought a new device in a hardware shop. He plans to use this new device to control the temperature at his home, automatically (based on some policies he may define) or on real-time using a portal provided by a third party, e.g., a service provider or city.
Security or Privacy Issues	The new device will leave any communication (sensor measurements or actuator commands) unprotected. A neighbour or a burglar may intercept the messages and infer from them what the persons in the home are doing, or if the place is empty. A hacker can have fun changing the temperature in the home, and rejoicing that the home user will arrive evenings to a freezing home.
User Requirements	UR-1: A user wants to securely introduce a new device into the network, so that afterwards messages sent by his device to the gateway and to other devices of his network are kept confidential and are not modified by unauthorized people.
Constraints, Out-of-scope topics	In order for our solution to work, the following things have to be in place • Configuration of the network and routing of messages • Devices with manufacturer based credentials or devices that allow pairing mechanisms • Credential store on the device • Functions to authenticate a device towards another device/server
Technical Requirements	Req. 2.6 19 Secure bootstrapping of operational cryptographic credentials Req. 2.6 20 Availability of initial credentials Req. 2.6 21 Support of different operational credentials types Req. 2.6 22 Avoidance of manual interactions during credential bootstrapping
Description of the Innovation	When a new device wants to join a network that is secured and has measures in place for authentication, integrity protection and confidentiality, a conflict exists: on the one hand, the new device needs security credentials to participate within the network, but on the other, it has no knowledge about the network and the network does not have knowledge about his credentials that would allow him to participate as authenticated network entity. As the distribution of credentials is a security sensitive step, the procedures must be protected to mitigate attacks during the bootstrapping phase.
Status of the Innovation	The innovation is currently being drafted as part of task 3.1 and a concept for bootstrapping security credentials for new devices joining a network will be described. Bootstrapping sequences for devices with and without manufacturer credentials will be specified. Implementation of protocols and mechanisms or integration of a bootstrapping environment into the trials is out of our scope.
Exploitation / Service on Market	This innovation is expected to be attractive to device vendors, since it would allow devices to securely join networks and retrieve the required credentials in a secure manner.
Business models & go to market approach	A RERUM security and privacy architecture is only as secure as the level of security of credentials and their deployment. If credentials are compromised during the bootstrapping phase, subsequent security measures are weak, even they are strong on the protocol and algorithm level. With the increase of published security attacks, cities, citizens end users are more and more interested to rely on secure systems.

Contribution 1: Secure Credential Bootstrapping

Title	Consent Manager (WP3)
Priority	High: One of the cornerstones of privacy is consent [127]. In some cases, consent can be given at subscription time, if three conditions are true: the data to be collected can be foreseen at this moment, if the data is not highly sensitive, and if the purpose of the collection can be defined a-priori. But in some cases, explicit consent must be provided on real-time and a mechanism for storing and verifying the presence of the consent must be developed.
Use Case Situation	(UC-O1, UC-I1, UC-I2) Example: An end user is travelling to the centre by car. His navigation system notifies him that the traffic is rather heavy. He would like to use a new service of the city that informs users about alternative routes, possible public transport alternatives, etc, offering a set of different parking places and different types of subscriptions for monthly transportation passes, etc. To use this service, the user must accept that the city receives his current location, the location of the place he is intending to reach. The city is allowed to disclose that information to the parking and transportation authorities in order to issue one-time tickets for the use of the parking space and the public transport.
Security or Privacy Issues	Today a simple "implicit consent" is used: the user by entering the OK to the system is implicitly accepting the conditions for the use of his private data. There is no proof of consent at a server side that is being checked when the transportation authority or the parking administration want to access the information to issue the tickets.
User Requirements	UR-2: The user is not comfortable with the "all-or-nothing" approach of current apps accessing location data. He would like the data to be transmitted to the city only when he wants and to the other parties (transportation, etc) only when he has allowed this (either by specific policies or on real time).
Constraints, Out-of-scope topics	Service providers have to be able to prove to the authorities or authorized auditors that they have procedures in place to collect and use personal information as declared and agreed. Users are required to have device with an advanced graphical user interface or with audio capabilities to receive consent request and to give their consent.
Technical Requirements	Requirement 2.6-11 User Consent and choice
Description of the Innovation	The consent manager enables dynamic consent requests and allows end customers to understand how their data are going to be collected and how it is intended to be used. The consent manager will display data collection policies from service providers to end users. This may be similar to P3P or EPAL (in the case of Web applications) [132].
Status of the Innovation	The innovation is an integral part of RERUM's architecture. The innovation could be implemented as a prototype, where the graphical display and the policy processor are simplified.
Exploitation / Service on Market	The consent manager and the privacy dashboard (see D2.3, section 6.11.2.4) are web-based systems, which can be developed and brought to market as standalone products. The concept behind both innovations allow high adaptation to different systems, such as app marketplaces, web services, etc.
Business models & go to market approach	RERUM is convinced that Privacy by Design and Default should no longer be regarded as something peculiar. They, we hope, will become a key selling point of innovative technologies and will allow the generation of more complex city services [129].

Contribution 2: Consent Manager

Title	Lightweight and Efficient Pseudonym System (WP3)
Priority	High: RERUM aims to provide a platform for privacy protected services in smart cities These services rely on the information provided by inhabitants, but this information should not allow the service providers to gain intrusive details of their subjects. At the same time citizens and service providers alike need to know that they are interacting with each other in an authentic way. This relationship is best provided by pseudonyms.
Use Case Situation	(All UCs) The end user is travelling around the city. The city relies on users to help by sending anonymous information about the current traffic conditions (more precisely the times required for trips by car, etc.), the locations most visited during the day and currently at the moment, the status of the garbage bins, any problems that the citizens encounter, etc..
Security or Privacy Issues	If information can be sent anonymously, malicious or careless members could send the city officials to incorrect places, as seen in Poland [133].
User Requirements	UR-3: Even if the information can be sent anonymously, the user wants really to get his problem solved and does not want that "anonymous" users send incorrect information to the city. UR-4: The city authorities want to be able to block people trying to pass significant amount of incorrect information to the city officials.
Constraints, Out-of-scope topics	Pseudonym generation and coordination requires devices that are able to compute cryptographic hashes.
Technical Requirements	Requirement 2.6-14: Data minimisation.
Description of the Innovation	Pseudonym systems in constrained environments use typically a resource-rich trusted third party that manages and generates pseudonyms for all participants (e.g., see [134]). In the Internet of Things it might not always be possible, or desired, to rely on such a third party. In this case, devices have to generate and coordinate pseudonyms themselves. The innovation describes how resource constrained devices can be able to generate and coordinate an infinite amount of pseudonyms efficiently. The innovation uses cryptographic hashes, which are easily manageable for constrained devices.
Status of the Innovation	The innovation will be used by Siemens AG within products in several BUs. The innovation will not be implemented for RERUM.
Exploitation / Service on Market	The innovation impacts any supplier of "smart" devices, vehicular networks as well as any system with privacy protection of their participants (such as web-based systems). The innovation will be used by Siemens AG in different business sectors.
Business models & go to market approach	RERUM is convinced that Privacy by Design and Default should no longer be regarded as something peculiar. They, we hope, will become a key selling point of innovative technologies and will allow the generation of more complex city services [129].

Contribution 3: Lightweight and Efficient Pseudonym System

Title	Privacy Policies as Software Artefacts (WP3)
Priority	High: The Internet of Things will allow interchanging data without any interaction. The interchange of personal data must not happen without the data subject's notice and consent.
Use Case Situation	(All UCs) Example from UC-I2: Users enter a smart building, say the main public market in a city. The moment the users enter the building, they are being monitored by the building's smart devices and the user's smart devices may interchange data with the building, in order to accommodate the user in terms of temperature and air quality, to localize particular places, , to get specific offers or advertisements from the nearby shops, etc.
Security or Privacy Issues	EU-Directive 2002/58/EC article 6 requires service providers to specify the purpose of the collected data and to always comply with it when processing private data. From the user perspective, this means that a user has to accept or reject every request from a service provider. Due to the massive interchange of data, it is not feasible to do this manually every time.
User Requirements	UR-5: The user requires to be able set by himself specific privacy policies for the Virtual Entities that are of his interest or he owns. The user requires also to be able to set specific policies for data collection and to request specific information to be given by the application/user that wants to have access to the respective VEs.
Constraints, Out-of-scope topics	Our solution is described with IoT-A's reference architectural model in mind, but it can be adapted to any architecture.
Technical Requirements	Requirement 2.6-12: Purpose legitimacy and specification
Description of the Innovation	The innovation proposes privacy policies as software artefacts. They are associated to the Virtual Entity belonging to a Data Subject. When taking decision about using Data or Service associated with the Virtual Entity, the policy is enforced.
Status of the Innovation	The innovation it will not be implemented.
Exploitation / Service on Market	RERUM internally discusses to push this innovation as a draft to standardisation bodies.
Business models & go to market approach	RERUM internally discusses to push this innovation as a draft to standardisation bodies.

Contribution 4: Privacy Policies as Software Artefacts

Title	Lightweight and Efficient Privacy Preserving Authentication (WP3)
Priority	High: End users and service providers need to interact in an authentic way while preserving the end user's privacy. Existing privacy enhancing technologies may not be adequate for all scenarios of IoT, as they use asymmetric cryptography, or require encryption or other energy-consuming algorithms.
Use Case Situation	(UC-O1, UC-I1, UC-I2) Example from UC-O2: The city asks citizens (and taxi drivers, etc) to help measuring the air quality in certain city areas and provides them devices for this purpose. The city receives and analyses the values and advises citizens to avoid certain areas until air quality normalises. An end user uses the bicycle sharing service of the city. He authenticates himself with a secret to use the bicycle, but he does not want to reveal who he is. On the other hand, the service provider wants to know who the user is in case he acts maliciously, if he leaves the urban perimeter, or in case of an accident.
Security or Privacy Issues	If the service provider can identify who authenticated himself or if he can identify the devices of a user, privacy-invasive conclusions about the user's preferred locations and habits can be drawn. At the same time, a service provider has to be protected from malicious use; he has to know that a user or a device is authentic.
User Requirements	UR-6: The user needs to be able to access services being authenticated, ensuring the protection of his identity. UR-7: The user needs to ensure the unforgeability and authenticity of messages he exchanges with the system.
Constraints, Out-of-scope topics	The devices used for authentication are capable of computing cryptographic hashes.
Technical Requirements	Req. 2.6-12: Purpose legitimacy and specification. Req. 2.6-1 Energy-efficient cryptographic primitives
Description of the Innovation	The innovation is a mechanism that resembles group signatures – a well-known privacy preserving authentication procedure based on asymmetric cryptography [135] – but uses only symmetric cryptography and cryptographic hashes.
Status of the Innovation	The innovation will be used by Siemens AG in different products. The innovation will not be implemented for RERUM.
Exploitation / Service on Market	RERUM internally discusses to propose this innovation as a draft to standardisation bodies. The innovation will be used by Siemens AG within its business units.
Business models & go to market approach	RERUM internally discusses to push this innovation as a draft to standardisation bodies.

Contribution 5: Lightweight and Efficient Privacy Preserving Authentication

Title	Implicit Certificate Based Device-to-Device Authentication (WP3)
Priority	High: IoT requires secure interaction directly between devices, or gateways and devices. This is somehow the IoT's `last mile'. For the overall IoT security, devices must mutually know, e.g. authenticate, each other. Other security mechanisms, e.g. like encryption or reputation-systems, also require a secure mutual authentication between devices.
Use Case Situation	(All UCs) The end user is introducing a number of new devices into the deployment he administrates; be it during the initial setup or when adding additional devices (sensors and actuators). These new devices are physically known to the end user and, following the end user's wish, are going to become authorised to participate in end user's deployment. He wants to limit, because the network bandwidth is sparse and data reported from known devices is going to be used for decisions. Hence, data from unknown devices shall be considered with additional care, e.g. needing additional confidentiality or reduced trust. In the traffic use case, assume the new device is mounted on a bus and is used to identify this particular bus. It talks to the device of a certain traffic light along the route allowing the bus to trigger a change to a green light.
Security or Privacy Issues	If other devices are not able to identify an authorised from an unauthorised device, an attacker can impersonate a legitimate device. This allows attacker to: a) send his traffic through the end user's infrastructure (DoS, reduce QoS) b) prevent reception of legitimate messages (attack routing of messages) Improper device-to-device authentication in the traffic management example, allows the attacker to trigger a flow of green lights for himself instead of the bus.
User Requirements	UR-8: The user needs to be sure that he will reliably exchange only legitimate information and commands through a network of legitimate devices. The end user bases decisions on gathered data, no "unauthorized and unknown" device must send potentially incorrect data to city applications or introduce wrong commands to actuators. City wants to protect networks from unauthorised use and allow optimal flow of legitimate messages. The legitimate messages shall be protected against malicious undetected tampering (UR-7).
Constraints, Out-of-scope topics	To work we build on credential bootstrapping being run (*Req. 2.6-20 Availability of initial credentials*) and require cryptographic algorithms on devices (*Req. 2.6-1 Energy-efficient cryptographic primitives*). Further we assume a RERUM Gateway instance already set up and allowing devices to communicate (mesh-type networks) with each other, and we assume an identity provider/certificate authority mutually trusted by devices willing to authenticate.
Technical Requirements	Req. 2.6-8 Device authentication. Req. 2.6 19 Secure bootstrapping of operational cryptographic credentials Req. 2.6 20 Availability of initial credentials Req. 2.6 21 Support of different operational credentials types
Description of the Innovation	The Device-to-Device Authenticator component running also on a RERUM device establishes mutual ``peer entity authentication" (RFC 4949 or ISO 7498-2). After a successful run of the protocol, both devices are assured the identity of the other device; This allows, among others, device-to-device encrypted and authenticated communication channels. The involved asymmetric cryptographic material is bound to each device by a lightweight certificate issued by a root of trust. To reduce the load of cryptographic operations RERUM will base on Elliptic Curve Cryptography and especially facilitate the concepts behind Implicit Certificates [136]. A schema of certificates for this will be detailed in RERUM
Status of the Innovation	The innovation is currently being drafted in terms of the actual protocol's message flow and the cryptographic underpinnings as part of WP3. RERUM

	internally discusses to push this innovation as a draft to standardisation bodies. After specification, RERUM will seek implementation on the newly developed hardware (ReMOTE). Depending on laboratory experiments RERUM decides if this innovation can be trialled to the full extend or only partially.
Exploitation / Service on Market	RERUM internally discusses to push this innovation as a draft to standardisation bodies.
Business models & go to market approach	RERUM is convinced that only with a strong protection of the lower networks links a secure networking infrastructure can be deployed and operated. In general we hope, that security will become a key selling point, as only secure networks will get deployed by end users seeking to operate IoT as part of reliable uninterrupted smart city services. RERUM internally discusses to push this innovation as a draft to standardisation bodies.

Contribution 6: Implicit Certificate Based Device-to-Device Authentication

Title	Improved spectrum utilization for IoT applications (WP4)
Priority	Medium: IoT requires improved network reliability, however hardware constrains hamper the deployment of this technology.
Use Case Situation	(All UCs) An end user (service provider/network operator) deploys a very large number of devices that have multiple network interfaces for accessing either WiFi or Cellular networks. The user must ensure the reliable operation of this number of devices to maximize network efficiency and avoid performance degradation due to congestion at the wireless links. The citizens will face improved network connectivity and lower costs due to the exploitation of the free unlicensed bands instead of the costly cellular networks.
Reliability/Availability/ Scalability/Efficiency Issues	Deploying large number of devices that access ISM bands raises issues of congestion and poor spectrum utilization. Conventional solutions are usually based on a single radio interface for transmitting data, or in the case that they involve more than one air interface, they do not support internetworking and universal resource allocation. If the device connectivity is not optimized, the network reliability will be degraded and the QoS of the services that the users receive will not meet their requirements. Poor radio resource utilization can degrade significantly the performance of the overall system.
User Requirements	UR-9: Users require improved QoS and availability, improved network reliability, improved radio resources utilization, which is translated in more connected devices and minimization of the expensive licensed spectrum utilization.
Constraints, Out-of-scope topics	The network architecture should comply with the 3GPP TS 23.234 version 11.0.0 Release 11 (I-WLAN).
Technical Requirements	Req. 2.3 1 Support of a large number of attached devices/objects Req. 2.3 2 Dynamic spectrum management Req. 2.3 4 Operation in unused spectrum bands Req. 2.3 7 Multi-technology and multi-operator connectivity Req. 2.3 9 Overall QoS Req. 2.4 6 RD Communication interfaces
Description of the Innovation	A novel algorithm has been developed, which centrally takes into account the network topology and near-optimally decides which RDs will connect to WiFi access points and which will connect to the cellular access points (i.e., base stations). The algorithm can be applied to a predetermined geographical area, according to the number of devices this area involves. Furthermore, the algorithm has the ability to include in the optimization problem, the fact that a common user with a smartphone can share the cellular broadband connection and serve as an access point (tethering) for a RD.
Status of the Innovation	The innovation will be tested via system simulators. Real world trials are not possible at the moment, since a network architecture complying with 3GPP TS 23.234 version 11.0.0 Release 11 is not available.
Exploitation / Service on Market	This innovation is in the process for being patented. This innovation is expected to be attractive to network operators, since it offers an improved utilization of radio resources and the converged network operation of WiFi/LTE architectures, especially for applications involving a large number of devices as in IoT applications.
Business models & go to market approach	Device vendors may request to exploit this innovation for building devices as described above.

Contribution 7: Improved spectrum utilization for IoT applications

Title	Energy efficiency for RDs with multiple air-interfaces (WP4)
Priority	High: energy efficiency in devices is of significant importance for IoT
Use Case Situation	(All UCs) Battery lifetime of devices may be an issue in IoT applications. The end-users require devices with improved lifetime, especially in cases where the replacement of the battery may be difficult. Radio transmissions are consuming a large amount of energy, which also depends on the radio interface that is utilized. In devices with multiple radio interfaces of different technology, the user will be able to select radio interface to be used depending on the remaining battery lifetime. Thus, the users will have improved network performance in terms of QoS and reliability.
Reliability/Availability/ Scalability/Efficiency Issues	With conventional solutions the devices have only a single radio interface for transmitting data, or in the case that they involve more than one air interface, they do not support automatic switching for energy consumption optimization.
User Requirements	UR-10: The end-user requires network reliability and improved battery lifetime for their IoT applications, as well as lower maintenance costs and not frequent battery changes.
Constraints, Out-of-scope topics	The following measurements shall be performed at the devices: The GSM Received Signal Strength Indicator (RSSI), the UMTS Received Signal Code Power (RSCP) or the LTE Received Power of the Reference Signal (RPRS) and the WiFi Received Signal Strength Indicator (RSSI). This means that the device has the ability to measure simultaneously the received signal power from two different radio interfaces.
Technical Requirements	Req. 2.3 1 Support of a large number of attached devices/objects Req. 2.3 2 Dynamic spectrum management Req. 2.3 4 Operation in unused spectrum bands Req. 2.3 7 Multi-technology and multi-operator connectivity Req. 2.3 9 Overall QoS Req. 2.4 6 RD Communication interfaces Req. 2.4 10 Low energy consumption
Description of the Innovation	This innovation enables RDs and Gateways to take advantage of their multiple air interfaces capabilities in order to minimize their energy consumption or increase their network connectivity. The RDs and gateways employ an algorithm that optimally switches between available access networks (i.e., WiFi and Cellular) in order to increase the provided signal-to-noise ratio (SNR), which results in reduced energy consumption or improved QoS depending on the user requirements.
Status of the Innovation	The innovation will be tested via system simulators.
Exploitation / Service on Market	This innovation is expected to be attractive to device vendors, since it would offer improved network performance, QoS experience and battery usage for IoT applications.
Business models & go to market approach	Device vendors may request to exploit this innovation for building devices as described above.

Contribution 8: Energy efficiency for RDs with multiple air-interfaces

Title	Enrich authorization process with reputation evaluation (WP3)
Priority	Low: The Privacy by Design philosophy of denying any access to those data that have not previously defined to be available for a given user and purpose collides with the nature of IoT of letting any device, including unknown ones to access any device for purposes that may be created dynamically with time. Hence, It is necessary to provide mechanisms to empower users letting them to define security criteria for unknown users or even unknown purposes based on the reputation of the requester. With this improvement we reduce the gap between the different concepts of SbD and IoT.
Use Case Situation	(All UCs) This innovation applies to all use cases. An end user requests to get access to some measurements invoking a RERUM service. The system has to perform an authorization process to grant access to the user, checking the credentials of the user, his past behaviour and his past requests to the system. Furthermore, the administrator of the system can allow or grant access to specific services only to trusted users. Thus, there is a need to include in the system a process for evaluating the reputation of the end users that access system services. In a similar case, when a user is sending measurements via his mobile phone (i.e. for traffic monitoring), his reputation must be evaluated before including his measurements into the traffic estimation module.
Security or Privacy Issues	The possible ability of the requester to fake his own reputation could lead to an improper raise of user privileges due to this mechanism.
User Requirements	UR-11: The user wants needs to be sure that only trusted users will participate in the decision making processes of the system and that no malicious users may affect the measurements for their benefit. The user requires a mechanism to calculate the reputation of the users and to define rules for evaluating the reputation of the requester himself.
Constraints, Out-of-scope topics	It is out of the scope of the project to provide an effective set of reputation rules, but to provide a way to evaluate them and prove that it is effective. As a PoC, the project will provide at least one initial and basic set of reputation rules.
Technical Requirements	Req. 2.5-10: Attribute based access control Req.2.5-27: Reputation mechanism for reliability, availability and trustworthiness
Description of the Innovation	The very nature of IoT demands that it must be possible that any device is able to access any service provided it is a legitimate access. The problem is normally that unknown users are prone to get rejected or allowed to have constrained access because of the lack of knowledge regarding the requester's service. This mechanism allows the administrator of the system to define rules for evaluating the reputation of a requester basing not only on the attributes of the user, which might not be useful for guest users, but also on the context.
Status of the Innovation	The project will implement the components for evaluating reputation policies and provide an initial set of policies as a proof of concept. It will also implement the mechanisms for ensuring this evaluation of the reputation is available to the authorization layer and provide at least one access policy that makes use of this reputation evaluation as a proof of concept. This innovation is expected to be part of the trial for UC-I2: Comfort Quality monitoring.
Exploitation / Service on Market	Consultancy service on development of reputation policies Enhanced authorization services
Business models & go to market approach	Consultancy service on development of reputation policies Reputation engine integrated with the authorization layer, which will be an asset of the security portfolio of Atos.

Contribution 9: Enrich authorization process with reputation evaluation

Title	**Integration of ABAC in IoT with support for specific business data contained in the request (WP3)**
Priority	High: Providing an advanced authentication mechanism is one of the most important features that need to be added to any IoT platform, due to the lack of IoT of security measures that allow to check the access of a requester to a given resource / service Medium: Additionally, the ability to define specific security constraints based on their own business rules.
Use Case Situation	(All UCs) A user is trying to access the position of a car, but his request is rejected because only policemen (users of a special type with pre-defined attributes) are allowed to get such type of sensitive information. Instead, the user is allowed to get the location of a bus, which is public information.
Security or Privacy Issues	The access to any service of resource from any device (which must be executing on behalf of a user) must be checked to comply with the security criteria defined in the system, even those based on information contained on the request that is specific for it.
User Requirements	UR-12: The user requires to be able to define specific access criteria so that the system can make decisions based on the attributes of the user that is issuing the request, and the context of the request.
Constraints, Out-of-scope topics	It is out of the scope of the project to define a complete set of security criteria, which are meant to be provided by the administrator of the system.
Technical Requirements	Req. 2.5-10: Attribute based access control
Description of the Innovation	Neither ABAC nor defining security criteria are innovative per se. What is innovative is providing full support for them in an IoT platform. Besides, Existing authorization mechanisms that allow defining security criteria for specific business logic require knowing the specific structure of the request a priori, which makes almost impossible to use them in any generic mechanism such as RERUM
Status of the Innovation	The access control engine will be demonstrated in all trials. The ability to define security criteria based on business specific data is expected to be demonstrated in at least one trial, but it is pending to define which one, because it depends very much on the exact definition of each trial, which will be defined in WP5. However, due to the huge complexity of defining and evaluating security criteria that cannot be defined as text, the implementation of RERUM will be constrained only to check security conditions for text based fields, but it will be designed so it can be easily upgraded in the future for supporting other kind of data if implemented.
Exploitation / Service on Market	Consultancy service on development of reputation policies. Enhanced authorization services.
Business models & go to market approach	Consultancy service on development of authorization engine and policies. Authorization engine will be one of the main assets of the Atos' security portfolio.

Contribution 10: Integration of ABAC in IoT with specific business data contained in the request

Title	SIEM in a generic IoT platform (WP3)
Priority	High: Monitoring and analysing the logs and events is the main way to detect anomalies and therefore know what needs to be improved to ensure the system, one of the priorities of the RERUM project.
Use Case Situation	(All UCs) A user that accesses a specific RERUM service (i.e. gets information about traffic) suddenly identifies that the service is malfunctioning (he sees no cars in front of him, while the application says that the traffic is high). Another case can be assumed when a user identifies that his personal information has been disclosed to third parties. Then, he realizes that there is a problem and needs to contact the service provider to report the incidence.
Security or Privacy Issues	The base problem is that if the monitored data are not analysed, the platform is not aware of their own problems. Network malfunctions, external attacks or problems with the QoS or the defined SLA could be happening. Vulnerabilities of the system may be being exploited without any knowledge or control.
User Requirements	UR-13: The user doesn't want to worry about reporting errors or malfunctions on the Smart Devices or Network to fix them. Those problems must be auto detected.
Constraints, Out-of-scope topics	Require self-monitoring mechanisms (Req 2.3.10) and / or monitors to gather information of status and events from generated logs.
Technical Requirements	Req. 2.5-5 Monitoring and traceability by the middleware Req. 2.3-5 Centralised management of constrained networks
Description of the Innovation	A Security Information and Event Management (SIEM) component allows the IoT platform to perform a real-time, and later forensic, analysis of the log data that helps on decision making. Can also respond to anomalous behaviour based on correlation rules making easier to take remediation actions as soon as problems are detected.
Status of the Innovation	This innovation will be demonstrated in most use cases, for example by implementing an "inaccuracy alert producer" that detects anomalies in sensor readings. The component is being adapted from an open source initial version, modifying agents, interfaces and specific rules to fit the peculiarities of this project.
Exploitation / Service on Market	Consultancy service on development of Security Information Systems Enriched and more flexible SIEM.
Business models & go to market approach	Consultancy service on development of Security Information Systems The SIEM itself and adaptation modules and agents used will be an asset of the security portfolio of Atos.

Contribution 11: SIEM in a generic IoT platform

Title	Incorporating adaptability to an IoT platform using PRRS and OAP (WP3, WP4)
Priority	High: The OAP resolves the problem of the dynamic actualization of the whole system by automation of software updates and patching. Fixing problems on the fly depends on finding the concrete solution for the raised problem; the PRRS aims to help in that crucial function.
Use Case Situation	(All UCs) A user that has deployed several devices for providing a smart application identifies that the devices are not working according to his requirements and needs to update their firmware. In another case, the user wants to utilize the existing deployment for providing a new service, which however requires more fine tuned security and privacy mechanisms. When this has to be done manually for a large number of devices, it increases significantly the maintenance costs and the difficulty, thus remote configuration and upgrading of the firmware of the devices should be allowed.
Security or Privacy Issues	If the installed software is not appropriate for the target hardware and fully compatible with his context or is not updated, the device could be vulnerable to attacks, failures or incompatibilities. The OAP mechanism represents actually itself vulnerability and should be implemented in a reliable and secure way.
User Requirements	UR-14: The user requires to be able to remotely configure and upgrade the firmware and the security mechanisms of his devices in an automated way, without needing any manual installation. UR-15: The administrator also requires low maintenance costs and low technical administration overhead.
Constraints, Out-of-scope topics	The PRRS needs to receive alerts in a predefined format; this is usually provided by a Monitor, in our case, alerts usually will be thrown by the SIEM, but the monitor giving information about the context could be replaced. A repository of software solutions (libraries or firmware) must also be provided externally. It must include as metadata the functionality of the solution and the requirements to install it. If a software update is faulty and would render the node unusable, the OAP functionality should be able to recover to a previous working version. When updating device firmware with OAP, it is possible to replace the entire binary file or only parts of it (modules). RERUM will only consider the former approach.
Technical Requirements	Req. 2.3-5 Centralised management of constrained networks Req. 2.3-10 Self-* mechanisms Req. 2.4-12 Over-the-Air Programming Req. 2.6-24 Find deployable software to RERUM devices
Description of the Innovation	Over the Air Programming built-in mechanism into the RERUM devices allows the maintenance of the system fixing bugs or security vulnerabilities, updating software, configuring devices and in general managing remotely the whole RERUM network, building a secure and adaptive system. The mechanism will be launched when a new device is added to any node of the RERUM network; and also when an alert is thrown and received in the Platform for Runtime Reconfiguration of Security (PRRS) that reacts depending on the context and the nature of the event.
Status of the Innovation	This innovation will be demonstrated in all trials, for example in the process of adding a new node to the network and check for updates or mandatory configuration. An adaptation of PRRS is being realized by extending it to allow external requests using a SOA and Linked Data to locate appropriate solutions in software repositories. Will be developed an OAP module that build the appropriate firmware to send to every RERUM device that requires update.

	The RERUM adapter will be capable of receiving a firmware image over a network interface, verifying its integrity and subsequently restarting the device to use this new version.
Exploitation / Service on Market	Consultancy service on development of context based security solutions and automation of processes.
Business models & go to market approach	That consultancy will be offered to the customers to enrich Smart Grids and Home Automation applications with adaptability capabilities. Enrich Smart Grids and Home Automation with adaptability capabilities.

Contribution 12: Incorporating adaptability to an IoT platform using PRRS and OAP

Title	Malleable Signatures for controllably reduced Integrity protection (WP3)
Priority	Medium: RERUM will first deploy end-to-end protection of integrity; then Malleable Signatures can balance them with authorised modifications by PETs.
Use Case Situation	(All UCs). Example: In the home energy monitoring UC, the end user deploys devices, e.g. a certified and trusted smart meter. As it monitors citizens they become data subjects. The end user must allow the data subject some control over the information, e.g. allow applying privacy preserving technologies that modify data according to data subject's privacy policy. This is an authorised modification; still the end-user would like to assure that the received data is only changed within limits and not arbitrarily.
Security or Privacy Issues	Standard end-to-end integrity protection is not compatible with a subsequent authorised modification by authorised third parties, e.g. the RERUM device: the protection is usually terminated at the authorised third party that will do the changes, e.g. it is must be trusted to not do arbitrary modifications. To reduce this trust in that entity is RERUM's reasons to research malleable signatures.
User Requirements	UR-16: In all UCs end users need to identify the origin of data and that it has not been modified in an unauthorised way. The end user's device is trusted; he wants to know that it was this specific device that gathered a measurement, and that received measurement are not modified by unauthorised third parties (UR-7) to take his decisions. To comply with EU data protection regulation or to offer additional privacy protection as a service, the end-user wants to enable the data subject, (citizen, employee) to have a third-party modifying date on behalf of the data subject within controllable limits.
Constraints, Out-of-scope topics	The realisation of this innovation depends that the following technical requirements are fulfilled to a sufficient degree: *Req. 2.4-2 Microcontroller performance* and *Req. 2.6-1 Energy-efficient cryptographic primitives*
Technical Requirements	Req. 2.6-2 Integrity protection of SL-I data in transit Req. 2.6-4 Authorised modification of integrity protected data Req. 2.6-5 Detection of authorised modification of integrity protected data Req. 2.6-14 Data minimisation Req. 2.6-15 Accuracy and quality
Description of the Innovation	RERUM devises a suitable integrity protection, following the concept of malleable signature; suitable to run on RD or Gateway. End-users can verify that a specific device signed its data. Signature carries the limits of authorised modifications following the concept of sticky policies. A data subject or third parties working on behalf of him can freely decide which privacy preserving manipulation to carry out. If within authorization, the signature remains valid.
Status of the Innovation	RERUM will select, advance and trial in lab experiments suitable malleable signature schemes. A full implementation of all necessary protocols and mechanisms for an integration of malleable signatures into the trials is out of our scope and effort. RERUM runs lab experiments generating data and a statement to all stakeholders if these advanced signature schemes are ready.
Exploitation / Service on Market	Malleable signatures adds to the privacy portfolio that either could attract new customers as a unique selling point or enable business models as they can be made compliant with privacy regulations.
Business models & go to market approach	RERUM is convinced that Privacy by Design and end-to-end Security should work together, and not oppose each other. We hope they will both become a key selling point of innovative technologies, e.g. complex city services [129].

Contribution 13: Malleable Signatures for controllably reduced Integrity protection

Title	RSSI-based CS encryption keys (WP3)
Priority	High. The measurements of the devices must be transmitted in a secure and energy efficient way.
Use Case Situation	A user deploys various devices for providing IoT applications and the devices can also be mobile. The devices use the Compressive Sensing framework to send measurements periodically to the overall system and need to encrypt the measurements. The user has to install encryption keys on the devices to be able to use the CS framework for saving energy in data transmission.
Security/Privacy OR Reliability/Availability/ Scalability/Efficiency Issues	In case the encryption key is pre-stored on the device, it can be stolen if the device gets hacked by a malicious user. Furthermore, a malicious user may be able to derive the static key by comparing the transmitted measurements with his own measurements. Moreover, manual installation of keys on devices is not easy or efficient and does not scale.
User Requirements	UR-17: The end user (or the service provider) needs to install a CS key for each one of the deployed devices. The user needs the key to be changed dynamically and not be pre-stored on the device. The user also needs to avoid manual installation or update of the key.
Constraints, Out-of-scope topics	The devices have to be able to store on their internal memory (not on the flash drive) the encryption key. The mobility of the device should not be very high. Multi-interface devices have to run this for every interface and every link. It can't work in multicast applications.
Technical Requirements	Req. 2.4-11 Lightweight dynamic data compression Req. 2.6-1 Energy-efficient cryptographic primitives Req. 2.6-2 Integrity protection of SL-I data in transit Req. 2.6-7 Confidentiality protection of personal data in transit Req. 2.6-23 Update of operational credentials
Description of the Innovation	A mechanism and a protocol for extracting and jointly agree on CS encryption keys using RSSI measurements is developed. A user doesn't need to have a pre-stored encryption key on his device. The encryption key for CS is extracted in a mutual process with the target device (i.e. GW) that he is connected and transmits the measurements. The encryption key can be changed dynamically when the user moves or when he changes the target device/GW he is connected to.
Status of the Innovation	This description and the specification of this mechanism will be implemented on RDs during the project lifetime and will be tested on lab experiments. Possibly it will also be tested in trials.
Exploitation / Service on Market	This mechanism can be integrated on devices and on services and has to be integrated with the adaptive CS based framework.
Business models & go to market approach	RERUM will integrate this mechanism as part of its system for providing secure and energy efficient data gathering and transmission from sensors and android phones. This can't be exploited as a standalone mechanism, rather than in a complete framework for gathering and encrypting measurements (e.g. together with the devices and the adaptive CS framework).

Contribution 14: RSSI-based CS encryption keys

Title	Adaptive CS-based data gathering (WP4)
Priority	High. The measurements of the devices must be transmitted in a secure and energy efficient way and must be reconstructed according to the QoS of the service they provide.
Use Case Situation	An end user (e.g. the city) has installed various sensors for e.g. environmental monitoring, comfort quality monitoring or home energy management and has specified the service requirements in terms of Quality of Service (QoS). The sensors gather a signal that is sparse in some domain, which means that it is slowly changing. The sensors have limited battery life, so the number of transmissions have to be minimized. The user has to be ensured that the overall service that provides the measurements from the devices maintains a minimum level of QoS in terms of data accuracy and that this won't require a very frequent change of device batteries, because in a city deployment with thousands of devices deployed, battery renewal is not easy.
Security/Privacy OR Reliability/Availability/ Scalability/Efficiency Issues	The measurements have to be protected and not be disclosed to third parties due to e.g. being sensitive for the user. Rare existing solutions for secure transmissions of data from devices are not lightweight. Frequent transmissions of data from device incur excessive load in the network, which does not allow the intermediate devices (in a route) to sleep, consuming more energy.
User Requirements	UR-7: The user needs to protect his measurements from malicious users. UR-18: The user needs to gather and transmit measurements with minimum energy consumption, while ensuring a minimum error rate at the receiver.
Constraints, Out-of-scope topics	The devices have to be able to support the adaptive framework in terms of memory storage. If the sparsity of the signal changes continuously the adaptive-CS scheme would need increased signaling.
Technical Requirements	Req. 2.2-2 Suitable Sensory data can be released to the application Req. 2.2-3 Rate of data collection Req. 2.3-9 Overall QoS Req. 2.4-10 Low energy consumption Req. 2.4-11 Lightweight dynamic data compression Req. 2.6-1 Energy-efficient cryptographic primitives Req. 2.6-7 Confidentiality protection of personal data in transit Req. 2.6-15 Accuracy and quality Req. 2.6-23 Update of operational credentials
Description of the Innovation	The adaptive CS-based framework utilizes the Compressive Sensing theory to simultaneously compress and encrypt batches of measurements from the devices to the server. The adaptive CS scheme changes the compression level when the sparsity of the measurement signal changes in order to ensure a specific pre-defined (according to the QoS requirements) reconstruction error at the receiver.
Status of the Innovation	During the lifetime of the project, the description and the specification of the framework will be provided, as well as an implementation of the framework on sensor devices and android phones. The framework will be tested in lab experiments and possibly also on the trials.
Exploitation / Service on Market	This framework can be integrated on devices to decrease their energy consumption and become more energy efficient. This framework can also be used for extracting events from the compressed measurements (i.e. raise alarms).
Business models & go to market approach	A service for energy efficient and secure data gathering from android phones and sensor devices can be developed.

Contribution 15: Adaptive CS-based data gathering

Title	Lightweight framework for sensor monitoring (WP3)
Priority	High. The performance of the devices must be monitored to identify networking problems.
Use Case Situation	A user (e.g. the network operator or the service provider) has installed various devices to provide IoT applications. The devices are wirelessly connected either forming a mesh network or directly to a gateway. The devices are all connected via ZigBee sharing the same channel. The user has to ensure that the network functions normally preventing outages and abnormal situations. Imagine a scenario in which a user service will raise an alarm when there is a fire in the house. However, the device that monitors the room for fire suddenly malfunctions and it is not able to send the alarm. A similar situation can be seen if there is a WiFi Access Point that uses the same frequencies with this device and it creates interference, so that the alarm packet is lost or delayed too much.
Reliability, Availability, Efficiency Issues	When a device in the network does not function normally, either due to battery outage or due to issues in the wireless links (increased interference, delay or errors) the performance of the overall system degrades significantly and the IoT application does not produce required results.
User Requirements	UR-19: The user needs to have an automated system for monitoring the status of the devices and of the network connections to avoid missing alarms and to ensure the functionality of the services. When the network interconnectivity is not functioning normally, the commands of the user may not be able to reach the device. For example, if one intermediate device in a route between the user and the target actuator has a battery outage, the commands of the user won't reach the actuator. Furthermore, due to wireless link problems, alarms raised from sensors (i.e. regarding a fire) may not be able to reach the user.
Constraints, Out-of-scope topics	The devices should be able to support the monitoring tool and should be able to transmit the measurements to the server. Monitoring nodes have to be spread out in the network to monitor the wireless links and the neighbour devices.
Technical Requirements	Req. 2.3-5 Centralised management of constrained networks Req. 2.3-9 Overall QoS Req. 2.3-10 Self-* mechanisms
Description of the Innovation	A self-monitoring tool that is able to provide network monitoring measurements to a central entity in the system is being developed. The tool will be installed on the devices that can support it or on specific devices that play the role of network monitors. The tool provides measurements for the wireless links and raises alarms when issues have been detected.
Status of the Innovation	The description and the specification of the tool will be provided within the project duration. An implementation of the tool and an early evaluation on lab experiments will be investigated.
Exploitation / Service on Market	The tool is mainly targeted for the network operators and the service providers for giving them measurements about the network performance.
Business models & go to market approach	The tool can only be exploited as part of the overall RERUM middleware implementation and not as a standalone tool.

Contribution 16: Lightweight framework for sensor monitoring

Title	Android-based multi sensing application (WP3, WP4, WP5)
Priority	Medium. Such multi-sensing and energy efficient applications can be used for crowd-sourcing IoT services.
Use Case Situation	(UC-O1, UC-O2, UC-I2) Imagine a scenario in which the city needs to gather sound level information or WiFi RSSI levels in the city areas. Instead of deploying thousands of sensors around the city, a crowdsourcing mobile application used by a large number of citizens can be exploited as a low-cost solution for gathering such information at a city level.
Reliability/Availability/ Scalability/Efficiency Issues	The users of the application have to be ensured this won't consume their battery and that personal information will not be disclosed. Existing frameworks don't pay much attention on energy efficiency, nor in secure transmission of data.
User Requirements	UR-20: Users may need to provide measurements and assist the cities into gathering large amounts of data that will help into extracting valuable information, i.e. for the sound levels in the city or for the radio pollution. By providing these data to the cities, they can identify polluted areas and act to resolve the situation that will be of benefit to the citizens.
Constraints, Out-of-scope topics	The type of measurements depend on the onboard sensors that each mobile phone has. Furthermore, different devices have sensors with different sensitivity, so there is a need for carefully fusing the data gathered from devices of different type.
Technical Requirements	Req. 2.2-2 Suitable Sensory data can be released to the application Req. 2.2-3 Rate of data collection Req. 2.2-4 Time-efficient connectivity of devices for data uploading to application Req. 2.3-9 Overall QoS Req. 2.4-10 Low energy consumption Req. 2.4-11 Lightweight dynamic data compression Req. 2.6-1 Energy-efficient cryptographic primitives Req. 2.6-2 Integrity protection of SL-I data in transit Req. 2.6-7 Confidentiality protection of personal data in transit Req. 2.6-23 Update of operational credentials
Description of the Innovation	This is an android application able to gather measurements from various on board sensors (e.g. light levels, sound levels, signal strength for mobile and WiFi, speed) and transmit them to a centralized server. The application includes the CS-based framework, in order to simultaneously encrypt and compress the gathered measurements.
Status of the Innovation	This is already on the stage of implementation and is almost complete. It will be evaluated in both lab experiments and trials.
Exploitation / Service on Market	This application can be utilized for crowd-sourcing applications that will be provided by either service providers or city authorities. The users have the ability to select which type of measurements they want to share with the authorities, to avoid disclosing data that they consider as sensitive.
Business models & go to market approach	The RERUM project will be able of providing secure crowd-sourcing services for the city authorities or service providers. It is important to provide applications that are secure and energy efficient at the same time.

Contribution 17: Android-based multi sensing application

Title	Framework for spectrum occupancy measurements (WP4)
Priority	High. Spectrum efficiency is of high importance due to the scarcity of the spectrum resources. Licensed users should also be protected.
Use Case Situation	(All UCs) Assuming that a user owns a device that is able to access multiple spectrum fragments. The user utilizes this device to connect to the RERUM framework and access smart city applications, but due to congestion in the spectrum, he needs to be ensured that the device has a reliable connection to the system and that its energy consumption is minimised.
Reliability/Availability/ Scalability/Efficiency Issues	There is a clear and proved trade-off between sensing the spectrum and accessing it. The more time a device senses the spectrum the less it has for accessing it. Furthermore, the energy spent for sensing the spectrum is very high (higher than when transmitting data). If the device senses the spectrum very frequently, the energy consumption of the device increases. Furthermore, a device that tries to access utilized spectrum bands will face collisions, lost packets and retransmissions or it will affect licensed users.
User Requirements	UR-21 The user needs to ensure the reliable connectivity of his devices, avoiding jamming attacks or avoiding utilizing congested spectrum bands. The user needs also to ensure that his devices do not consume more energy for running intelligent spectrum-related mechanisms. UR-22: A user needs to avoid interfering with licensed users when transmitting.
Constraints, Out-of-scope topics	The user device has to be SDR-capable for setting by software its transmission parameters. Furthermore, the spectrum policies have to change so that unlicensed access to TV bands and licensed frequencies will be allowed.
Technical Requirements	Req. 2.3-1 Support of a large number of attached devices/objects Req. 2.3-2 Dynamic spectrum management Req. 2.3-3 distributed spectrum selection Req. 2.3-4 Operation in unused spectrum bands Req. 2.4-6 RD Communication interfaces Req. 2.4-7 Reconfigurable network interfaces Req. 2.4-10 Low energy consumption
Description of the Innovation	A mechanism for energy efficient gathering of spectrum occupancy measurements is being developed. This framework will allow SDR-capable devices to extract statistics about the spectrum usage of portions of the wireless spectrum and identify the optimum period for sensing these portions (instead of sensing them at every time slot).
Status of the Innovation	During the lifetime of the project the description and the specification of the mechanism will be developed. A draft implementation will be attempted and evaluated in lab experiments. Due to the lack of policies and regulations for allowing access to TV-bands, this mechanism will not be implemented in the trials.
Exploitation / Service on Market	This mechanism can be exploited in various ways, e.g. it can be installed on SDR devices to optimize the spectrum sensing mechanism in an energy efficient way, it can be used to model the spectrum occupancy at different spectrum bands and it can also be used for creating spectrum maps in city areas.
Business models & go to market approach	This mechanism must be installed on capable RERUM devices and must be integrated in the overall RERUM system to allow the optimum networking of the devices. Nevertheless, the mechanism can also be exploited as part of a different standalone system for creating spectrum occupancy maps.

Contribution 18: Framework for spectrum occupancy measurements

Title	Lightweight spectrum assignment framework (WP4)
Priority	High. Spectrum efficiency is of high importance due to the scarcity of the spectrum resources. Licensed users should also be protected.
Use Case Situation	(All UCs) A user has deployed many devices in a city area for providing IoT applications. The devices are wirelessly connected and access standard ISM bands, which are overcrowded. The user must optimize the networking connectivity of the devices in order to have maximum QoS for the services.
Reliability/Availability/ Scalability/Efficiency Issues	If the devices do not select the optimum central frequency and bandwidth they may face congestion and the system may encounter loss of data availability due to the inability of the devices to transmit data. Furthermore, a device that tries to access utilized spectrum bands will face collisions, lost packets and retransmissions or it will affect licensed users.
User Requirements	UR-21, UR-22: A user needs to have high QoS for his services and needs to know that whenever he wants to transmit or receive something he will be able to do so by accessing unused portions of spectrum. UR-23: The network operator needs to ensure maximum spectrum efficiency, maximum network reliability and data availability.
Constraints, Out-of-scope topics	The user device has to be SDR-capable for setting by software its transmission parameters. Furthermore, the spectrum policies have to change so that unlicensed access to TV bands and licensed frequencies will be allowed.
Technical Requirements	Req. 2.3-2 Dynamic spectrum management Req. 2.3-3 distributed spectrum selection Req. 2.3-4 Operation in unused spectrum bands Req. 2.3-7 Multi-technology and multi-operator connectivity Req. 2.3-9 Overall QoS Req. 2.4-6 RD Communication interfaces Req. 2.4-7 Reconfigurable network interfaces Req. 2.4-10 Low energy consumption
Description of the Innovation	A mechanism for analysing the state of the wireless spectrum and select the most suitable frequency and bandwidth for providing the required QoS for the service it provides will be implemented. The mechanism will be lightweight so that it can run on IoT devices and it will be able to provide optimal solutions. The devices will be able to change their radio transceiver parameters in order to select the best central frequency, bandwidth, modulation and coding for the transmission
Status of the Innovation	During the lifetime of the project the description and the specification of the mechanism will be developed. A draft implementation will be attempted and evaluated in lab experiments. Due to the lack of policies and regulations for allowing access to TV-bands, this mechanism will not be implemented in the trials.
Exploitation / Service on Market	This mechanism can be exploited in various ways, e.g. it can be installed on SDR devices to optimize the way they access the spectrum in an energy efficient way, it can be used in a cooperative way to maximize the spectrum efficiency and minimize the interference in a network of devices and it can also be used to minimize transmission power when selecting lower spectrum bands for accessing.
Business models & go to market approach	This mechanism must be installed on capable RERUM devices and must be integrated in the overall RERUM system to allow the optimum networking of the devices and the optimum spectrum allocation. Nevertheless, the mechanism can also be exploited as part of a different standalone system for enabling high data rate transmissions in an ad hoc manner.

Contribution 19: Lightweight spectrum assignment framework

Title	**Federations of VRD, their modelling language and the Federation Execution Engine (WP2)**
Priority	Medium-Low: Federations – similar to other research projects, RERUM offers a service transparently comprising one or more devices, and a language which allows the logical description of their interactions. In RERUM, the service can run with relative flexibility either inside the RERUM instanced; or localized, in the relevant sensor network.
Use Case Situation	(All UCs) A user wants to utilize an advanced service for managing the comfort quality of his home. This service requires a set of multiple sensors and actuators working in a complementary fashion: e.g. the ambient and water temperature could be adjusted based on various indoor and outdoor temperature, and humidity sensors readings, both taken over a relevant period of time.
Reliability/Availability/ Scalability/Efficiency Issues	Without Federations, a composition of services would have to be coordinated and executed by the users themselves. This would incur a computational and networking overhead due to the traffic, as well as to require a permanent connection to the RERUM for both sensors and the user. Furthermore, the composition and its logic would only be accessible to the single user.
User Requirements	UR-24: The user needs to be able to define new services that are a composition of existing services from potentially several existing devices, as well as the logic of their interactions. This gives end user the flexibility to create more complex services without the need to install new devices every time a more complex service is needed.
Constraints, Out-of-scope topics	N/A
Technical Requirements	Req. 2.4.-13 Exposure of RD to applications Req. 2.4.-14 RERUM to RD interface Req. 2.4.-15 Differences between Federated RD and RD Req. 2.4-18 RD to RD communication in Federation
Description of the Innovation	RERUM provides for Federations an accessible and expressive modelling language; and the components which handle the selection of the suitable devices, their communication and the execution of the logic of the Federation – the Federation Manager and Federation Execution Engine. The latter, flexible, is able run as close as possible to the network or networks which contains the relevant devices.
Status of the Innovation	The Federation Execution Engine and the Federation modelling language are currently being drafted, part of task 2.2. The implementation for the prototype and demonstrator will be based on existing, mature platforms, e.g. JBoss Switchyard; but which will offer less flexibility.
Exploitation / Service on Market	By introducing the option of decoupling the executed task from the RERUM cloud (and performing the task into the local network), the innovation is expected to be attractive to both end users and service providers, since it would offer a more reliable and - for localized scenarios, a less complex method of composing services with complex requirements.
Business models & go to market approach	The Federations and Federation Execution Engine components can also be integrated outside RERUM, in similar research or commercial projects.

Contribution 20 Federations of VRD, their modelling language and the Federation Execution Engine

Title	Lightweight Datagram Transport Layer Security (DTLS) Protocol (WP3)
Priority	Medium: although important to ensure the secure communication between devices, the hardware requirements don't allow the innovation's wide adoption
Use Case Situation	(All UCs) A user, e.g., a city, deploys a sewage-mentoring system, in which subsets of RERUM devices have a specific monitoring capabilities, i.e., some of them measure temperature, while others detect selected heavy elements. In order to collect data effectively and trigger an alarm, some RERUM devices are configured to communicate with other RERUM devices, e.g., those without heavy element sensing capabilities need to be aware of such data.
Security or Privacy Issues	If not secured, such communication between two RERUM devices is prone to impersonation, eavesdropping or message forgery.
User Requirements	UR-25: The user requires secure mechanisms implemented in a RERUM device that allows a device-to-device authentication along with data integrity (UR-7) and confidentiality of exchanged messages.
Constraints, Out-of-scope topics	Our solution requires special purpose cryptographic coprocessors integrated in the main RERUM device microcontroller.
Technical Requirements	Req. 2.6-1 Energy-efficient cryptographic primitives Req. 2.6-2 Integrity protection of SL-I data in transit Req. 2.6-20 Availability of initial credentials Req. 2.6-21 Support of different operational credentials types Req. 2.4 10 Low energy consumption Req. 2.4-2 Microcontroller performance
Description of the Innovation	DTLS standard or any other DTLS-based protocol might be used as a backbone of secure communication between RERUM devices. However, the performance of many public key primitives used in this protocol is considered as inefficient while executing in resource-constrained environment. RERUM will utilise cryptographic coprocessors available in the target TI CC2538 microprocessor to implement cryptographic primitives in much more efficient way, i.e., minimising processing time, code footprint and power consumption of RERUM devices.
Status of the Innovation	The innovation in currently under investigation. In case of successful prototype implementation the solution is likely to be demonstrated in the trials.
Exploitation / Service on Market	This innovation might increase interests of various chip manufactures to facilitate cryptographic coprocessors in their designs.
Business models & go to market approach	This is the main component of a RERUM device and could be one of its strong selling points.

Contribution 21: Lightweight Datagram Transport Layer Security (DTLS) Protocol

Title	6LoWPAN Multicast (WP4)
Priority	Medium: it can apply only to applications that require multicast, but it can significantly improve them
Use Case Situation	This innovation is applicable to the "Environmental monitoring" (UC-O2) and the two indoor Use Cases (UC-I1) and (UC-I2). It is of relevance on situations when the user needs to communicate with multiple devices simultaneously, for example to query for the presence of a device supporting a specific functionality.
Security or Privacy Issues	Encryption of multicast messages at the network layer requires all recipients to share the encryption key with the message's source node. Dynamic key agreement is challenging, since it involves more than two nodes (possibly a very high number of them), and the identities of the nodes is not known in advance. Encryption therefore requires either pre-shared keys or a group key scheme.
User Requirements	UR-26: In scenarios involving point-to-multipoint traffic, transmitting to each destination individually with unicast leads to poor utilization of network bandwidth, excessive energy consumption caused by the high number of packets and suffers from low scalability as the number of destinations increases. For UC-O2 in particular, it is expected that networks will be formed by a potentially very high number of RDs and therefore scalability is a requirement. In cases when the RDs are powered by batteries, it is impractical or outright untenable to replace batteries very frequently due to high management cost and possibly hard-to-reach installation locations. Thus, long battery life is important. For devices powered from mains, low energy consumption is also important in order to reduce financial cost, but also in order to comply with national and international regulations where applicable.
Constraints, Out-of-scope topics	During RERUM, multicast messages will be encrypted at the data link layer on a hop-by-hop basis, but will be unencrypted at the network layer. Developing a group key scheme is out of the project's scope. When the multicast traffic source is a node in the internet (outside the boundaries of the RERUM network), end-to-end multicast forwarding relies on suppport of the Multicast Listener Discovery (MLD) or similar protocol at the gateway. Implementation of MLD is out of the project's scope and multicast forwarding will be limited to within the boundaries of a single 6LoWPAN.
Technical Requirements	Req. 2.3-1 Support of a large number of attached devices/objects Req. 2.4-10 Low energy consumption Req. 2.4-12 Over-the-Air Programming Req. 2.4-14 RERUM to RD interface Req. 2.6-26 Secure design and implementation of RERUM components Req. 2.6-27 Reputation mechanism for reliability, availability and trustworthiness
Description of the Innovation	The BMFA multicast forwarding algorithm for 6LoWPANs. BMFA is specific for 6LoWPANs where unicast routing is handled by the RPL protocol. BMFA takes advantage of the fact that RPL perceives a 6LoWPAN as a tree topology, which it uses in order to forward IPv6 datagrams to multiple destinations.
Status of the Innovation	This innovation has been implemented in C for the Contiki Operating System. This innovation will be deployed and demonstrated during RERUM's field trials.
Exploitation / Service on Market	The implementation may be released with an open source license for wider adoption. Additionally, it may contributed to Contiki for potential inclusion in the project's main repository.
Business models & go to market approach	The mechanism is not specific to RERUM: It can be deployed on any RPL-routed 6LoWPAN and it can therefore be adopted very widely in the longer term.

Contribution 22: 6LoWPAN Multicast

Title	Low participatory RD energy and computational consumption (WP4, WP5)
Priority	High: To achieve meaningful participatory sensing a high user penetration is required. In the case that a citizen will have to download some app on a resource constrained device, it has to be ensured that neither the app nor the security and data protection mechanisms provided with the app drain the battery.
Use Case Situation	(Applies to all UCs) Example of UC-O1: The citizen carries an RD (smartphone) that has downloaded an app for participatory sensing. The city relies on large numbers of citizens that will operate as participatory sensors, limiting installation costs. With this information, the city can analyse current traffic and feedback traffic state information to navigation systems of participants. By doing this, the traffic can be distributed throughout the city to avoid congestions.
Security or Privacy/ Reliability/Availability/ Scalability/Efficiency Issues	Simple information from a traffic participant, such as GPS position, average driving speed and date of the information, can be enriched with information of geo-location systems to draw detailed conclusions about the habits of the participant. There are scalability issues when receiving and processing information from thousands of devices. The reliability of the results depend on the age of information, meaning that when the measurements are very old (due to i.e. limited connectivity, delays, etc.) the traffic may have changed and this will result in wrong results.
User Requirements	UR-18, UR-20, UR-21: The user requires to participate in the crowdsourcing application with the minimum cost in terms of battery consumption and monetary cost. Thus the user requires an energy efficient application with minimum number of data exchanges.
Constraints, Out-of-scope topics	The innovation can be applied to scenarios where any kind of data analysis information is collected and if applicable, dynamically fed back to the end users or to any other situations (say, city planning purposes) where collaborative collection of data and its analysis is needed. However, the results are not very accurate when a very small number of users use the traffic monitoring application
Technical Requirements	Requirement 2.4-6: RD Communication Interfaces Requirement 2.4-10: Low Energy Consumption Requirement 2.6-1: Energy Efficient Cryptographic Primitives Requirements 2.6-14: Data minimisation
Description of the Innovation	Traffic use case participants collect geo-location information for the benefit of the city, with low battery drain. This innovation ensures that both, the selection of the information to be collected, the location estimation and data protection are energy efficient. The privacy enhancing technology for geo-location privacy used in this scenario is one example of additional mechanisms that, apart from functionality, have to be provided in an energy efficient way. In detail, this PET allows collecting detailed information of traffic participants, while maintaining anonymity and authenticity of the provided information. The city or the service provider receives accurate records, but there is no indication about who generated them, or if they come from one or multiple participants. The service uses multiple alternative location sensors that provide location estimates to be used for both energy efficient sampling strategy and transmission policy.
Status of the Innovation	The innovation is currently being developed. The innovation will be tested in lab experiments and possibly in trials.
Exploitation / Service	• The innovation is in itself a key enabler for the adoption of participatory

on Market	systems. Indeed any service/system that can adopt energy-preserving mechanisms developed within this innovation thrust will have a clear edge over the competition.
Business models & go to market approach	• Consulting efforts to partner cities for development of participatory apps • Approach local traffic authorities • Possible propose of invention to standardization bodies

Contribution 23: Low participatory RD energy and computational consumption

Title	Enablers for large numbers of participatory RDs (WP4)
Priority	High: IoT relies on the efficient interconnectivity of a large number of devices.
Use Case Situation	(All UCs) The city and the service providers rely on a large number of devices providing accurate measurements in order to produce accurate results for the IoT applications. Especially in the collection of traffic information or mass energy billing/planning from the perspective of an indoor scenario, the required number of measurements to produce meaningful results is very high. The end user is proving such data (mobility or energy) to obtain as benefit improved traffic information/conditions or more beneficial power pricing schemes.
Security/privacy/ Reliability/Availability/ Scalability/Efficiency Issues	In participatory applications, there are various security issues related with malicious users sending false information to affect the decisions of the system for their benefit. Furthermore, the applications and the system have to ensure that no private user information will be gathered and made available to third parties.
User Requirements	UR-15: The citizen: application/benefit from participation must be beneficial in short/mid-term to ensure participation. UR-18: The city: increase the number of participating private users so as to reduce costs for installations in traffic estimation, perform this in a trustworthy manner to ensure that no data manipulation can occur and that the data is reliable.
Constraints, Out-of-scope topics	The age of information plays a significant role in order to have reliable results. Delayed information have to be discarded. The network interconnectivity of the devices has to ensure the on-time delivery of the data.
Technical Requirements	Req. 2.2-2 Suitable Sensory data can be released to the application Req. 2.2-3 Adjustable rate of data collection Req. 2.3-1 Support of a large number of attached devices/objects Req. 2.4-10 Low energy consumption
Description of the Innovation	Provide solutions that scale well for large numbers of RDs focusing in mechanisms that can impede performance of the system in terms of communication bottlenecks, energy overconsumption, and storage.
Status of the Innovation	The innovation is currently being developed within T4.4, early mathematical models indicate such properties in terms of information routing over virtualized networking infrastructures. This innovation will be tested via simulations.
Exploitation / Service on Market	The innovation is required for the wide adoption of participatory systems. This can be easily adapted to support any type of service that requires data from large numbers of devices in an energy efficient way and will help the service to have a clear edge over the competition.
Business models & go to market approach	• Consulting efforts to partner cities for development of participatory apps • Approach local traffic authorities • Possible propose of invention to standardization bodies

Contribution 24: Enablers for large numbers of participatory RDs

Title	Enhanced wireless node hardware as low-performance RERUM devices (WP4)
Priority	High: there is an ultimate requirement for a more powerful IoT device that is able to run the advanced security, privacy and reliability mechanisms of RERUM, while at the same time its energy consumption remains very low.
Use Case Situation	(All UCs) An end-user aims to install IoT devices for providing smart city applications. The user makes a market research and finds out that existing state of the art IoT devices basically lack mechanisms for providing secure and trustworthy transmissions of data, allowing them to be gathered by malicious external users.
Reliability/Availability/ Scalability/Efficiency Issues	Existing devices are not able to support advanced mechanisms for security, privacy and reliability. Furthermore, the networking capabilities of existing devices are very limited and do not provide opportunities for providing advanced IoT services. Devices need to have high computational power, memory and other specifics like cryptographic co-processor/acceleration being energy efficient at the same time.
User Requirements	UR-27: Users and use cases demand devices with low-power consumption, low cost, small form factor, flexibility on connecting different type of sensors and communicating, easy to use, with different interfaces and performance enough to run a secure, private and reliable application and communication in the Smart Cities environment.
Constraints, Out-of-scope topics	The development of a brand new hardware will include different revisions including the user's experience and fixing the problems arisen during the first pilots, which in this case will be the RERUM use cases. Therefore the RERUM devices likely will need to be improved during or after the project till they can be considered an innovation at all. These devices will be also hardware based and will not run any firmware by default, so they will be an enabler platform to implement a RERUM device but will require to be programmed with a firmware including the RERUM middleware to be considered a RERUM device.
Technical Requirements	Req. 2.2-1 - Remote control of RDs Req. 2.2-2 - Suitable Sensory data can be released to the application Req. 2.3-4 - Operation in unused spectrum bands Req. 2.3-10 - Self-* mechanisms Req. 2.4-2 - Microcontroller performance Req. 2.4-3 - Autonomous operation, processing consumption and low-power modes Req. 2.4-4 - Volatile memory Req. 2.4-5 - Persistent storage Req. 2.4-6 - RD Communication interfaces Req. 2.4-7 - Reconfigurable network interfaces Req. 2.4-10 - Low energy consumption Req. 2.4-12 - Over-the-Air Programming Req. 2.6-1 - Energy-efficient cryptographic primitives Req. 2.6-24 - Find deployable software to RERUM devices
Description of the Innovation	The main features of this new device include: • Micro-processing unit of ultimate generation. • Ultra-low power consumption modes and mechanisms. • Extended volatile memory and flexible non-volatile storage solution. • Dual RF interface on 2.4GHZ and sub-1GHz ISM bands.

	• Multiple power supplies options. • Multiple sensors' connectivity options. • Embedded firmware flashing tool with open source tool-chain.
Status of the Innovation	The specifications and the design of the hardware, created from the requirements gathered in the D2.2 have been done as part of the work of the tasks 2.2, 4.3 and 4.4. The implementation has just started, as the initial step on T5.2 and first prototypes will be ready before end of project's M18, February 2015. The innovation will be used both in lab experiments (T5.3) and in the trials on both cities (T5.4 & T5.5).
Exploitation / Service on Market	The design will be opened to the WSN/IoT community and the new device will be commercialized as a development platform for other research works or as infrastructure for other deployments that want to use the results of RERUM project
Business models & go to market approach	The devices will be sold on an online marketplace specialized in this kind of products, together with its compatible sensors and accessories, to offer a complete solution to the customers

Contribution 25: Enhanced wireless node hardware as low-performance RERUM devices

Title	**Pervasive environmental monitoring in cities using public transportation as sensing spots (WP5)**
Priority	Medium: the use of mobile sensing platforms on buses for avoiding the installation of fixed devices can reduce costs for the cities.
Use Case Situation	The cities install a new service for measuring some environmental parameters (mainly weather, noise, air quality and components and electro-magnetic radiation). In other to increase the number of areas to be measured, without requiring the deployment of many devices, the cities se the public transportation system, installing sensors on buses in order to get information of multiple spots, correlating the measurements with a positioning system that is already present in this kind of vehicles for tracking purposes.
Reliability/Availability/ Scalability/Efficiency Issues	Existing environmental monitoring systems are based on fixed devices installed on city areas (squares, roads), which induces scalability and cost issues when more places need to be monitored by the system.
User Requirements	UR-28: The user (service provides/city) needs to be cost-efficient and avoid deploying large number of devices for environmental monitoring, as this application can be provided by mobile sensors in a reliable way. The user however requires that the measurements are reliable and of a specific quality.
Constraints, Out-of-scope topics	This kind of measurements are only able to be performed with data with a low-frequency behaviour, this is, without big changes in short periods of time, such the outdoor ambient temperature, because every single spot of the routes will have a very low sampling frequency, namely every time a bus (or whatever public transportation vehicle we will use in this approach) with sensors go by that position. The cross-reference between the parameters measured and changes on this parameter made by the vehicle with the sensor elements installed. This means we should be very careful on how we measure, for instance, the noise or the air quality within a vehicle that make noise and contamination. This is going to be quite challenging and using electric (or even gas fuelled) vehicles (like buses, trolleys, trams, trains, etc.), everyday more common, could be a solution. Finally, the installation, the service and the maintenance shall be performed by the company, public or private, in charge of the public transportation system, making necessary to train them according.
Technical Requirements	Req. 2.2-2 - Suitable Sensory data can be released to the application Req. 2.2-3 - Rate of data collection Req. 2.2-4 - Time-efficient connectivity of devices for data uploading to application Req. 2.3-1 - Support of a large number of attached devices/objects Req. 2.3-2 - Dynamic spectrum management Req. 2.3-3 - Distributed spectrum selection Req. 2.3-4 - Operation in unused spectrum bands Req. 2.3-6 - Partitioning of the network into clusters Req. 2.3-7 - Multi-technology and multi-operator connectivity Req. 2.3-9 - Overall QoS Req. 2.4-1 - Enclosure IP rating Req. 2.4-7 - Reconfigurable network interfaces Req. 2.4-9 - Gateway communication interfaces Req. 2.6-7 - Confidentiality protection of personal data in transit Req. 2.6-11 - User Consent and choice

	Req. 2.6-15 - Accuracy and quality
Description of the Innovation	The idea is to use public transportation system to perform pervasive measurements in the city. The sensing elements, installed in vehicles with communication to the RERUM network will gather the data and send it upwards, to the servers, using gateways deployed in fix locations in the city, using other RERUM devices installed acting as data routers, or just installing in the same vehicle a RERUM gateway. This data, correlated with the location, will give to the city the chance to have virtually multiple sensing elements deployed in the streets, taking one sample every time a vehicle with that sensors passes by the same location, with a minimum budget, only requiring to isolate that measurements from the alteration made by the vehicle itself. The location information could be used at the same time as an input for the UC-O1 (traffic management).
Status of the Innovation	The innovation is already being defined on current task T5.1 and will be clarified in D5.1. But will be on the trials (T5.4 & T5.5) where they are going to be definitely implemented.
Exploitation / Service on Market	If the trials succeed and the constraint are demonstrated not to be a show-stopper, a new way to provide this pervasive measurements will be disclosed and disseminated to the cities worldwide through publications and congresses such as the Smart City Expo & World Congress. With that, any other company with the appropriated skill could offer a product based on this research.
Business models & go to market approach	The cities participating in the project, among others, could use this open innovation to improve their smart city's projects, especially on the budget side.

Contribution 26: Pervasive environmental monitoring in cities using public transportation as sensing spots

4.3 User requirements

The previous 26 contributions are aimed at solving issues that the end user (mostly a citizen) encounters in given concrete situations in the Use Cases. The corresponding User Requirements are summarized as follows:

id	User requirement	UC applicability	Requirement source
UR-1	User can securely deploy new devices in the network without the need to manually install security credentials in every device.	All UCs	Citizen/end-user
UR-2	User requires his data to only be processed by third parties after he gives his consent to do so or after he defines specific policies.	UC-O1, UC-I1, UC-I2	Citizen/end-user
UR-3	User requires to be able to send data anonymously for smart cities applications.	UC-O1, UC-I1, UC-I2	Citizen/end-user, City
UR-4	City officials / authorities / administrators needs to be able to validate the data that originate from anonymous users and avoid the latter affecting the precision and the usability of the system data.	All UCs	City, Service providers
UR-5	User shall be able to create Privacy Policies that define why and under which conditions a service provider may repeatedly access his data.	All UCs	Citizen/end-user City, Service providers
UR-6	User should be able to authenticate himself or/and a device without disclosing information that is not necessary for the authentication. Still the authentication must be strong enough to ensure unforgeability and authenticity of messages.	UC-O1, UC-I1, UC-I2	Citizen/end-user
UR-7	User requires his messages to not be forged by malicious users.	All UCs	Citizen/end-user
UR-8	City officials / administrators require to protect networks from unauthorised use and allow optimal flow of legitimate messages through legitimate devices.	All UCs	City, Service providers
UR-9	User requires improved QoS for the services he receives and high availability and reliability of his device's network connectivity.	All UCs	Network operators, Citizens
UR-10	User requires improved battery lifetime for devices with multiple radio interfaces.	All UCs	Citizen/end-user
UR-11	User needs to be sure that only trusted users will participate in the decision making processes of the system (no malicious users should interfere with the measurements for their benefit)	All UCs	Citizen/end-user
UR-12	User should be able to set access criteria to IoT services based on user attributes and context of requests.	All UCs	Service provider

			(could also be a Citizen/end-user)
UR-13	User needs to avoid manual monitoring of the system and manual reporting of errors, but requires automatic detection of errors and malfunctions.	All UCs	Citizen/end-user , Service provider
UR-14	User should be able to remotely configure and upgrade the firmware and the security mechanisms of his devices in an automated way, without needing any manual installation.	All UCs	Citizen/end-user, Network and service provider
UR-15	User requires low maintenance costs and low technical administration overhead.	All UCs	Network and service provider, Citizen/end-user
UR-16	User needs (in some cases) to identify origin of data and that it has not been modified in an unauthorised way, but allow limited authorised modifications.	All UCs	Citizen/end-user, service providers
UR-17	User needs to avoid having pre-stored encryption keys and allow dynamic encryption dynamic encryption keys that are not locally stored.	All UCs	Citizen/end-user, Service provider
UR-18	User needs to gather and securely transmit the measurements with the lowest possible energy consumption, maintaining a specific QoS.	All UCs	Citizen/end-user
UR-19	User needs to have an automated system for monitoring the status of the devices and of the network connections to avoid missing alarms and to ensure the functionality of the services.	All UCs	Citizen/end-user, Service provider
UR-20	User wants to have energy efficient applications for contributing to various IoT applications such as environmental sensing and traffic monitoring.	UC-O1, UC-O2, UC-I2	City, Service provider
UR-21	User needs to have reliable and energy efficient networking connectivity at his devices.	All UCs	Citizen/end-user, Vendors
UR-22	User has to avoid creating interference to licensed users when transmitting data.	All UCs	Citizen/end user, Vendors
UR-23	City officials / administrators needs to increase spectrum efficiency and network reliability in order to avoid congesting the wireless spectrum and degrade the network performance.	All UCs	Network providers, Service providers
UR-24	Users can define in their service request a composition of devices (what we call, a federation), as well as the logic of their interactions.	All UCs	Citizen/end-user, Service providers
UR-25	User requires open solutions for authentication between devices, ensuring the integrity of their data as well as the confidentiality.	All UCs	Citizen/end-user, Vendor, hardware

			manufacturers
UR-26	User wants to send information quickly and reliably from one point in the network to many devices, e.g. to spread important information like alerts or updates quickly.	UC-O2, UC-I2	Citizen/end-user, Network providers, Service providers
UR-27	User needs advanced devices capable to handle security, privacy and reliability mechanisms for protecting their privacy and the integrity of their data.	All UCs	Citizen/end-user, Vendors and hardware manufacturers
UR-28	City officials / administrators needs to minimise the amount of deployed sensors for environmental monitoring by exploiting mobile sensors.	UC-O2, UC-O1	City, Service provider

Table 26 User Requirements

5 Conclusions

Two outdoor (smart transportation and environmental monitoring) and two indoor (home energy management and comfort quality monitoring) use-cases are considered within the RERUM project. A brief review of the state of the art has been performed, in which we analysed the various approaches that have been followed by different research projects regarding implementation of the specific UCs considered by RERUM. In past research projects, the implemented and used security, privacy and reliability mechanisms are based on conventional security protocols and algorithms used in standard communication networks. However, the existing security schemes cannot always adapt to the specific needs, requirements and characteristics of each application, resulting in several implementation limitations and decreased security and privacy. For example, some data encryption algorithms may be too computationally intensive for low-complexity low-power consumption sensors, resulting in reduced lifetimes, or they may produce too many overhead bits with respect to the actual information data.

On the contrary, in RERUM use-cases a different approach will be followed, putting security and privacy in the core of our system, using the requirements of each use-case for developing an architecture that is secure and privacy-preserving by design. RERUM aims to ensure the reliable operation of the system, the trustworthy exchange of information between the smart objects and the foreseen smart city applications. Furthermore, the project will develop mechanisms for preserving the privacy and non-disclosure of the end-user data and patterns (i.e. a pattern in lights could show the hours that a user is absent, which may be used by burglars), supporting the “always connected” nature of both indoor and outdoor smart objects. Another important goal is to secure the network and avoid attacks, such as jamming, passive listening, data falsification, etc. and enable the automatic secure configuration of smart objects and avoid network failures.

To this end, each use-case was analysed in order to define:

- the key challenges, with focus on security and privacy
- the hardware elements that are involved (e.g., sensors, actuators, smart objects, gateways, etc.),
- the stakeholders, their expected benefits and their roles in each use-case
- the candidate network interfaces
- the data that will be sensed
- actions that will be performed by the objects

The UC definitions will be used for extracting the system requirements for realizing the RERUM concept of privacy and security by design. Besides the UC analysis, the first step towards the identification of the requirements was the threat analysis for the smart city applications. This analysis followed a three-step methodology, beginning with an asset-centric approach, which included a Confidentiality, Integrity and Availability (C-I-A) analysis and subsequently conducting an attacker-centric analysis by looking at specific threats against Authentication / Authorization / Accounting (AAA). The third step was the analysis of the Privacy Threats within the use-cases. The identification of the IT assets is a critical aspect towards the threat analysis for each of the RERUM UCs, and more importantly the design of those mechanisms for ensuring the security and privacy. These assets include the authentication credentials, user data (e.g., sensed and actuation data), command and control data, network data, as well as the software of the system components.

Common use-cases such as smart homes, smart transportation and environmental monitoring impose many and critical threats against the confidentiality, integrity and availability of data (e.g., user, actuation, control and command) and software. In addition, threats against authentication, authorization and accounting will often result in breaches against confidentiality, availability and integrity of the aforementioned types of data. This deliverable presented a thorough analysis of these possible threats and will be the basis for the identification of the system requirements and the

system architecture. Besides the security threats, the design of the RERUM system will take into consideration the privacy issues, which arise due to the need to automatically collect, store, use and disclose personal information of the users (e.g., location, energy consumption information), that can reveal sensitive personal information, which could be potentially used to construct a profile of a user.

Finally, this deliverable provided the connection between the user requirements that stem from the cities', citizens' and stakeholders' needs and the fundamental issues that have to be resolved for realizing the smart cities applications. Several use case situations were identified in order to demonstrate those needs and how RERUM can provide solutions to these situations. For each of these situations the innovations that will be developed in the RERUM technical workpackages (WP3 and WP4) were briefly described along with the exploitation plans and business models.

References

[1] Merriam-Webster Online: Dictionary and Thesaurus www.merriam-webster.com
[2] IoT-A project, D1.5 - Final Architectural Reference Model for the IoT, July, 2013.
[3] ATIS Telecom glossary, www.atis.org/glossary/
[4] Standard, Federal. "1037C." Department of Defence Dictionary of Military and Associated Terms in support of MIL-STD-188 (1996).
[5] Shirey, R. "RFC 4949–Internet Security Glossary." (2007).
[6] Shirey, Robert. "RFC 2828: Internet security glossary." The Internet Society (2000).
[7] Cisco, "The Internet of Everything for Cities", 2013.
[8] A. Caragliu, C. Del Bo, and P. Nijkamp, "Smart cities in Europe. Series Research Memoranda 0048. VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics 2009.
[9] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, A. Oliveira, "Smart cities and the future internet: towards cooperation frameworks for open innovation," In The future internet, pp. 431-446, Springer Berlin Heidelberg, 2011
[10] D. Work, O.-P. Tossavainen, S. Blandin, A. Bayen, T. Iwuchukwu, and K. Tracton, An ensemble Kalman filtering approach to highway traffic estimation using GPS enabled mobile devices, 47th IEEE Conference on Decision and Control, pp. 5062-5068, Cancun, Mexico, 2008.
[11] D. V. Gibson, G. Kozmetsky, and R. W. Smilor (eds.), "The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks,"*Rowman & Littlefield*, New York, 1992.
[12] R. Stanica, M. Fiore, and F. Malandrino. "Offloading Floating Car Data." World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a. IEEE, 2013.
[13] D. Work, S. Blandin, O.-P. Tossavainen, B. Piccoli and A. Bayen, A traffic model for velocity data assimilation, Applied Mathematics Research eXpress (AMRX), 2010(1), pp. 1-35, 2010.
[14] A. Bayen, Guaranteed bounds on highway travel times using probe and fixed data, C. Claudel, A. Hofleitner, N. Mignerey,88th Transportation Research Board Annual Meeting, Washington D.C., January 10-14, 2009.
[15] A. Pascale, M. Nicoli, F. Deflorio, B. Dalla Chiara, and U. Spagnolini, "Wireless sensor networks for traffic management and road safety". Intelligent Transport Systems, IET , vol.6, no.1, pp.67-77, 2012.
[16] A. Allström, D. Gundlegard M. Holmstedt, and J. Archer "METRA – Alternative methods for cost-effective traffic data collection", Trafikverket Report, 2012.
[17] University of Maryland Transportation Studies Center: Final Evaluation Report for the CAPITAL-ITS Operational Test and Demonstration Program, University of Maryland, College Park, 1997.
[18] J. Steenbruggen, M. Borzacchiello, P. Nijkamp, and H. Scholten, Mobile phone data from GSM networks for traffic parameter and urban spatial pattern assessment: a review of applications and opportunities. GeoJournal, 7(2), 2013.
[19] D. Gundlegård and J. Karlsson, "Road Traffic Estimation using Cellular Network Signaling in Intelligent Transportation Systems" Wireless technologies in Intelligent Transportation Systems, Nova Science Publishers, 2009.
[20] V. D. Blondel et al. (eds) Data for Development: the D4D Challenge on Mobile Phone Data. May 2013.
[21] Civitas Initiative, online at: http://www.civitas.eu/
[22] iTetris, online at: : http://www.ict-itetris.eu/
[23] Carbotraf, online at: www.carbotraf.eu/
[24] Streetlife, online at: http://www.streetlife-project.eu/
[25] Movesmart, online at: www.movesmartfp7.eu/
[26] The mobile millennium project, online at: http://traffic.berkeley.edu/
[27] The mobile millennium Stockholm, online at: http://www.mobilemillenniumstockholm.se/
[28] CITIZENSENSE, ERC, http://www.citizensense.net

[29] TWISNET, EU FP7, http://www.twisnet.eu
[30] EVERYAWARE, EU, FP7, http://www.everyaware.eu
[31] SAFECITY, EU FP7, http://www.safecity-project.eu
[32] ENVIRONMENTOR, EU FP7, http://www.environmentor-project.com [dead link]
[33] DIADEM, EU FP7, http://www.ist-diadem.eu [dead link]
[34] SEMSORGRID4ENV, EU FP7, http://www.semsorgrid4env.eu [dead link]
[35] AirQualityEgg DIY project, http://airqualityegg.com/
[36] Pollux'NZ DIY project, http://ckab.com/polluxnz-city
[37] MyAirBase product, http://www.myairbase.com/
[38] NoiseTube project, http://noisetube.net/#&panel1-1
[39] Air Casting project, http://aircasting.org/
[40] SensePod product, from Sensaris, http://www.sensaris.com/products/senspod/
[41] Opensense, open source project, http://www.opensense.ethz.ch/trac/
[42] European Commission. "Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions, Taking stock of the Europe 2020 strategy for smart, sustainable and inclusive growth." Brussels, 5.3.2014, COM(2014) 130 final.
[43] 3eHouses, EU FP7 project. http://www.3ehouses.eu/
[44] DEHEMS, EU FP7 project. http://www.dehems.eu/
[45] ADDRESS, EU FP7 project. http://www.addressfp7.org/
[46] PEBBLE, EU FP7 project. www.pebble-fp7.eu/
[47] SmartCoDe, EU FP7 project. www.fp7-smartcode.eu/
[48] J. Zhang, Q. Li, and E. M. Schooler. "iHEMS: An information-centric approach to secure home energy management." *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012.
[49] G. Kalogridis and D. Saraansh, "PeHEMS: Privacy enabled HEMS and load balancing prototype." *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012.
[50] D. He, et al. "Secure service provision in smart grid communications. "*Communications Magazine, IEEE* 50.8, 2012.
[51] AAL initiative, http://ps.aal-europe.eu/activity-profile/aalpartnersearch.2012-02-16.7887848960
[52]Intasense, European Commission's Energy Efficient Buildings PPP, http://www.intasense.eu/
[53] Cetieb, EU FP 7 project, www.cetieb.eu
[54] SMooHS, EU FP 7 project, www.smoohs.eu
[55] Tibucon, EU FP 7 project, www.tibucon.eu
[56] Nest products, https://nest.com
[57] Netatmo devices, http://www.netatmo.com/
[58] Sensorist devices, http://sensorist.com/
[59] Home automation DIY examples, http://homeautomation.pl/, http://james.lipsit.com/home.htm or http://hacknmod.com/hack/diy-home-automation-tutorial/
[60] Sweden Institute of Computer Science, https://www.sics.se/
[61] Fraunhoffer IIS, http://www.iis.fraunhofer.de/en/bf/ec/dk/sn.html
[62] Smart-Homes Technological Center, Netherlands, http://www.smart-homes.nl/Guillaume Leduc, "Road Traffic Data: Collection Methods and Applications" JRC Technical Notes (JRC 47967) -2008.
[63] Chavi Dhingra, Measuring Public Transport Performance, GmbH, Germany, 2011
[64] DASH 7 White paper http://www.dash7.org/DASH7%20WP%20ed1.pdf
[65] The Environmental Noise Directive, http://ec.europa.eu/environment/noise/directive.htm

[66] J. C. Herrera, D. B. Work, R. Herring, X. J. Ban, Q. Jacobson, and A. M. Bayen, Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment. Transportation Research Part C: Emerging Technologies, *18*(4), 568-583, (2010).
[67] E. De Cristofaro, and C. Soriente, Extended Capabilities for a Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI), 2013.
[68] Traffic-related air pollution substantial public health concern, Science Daily, Oct '13, http://www.sciencedaily.com/releases/2013/10/131021131002.htm
[69] How we contribute to Air Pollution and Climate Change, British Columbia Government, http://www.bcairquality.ca/101/pollution-climate-causes.html
[70] Particulate Matter PM10, EPA, USA Government, http://www.epa.gov/airtrends/aqtrnd95/pm10.html
[71] PM10, EEA definition, http://www.eea.europa.eu/themes/air/air-quality/resources/glossary/pm10
[72] ENVI, Environment, Public Health and Food Safety Committee of the European Parliament, http://www.europarl.europa.eu/committees/en/envi/home.html
[73] ZigBee Alliance web page. http://www.zigbee.org/
[74] IEEP, Institute for European Environmental Policy, http://www.ieep.eu
[75] Hui Zhang, DongEun Kim, Edward Arens, Elena Buchberger, Fred Bauman, and Charlie Huizenga, Comfort, perceived air quality, and work performance in low-power task-ambient conditioning system, Center for the Built Environment (CBE), University of California, Berkeley
[76] Acoustic Glossary, http://www.acoustic-glossary.co.uk
[77] http://www.healthy-house.co.uk/information-on-electromagnetic-stress
[78] ISO/IEC 10040, "Information technology - Open Systems Interconnection - Systems management overview - Part 4: Management framework", 1998
[79] Dolev, Danny; Yao, Andrew C.: On the Security of Public Key Protocols. IEEE Transactions on Information Theory, vol. it - 29, no. 2, March 1983.
[80] Federrath, Hannes Dr.; Pfitzmann, Andreas Prof. Dr.: Originally published in German language in: 2.1 Technische Grundlagen. In: Alexander Rossnagel (Hg.): Handbuch des Datenschutzrechts, TU Dresden, Beck Verlag, 2002.
[81] Biba, K. J. "Integrity Considerations for Secure Computer Systems", MTR-3153, Mitre Corporation, Juni 1975.
[82] Bell, David (2005): "Looking Back at the Bell - La Padula Model." ACSAC (Annual Computer Security Applications Conference) 2005 proceedings of the 21st ACSAC, Tucson, AZ. IEEE Xplore.
[83] Howard, M., Lipner, S.: The Security Development Lifecycle : SDL : A Process for Developing Demonstrably More Secure Software. Microsoft Press (2006).
[84] D. J. Solove, "A taxonomy of privacy", University of Pennsylvania Law Review, vol 154, no. 3, 2006.
[85] D. J. Solove, Understanding Privacy. Harvard University Press, May 2008.
[86] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (Version 0.33 April 2010)," tech. rep., TU Dresden and ULD Kiel, April 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
[87] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements", Requirements Engineering, vol. 16, pp. 3-32, 2011
[88] IEEE Standards Association, Guidelines for 64-bit Global Identifier (EUI-64TM)
[89] Lu, Z., Lu, X., Wang, W., Wang, C.: Review and evaluation of security threats on the communication networks in the smart grid. In: MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010. (2010) 1830–1835.
[90] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, The new casper: A privacy-aware location-based database server. In ICDE, 2007.

[91] B. Gedik, and L. Liu, Location privacy in mobile systems: A personalized anonymization model. In Proc. of ICDCS, 2005.
[92] G. Ghinita, P. Kalnis, and S. Skiadopoulos, Prive: anonymous location-based queries in distributed mobile systems. In Proc. of WWW, 2007.
[93] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, Preventing location-based identity inference in anonymous spatial queries. TKDE, 2007.
[94] P. Golle, and K. Partridge, On the anonymity of home/work location pairs. In Proc. of Pervasive, 2009.
[95] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, Enhancing security and privacy in traffic-monitoring systems. In IEEE Pervasive Computing Magazine, 2006.
[96] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, A. Preserving privacy in gps traces via uncertainty-aware path cloaking. In Proc. of CCS, 2007.
[97] A. Beresford, and F. Stajano, Mix zones: User privacy in location-aware services. In Proc. of Pervasive Computing, 2004.
[98] T. Jiang, H. J. Wang, and Y.-C. Hu, Preserving location privacy in wireless lans. In Proc. of MobiSys, 2007.
[99] Preserving Location Privacy in Geo-Social Applications Krishna P. N. Puttaswamy, et.al. UC Santa Barbara.
[100] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, “Enhancing wireless location privacy using silent period,” in Proceedings of the 2005 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA, pp. 1187–1192, March 2005.
[101] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, “Silent cascade: Enhancing location privacy without communication qos degradation,” in Security in Pervasive Computing, Third International Conference, SPC 2006, York, UK, April 18-21, 2006, Proceedings, ser. Lecture Notes in Computer Science, vol. 3934. Springer, pp. 165–180, 2006.
[102] L. Butty´an, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A practical pseudonym changing scheme for location privacy in VANETs,” in Proceedings of the IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 2009. IEEE, October 2009.
[103] F. Scheuer, K.-P. Fuchs, and H. Federrath, “A Safety-Preserving Mix Zone for VANETs,” in Proceedings of Trust, Privacy and Security in Digital Business - 8th International Conference, TrustBus 2011, Toulouse, France, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2011, vol. 6863, pp. 37–48, 2011.
[104] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: Why simple pseudonym change is not enough,” in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on. IEEE, pp. 176–183, 2010.
[105] D. Gollmann, “Veracity, plausibility, and reputation,” in Information, Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems. Springer, pp. 20–28, 2012.
[106] T. Winter (Ed.), P. Thubert (Ed.), A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. P. Vasseur, and R. Alexander, “RPL: IPv6 Routing Protocol for Low power and Lossy Networks,” RFC 6550, Mar. 2012.
[107] Gobbo, Nicola and Merlo, Alessio and Migliardi, Mauro: “A Denial of Service Attack to GSM Networks via Attach Procedure”. Lecture Notes in Computer Science (LNCS), Security Engineering and Intelligence Informatics, volume 8128. Springer Berlin Heidelberg, 2013.
[108] A. Cooper, H. Tschofenig, B. Aboba, J. Peterson, J. Morris, M. Hansen, R. Smith: “Privacy Considerations for Internet Protocols”, RFC 6973, 2013
[109] G. Montenegro, N. Kushalnagar, J. W. Hui, and D. E. Culler: “Transmission of IPv6 packets over IEEE 802.15.4 networks,” RFC 4944, Sep. 2007.
[110] Z. Shelby, (Ed), S. Chakrabarti, E. Nordmark, C. Bormann: “Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)”, RFC 6775, 2012.
[111] D. Plummer: “An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48 bit Ethernet Address for Transmission on Ethernet Hardware”, RFC 826, 1982

[112] R. Droms: “Dynamic Host Configuration Protocol”, RFC 2131, 1997.
[113] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney: “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC 3315, 2003.
[114] E. Rescorla, N. Modadugu: “Datagram Transport Layer Security”, RFC 4347, 2006.
[115] P. Ilia, G. Oikonomou, T. Tryfonas: “Cryptographic Key Exchange in IPv6-Based Low Power, Lossy Networks”, in Proc. Workshop in Information Theory and Practice (WISTP 2013), ser. Lecture Notes in Computer Science, 7886, pp. 34-49, 2013.
[116] J. Moira ,West-Brown, et al.: Handbook for Computer Security Incident Response Teams 2nd Edition: April 2003, CMU/SEI-2003-HB-002.
[117] Hossein Bidgoli: Handbook of Information Security, 3-Volume Set, Wiley, ISBN: 978-0-471-64833-8, 3366 pages, February 2006.
[118] Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, 1080 pages, Wiley, ISBN: 978-0-470-06852-6, April 2008.
[119] Data Attacks Are Right on Track for Another Devastating Year, http://www.entrust.com/data-attacks-right-track-another-devastating-year/ 2014.
[120] Peter Gutmann: Everything you Never Wanted to Know about PKI but were Forced to Find Out, University of Auckland.
[121] Wikipedia: DigiNotar http://en.wikipedia.org/wiki/DigiNotar Version of 13 October 2014.
[122] The Register: New hack on Comodo reseller exposes private data, http://www.theregister.co.uk/2011/05/24/comodo_reseller_hacked/.
[123] The Register: FLASH drive :http://www.theregister.co.uk/2014/10/03/badusb_poc/.
[124] http://www.forbes.com/sites/danielnewman/2014/08/20/there-is-no-privacy-on-the-internet-of-things/.
[125] http://www.theinquirer.net/debate/11/the-internet-of-things-will-kill-privacy
[126] Ovidiu Vermesan & Peter Friess (Editors): Internet of Things Applications - From Research and Innovation to Market Deployment, The River Publishers Series in Communications ISBN: 9788793102941, June 2014.
[127] EU Directives 2002/58/EC and 95/46/EC art. 6 1(b).
[128] European Directive 95/46/EC art.12 (b).
[129] Mauritius Declaration on the Internet of Things, Adopted Resolution, 36th International Conference of Data Protection and Privacy Commissioners, http://www.privacyconference2014.org/en/about-the-conference/resolutions.aspx
[130] Rob van Kranenburg, Erin Anzelmo, Alessandro Bassi, Dan Caprio, and Sean Dodson: The Internet of Things, Paper Prepared for the 1st Berlin Symposium on Internet and Society October 25-27, 2011.
[131] http://www.techradar.com/news/world-of-tech/google-s-chief-internet-evangelist-says-privacy-increasingly-difficult-to-achieve-1201175.
[132] http://pdf.aminer.org/000/667/287/specifying_privacy_policies_with_p_p_and_epal_lessons_learned.pdf.
[133] http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.
[134] http://www.cs.umn.edu/~zhzhang/Papers/Virtual%20id%20routing-MobiArch08.pdf.
[135] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/GruPA/GruPA.pdf?__blob=publicationFile.
[136] Daniel R. L. Brown, Matthew J. Campagna and Scott A. Vanstone; Security of ECQV-Certified ECDSA Against Passive Adversaries; 2011.

